International Review of the Red Cross, Page 1 of 18.
doi:10.1017/S1816383124000705

IRRC

The use of facial recognition for targeting under international law

Ido Rosenzweig[1,2]* and **Magdalena Pacholska**[3]†

[1]Director of Research (Terrorism, Belligerency and Cyber), Minerva Center for the Rule of Law under Extreme Conditions (Minerva RLEC), Faculty of Law and School of Environmental Studies, University of Haifa, Haifa, Israel

[2]Chairperson, ALMA – Association for the Promotion of International Humanitarian Law, Petach-Tiqwa, Israel

[3]Researcher, Minerva RLEC, Faculty of Law and School of Environmental Studies, University of Haifa, Haifa, Israel

*Corresponding author email: ido.rose@gmail.com

Abstract

In the quest for "identity dominance" over the enemy, armed forces are increasingly leveraging biometrics for a variety of purposes. This paper focuses on the combat employment of one of them – facial recognition, which, unlike other biometrics,

† The views expressed in this publication are solely those of the authors and do not represent the positions of any institutions or organizations they have been affiliated with. The authors would like to express their appreciation to the *Review* editing team and the reviewers. Any mistakes or errors are ours alone.

does not appear to have been widely utilized for targeting purposes yet. With the purchasing patterns of advanced militaries suggesting that such a development is around the corner, this paper assesses the compliance with international humanitarian law (IHL) of the use of facial recognition technologies for targeting purposes. It peruses the applicable legal framework to demonstrate that IHL is neutral towards the use of new technologies and that the right to privacy under international human rights law does not preclude the use of biometrics in hostilities. The analysis zooms in on two specific use cases in which facial recognition is likely to be employed on the battlefield, namely (1) targeted killings against combatants and (2) targeted killings against civilians directly participating in hostilities. The paper closes with an acknowledgment that while facial recognition does have obvious operational benefits, it also has the potential to exacerbate targeting practices that stretch the limits of IHL.

Keywords: international humanitarian law, facial recognition technologies, targeted killings, right to privacy, international human rights law, laws of armed conflict, autonomous weapon systems.

Introduction

Whether in Gaza for the purposes of identifying hostages[1] or in Ukraine to identify the deceased or prisoners of war,[2] facial recognition technologies (FRTs) powered by artificial intelligence (AI) are increasingly being utilized on modern battlefields. Recourse to FRTs is part of a broader trend among many military forces of "leverag[ing] biometrics to establish 'identity dominance' over the enemy".[3] The concept of biometrics can refer to both a process and a characteristic. It is understood as the automated recognition of individuals based on their behavioural or biological features, such as iris, gait, fingerprint, or face topography.[4] First rolled out on a major scale in a military context in Afghanistan over two decades ago as a force protection measure to counter a battlefield threat,[5] biometric recognition is now used for both defensive and offensive purposes.[6] While biometrics have reportedly been employed for

1 "Israeli Tech Workers Bring Innovation, AI to Search for Hostages in Gaza", *Times of Israel*, 26 October 2023, available at: www.timesofisrael.com/israeli-tech-workers-bring-innovation-ai-to-search-for-hostages-held-in-gaza/ (all internet references were accessed in December 2024).
2 Alexa Hagerty, "In Ukraine, Identifying the Dead Comes at a Human Rights Cost", *Wired*, 22 February 2023, available at: www.wired.com/story/russia-ukraine-facial-recognition-technology-death-military/.
3 Leah West, "Face Value: Precautions versus Privacy in Armed Conflict", in Russell Buchan and Asaf Lubin (eds), *The Rights to Privacy and Data Protection in Times of Armed Conflict*, NATO CCDCOE Publications, Tallinn, 2022, p. 133.
4 William C. Buhrow, *Biometrics in Support of Military Operations: Lessons from the Battlefield*, Taylor & Francis, Boca Raton, FL, 2017, p. 8.
5 L. West above note 3, p. 134.
6 *Ibid.*, p. 135.

https://doi.org/10.1017/S1816383124000705 Published online by Cambridge University Press

targeting,[7] little is known about the use of FRTs for such purposes so far.[8] However, given that some States are already in possession of drones equipped with facial recognition software for target acquisition,[9] it is reasonable to expect that FRT-based targeting is around the corner.

Such an inevitability brings to the fore a question of FRTs' compliance with the applicable international law norms, especially international humanitarian law (IHL) and international human rights law (IHRL). Whether for misconceptions of military decision-making processes or misunderstandings of how advanced technologies are actually deployed, the combat use of new technological tools in general, and those powered by AI in particular, continues to cause quite a stir. This contribution aims to counter the ubiquitous *Terminator*-esque narratives in the literature[10] by offering a practice-based examination of the impact and risks that FRT-based targeting during armed conflict might have under public international law.

The article is structured as follows. To approach the issues at hand with evidence-based knowledge rather than sci-fi-anchored inclination, the first section provides an overview of the existing FRTs and the algorithms they are based on. The second section starts with a reiteration of the technological neutrality of IHL and continues with a reflection on the challenges in applying relevant IHRL norms, chiefly the right to privacy and the right to life, in the context of armed conflict in general and the conduct of hostilities in particular. The third section examines the practical implementation of FRTs in combat – that is, targeted killings. The fourth section offers some concluding remarks.

A few clarifying thoughts are needed before proceeding with the analysis. First and foremost, this article does not aspire to provide a comprehensive examination of the potential legal exposure that the use of biometrics as such, or even specifically FRTs, might generate for armed forces and the States they belong to.[11] In particular, it does not deal with data protection regulations, which

7 According to the unclassified 2014 US Center for Army Lessons Learned (CALL) handbook on biometrics in Afghanistan, "[b]iometrics should be fully embedded into the targeting process". CALL, *Commander's Guide to Biometrics in Afghanistan*, Handbook No. 11–25, 2014, p. 20, available at: https://info.publicintelligence.net/CALL-AfghanBiometrics.pdf.

8 Allegations have been made in recent months about Israel using AI for such purposes in the Gaza Strip, but the details on the exact manner in which AI-enabled FRTs are used remain contested. See, for instance, David Wallace-Wells, "What War by A.I. Actually Looks Like", *New York Times*, 10 April 2024, available at: www.nytimes.com/2024/04/10/opinion/war-ai-israel-gaza-ukraine.html.

9 Note that already in early 2023, the US Department of Defense (DoD) had procured facial recognition software for target acquisition to be carried by small military drones. For media coverage on the contract, see Matthew Gault, "US Military Signs Contract to Put Facial Recognition on Drones", *Vice*, 27 February 2023, available at: www.vice.com/en/article/7k85qe/us-military-signs-contract-to-put-facial-recognition-on-drones.

