CyCon 2024: Over the Horizon
16th International Conference on Cyber Conflict
C. Kwan, L. Lindström, D. Giovannelli, K. Podiņš, D. Štrucl (Eds.)
2024 © NATO CCDCOE Publications, Tallinn

Military Psychological Operations in the Digital Battlespace: A Practical Application of the Legal Framework

Anastasia Roberts
Independent Legal Consultant
United Kingdom

Adrian Venables
Senior Lecturer
Cyber Security Masters
Programme Manager
Tallinn University of Technology
Estonia

Abstract: This paper aims to clarify the legal framework for military psychological operations (PsyOps) in the digital battlespace during international armed conflict (IAC), with a particular focus on civilian protection. This is to support its practical application in military training and planning. The impetus for this paper is twofold: the increasing complexity and scope of PsyOps from a technological perspective and the resurgence of IAC, impacting military training and planning. To provide practical context, the North Atlantic Treaty Organization (NATO) and its member states are used as a focal point for this discussion. The roles of both international human rights law (IHRL) and international humanitarian law (IHL) in regulating military PsyOps are considered. The inherent tension between the two bodies of law, due to their different origins, is then discussed. This paper concludes that the two bodies of law can in fact be reconciled. This is by using IHL provisions that regulate PsyOps from a civilian protection perspective to encompass broader human rights concerns. This paper advocates for the development of a comprehensive assessment and authorization process for training and planning for military PsyOps in IAC based on IHL.

Keywords: *international armed conflict, international humanitarian law, international human rights law, civilian protection, psychological operations*

1. INTRODUCTION

This paper aims to clarify the legal framework for military psychological operations (PsyOps) in the digital battlespace during international armed conflict (IAC). This is to support its practical application in military training and planning. To provide context, the North Atlantic Treaty Organization (NATO) and its member states will be used as a focal point for this discussion.

There is no universally agreed definition of PsyOps. However, this paper will use the NATO definition: *'Planned activities using methods of communication and other means directed at approved audiences in order to influence perceptions, attitudes and behaviour, affecting the achievement of political and military objectives.'*[1]

The impetus for this paper is twofold. Firstly, the increasing complexity and scope of PsyOps from a technological perspective. Secondly, the resurgence of IAC, impacting military training and planning.

PsyOps are certainly not new, but advances in information and communications technologies (ICT) have expanded their potential reach and depth. In terms of reach, audiences selected for influence activity can now be accessed at scale through the internet, particularly with mobile technology facilitating virtually constant user access. In terms of depth, influence can be effected in more targeted and intrusive ways. For example, in the context of the Russia–Ukraine conflict, some Ukrainian military personnel reportedly received personalized messages on their own devices, coercing them to surrender.[2] Digitalization has also enabled more covert means of influence, to the extent that audiences may not even realize that they are being influenced. For example, in 2022, Meta (formerly Facebook) announced that it had removed a number of Russia-sponsored fake social media accounts. These were masquerading as credible news agencies and disseminating false reporting, or disinformation, about the situation in Ukraine.[3]

The Israeli response to the Hamas attacks of 7 October 2023 has also been marked by sophisticated PsyOps on both sides. Israel has employed its covert 'Influence Unit' to both shape the media's perception of the war and target Hamas terrorists.[4] Hamas

1 NATO Allied Joint Publication 3.10.1, *Allied Joint Doctrine for Psychological Operations with UK National Elements* (edn B, vers 1, 2014) para 0102 <https://www.gov.uk/government/publications/ajp-3101-allied-joint-doctrine-for-psychological-operations> accessed 4 March 2024.

2 Matthew Roscoe, 'Russia's Special Services Accused of Sending Threatening Messages to Ukrainian Soldiers' (*EuroWeekly News*, 8 June 2022) <https://euroweeklynews.com/2022/06/08/russia-threatening-message-ukrainian-soldiers/> accessed 4 March 2024.

3 Dan Milmo, 'Facebook Takes Down Ukraine Disinformation Network and Bans Russian-Backed Media' *The Guardian* (28 February 2022) <https://www.theguardian.com/technology/2022/feb/28/facebook-takes-down-disinformation-network-targeting-ukraine-meta-instagram> accessed 4 March 2024.

4 Eric Cortellessa and Vera Bergengruen, 'Inside the Israel-Hamas Information War' *Time* (22 December 2023) <https://time.com/6549544/israel-and-hamas-the-media-war/> accessed 4 March 2024.

has also employed PsyOps under the guise of hacktivist campaigns of #OpIsrael and #FreePalestine using a range of social media outlets.[5]

It could be argued that these technological advances do not fundamentally alter the underlying legal regime for PsyOps and that the legal issues raised by PsyOps have not changed. In the purest sense, this is true. However, the difference lies in the practical application of the legal regime to more complex means of influence. Leaflet drops and radio-in-a-box can generally be limited geographically and addressed to specific audiences, enabling their effects to be anticipated. The use of social media, with its potential for rebroadcasting and manipulation, is more difficult to control and assess.

