INTERNATIONAL LAW STUDIES

*Published Since 1895*

# The Legal Boundaries of (Digital) Information or Psychological Operations Under International Humanitarian Law

*Tilman Rodenhäuser*

100 INT'L L. STUD. 541 (2023)

Volume 100

2023

*Published by the Stockton Center for International Law*

ISSN 2375-2831

# The Legal Boundaries of (Digital) Information or Psychological Operations Under International Humanitarian Law

*Tilman Rodenhäuser*[*]

CONTENTS



* Legal adviser at the International Committee of the Red Cross.

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

## I. INTRODUCTION

"Information operations" or "psychological operations" have long been part of armed conflicts.[1] Among Western militaries, they are commonly understood as the employment of communication or other means to influence the views, attitudes, or behavior of adversaries or civilian populations to achieve political and military objectives.[2] Chinese military strategy describes "psychological offense and defense" as "a combat action that uses specific information and media to influence the psychology and behavior of the target object through rational propaganda, deterrence and emotional guidance based on strategic intentions and combat missions."[3] Likewise, Russian military doctrine elaborates on concepts such as "psychological warfare" and on "war against mentality."[4] Non-State armed groups conduct such operations,

1. There are no universal legal definitions of the notions "information operations" or "psychological operations." Different militaries use different notions. In this article, the terms are used interchangeably and in accordance with the broad understanding provided in this introduction.

2. *See, e.g.*, RÉPUBLIQUE FRANÇAISE, MINISTÈRE DES ARMÉES, MANUEL DE DROIT DES OPÉRATIONS MILITAIRES 224 (2022) [hereinafter FRENCH MILITARY MANUAL]; NORWEGIAN MINISTRY OF DEFENCE, MANUAL OF THE LAW OF ARMED CONFLICT 199 (2018) [hereinafter NORWEGIAN MILITARY MANUAL]; NATO, Allied Joint Publication 3.10.1, Allied Joint Doctrine for Psychological Operations, at 1-1, 1-3 (ed. B, ver. 1, 2014); *Information Operations*, Joint Chiefs of Staff, Joint Publication 1-02, DOD Dictionary of Military and Associated Terms 113 (current through Mar. 2017), https://apps. dtic.mil/sti/pdfs/AD 1029823.pdf (defining information operations as "The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own"); *see also* Pontus Winther, International Humanitarian Law and Influence Operations: The Protection of Civilians from Unlawful Communication Influence Activities during Armed Conflict 41 (2019) (Ph.D. dissertation, Uppsala University).

3. CHINA NATIONAL DEFENSE UNIVERSITY, THE SCIENCE OF MILITARY STRATEGY, ch. 11, sec. 10 (2020).

4. For analysis and discussion, *see* Lora Saalman et al., *Cyber Posture Trends in China, Russia, the United States and the European Union* 9–10, SIPRI (Dec. 2022), https://www.sipri.org/publications/2022/other-publications/cyber-posture-trends-china-russia-united-states-and-european-union. Member States of the Shanghai Cooperation Organization have identified digital information operations as a major threat to "international information security," in particular, if used as part of "information warfare," which they define as "a confrontation between two or more states in the information space with the aim of . . . undermining political, economic and social system [or] psychologically manipulating masses of the population to destabilize society and the State." Agreement Between the Governments

too: Hassan Nasrallah, the leader of Hezbollah, stated that "it is well known that the most advanced weapon is psychological warfare."[5] The Islamic State group reportedly used social media "as a key recruiting tool, source of fundraising, and platform for disseminating graphic propaganda to a global audience."[6] With the rapid growth of information and communication technology over the past decade, the scale, speed, and reach of information or psychological operations have increased significantly, raising concerns about their possible humanitarian impact.[7]

States and non-State armed groups are using information or psychological operations for a variety of objectives. Some operations may be required to implement international humanitarian law (IHL) obligations.[8] For example, information operations can serve to give an effective advance warning of an attack or to help direct civilians to safety.[9] In addition, parties to an armed conflict commonly use information or psychological operations to mislead the adversary or to induce the adversary to act recklessly ("ruses of war").[10] They also use various communication channels to propagate their

---

of State Members of the Shanghai Cooperation Organization on Cooperation in the Field of Ensuring International Information Security, annex 1, June 16, 2009 (unofficial translation available at https://ccdcoe.org/uploads/2018/10/SCO-090616-IISAgreement.pdf). Note that in this definition, the scope of information warfare is probably wider than the notion of armed conflict as defined under international humanitarian law.