10 The literature on emerging disruptive technologies is replete with narratives referencing the *Terminator* films and other sci-fi tales of robots run amok. For an overview of these narratives see Tom F. A. Watts and Ingvild Bode, "Machine Guardians: The Terminator, AI Narratives and US Regulatory Discourse on Lethal Autonomous Weapons", *Cooperation and Conflict*, Vol. 59, No. 1, 2024.

11 For an overview of the military use of biometrics, see Marten Zwanenburg, "Biometrics on the Battlefield", *Articles of War*, 21 October 2020, available at: https://lieber.westpoint.edu/biometrics-on-the-battlefield/.

https://doi.org/10.1017/S1816383124000705 Published online by Cambridge University Press

differ greatly in various national and regional regimes;[12] we leave this aspect of military legal interoperability to other commentators.[13] Also not addressed in this article, but admittedly relevant for a wider inquiry into the subject, are various pre-deployment aspects of FRTs such as the data mining, collection and processing necessary for the designing and testing of a given software. Finally, while recognizing that in contemporary theatres, armed forces perform many functions, including law enforcement (in occupied territories, for example),[14] we focus on the use of FRTs in combat. This is an important distinction. Despite the increased tendency to cast (mis)judgement on the military utility and legality of FRTs based on the increasingly stringent regulation on the use of biometrics by law enforcement authorities in many jurisdictions,[15] both the legal framework and the operational reality of an armed conflict differ greatly from peacetime policing. While some analogies might admittedly be made between peacetime policing and law enforcement functions performed by the military, it is conceptually fallacious to extend such conclusions to the conduct of hostilities in armed conflict. It is the latter category that the rest of this article deals with.

Technological overview

"Facial recognition technologies" is an umbrella term denoting various technologies of differing levels of advancement. In fact, different layers of facial scanning technologies exist, with each one having different purposes and outcomes. The simplest layer is facial detection technology,[16] used, for example, by cameras to focus on faces when a picture is taken.[17] The second layer is emotion detection, which enables commercial companies to analyze facial expressions and infer

12 On the regulation of FRTs in the United States and the European Union respectively, see Jake Laperruque, "The Facial Recognition Act: A Promising Path to Put Guardrails on a Dangerously Unregulated Surveillance Technology", *Lawfare*, 1 November 2022, available at: www.lawfaremedia.org/article/facial-recognition-act-promising-path-put-guardrails-dangerously-unregulated-surveillance-technology; Tambiama Madiega and Hendrik Mildebrath, *Regulating Facial Recognition in the EU*, PE 698.021, European Parliamentary Research Service, September 2021, available at: www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf.

13 Sebastian Cymutta, Marten Zwanenburg and Paul Oling, "Military Data and Information Sharing – a European Union Perspective", *14th International Conference on Cyber Conflict: Keep Moving*, Tallinn, 2022. On military interoperability generally, see David S. Goddard, "Understanding the Challenge of Legal Interoperability in Coalition Operations", *Journal of National Security Law and Policy*, Vol. 9, No. 2, 2018.

14 On this aspect specifically, see Keren Weitzberg, "Biometrics and Counter-Terrorism: Case Study of Israel/Palestine", Privacy International, 28 May 2021, available at: https://privacyinternational.org/report/4527/biometrics-and-counter-terrorism-case-study-israelpalestine.

15 Sofia Gomez, "The Dangers of Militarizing Racist Facial Recognition Technology", *Georgetown Security Studies Review*, 30 September 2020, available at: https://georgetownsecuritystudiesreview.org/2020/09/30/the-dangers-of-militarizing-racist-facial-recognition-technology/; Parmy Olson, "Bringing Facial Recognition to War is a Bad Idea", *Japan Times*, 29 April 2022, available at: www.japantimes.co.jp/opinion/2022/04/29/commentary/world-commentary/facial-tech-war/.

16 T. Madiega and H. Mildebrath, above note 12, p. 1, para. 1.1.1.2.

17 Evan Selinger and Brenda Leong, "The Ethics of Facial Recognition Technology", in Carissa Véliz (ed.), *The Oxford Handbook of Digital Ethics*, Oxford University Press, Oxford, 2024.

https://doi.org/10.1017/S1816383124000705 Published online by Cambridge University Press

emotions, and often incorporates additional features to collect basic demographic data, such as gender and age, about their potential clients. The third, most advanced layer is facial recognition technology,[18] based on the collection of information through a point-based design that analyzes a person's facial structure. The information about each person is collected and stored in a database for comparison with future data. While facial recognition is considered to be the least accurate biometric (in comparison with iris recognition, fingerprint identification and gait recognition), it is often used because it can be collected from a distance and does not require active participation by the subjects being analyzed.[19] As such, it is arguably particularly apt to be used for lethal targeting, as the enemy does not need to be aware that his adversaries own his biometrics and can use them for attack.

The process of using the biometric point-based system is composed of four main steps. The first is finding face(s) within a photo or a video sequence (both can contain more than one face). The second step is to extract the available data about the obtained face, and the third step is to process that data into the biometric point-based system and create a mathematical formula called a "faceprint". The fourth step is to compare the new faceprint with an existing database.[20] This process also enables data sharing between different databases, which is sometimes referred to as a "ping and ring" mechanism:[21] one operator conducts an inquiry with other operators (such as different government agencies or equivalent agencies in different countries) to inquire if the faceprint is available on their specific databases (ping), and if they provide a positive answer, the operator contacts them directly (ring) to ask for the relevant data.[22]

From a technical point of view, FRTs refer to AI algorithms that can identify individuals from images and videos through the analysis of facial features.[23] Such systems have been in use in different industries since the 1960s, but it wasn't until the early 2000s that this technology made the leap into commercial, governmental and security use.[24] Throughout the years, FRTs and the algorithms that operate them have significantly developed. One of the major

18 *Ibid.*

19 Mark Andrejevic and Neil Selwyn, "Facial Recognition Technology in Schools: Critical Questions and Concerns", *Learning, Media and Technology*, Vol. 45, No. 2, 2020, p. 116.

20 Oleh Basystiuk, Nataliia Melnykova and Zoriana Rybchak, "Machine Learning Methods and Tools for Facial Recognition Based on Multimodal Approach", *Proceedings of the 5th International Workshop on Modern Machine Learning Technologies and Data Science*, Lviv, 2023, p. 6, available at: https://ceur-ws.org/Vol-3426/paper13.pdf.

21 S. Cymutta, M. Zwanenburg and P. Oling, above note 13, pp. 222–223.

22 *Ibid.* It should be noted that with a lack of a unified method of facial recognition, the "ping" process is limited to databases using the same data protocols, or at least similar and comparable ones. See, for example, Chris Burt, "NATO Launches In-House Biometrics System for Secure Data-Sharing", *BiometricUpdate.com*, 18 November 2020, available at: www.biometricupdate.com/202011/nato-launches-in-house-biometrics-system-for-secure-data-sharing.