The second stimulus for this paper is the fact that NATO and its member states are currently having to readjust their thinking, training and planning to fully encompass the potential for IAC. This is after decades of focusing on non-international armed conflict (NIAC) and situations below the threshold of armed conflict. The Russia–Ukraine conflict has demonstrated that IAC is still a reality. Estonia's Foreign Intelligence Service has only recently issued a warning that Russia is preparing for a war with NATO within the next decade.[6] The potential for fighting between Israel and Hamas to escalate to involve third-party states also supports the increased threat of IAC, as does the increasing tension between China and Taiwan.

NATO and its member states must start to consider how they will employ PsyOps in full-scale war fighting as opposed to the more limited context of counter-insurgency seen in Iraq and Afghanistan. This requires a comprehensive understanding of the legal regime governing PsyOps in IAC, which is different from that applicable in sub-threshold situations or even, to an extent, in NIAC.

Understanding the legal regimes applicable to different types of operations can be challenging for military personnel. This has not been helped by the fact that the line between peacetime and armed conflict, and their different legal regimes, has become increasingly blurred in common understanding in recent years, with constant references to 'grey-zone activity'. Furthermore, there is an ongoing tension between international humanitarian law (IHL) and international human rights law (IHRL), particularly in the context of IAC. IHL is the specialized body of law in armed conflict, but IHRL also applies as a matter of legal principle, subject to complex jurisdictional issues.

5 '#OpIsrael, #FreePalestine and #OpSaudiArabia – How Cyber-Threat Actors Coordinate PSYOPS Campaigns with Kinetic Military Actions' (*Resecurity*, 9 October 2023) <https://www.resecurity.com/blog/article/opisrael-freepalestine-and-opsaudiarabia-how-cyber-actors-capitalize-on-war-actions-via-psy-ops> accessed 4 March 2024.

6 Sergey Goryashko, Pierre Emmanuel Ngendakumana, 'Russia Gearing Up for Decade-Long Duel with West, Estonia Warns' *Politico* (13 February 2024) <https://www.politico.eu/article/russia-prepares-for-decade-long-confrontation-with-west-estonia-warns/> accessed 4 March 2024.

Specific human rights concerns have been raised about the impact of PsyOps on civilians in armed conflict, in terms of privacy[7] as well as freedom of opinion and expression.[8] In this context, IHL has been criticized for not sufficiently regulating PsyOps, addressing them only *'tenuously and non-systematically'*[9] and taking *'a remarkably lenient approach'*[10] to them. How should this tension between IHL and IHRL be approached in military training and planning for PsyOps in IAC? A number of national military manuals provide guidance on PsyOps, but not to this level of detail. Furthermore, many were written some time ago. The well-known lawyer's response that the answer depends on the circumstances is unhelpful.

This paper will attempt to clarify the legal regime for PsyOps in IAC for the purposes of military training and planning. Given the concerns raised about civilian protection, it will focus on this aspect of the regime. To provide practical context, it will first consider how NATO and its member states employ and regulate PsyOps from a doctrinal perspective. The paper will then consider IHRL concerns before moving on to consider whether IHL can in fact address these concerns, in an effort to reconcile the two bodies of law. This paper concludes that the two bodies of law can be reconciled and advocates for the development of a comprehensive assessment and authorization process for training and planning military PsyOps based on IHL.

To be clear, this paper does not seek to break fresh academic ground but merely to re-establish some order in what has become a confused space by proposing a pragmatic way forward in terms of military training and planning for PsyOps in IAC.

2. MILITARY DOCTRINE AND GUIDANCE

By examining available NATO and national doctrine and guidance, it is possible to extrapolate common approaches to the use and regulation of PsyOps, which are outlined below. NATO doctrine is particularly useful as it indicates a degree of consensus between a large body of states, albeit in broad and non-operationally specific terms.

7 Russell Buchan and Asaf Lubin (eds), *The Rights to Privacy and Data Protection in Times of Armed Conflict* (NATO CCDCOE Publications 2022) 3.

8 OHCHR 'Disinformation and Freedom of Opinion and Expression During Armed Conflicts: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (12 August 2022) UN Doc A/77/288 <https://www.ohchr.org/en/documents/thematic-reports/a77288-disinformation-and-freedom-opinion-and-expression-during-armed> accessed 4 March 2024.

9 Robin Geiss and Henning Lahmann, 'Protecting the Global Information Space in Times of Armed Conflict' (2021) The Geneva Academy of International Humanitarian Law and Human Rights Working Paper 8 <https://www.geneva-academy.ch/news/detail/ 452-three-papers-map-contentious-issues-related-to-the-application-of-international-law-to-military-cyber-operations> accessed 4 March 2024.

10 Eian Katz, 'Liar's War: Protecting Civilians from Disinformation during Armed Conflict' (2020) 102 [914] IRRC 659, 663.

A. Audiences

Those selected for influence effect are known as target or targeted audiences (TAs). TAs may include civilians as well as adversary audiences. NATO PsyOps doctrine refers to TAs as ranging *'from populations to decision-makers at all levels'*.[11] The US Law of War Manual[12] supports this broad TA base, specifically referring to civilian and neutral audiences, as does the French Law of Military Operations Manual.[13]

B. Analysis

TAs are analysed to understand how best to influence them. This is known as target audience analysis (TAA), defined in NATO doctrine as *'the focused examination of targeted audiences to create desired effects'*.[14] PsyOps relies on *'extensive information and intelligence'* about the TAs. This includes their location, vulnerabilities, susceptibilities, strengths and weaknesses, and social and cultural characteristics, among other requirements.[15]

C. Enablement

Cyber operations may be used as an enabler for PsyOps activity. NATO cyber doctrine explains that cyber operations can support PsyOps by *'providing both a vector for deploying information and effects that influence targeted audiences'*.[16] The French manual refers to the use of messaging through internet-based social networks as a means of effecting influence.[17]

D. Targeting

NATO doctrine is clear that PsyOps capability does not sit in isolation but also contributes to other military activities.[18] One of these is targeting, which is the employment of lethal or non-lethal capability against selected adversary targets to create specific physical, virtual or cognitive effects.[19] In NATO targeting doctrine, the definition of target includes a person or group of people, including their mindset, thought processes, attitudes and behaviours.[20] More recent doctrine specifically refers

11 NATO (n 1) para 0126.

12 US Department of Defense, *Law of War Manual* (12 June 2015, updated July 2023) para 5.26.1.2 <https://media.defense.gov/2023/Jul/31/2003271432/-1/-1/0/DOD-LAW-OF-WAR-MANUAL-JUNE-2015-UPDATED-JULY%202023.PDF> accessed 4 March 2024.

13 Le ministère des Armées, *Manuel de Droit des Opérations Militaires* (2022) para 8.1.3.1. <https://tinyurl.com/2an95hzs> accessed 4 March 2024.

14 NATO Allied Joint Publication 10.1, *Allied Joint Doctrine for Information Operations with UK National Elements* (edn A, vers 1, 2023) LEX-11 <https://www.gov.uk/government/publications/allied-joint-doctrine-for-information-operations-ajp-101> accessed 4 March 2024.

15 NATO (n 1) para 0118.

16 NATO Allied Joint Publication 3.20, *Allied Joint Doctrine for Cyberspace Operations* (edn A, vers 1, 2020) para 1.32 <https://www.gov.uk/government/publications/allied-joint-doctrine-for-cyberspace-operations-ajp-320> accessed 4 March 2024.

17 Le ministère des Armées (n 13) para 8.1.3.1.

18 NATO (n 1) paras 0124–0135.

19 NATO Allied Joint Publication 3.9, *Allied Joint Doctrine for Joint Targeting*, (edn B, vers 1, 2021) para 1.2.2 <https://www.gov.uk/government/publications/allied-joint-doctrine-for-joint-targeting-ajp-39a> accessed 4 March 2024.

20 ibid LEX-17.

to audiences or organizations in the target definition.[21] PsyOps capability supports target analysis and advises on the most effective means of creating the desired effects as well as directly delivering influence effect when this is the selected means.

E. Attribution

PsyOps have traditionally been categorized according to their attributability; that is to say whether they are ascribable to a source. White PsyOps involve fully attributed products. Grey PsyOps involve products that do not specifically reveal their source. Black PsyOps involve products that appear to emanate from a source other than the true one. NATO PsyOps doctrine states that PsyOps are generally attributable to NATO, to preserve credibility. However, from a national perspective, the UK position is that UK PsyOps are *'predominantly, but not exclusively, "white"'*.[22]

F. Truthfulness

NATO's position is that PsyOps products must be based on true information and that using false information is counter-productive to the long-term credibility and success of PsyOps.[23] In contrast, the German Law of Armed Conflict Manual appears to acknowledge the reality that sometimes PsyOps may not be truthful. It states that *'it is permissible to exert political and military influence by spreading – even false – information to undermine the adversary's will to resist and to influence their military discipline (e.g. calling on them to defect, surrender or mutiny)'*.[24]

G. Authorization

In accordance with NATO PsyOps doctrine, TAs and PsyOps effects must be approved by the North Atlantic Council through the submission of an operational plan.[25] This will include any rules of engagement for PsyOps activity.[26] The operational plan will provide the overarching regulatory framework for PsyOps and detail its interaction with other capabilities and functions, including the targeting process. In the context of the operation itself, specific PsyOps plans and products must be approved at the appropriate level of command, including any enabling cyber operations.[27] Approval is subject to consideration of any predicted cognitive, virtual and physical impact.[28] NATO doctrine also mandates the close involvement of a legal adviser in both lethal and non-lethal targeting, including PsyOps, to ensure compliance with the legal framework.[29]

21 NATO (n 14) LEX-11.
22 NATO (n 1) para 0115.
23 NATO (n 1) para 0114.
24 German Joint Service Regulation (ZDv)15/2, *Law of Armed Conflict Manual* (1 May 2013) para 487 <https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/GER-Manual-Law-of-Armed-Conflict.pdf> accessed 4 March 2024.
25 NATO (n 1) para 0509.
26 NATO (n 1) para 0311.
27 ibid.
28 NATO (n 14) para 4.35.
29 NATO (n 19) para 1.6.1; NATO (n 14) para 3.9.