23 William Crumpler, "How Accurate are Facial Recognition Systems – and Why Does It Matter?", Center for Strategic and International Studies, 14 April 2020, available at: www.csis.org/blogs/strategic-technologies-blog/how-accurate-are-facial-recognition-systems-and-why-does-it.

24 "A Brief History of Facial Recognition", NEC, 12 May 2022, available at: www.nec.co.nz/market-leadership/publications-media/a-brief-history-of-facial-recognition.

https://doi.org/10.1017/S1816383124000705 Published online by Cambridge University Press

developments has been the change from a single-mode approach – which was usually based on comparison with a single photo – to a multi-source approach. The multimodal approach uses different machine learning algorithms, such as deep learning, support vector machines and decision trees, to analyze, interpret and compare data from multiple and different modalities (such as images, video and audio) in order to conduct facial recognition.[25] As a result, the speed of recognition has increased tremendously,[26] and at the same time, the success rate of facial recognition systems can reach over 99% in ideal conditions – i.e., when comparing designated photos taken for the purpose of facial recognition.[27] However, when it comes to photos of lower quality, such as when either or both photos were taken in motion or without a clear background, the recognition error rate can reach 20% and above.[28]

The meaning of the error rate includes, *inter alia*, the problems of false positives and false negatives. A false positive means that the FRT will alert the user that the two photos which are being compared are similar even though they are not. This would lead to the false identification of one person as someone else. A false negative relates to a situation where the system fails to identify a specific person. To minimize the risk of false positives, some algorithms have a confidence threshold that will only return a positive result if the analysis leads, for example, to 99% certainty.[29] The cost of using such a safety mechanism, however, is a significant increase in false negative results.[30] A very colourful example of the importance of the confidence threshold can be seen in a facial recognition experiment run by the American Civil Liberties Union (ACLU). In the experiment, the ACLU used Amazon's Rekognition FRT and found that twenty-eight members of the US Congress, out of a total of 533 members, were wrongly matched with mugshots of people who had been arrested.[31] In response, Amazon published that the ACLU had used a confidence threshold of 80% and not 95% as was recommended for law enforcement activities.[32] As far as the authors are aware, no unclassified military information on the threshold of confidence required for battlefield employment of FRTs is available in the public domain.

Lastly, it is worth distinguishing between biometric identification, which enables one to identify a person apart from others (finding a specific strand of hay

25 O. Basystiuk, N. Melnykova and Z. Rybchak, above note 20, p. 2.
26 *Ibid.*
27 Patrick Grother, Mei Ngan and Kayee Hanaoka, *Face Recognition Technology Evaluation (FRTE), Part 2: Identification, National Institute of Standards and Technology*, NISTIR 8271 Draft Supplement, 21 February 2024, p. 8, available at: https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf.
28 *Ibid.*, pp. 8–9.
29 W. Crumpler, above note 23.
30 *Ibid.*
31 Jacob Snow, "Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots", ACLU, 26 July 2018, available at: www.aclu.org/news/privacy-technology/amazons-face-recognition-falsely-matched-28
32 Kif Leswing, "Read Amazon's Full Response to the ACLU Report about Its Facial Recognition Software Misidentifying Members of Congress as Previously Arrested", *Business Insider*, 26 July, 2018, available at: www.businessinsider.com/amazon-response-to-aclu-facial-recognition-study-congress-member-photos-2018-7.

https://doi.org/10.1017/S1816383124000705 Published online by Cambridge University Press

in a haystack), and biometric authentication, which enables one to confirm the identity of a specific person, much like when someone opens their computer or phone using a facial recognition protection system.[33] From an operational perspective, identification would be the form of facial recognition apt for targeted killings of civilians directly participating in hostilities, while authentication would be a particularly useful tool for targeted killings of combatants (see discussion below).

Legal and conceptual framework

IHL and new technologies

One of the prominent features of the ongoing debate on emerging disruptive technologies is the pervasive conflation of legal and ethical standards.[34] The latter, often disguised under the pretence of the protection of human dignity, usually underpin appeals to ban a given technology.[35] While not dismissing such considerations out of hand, it is our position that they do not, as such, influence the legal assessment of the potential use of a given technological tool. IHL is already built on a delicate balance between humanitarian concerns and military necessity,[36] and it is neither necessary nor practical to further convolute the examination of a given means or method of warfare with abstract, broadly conceived deontological concerns. To wit, it is our position that while IHL factors in humanitarian imperatives, it is technology-neutral and can be applied "effectively and fairly in different technological contexts".[37]

Another manoeuvre frequently used by opponents of "militarizing" a given technological tool is grounding the argument in a fictional case study, which often aggrandizes the capabilities of a given tool and/or sets it in a clearly unlawful context.[38] Such approaches might be intellectually entertaining, but they fail to

33 T. Madiega and H. Mildebrath, above note 12, p. 1, para. 1.1.1.1. See also Alan Goode, "Biometric Identification or Biometric Authentication?", Veridium, 11 July 2018, available at: https://veridiumid.com/biometric-identification-and-biometric-authentication.

34 See, for instance, the discussion on the conflation between the legal standard of military necessity and the ethical principle of necessity in Stuart Russell, "Banning Lethal Autonomous Weapons: An Education", *Issues in Science and Technology*, Vol. 38, No. 3, 2022, p. 62.

35 Peter Asaro, "On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision-Making", *International Review of the Red Cross*, Vol. 94, No. 886, 2012; Future of Life Institute, "Slaughterbots", *YouTube*, 2017, available at: www.youtube.com/watch?v=9CO6M2HsoIA; Future of Life Institute, "Why We Should Ban Lethal Autonomous Weapons", *YouTube*, 2019, available at: www.youtube.com/watch?v=LVwD-IZosJE; Campaign to Stop Killer Robots, "English", *YouTube*, 2022, available at: www.youtube.com/watch?v=xUU8YHa_Cjg.

36 Frédéric Mégret, "The Limits of the Laws of War", in Bardo Fassbender and Knut Traisbach (eds), *The Limits of Human Rights*, Oxford University Press, 2019, pp. 290–292.

37 Rebecca Crootof, "Regulating New Weapons Technology", in Ronald T. P. Alcala and Eric Talbot Jensen (eds), *The Impact of Emerging Technologies on the Law of Armed Conflict*, Oxford University Press, Oxford, 2019, pp. 15–17. See also Rain Liivoja, "Technological Change and the Evolution of the Law of War", *International Review of the Red Cross*, Vol. 97, No. 900, 2015.