3. IHRL CONSIDERATIONS

By contextualizing PsyOps in the previous section, it can be understood how their conduct could raise human rights concerns. This is most clearly the case in relation to the possible impact on the right to freedom of opinion under IHRL, which provides for the freedom to hold opinions without interference.[30]

The UN's Special Rapporteur on the promotion of the rights of freedom of opinion and expression has asserted that *'coercive, involuntary or non-consensual manipulation of the thinking process to develop an opinion'* is a violation of the right to freedom of opinion. This includes *'techniques that allow State ... actors to access and influence the thoughts and opinions of people without their knowledge or consent'*.[31]

Violation of the right to freedom of opinion is not only an ethical issue; it could also have practical consequences. As the Special Rapporteur notes, in the context of armed conflict, disinformation about the location and nature of hostilities, the displacement of troops or population, or the existence and accessibility of safe areas and essential services could lead people *'to make wrong and dangerous decisions'*.[32]

Freedom of expression is also potentially engaged in the sense that it incorporates the right to seek and receive information.[33] The Special Rapporteur notes that the use of disinformation and other manipulation of online content could disrupt the free flow of information, which has been described as a *'critical element'* of the right.[34] This is particularly so in armed conflict, where the right to receive accurate, trustworthy information to inform decision-making becomes a *'survival right'*.[35]

In the NATO context, such concerns are to some extent mitigated by the policy constraints in NATO doctrine that PsyOps should be truthful and attributable. However, this will not necessarily be replicated in the doctrines of all state militaries.

A further concern is the right to privacy. This right provides that no one shall be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence, or to attacks upon their honour and reputation.[36] Privacy is generally

30 See, for example, International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 17, art 19 (ICCPR).
31 OHCHR, 'Disinformation and Freedom of Opinion and Expression: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (13 April 2021) UN Doc A/HRC/4725, para 36 <https://www.ohchr.org/en/calls-for-input/report-disinformation> accessed 4 March 2024.
32 OHCHR (n 8) para 21.
33 ICCPR (n 30) art 19.
34 OHCHR (n 31) para 38.
35 OHCHR (no 8) para 5.
36 ICCPR (n 30) art 17.

understood to include information privacy as a derivative right.[37] The means available now to inform and employ PsyOps have greater implications for this right. The right may be engaged in the PsyOps context by intelligence collection on TAs, particularly as PsyOps become more targeted and noting the extent of information that NATO PsyOps doctrine states is required for TAA. It may also be engaged if private information is published about a civilian subject, particularly where it relates to sensitive aspects of someone's private life, such as their sexuality.

The difficulty in addressing human rights concerns as part of military training and planning for IAC is that the application of IHRL to armed conflict, and particularly IAC, is complex. As a matter of legal principle, human rights continue to apply in armed conflict, just as in peacetime.[38] However, a state is only bound by human rights obligations where that state has legal jurisdiction. The human rights regime was primarily designed for a peacetime context, to regulate the relationship between a state and individuals within that state, so its juridical scope was primarily territorial. While it is now accepted that in certain circumstances human rights can have extraterritorial application,[39] precisely when a state's extraterritorial jurisdiction arises is not entirely settled. The two most widely accepted bases for extraterritorial jurisdiction are where the agents of a state exercise physical power and control over individuals outside their territory and where a state has effective control over the territory of another state. A clear example of the first basis is military detention.[40] However, the law is far from settled in terms of what precisely constitutes effective control for the second basis, as every situation turns on its own facts. Even in full war fighting in IAC, where it could reasonably be assumed that any form of effective control is impossible, there is still a view that a state could have sufficient effective control to trigger IHRL obligations.[41]

If there is jurisdiction, the second step is to determine which human rights the state is bound to uphold. Do all rights apply? Again, there is no straightforward answer to this. For effective control cases, it would appear that which human rights are in scope is a matter of the level of control being exercised; that is, how 'effective' control actually is. At the highest end of this scale, where a state exercises a level of control akin to that in its national territory, the full range of human rights must be applied. However, in situations where control is more fragile, only those human rights that are

37 Robin Geiss and Henning Lahmann, 'Protection of Data in Armed Conflict' (2021) The Geneva Academy of International Humanitarian Law and Human Rights Working Paper, 8 <https://www.geneva-academy.ch/news/detail/ 452-three-papers-map-contentious-issues-related-to-the-application-of-international-law-to-military-cyber-operations> accessed 4 March 2024.

38 See, for example, *Legal Consequences of the Construction of a Wall* (Advisory Opinion) ICJ Rep 136, paras 106, 111.

39 See, for example, *Al-Skeini and Others v the United Kingdom* (GC) App no 55721/07 (ECtHR, 7 July 2011) para 149.

40 See, for example, *Hassan v the United Kingdom* (GC) App no 29750/09 (ECtHR 16 September 2014) para 76.

41 Marko Milanovic, 'Georgia v. Russia No. 2: The European Court's Resurrection of Bankovic in the Contexts of Chaos' (*EJIL: Talk!*, 25 January 2021) <https://www.ejiltalk.org/georgia-v-russia-no-2-the-european-courts-resurrection-of-bankovic-in-the-contexts-of-chaos/> accessed 4 March 2024.

'realistically relevant in the context' apply.[42] For the jurisdiction model based on state agent physical power and control over an individual, the state in question is under an obligation *'to secure to that individual the rights and freedoms … that are relevant to the situation of that individual'*.[43] So again, which rights are in scope will be context-dependent.

To date, the International Court of Justice and regional human rights courts have not considered the right to privacy or to freedom of opinion and expression in the context of armed conflict in any detail. It is therefore difficult to assess the level of control that would be needed for these rights to be in scope. Presumably it would be high, so as to have the resources and enforcement infrastructure in place to guarantee these rights. Even then, it is possible for the state's level of control to decrease again. In this case, the human rights applicable at any particular time could be in a state of constant flux.

If it is accepted that the rights to privacy and freedom of opinion and expression may be engaged in certain situations of IAC, what is the interaction between IHL and IHRL? The approach taken by the European Court of Human Rights (ECtHR) in *Georgia v Russia* (II)[44] was that the two regimes are applied concurrently, with each body of law mutually informing the interpretation of the other. One will only take precedence where there is a direct conflict between them that cannot be resolved other than by a policy decision to apply one over the other. A direct conflict between IHL and IHRL can certainly be envisaged. If all military PsyOps are required to be openly attributable and truthful or contain a caveat on their reliability, this may significantly impact their utility in the context of IAC. This direct conflict would then require a policy decision as to which body of law applies. This would almost certainly create uncertainty for military PsyOps personnel and lead to potential errors in the application of the legal framework.

It is not the intention of this paper to dismiss IHRL, but the reality is that when training military personnel, it is imperative to ensure that the legal parameters of their proposed activity are clear and to avoid context-based solutions. In contrast to the uncertainty about the scope and application of IHRL to IAC, IHL has no context-specific degrees of application. Accordingly, it may be preferable to consider whether the concerns about PsyOps raised by IHRL can be addressed and encompassed by IHL. This is the purpose of the next section.

42 Antal Berkes, *International Human Rights Law Beyond State Territorial Control* (CUP 2021) 42–43.
43 *Al-Skeini* (n 39) paras 138–140.
44 *Georgia v Russia (II)* (GC), App no 38263/08 (ECtHR, 21 January 2021).

4. THE IHL FRAMEWORK

Military PsyOps activity in IAC, just as any other military activity, must comply with IHL. The key foundational documents for IHL relevant to this paper are the four Geneva Conventions (GCI, GCII, GCIII and GCIV)[45] along with their first Additional Protocol (AP I).[46] At the time that these were written, their primary concern was to regulate the use of kinetic force, as this posed the greatest danger to civilians.

Against this background, it is unsurprising that IHL contains no specific provisions addressing the right to freedom of opinion and expression or the right to privacy. It is also unsurprising, given the generally non-kinetic nature of PsyOps, that reference to influence activity in IHL is limited. The key provision is Article 37(2) AP I, which deals with ruses of war, defined as acts that are intended to mislead an adversary or to induce them to act recklessly. It is widely accepted that PsyOps are ruses of war. The ICRC commentary to AP I specifically gives as an example of a ruse *'resorting to psychological warfare methods by inciting the enemy soldiers to rebel, to mutiny or desert'*.[47] State practice also supports the categorization of PsyOps as ruses of war; for example, the Australian Law of Armed Conflict Manual explicitly refers to PsyOps as *'legitimate ruses'*.[48] There is also academic support for this categorization[49]

Ruses of war are not prohibited, provided that they are not perfidious and do not infringe any other applicable legal rule. A perfidious act is one designed to make the adversary believe that they are entitled to receive or must grant protection under IHL, in order to exploit this confidence to capture, kill or wound the adversary.[50] The prohibition on perfidy provides only a limited means of regulating PsyOps from a civilian protection perspective, given its adversary focus and narrow scope, and will not be considered further here. There are, however, other rules of IHL that do regulate PsyOps from this perspective. Before moving on to look at these, one particular issue that frequently causes confusion must be considered: can PsyOps, as ruses of war, be directed at civilians?