38 For a critique of this trend and an overview of various catastrophic scenarios used to demonize military technologies, see Nathan Gabriel Wood, "Regulating Autonomous and AI-Enabled Weapon Systems: The Dangers of Hype", AI and Ethics, Vol. 4, No. 3, 2024.

https://doi.org/10.1017/S1816383124000705 Published online by Cambridge University Press

advance the conversation on the legal reverberations of military technologies. The fact that one can imagine a situation in which an item of military equipment is used in breach of IHL does not make the equipment unlawful. In fact, most, if not all, military equipment can be used in ways that are not in compliance with the most fundamental principles of IHL.[39] In other words, in the case of the technology at hand, one could inquire whether, for example, the use of an anti-personnel autonomous weapon system capable of acquiring and engaging targets based solely on a positive identification from an FRT, with no further restriction on the temporal or geographical limits and no option to abort, complies with IHL, but this question, framed in this way, would be highly abstract and divorced from the reality. In practice, armed forces take advantage of biometrics as "a complementary source of information to build the layers of knowledge and insights into the individual of potential interest".[40] Consequently, a hard-headed examination of a given tool's impact and risks should focus on the tool's normal or expected uses, taking into account that in practice, in the majority of circumstances, FRT deployment would augment a combatant's decision-making rather than serving as the only source of targeting intel.[41] As the discussion below demonstrates, especially in the context of targeted killings, it is not inconceivable that facial recognition might be compliant with IHL if other conditions are met.

Furthermore, a pragmatic reflection on the combat use of FRTs requires a determination of the factual circumstances in which depriving the enemy of anonymity – which is considered by some intelligence experts to be "the most powerful weapon on earth"[42] – provides the armed forces with the upper hand.[43] Note that the power of anonymity comes into play mainly in conflicts with an asymmetric element. In a textbook international armed conflict, the identity of the members of the opposing forces, as distinguished from the civilian population via a uniform or a fixed distinctive sign recognizable at a distance,[44] is generally legally and operationally irrelevant.[45] Consequently, it can be expected that FRTs are likely to be used in two conceptually overlapping use cases: targeted killings

39 As aptly noted by the International Committee of the Red Cross (ICRC), albeit in the context of weapons specifically, "[a] State is not required to foresee or analyse all possible misuses of a weapon, for almost any weapon can be misused in a way that would be prohibited". Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols*, ICRC, Geneva, 1987 (ICRC Commentary on the APs), para. 1469.

40 NATO Communications and Information Agency, "Countering Terrorism: NATO Agency Aids in the Development of Biometric Capabilities", 18 November 2020, available at: www.ncia.nato.int/about-us/newsroom/countering-terrorism-nato-agency-aids-in-the-development-of-biometrics-capabilities.html.

41 L. West, above note 3, p 137.

42 Joshua Steinhauer, "US Biometric and Identity Intelligence Programme", *Keesing Platform*, 1 June 2014, available at: https://platform.keesingtechnologies.com/us-biometric-and-identity-intelligence-programme-4/.

43 M. Zwanenburg, above note 11.

44 Geneva Convention (III) relative to the Treatment of Prisoners of War of 12 August 1949, 75 UNTS 135 (entered into force 21 October 1950), Art. 4, as interpreted in Nils Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, ICRC, Geneva, 2009 (ICRC Interpretive Guidance), p. 22, available at: www.refworld.org/docid/4a670dec2.html.

45 See, however, calls to revisit such an assumption, in Ido Rosenzweig, "'When You Have to Shoot, Shoot!' Rethinking the Right to Life of Combatants during Armed Conflicts", *International Review of the Red Cross*, Vol. 106, No. 926, 2024.

https://doi.org/10.1017/S1816383124000705 Published online by Cambridge University Press

and directing attacks against persons directly participating in hostilities. Before examining these use cases in turn in the next section, a few clarifying words on the right to privacy and its application in active hostilities, as well as on the implications of the use of FRTs on the right to life, are necessary.

The right to privacy in armed conflict

IHL might be the main body of law governing armed conflicts, but it is not the only one; it is by now largely uncontroversial that IHRL does not cease to apply in times of armed conflict.[46] As noted by Noam Lubell and Nancie Prud'homme, "[t]he existence of a relationship between [IHRL] and [IHL] is now widely accepted. Their concurrent application is at present more or less a fait accompli, but there remain debates on the nature of their interaction."[47]

Revisiting the various models of IHL and IHRL interplay is beyond the scope of this article.[48] What matters from the military operational perspective is that FRTs are, in fact, fairly intrusive, and their deployment does interfere with the privacy of the local population.[49] However, it does not automatically mean that a party to the conflict deploying FRTs to augment its targeting decision-making violates its international obligations. This is because IHL protects (some facets of) the protected persons' privacy only in the context of detention (and arguably occupation),[50] and no IHL provision touches upon the privacy implications of the conduct of hostilities.

In turn, whether or not the IHRL right to privacy applies depends, in the first place, on where the attack is taking place. Extraterritorial application of IHRL is another vexed topic, a detailed examination of which is again beyond the scope of this contribution.[51] For the purposes of the present discussion, it suffices

46 Oona A. Hathaway *et al.*, "Which Law Governs during Armed conflict? The Relationship between International Humanitarian Law and Human Rights Law", *Minnesota Law Review*, Vol. 96, 2012, p. 1899; Human Rights Committee, General Comment No. 36, "Article 6 (Right to Life)", UN Doc. CCPR/C/GC/36, 3 September 2019 (General Comment 36), para. 64.

47 Noam Lubell and Nancie Prud'homme, "Impact of Human Rights Law", in Rain Liivoja and Tim McCormack (eds), *Routledge Handbook of the Law and Armed Conflict*, Routledge, London, 2016, pp. 106–107.

48 Among a plethora of approaches, see, in particular, O. A. Hathaway *et al.*, above note 46, p. 1883; Cordula Droege, "The Interplay between International Humanitarian Law and International Human Rights Law in Situations of Armed Conflict", *Israel Law Review*, Vol. 40, No. 2, 2007; Noam Lubell, "Challenges in Applying Human Rights Law to Armed Conflict", *International Review of the Red Cross*, Vol. 87, No. 860, 2005; Françoise J. Hampson, "The Relationship between International Humanitarian Law and Human Rights Law from the Perspective of a Human Rights Treaty Body", *International Review of the Red Cross*, Vol. 90, No. 871, 2008.

49 For a detailed discussion on how various new technologies interfere with the privacy of the population, see Eliza Watt, "The Principle of Constant Care, Prolonged Drone Surveillance and the Right to Privacy of Non-Combatants in Armed Conflicts", in R. Buchan and A. Lubin (eds), above note 3, p. 157.

50 For a succinct examination of various IHL provisions touching upon privacy, see M. Zwanenburg, above note 11. See in particular the comments on how the scope of Article 27 of Geneva Convention IV is interpreted in practice.

51 Marko Milanović and Tatjana Papić, "The Applicability of the ECHR in Contested Territories", *International and Comparative Law Quarterly*, Vol. 67, No, 4. 2018, p. 779; Samantha Besson, "The Extraterritoriality of the European Convention on Human Rights: Why Human Rights Depend on

https://doi.org/10.1017/S1816383124000705 Published online by Cambridge University Press

to underline that in light of current international case law, it can reasonably be argued that if a given territory was not controlled by a party to a conflict *prior* to the conflict, active hostilities preclude the establishment of effective control by the State over an area which would trigger IHRL applicability.[52] In other words, if an attack is conducted against a target outside of a State territory in "the context of chaos" characteristic for active hostilities, the right to privacy does not apply, as the so-called personal model of jurisdiction based on "State agent authority and control" cannot be established either.[53]

When the attack is taking place in the territory under the effective control of a party to the conflict, the right to privacy does apply, but it should not be read to imply that the combat use of FRTs necessarily breaches a State's IHRL obligations. The right to privacy, whether customary or treaty-based,[54] protects the local population only against arbitrary (and/or unlawful) interferences.[55] What is arbitrary/unlawful in armed conflict ought to be interpreted first and foremost in light of IHL,[56] which, as will be further discussed below, prioritizes doing everything feasible to verify whether the target is a military objective over the privacy rights of the local population. Many theories have been put forward as to

Jurisdiction and What Jurisdiction Amounts to", *Leiden Journal of International Law*, Vol. 25, No. 4, 2012, p. 857.

52 See in particular European Court of Human Rights (ECtHR), *Georgia v. Russia (II)*, Appl. No. 38263/08, Judgment (Merits), 21 January 2021, reaffirming the standard outlined in ECtHR, *Banković and Others v. Belgium and Others*, Application no 52207/99, Decision (Grand Chamber), 12 December 2001, paras 74–81. As the Court made clear in the *Georgia* case at para. 126, "in the event of military operations – including, for example, armed attacks, bombing or shelling – carried out during an international armed conflict, one cannot generally speak of 'effective control' over an area. The very reality of armed confrontation and fighting between enemy military forces seeking to establish control over an area in a context of chaos means that there is no control over an area.") For a detailed analysis of the discrepancies on that point in the jurisprudence of the ECtHR, see Marten Zwanenburg, "The Use of OSINT for Military Operations Abroad under International Humanitarian Law and International Human Rights Law", Chinese Journal of International Law, Vol. 23, No. 3, 2024, paras 89–90.

53 Note that in the *Georgia* case, above note 52, the Grand Chamber also explicitly held that at para. 137 that "the very reality of armed confrontation and fighting between enemy military forces seeking to establish control over an area in a context of chaos not only means that there is no 'effective control' over an area as indicated above (see paragraph 126), but also excludes any form of 'State agent authority and control' over individuals". For a discussion on that aspect of the decision, see Floris Tan and Marten Zwanenburg, "One Step Forward, Two Steps Back? Georgia v Russia (II), European Court of Human Rights, Appl No 38263/08", *Melbourne Journal of International Law*, Vol. 22, No. 1, 2021, p. 136.

54 While the exact scope of the right to privacy, including whether or not it extends to "data" privacy, remains debated, the negative obligation not to arbitrarily or unlawfully interfere with a person's privacy is widely recognized as customary. For a comprehensive argument in favour of the customary status thereof, see Alexandra Rengel, *Privacy in the 21st Century*, Martinus Nijhoff, Leiden, 2013, p. 108.

55 Universal Declaration of Human Rights, UNGA Res. 217 A(III), 10 December 1948, Art. 12; International Covenant on Civil and Political Rights, 999 UNTS 171, 16 December 1966 (entered into force 23 March 1976) (ICCPR), Art. 17; Human Rights Committee, General Comment No. 16, "Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation", 8 April 1988. See also the regional instruments: Charter of Fundamental Rights of the European Union, OJ 2012/C 326/02, 2012, Art. 7; European Convention for the Protection of Human Rights and Fundamental Freedoms, 5 ETS, 1950, Art. 8; American Convention on Human Rights, 18 July 1978 (entered into force 18 July 1978), Art. 11.

56 As the International Court of Justice did to determine what "arbitrary deprivation of life" means in the context of armed conflict. See International Court of Justice, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, *ICJ Reports 1996*, para. 25.

https://doi.org/10.1017/S1816383124000705 Published online by Cambridge University Press

what principles need to be met to ensure that the interference with the right to privacy is not arbitrary,[57] but all recognize that compliance with their recommended principles is always context-specific.[58] As Daniel Bethlehem has aptly observed, "[a]s a rule of thumb, the closer one gets to the battlefield, the less amenable to reasonable application are most provisions of [IHRL]".[59] This is definitely the case for non-absolute rights with built-in exceptions, such as the right to privacy.

The right to life and the use of FRT-based targeting

Another fundamental human right that needs to be mentioned in the context of FRTs and targeting is the right to life. Even if we reject the alarmist approaches calling for a complete ban on the use of AI and FRTs on the battlefield, some points of concern remain. The right to life, enshrined, *inter alia*, in Article 6 of the International Covenant on Civil and Political Rights, says that "[e]very human being has the inherent right to life. This right shall be protected by law. No one shall be arbitrarily deprived of his life."[60] In its General Comment 36, published in 2019, the United Nations (UN) Human Rights Committee noted in the context of the application of that right during armed conflicts that "[u]se of lethal force consistent with international humanitarian law and other applicable international law norms is, in general, not arbitrary".[61] This raises an important question: can a mistaken strike – that is, an attack against a person mistakenly classified as a military objective – be classified as inconsistent with IHL and therefore arbitrary?

In the context at hand, a mistaken strike would likely be a consequence of a false positive – i.e., incorrect recognition – as described in the technological overview earlier in this article. In the context of an armed conflict, when the adversary combatants are anonymous, and they are targeted for their status and not for their personal identity, a false positive should not make much of a difference. However, when identity is an element of the targeting process, such as in the case of targeted killings (see further discussion below), false positives can lead to attacking the wrong person. If that person is still a lawful target as a combatant or a civilian taking direct part in hostilities, there is no *prima facie* violation of IHL, and thus, in general, no violation of the right to life.[62]

57 Lubin, for instance, identifies five principles necessary for a State to lawfully interfere with the privacy rights of the local population (legality, necessity, proportionality, adequate safeguards, effective remedies in case of transgressions). See Asaf Lubin, "The Rights to Privacy and Data Protection under International Humanitarian Law and Human Rights Law", in Robert Kolb, Gloria Gaggioli and Pavle Kilibarda (eds), *Research Handbook on Human Rights and Humanitarian Law: Further Reflections and Perspectives*, Edward Elgar, London, 2022, pp. 468–471.