45 Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 31 (GCI); Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 85 (GCII); Geneva Convention Relative to the Treatment of Prisoners of War (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 135 (GCIII); Geneva Convention Relative to the Protection of Civilian Persons in Times of War (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 287 (GCIV).

46 Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol 1) (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 (AP I).

47 Yves Sandoz and others (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff Publishers 1987) para 1521.

48 *Law of Armed Conflict* (Australian Defence Doctrine Publication 06.4, May 2006) para 7.1 <https://www.onlinelibrary.iihl.org/national-military-manuals/> accessed 4 March 2024.

49 Michael N Schmitt and Liis Vihul (eds), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, CUP 2017) 496.

50 AP I (n 46) art 37(1).

The military doctrine explored earlier appears to accept, in framing its potential TAs, that PsyOps may be directed at civilians. This is supported by the *Tallinn Manual*'s International Group of Experts (IGE), which agreed that *'psychological operations such as making propaganda broadcasts and dropping leaflets are permitted even if against civilians'*.[51] However, at first glance, this seems hard to reconcile with the IHL principle of distinction, which provides that civilians must not be the object of attack.[52]

The key point is that distinction only governs attacks, the main characteristic of which is the use of violence or force.[53] The US Law of War Manual addresses this issue directly. It states that the principle that military operations must not be directed against civilians does not prohibit military operations short of violence that are militarily necessary. It gives PsyOps as an example.[54] The *Tallinn Manual*'s IGE also agreed that non-violent operations, such as psychological cyber operations, do not qualify as attacks.[55]

However, while PsyOps may not directly involve the use of kinetic force, they may nevertheless cause violent effects. An example would be PsyOps that incite violent public disorder as a means of destabilizing the adversary state, resulting in civilian death and injury and damage to civilian property. The French Law of Military Operations Manual also addresses this issue. It refers specifically to the use of PsyOps to discredit someone. Where the consequences of such an operation could lead indirectly to the neutralization of the targeted individual by, for example, the adversary, the full kinetic targeting process must be applied.[56]

If violent effects are identified during operational planning as a reasonably foreseeable consequence of the PsyOp in question, the operation is in fact an attack. As an attack, it is subject to the principle of distinction and all other IHL provisions governing attack. This is the same approach applied to assess whether planned cyber operations reach the level of attack.[57]

It would seem unlikely that many military PsyOps will cause violent effects so as to render them attacks, given their non-kinetic nature. Nevertheless, this issue must still be considered in military planning. For military planning purposes, the question is whether PsyOps are reasonably expected to cause violent effects. Accordingly, even if not *prima facie* an attack, all proposed PsyOps should be subject to an assessment

51 Schmitt and Vihul (n 49) 421.
52 AP I (n 46) art 48.
53 ibid art 49(1); Sandoz and others (n 47) para 1875; Schmitt and Vihul (n 49) para 422.
54 US Department of Defense (n 12) para 5.2.2.1.
55 Schmitt and Vihul (n 49) 15.
56 Le ministère des Armées (n 13) para 8.1.3.1.
57 Schmitt and Vihul (n 49) 415, 416.

and authorization process, with legal support. This should involve a multi-stakeholder discussion on the proposed operation, working through its potential ramifications.

A further associated issue is whether data is an object for the purposes of targeting and therefore also subject to the principle of distinction that states that civilian objects, as well as civilians, must not be attacked. This is clearly relevant to PsyOps that seek to manipulate or delete data (for example, social media content). Academic opinion remains divided, but the majority of the *Tallinn Manual*'s IGE were of the view that data cannot be an object due to its intangible nature.[58] Using this approach, cyber-enabled PsyOps to manipulate or delete data, be it of a military or civilian nature, are not considered attacks in the absence of any accompanying physical damage or destruction.

Even if it is accepted that PsyOps activity will rarely be categorized as an attack, IHL does contain other more general provisions that protect civilians, directly or indirectly. These are considered below.

A. Obligation of Constant Care

Article 57(1) of AP I states that in the conduct of 'military operations', constant care shall be taken to spare the civilian population, civilians and civilian objects. The concept of military operations would appear to be broader than attack. This is based on the fact that the subsequent sub-article, Article 57(2), goes on to deal specifically with attacks. If the term 'military operations' is considered to be broader than attack, this would extend the reach of the obligation, enhancing the protection of civilians.

That military operations and attacks are distinct terms is supported by the ICRC commentary to AP I. This states that military operations should be understood to mean all the movements and activities carried out by armed forces related to hostilities.[59]

The UK Law of Armed Conflict Manual also supports a broad interpretation of military operations, pointing out that this term has *'a wider connotation than "attacks" and would include the movement or deployment of armed forces'*.[60] There is also academic support to extend the understanding of military operations to non-kinetic operations. It has been asserted that the term should encompass *'all informational operations necessary to support military activities including intelligence collection'*.[61] This would clearly capture PsyOps, including TAA.