58 L. West, above note 3, p. 144.

59 Daniel Bethlehem, "The Relationship between International Humanitarian Law and International Human Rights Law in Situations of Armed Conflict", *Cambridge Journal of International and Comparative Law*, Vol. 2, No. 2, 2013, p. 191.

60 ICCPR, above note 55, Art. 6.

61 General Comment 36, above note 46, para. 67.

62 *Ibid.* In this case we assume, for the sake of a clean analysis, that the attack did not include any expected collateral damage.

https://doi.org/10.1017/S1816383124000705 Published online by Cambridge University Press

A situation is legally more problematic when the person directly attacked was not a lawful target,[63] leading ostensibly to the violation of the principle of distinction, pursuant to which "[t]he civilian population as such, as well as individual civilians, shall not be the object of attack".[64] While the level of certainty required under the principle of distinction is subject to lingering debate in scholarship,[65] it is generally accepted that absolute certainty regarding whether the target is a military objective is not required.[66] A determination of whether a given mistaken engagement is unlawful hinges on compliance with the obligation to do everything feasible to verify that the target is a military objective.[67] There is no doubt that the obligation to verify targets is an obligation of means, not of result, but it could be argued that employing an insufficiently unreliable FRT violates a duty of care,[68] and a mistaken attack based on a false positive identification should be considered indiscriminate and thus arbitrary.

This does not mean, however, that an FRT cannot be used for targeting if it is less than 100% accurate; as will be discussed in the next section, there are several safety mechanisms to reduce such risks.

FRT-augmented targeting: The use cases

When it comes to the use of FRTs for targeted killings as a method of warfare, the discussion focuses on the fundamental principles of IHL and especially distinction and precautions with regard to the decision to use force against an individual. The use of targeted killings has become a common practice either within armed conflicts or as a tool for self-defence,[69] usually extraterritorially. Although the notion of "targeted killings" does not appear in either codified or customary IHL, it is a

63 Divergent approaches exist to the question of whether or not a person can be considered a military objective. For clarity of the present analysis, persons that can be attacked in accordance with IHL are referred to as "lawful targets".

64 Protocol Additional (I) to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, 1125 UNTS 3, 8 June 1977 (entered into force 7 December 1978) (AP I), Art. 51(2).

65 There is a great shortage of case law regarding unintended engagements, but the issue has been subject to extensive litigation in the ECtHR case of *Ukraine and the Netherlands v. Russia* (Appl. Nos 8019/16, 43800/14 and 28525/20). At the time of writing, the Grand Chamber judgment is still forthcoming.

66 Tsvetelina van Benthem, "Targeting Mistakes and Other Unintended Engagements in Armed Conflict: The Explosion at Al-Ahli Hospital in Gaza", *EJIL: Talk!*, 17 May 2024, available at: www.ejiltalk.org/targeting-mistakes-and-other-unintended-engagements-in-armed-conflict-the-explosion-at-al-ahli-hospital-in-gaza/; Ian Henderson, The Contemporary Law of Targeting, Martinus Nijhoff, Leiden, 2009, pp. 161–167; Magdalena Pacholska, '"Neither Criminal nor Civil": Russian State Responsibility for Conduct of Hostilities Violations in Ukraine", *Texas Tech Law Review*, Vol. 56, No. 1, 2023, pp. 166–169.

67 AP I, Art. 57(2)(a)(i); Jean-Marie Henckaerts and Louise Doswald-Beck (eds), *Customary International Humanitarian Law*, Vol. 1: *Rules*, Cambridge University Press, Cambridge, 2005 (ICRC Customary Law Study), Rule 16, available at: https://ihl-databases.icrc.org/en/customary-ihl/rules.

68 Janina Dill, "Do Attackers Have a Legal Duty of Care? Limits to the 'Individualization of War'", *International Theory*, Vol. 11, No. 1, 2019.

69 Kenneth Anderson, *Targeted Killing and Drone Warfare: How We Came to Debate Whether There Is a "Legal Geography of War"*, Legal Studies Research Papers Series, American University Washington College of Law, 26 April 2011.

https://doi.org/10.1017/S1816383124000705 Published online by Cambridge University Press

typically defined as "the intentional, premeditated, and deliberate use of lethal force against a specific individual who is not in the physical custody of the perpetrator".[70] In simpler terms we can refer to this as "identified targeting". Therefore, intentionally attacking an individual based on facial recognition aligns precisely with this definition, thereby raising significant questions about compliance with IHL when the action takes place within the framework of an armed conflict.

Attacks against human targets

When it comes to the conduct of hostilities, and especially targeting, IHL is very straightforward. Direct attacks can only be conducted against a person who constitutes a lawful target – either a combatant or a civilian taking direct part in hostilities.[71] What exactly amounts to direct participation in hostilities (DPH) remains perhaps one of the most controversial concepts in contemporary IHL doctrine and practice.

In the absence of any treaty definition or uniform State practice supported by *opinio juris*, the International Committee of the Red Cross's (ICRC) 2009 *Interpretive Guidance on the Notion of Direct Participation in Hostilities* (ICRC Interpretive Guidance),[72] in concert with its ensuing critiques[73] and the responses thereto,[74] is widely considered a legal touchstone on how to interpret DPH in contemporary counter-insurgency operations. Broadly speaking, the ICRC Interpretive Guidance distinguishes between "sporadic" DPH (resulting in the temporal scope of loss of protection during "the execution of a specific act of [DPH], as well as the deployment to and the return from the location of its execution") and "continuous combat function" (CCF)[75] resulting in the loss of protection due to one's status in an organized armed group and their role in it.[76] While the distinction between the two categories has been subject to fierce criticism, and the notion of CCF was originally restrained to non-international armed conflicts, the prevailing view nowadays appears to be that members of an organized armed group (or an

70 Philip Alston, *Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions*, UN Doc. A/HRC/14/24/Add.6, 28 May 2010, para. 1.
71 *Ibid.*, para 30; ICRC Customary Law Study, above note 67, Rule 1.
72 ICRC Interpretive Guidance, above note 44.
73 Among many, see, in particular, W. Hays Parks, "Part IX of the ICRC 'Direct Participation in Hostilities' Study: No Mandate, No Expertise, and Legally Incorrect", *New York University Journal of International Law and Politics*, Vol. 42, No. 3, 2010; Kenneth Watkin, "Opportunity Lost: Organized Armed Groups and the ICRC 'Direct Participation in Hostilities' Interpretive Guidance", *New York University Journal of International Law and Politics*, Vol. 42, No. 3, 2010; Michael N. Schmitt, "Deconstructing Direct Participation in Hostilities: The Constitutive Elements", *New York University Journal of International Law and Politics*, Vol. 42, No. 3, 2010; Bill Boothby, ""And for Such Time As': The Time Dimension to Direct Participation in Hostilities", *New York University Journal of International Law and Politics*, Vol. 42, No. 3, 2010; Dapo Akande, "Clearing the Fog of War? The ICRC's Interpretive Guidance on Direct Participation in Hostilities", *International and Comparative Law Quarterly*, Vol. 59, No. 1, 2010.
74 Nilz 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", *New York University Journal of International Law and Politics*, Vol. 42, No. 3, 2010.
75 ICRC Interpretive Guidance, above note 44, pp. 65, 70.
76 *Ibid.*

https://doi.org/10.1017/S1816383124000705 Published online by Cambridge University Press

armed wing of a terrorist organization) may be targeted similarly to members of State armed forces.[77] Put differently, the operational reality of counter-insurgency has stimulated an evolution of DPH from a purely conduct-based notion into a more fluid mix of one's conduct and status. That said, irrespective of the DPH interpretation adopted, parties to the conflict are obliged to do everything "feasible"[78] to verify that targets are military objectives before launching an attack.[79] Compliance with the obligation to do one's best to verify the nature of the target, just like all facets of the principle of precaution, is therefore closely tied to the collection and analysis of information about potential targets.[80]

How do FRTs fit into this matrix of norms? From a tactical operational perspective, augmenting combatant decision-making with insights from FRTs offers obvious benefits:

> [T]he use of FRT to scan a crowd of faces and run those images against a database of known combatants and non-combatants could significantly enhance operational effectiveness and ensure compliance with IHL. Not only would it allow for the more efficient use of violence, but FRT deployment could also augment a soldier's decision-making and save the lives of innocent civilians.[81]

Such reasoning, however, does not hold in cases of "sporadic" DPH, in which one's identity is irrelevant and only their conduct matters. But it does work very well for status-based interpretations of DPH, when a party to the conflict has prior knowledge of one's membership in an organized armed group and is in possession of other intelligence suggesting that they constitute a threat. This is arguably a widespread practice among many States engaged in counter-insurgency, chiefly the United States and France,[82] and the increasing use of FRTs for targeting is likely to make it sprawl further. While debates concerning target selection resting on the objective of pre-empting threats continue, it needs to be noted that such practices are not free of pitfalls. Crucial among these is the blurring of the line between individuals who continue to pose a threat to a party to the conflict and those who did engage in hostile actions before but are no longer a threat and are instead attacked on a punitive basis, which would be incongruent with IHL.

77 For a detailed overview of various positions leading to that conclusion, see Rebecca Mignot-Mahdavi, "Rethinking Direct Participation in Hostilities and Continuous Combat Function in Light of Targeting Members of Terrorist Non-State Armed Groups", *International Review of the Red Cross*, Vol. 105, No. 923, 2023.

78 The US DoD has traditionally been sceptical of the inclusion of "everything" in the phrase "everything feasible"; the revised DoD *Law of War Manual* omits that term (referring to "taking feasible precautions" instead of "doing everything feasible"). See the analysis in Kobi Leins and Helen Durham, "2023 DoD Manual Revision – To Shoot, or Not to Shoot… Automation and the Presumption of Civilian Status", *Articles of War*, 28 August 2023, available at: https://lieber.westpoint.edu/shoot-not-shoot-automation-presumption-civilian-status/.

79 AP I, Art. 57(2)(a). See also ICRC Customary Law Study, above note 67, Rule 16.

80 L. West, above note 3, p. 141.

81 *Ibid.*, p. 137.

82 R. Mignot-Mahdavi, above note 77, p. 1030.

https://doi.org/10.1017/S1816383124000705 Published online by Cambridge University Press

FRT-based targeted killings

Some discussions have taken place about the potential requirement to capture instead of killing when the option is available,[83] but to focus on the specific question of the use of FRTs and its compliance with the principle of distinction, in this subsection we are going to continue under the following four basic assumptions:

1. the designated target constitutes a lawful target;
2. there is an imminent necessity to neutralize the targeted person;
3. no excessive collateral damage is expected from the attack; and
4. no less-than-lethal alternative would neutralize the threat posed by the individual.

In such admittedly ideal circumstances, the crux of the operation lies in the positive identification of the target. In practice, this can be done by human agents through visual confirmation (which often includes putting those agents at substantial risk) or by recourse to FRTs (authentication function). This aspect of the process raises a few important questions that require further discussion. What is the importance of having a "person in the loop" during an FRT-augmented targeting operation? How should a potential false positive result be factored in? What are the implications of a mistaken identity in the course of an FRT-based targeted killing operation?

The following two scenarios are meant to clarify the relevant theoretical and practical questions about targeted killing operations that are based on FRTs.

- In **scenario A**, an elite unit is deployed with an operation to target person X. An unmanned aerial vehicle (UAV) with a camera scans the area and uses an FRT to authenticate the target. The unit's commander gives the order to engage and neutralize person X.
- In **scenario B**, an assault UAV is deployed with an operational order to target person Y when she is alone in a secluded location. The UAV scans the area and uses an FRT to authenticate the target. On the basis of that confirmation, the UAV system attacks and kills person Y.

The main difference between these two scenarios is the human factor. In scenario A, the final decision to launch the attack is taken by the unit on the ground, and in scenario B, the UAV operates as a highly automated weapon.[84] In both scenarios, the decision to attack is based on the positive identification by the FRT. If, in scenario A, the unit operates immediately without any additional confirmation, there is no difference between the scenarios from a legal perspective. However, if the unit has the option to corroborate the result provided by the FRT, this

83 See, for example, *Israeli High Court of Justice, Public Committee against Torture in Israel et al. v. The Government of Israel*, HCJ 769/02, 2006, available at: www.haguejusticeportal.net/Docs/NLP/Israel/Targetted_Killings_Supreme_Court_13-12-2006.pdf.

84 William H. Boothby, "Highly Automated and Autonomous Weapons", in William H. Boothby (ed.) *New Technologies and the Law in War and Peace*, Cambridge University Press, Cambridge, 2018, pp. 142–143.

https://doi.org/10.1017/S1816383124000705 Published online by Cambridge University Press

introduces a safety mechanism in the process of identification. Another way to include a person in the loop of the decision-making process is to condition the positive approval with another safety mechanism of human confirmation. This might reduce the chances of false positives, but at the same time, it will increase response time between the positive identification and the execution of the attack. When we consider that human-level facial recognition performance is at 97.53%,[85] and that non-ideal conditions increase the error rate, the importance of using a person in the loop becomes even more significant to reduce both false positives and false negatives.