58 Schmitt and Vihul (n 49) 437.

59 Sandoz and others (n 47) paras 1936, 2191.

60 *The Joint Service Manual of the Law of Armed Conflict* (UK Joint Service Publication 383, 2004) para 532 <https://www.gov.uk/government/groups/development-concepts-and-doctrine-centre#legal> accessed 4 March 2024.

61 Asaf Lubin, 'The Duty of Constant Care and Data Protection in War' in Laura A Dickinson and Edward Berg (eds), *Big Data and Armed Conflict: Legal Issues Above and Below the Armed Conflict Threshold*, Indiana Legal Studies Research Paper No. 473, 11 <https://ssrn.com/abstract=4012023> accessed 4 March 2024.

In terms of the precise scope of the obligation, the UK Law of Armed Conflict Manual explains the obligation as *'the commander will have to bear in mind the effect on the civilian population of what he is planning to do and take steps to reduce that effect as much as possible'*.[62] However, it remains unclear what harm civilians are meant to be spared from. Some doubt has been expressed as to whether the concept of harm in this context can be expanded beyond violent effects, noting the lack of supporting state practice.[63] However, there is an opposing academic view that the types of harm covered are not limited in this way and have a broader scope.[64]

Notwithstanding opposing views on the concept of harm, the purpose of this provision is clear: to protect civilians. The obligation of constant care should be considered as part of the general assessment and authorization process for PsyOps proposed earlier. The provision provides a valuable bridge between PsyOps that are attacks and those that are military operations, and it provides a hook to consider some of the broader questions about the protection of civilians raised by IHRL. A common-sense approach should be applied to work through the potential implications of a proposed operation for civilian protection and to consider mitigation and alternative courses of action.

B. Prohibition on Terrorizing the Civilian Population

Article 51(2) of AP I prohibits attacks or threats of attack that are primarily intended to spread terror, or extreme fear, among the civilian population. In the PsyOps context, threats of violence are likely to be most relevant. The French Law of Military Operations Manual gives as an example threatening civilians with attack if they do not leave an area as instructed.[65] Simply disseminating PsyOps products on social media with terrorizing content, for example, footage of an actual attack, with no articulated threat would not meet the threshold, although it may trigger the obligation to take constant care.[66]

This raises the question of whether a threat of attack may be implied. For example, leaflets dropped by the Israeli Defence Force on Gaza residents in October 2023 warned the civilian population to leave the area immediately or risk their lives, ostensibly constituting a precautionary measure under Article 57 (2) AP I. However, the leaflets added that anyone choosing not to evacuate may be considered an accomplice in a terrorist organization.[67] This could be construed as an implied threat of violence against civilians who choose not to leave their homes, to terrorize them into compliance.

62 *UK Manual of the Law of Armed Conflict* (n 60) para 5.32.1.
63 Geiss and Lahmann (n 9) 13.
64 Lubin (n 61) 14, 15.
65 Le ministère des Armées (n 13) para 8.1.3.1.
66 Geiss and Lahmann (n 9) 12.
67 Donatella Rovera, 'Amnesty International, Israel/OPT: Israeli Army Threats Ordering Residents of Northern Gaza to Leave May Amount to War Crimes' (*Amnesty International*, 25 October 2023) <https://www.amnesty.org/en/latest/news/2023/10/israel-opt-israeli-army-threats-ordering-residents-of-northern-gaza-to-leave-may-amount-to-war-crimes/> accessed 4 March 2024.

The prohibition on terrorizing civilians should be specifically considered during military planning for PsyOps, as part of the suggested general assessment and authorization process. Proposed PsyOps products should be scrutinized during military planning to ensure that they cannot be construed to contain either an implied or express threat of attack against civilians. This includes how PsyOps products are disseminated to ensure that products designated for an adversary TA, which may directly threaten violence, are not inadvertently disseminated to civilians.

Of note, PsyOps should not use images or video footage of identifiable dead bodies to instil fear among civilians. Several IHL provisions mandate that the dead must be respected and protected during armed conflict.[68]

C. Obligation of Humane Treatment

Common Article 3 (CA3) of all four Geneva Conventions sets a benchmark for the humane treatment of persons taking no active part in hostilities in armed conflict. Outrages upon personal dignity, in particular humiliating and degrading treatment, are specifically prohibited.

CA3 is supplemented by specific provisions in the Conventions. For civilians, this is Article 27 GCIV. Civilians who find themselves *'in the hands of'*[69] the adversary, either during hostilities or in occupation are entitled to humane treatment and to protection against insults and public curiosity. They are entitled to respect for their persons, their honour and their family rights. This mirrors the protections provided to prisoners of war under GCIII.

The ICRC commentary on Article 27 states that respect for someone's person encompasses both intellectual and physical aspects. Accordingly, individual persons' names or photographs, or aspects of their private lives must not be publicized. Individuals must also not be slandered or insulted, nor should any other action be taken that may affect their reputation.[70] This would appear to prohibit PsyOps that seek to discredit or undermine a civilian subject, for example, by releasing sensitive private information about them. Not only could this be humiliating, but it could also, depending on the information released, place them in physical danger.

There is some dispute about the scope of Article 27. It undoubtedly protects civilians in the physical control of an adversary, such as detainees, and civilians living in occupied territory. However, there appears to be a gap in terms of general coverage before military occupation has been established – that is, during the war-fighting phase.[71]

68 GCIV (n 45) art 16(2); AP I (n 46) art 34(1).

69 GCIV (n 45) art 4.

70 Jean S Pictet (ed), *Geneva Convention Relative to the Protection of Civilian Persons in Time of War. Geneva, 12 August 1949: Commentary* (ICRC 1958).

71 Kubo Mačák and Mikhail Orkin, 'Who Is Protected by the Fourth Geneva Convention? The Case of Civilians in Invaded Territory' (*Lieber Institute West Point*, 15 August 2022) <https://lieber.westpoint.edu/who-is-protected-civilians-invaded-territory/> accessed 4 March 2024.

Nevertheless, given that Article 27 is an expansion of CA3, it should be read in the spirit of that provision and considered during military planning for PsyOps, as part of the suggested general assessment and authorization process. This is particularly so as its provisions may go some way to addressing concerns about privacy.

D. Obligation to Respect and Protect Medical Services

Several IHL provisions mandate that medical personnel and units, both military and civilian, must be respected and protected and may not be attacked.[72] It has been suggested that this protection includes personal medical data, such as patient records, as well as any other data *'belonging to medical units and their personnel'*.[73] This approach would clearly prohibit the cyber-enabled extraction and use or manipulation of personal medical data for PsyOps purposes from a medical unit or a healthcare professional.

According to the *Tallinn Manual*'s IGE, 'respecting' medical services and infrastructure implies a state's obligation to refrain from carrying out operations that impede or prevent medical personnel from performing their medical functions or that otherwise adversely affect the humanitarian functions of medical personnel.[74] It is clear that the extraction and use/manipulation of personal medical data could be detrimental to the functioning and humanitarian purpose of a medical unit, in terms of both patient trust and medical treatment.

This also ties in with broader concerns about the use of disinformation to distort information vital to securing human needs, including medical services. This was seen in the COVID pandemic, with people declining to be vaccinated as a result of disinformation about the health risks of vaccines.[75] In an armed conflict scenario, disinformation could be used to discredit medical units and personnel in order to discourage people from using their services, with implications for their physical well-being. From a military PsyOps perspective, such operations would be strictly prohibited. Particular attention must be paid to whether planned PsyOps may affect medical services during the recommended assessment and authorization process.

5. CONCLUSION

Despite the observation that PsyOps has *'basically only the prohibition of perfidy as a constraint'*,[76] it can be seen that there are in fact a number of provisions in IHL

72 See, for example, GCI (n 45) arts 19, 24, 25, 35 and 36; AP I (n 46) arts 12, 15, 21–24 and 26.
73 Schmitt and Vihul (n 49) 515.
74 ibid 514.
75 Ronin Emmott, 'Russia, China Sow Disinformation to Undermine Trust in Western Vaccines: EU' (*Reuters*, 28 April 2021) <https://www.reuters.com/world/china/russia-china-sow-disinformation-undermine-trust-western-vaccines-eu-report-says-2021-04-28/> accessed 4 March 2024.
76 Geiss and Lahmann (n 9) 3.

that are relevant to and regulate PsyOps from a civilian protection perspective. While IHL does not specifically address the human rights concerns discussed earlier, these provisions provide the mechanism for these broader concerns to be considered as part of military planning.

Accordingly, in the context of training and planning for PsyOps in IAC, the military focus should remain on IHL as the overarching legal framework. All proposed PsyOps should be subject to an assessment and authorization process, in the course of which the wider implications of a particular operation for civilians and the civilian population should be considered. This process should be legally supported, in the same way as the targeting process. For NATO and its member states, this process is already envisaged in NATO doctrine and simply requires development, acknowledging the increased complexity of PsyOps in light of advances in ICT.

While some may be sceptical as to whether states will be willing to apply an expansive interpretation of IHL to accommodate wider civilian protection concerns, it should be noted that NATO doctrine, which demonstrates general consensus between 32 states, already addresses some of these concerns. It mandates that NATO PsyOps should be generally truthful and attributable, which is not in fact a requirement of IHL, and expressly requires a broad consideration of their potential effects.

Above all, a degree of reality and pragmatism needs to be applied when considering training and planning for military PsyOps in IAC. The legal regime must be articulated clearly so that military personnel know the parameters they are operating within; there is no room for lengthy academic debate. An overemphasis on IHRL, given its uneven and contextual application, may cause confusion. The focus should be on strengthening IHL, emphasizing its essential humanitarian purpose and using its existing provisions to ensure that the protection of civilians is a central consideration in training and planning for military PsyOps in IAC.