But what happens when we part from that ideal scenario and consider that under the fog of war and combat fatigue, combatants are substantially more prone to making mistakes?[86] FRTs, like other advanced technologies, are immune to such factors. One must wonder if, under adversarial conditions, the reliance on FRTs, especially with a high enough confidence threshold, would not be more beneficial than relying on the person in the loop to make the final call.

Another way to look at the verification process can be on the side of the system. As was noted in the technological overview earlier in this article, some FRTs include safety mechanisms to reduce the chances of false positives.[87] In the context of the two targeting killing scenarios presented above, there are two potential safety mechanisms to prevent false positive as well as false negative results. One safety mechanism is the combatants executing the attack in scenario A after the information from the FRT has been transmitted to them. The question of adding such a safety mechanism becomes complicated, however, when we consider the risk that the combatants might have to take upon themselves in order to verify the identity of the target and, at the same time, the level of the immediate threat posed by the target, as well as the likelihood of another opportunity to engage the target presenting itself. Naturally, if the threat is not immediate and the next chance to engage the target is on the horizon, even though that person might still constitute a lawful target, the operational decision might have to be to cancel the attack because of the doubt about the identity of the target,[88] in order to avoid directly attacking a civilian. Another possible safety mechanism could be fixed at the comparison point, before the information is transmitted for execution. If, at that point, there were another way to double-check the decision, especially when the compared data is not of the highest quality, it would allow for a reduction in the chances of false positives and negatives. Such a safety mechanism could work for both scenarios. On the other hand, if the compared data is of high value and the confirmation rate is higher

85 Justin Lee, "Ping An Technology Developing AI Face Recognition Technology with Record Results", *BiometricUpdate.com*, 15 March 2017, available at: www.biometricupdate.com/201703/ping-an-technology-developing-ai-face-recognition-technology-with-record-results.

86 For an argument that technical solutions are preferable to humans in some roles due to the fact that they will not be affected by the psychological, physiological or cognitive limitations that impact humans, see Ronald Arkin, *Governing Lethal Behavior in Autonomous Robots*, Chapman and Hall, Boca Raton, FL, 2009.

87 W. Crumpler, above note 23.

88 AP I, Art. 50(1).

https://doi.org/10.1017/S1816383124000705 Published online by Cambridge University Press

than the human recognition rate (i.e., it is over 97.53%), there seems to be no need for such a safety mechanism, especially if the timing of the attack is crucial. (The timing element could serve an important aspect as part of ensuring that "everything feasible" is done to ensure that the target is indeed legal while taking into account the practical circumstances at the time of the attack.[89])

Conclusions

Facial recognition is a rapidly developing technology, and it is expected that it will continue to evolve in the coming years. At the time of writing this paper, the technological ability to identify or authenticate a person's face through biometric means can be very accurate in ideal conditions but less than reliable in field conditions. The use of FRTs by armed forces for targeting purposes does not violate *prima facie* any rule of IHL; similarly to other advanced technologies, the crucial question is how FRTs are employed.

FRTs have the potential to increase compliance with the principle of distinction. This holds true in regard to targeted killings of both combatants and status-based civilians who are directly participating in hostilities. When used properly, the battlefield deployment of FRTs can reduce the risks to both adversary civilians and the attacking combatants.

From the perspective of compliance with IHL, the use of FRTs brings up several challenges. It is the position of the authors that the main legal risk that FRTs generate actually precedes deployment and lies with the collection and processing of personal data. As such, it is not regulated by IHL, with the exception of Article 36 of Additional Protocol I.[90] From an operational, user's perspective, the core objection to FRTs relates to their (un)reliability in an uncontrolled environment. Such reliability depends on two crucial aspects: the system's ability to provide a positive identification, and the ability to prevent or flag situations of false positive/negative results in suboptimal field conditions. The problems of both false positives and false negatives are different in their basis but similar in the outcome: misidentification of the target. Without proper safety mechanisms, false positives can lead to the targeting of the wrong person – either a lawful target (e.g., a different combatant or a civilian directly participating in hostilities) or an uninvolved civilian, which in the latter case might also constitute an arbitrary deprivation of life. False negatives, on the other hand, can lead to missing a chance to neutralize a desirable target, which is usually a person of significant interest. The main (and at this point of technological development, probably also the only) safety mechanism that can mitigate reliability concerns is to include a human in the loop. The human can be at the comparison point (i.e., before the approval is transmitted), at the execution point (after the approval has been transmitted), or both. This will not necessarily prevent any mistakes

89 ICRC Commentary on the APs, above note 39, para. 2198.
90 AP I, Art. 36.

https://doi.org/10.1017/S1816383124000705 Published online by Cambridge University Press

completely, but it will ensure that the human recognition rate of 97.53% will be considered as part of the decision-making process. In any event, the use of FRTs will help to reduce the risk to one's own combatants while also increasing protection to uninvolved civilians who might otherwise have been harmed in the course of a larger operation (even when the collateral damage would not be considered excessive) to confirm the identity of the targeted person.

An argument can be made that such an assessment will change once FRTs develop and can provide a rate of confirmation higher than the human one, even in suboptimal field conditions. Should that happen, there will be no logical reason to rely on human confirmation as preferable to technological confirmation. Therefore, the use of an assault UAV which can conduct a targeted killing operation against an identified target without excessive collateral damage could be conducted without any human interference, allowing for a much quicker and more accurate operation without the need to risk the life of one's own forces. Moreover, in case there are more persons alongside the designated target, FRTs could be used to identify them and to clarify whether they are also lawful targets (if, for example, they are directly participating in hostilities), and in such a case, since there is no expected collateral damage to human life, and thus no blatant proportionality considerations, engage the target. This, of course, will not be applicable when some of the persons in the vicinity of the designated target are uninvolved civilians or when the FRT is unable to confirm their identity, and there is therefore doubt about their classification.

The possibilities of incorporating biometric technologies on the battlefield are wide and diverse. In this paper, we have focused on the use of FRTs to recognize persons on the battlefield for the purpose of targeting. However, using FRTs, the future might also include more sophisticated options, such as identifying DPH behaviour.[91] As long as the technology is reliable enough, there is no reason to fear it. In the long run, and if used properly, it can lead to a significant decrease in casualties on the battlefield. However, we must finish with a word of caution – technology is a user-sensitive tool, and if used recklessly, it will create more damage than value.

91 This does not necessarily mean that the present analysis should be assumed to apply *mutatis mutandis* to such behaviour-identifying techniques.

https://doi.org/10.1017/S1816383124000705 Published online by Cambridge University Press