5. Stephen Keith Mulhern, An Analysis of Hezbollah's Use of Irregular Warfare 41 (2012) (on file with author) (quoting Hassan Nasrallah). Reportedly, Hezbollah has an "Information and Media Unit" that runs "media camps" to train people in information operations. *See* János Besenyő et al., *Hezbollah and the Internet in the Twenty-First Century*, 36 INTERNATIONAL JOURNAL OF INTELLIGENCE AND COUNTER INTELLIGENCE 669 (2023).

6. Laura Courchesne & Brian McQuinn, *After the Islamic State: Social Media and Armed Groups*, WAR ON THE ROCKS (Apr. 9, 2021), https://warontherocks.com/2021/04/after-the-islamic-state-social-media-and-armed-groups/.

7. INT'L COMM. OF THE RED CROSS, HARMFUL INFORMATION: MISINFORMATION, DISINFORMATION AND HATE SPEECH IN ARMED CONFLICT AND OTHER SITUATIONS OF VIOLENCE 10 (July 9, 2021) (finding "High internet speed and availability; social media's omnipresence and access; the use of algorithms and artificial intelligence to 'optimise' user experience; and the large, unregulated, easy to access digital environments are all elements that, in conjunction with traditional media and information flows, make [misinformation, disinformation, and hate speech] more pervasive and powerful today than in the past").

8. *See, e.g.*, Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 57(2)(c), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I]; 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, r. 20 (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2005).

9. *See also* FRENCH MILITARY MANUAL, *supra* note 2, at 225.

10. For instance, the German Military Manual states: "It is permissible to exert political and military influence by spreading—even false—information to undermine the adversary's

views or "narrative" to influence domestic and international audiences, to mobilize support, or to recruit soldiers or fighters, for example, by discrediting other parties to a conflict.[11] These operations are often considered lawful, yet there can be a fine line between campaigns conducted to raise support or influence political decisions and hateful narratives that result in violence.

In fact, disinformation and hate speech have been used to harm civilian populations during armed conflict. The UN Special Rapporteur on the Freedom of Expression has voiced concern that a common feature of today's disinformation and hate speech in armed conflict is an "increasing focus on civilian populations rather than military personnel."[12] According to her, disinformation and hate speech have been used to "whip up hatred among the population, dehumanize the other side and incite gross violations of human rights, war crimes, crimes against humanity and genocide."[13] In addition, disinformation about the nature and location of hostilities or where to find safety has made it increasingly difficult for civilians to make life-saving decisions.[14] Parties to armed conflicts have also spread disinformation about humanitarian organizations, disrupting humanitarian access and assistance and undermining the trust of affected populations in humanitarian activities.[15]

---

will to resist and to influence their military discipline (e.g. calling on them to defect, to surrender or to mutiny)." BUNDESMINISTERIUM DER VERTEIDIGUNG (Germany), ZDV 15/2, BUNDESMINISTERIUM DER VERTEIDIGUNG, ZDV 15/2, HUMANITÄRES VÖLKERRECHT IN BEWAFFNETEN KONFLIKTEN ¶ 487 (2013) [hereinafter GERMAN MILITARY MANUAL]. *See also* CHIEF OF THE GENERAL STAFF (CANADA), B-GJ-005-104/FP-021, LAW OF ARMED CONFLICT AT THE OPERATIONAL AND TACTICAL LEVELS ¶ 710 (2001) [hereinafter CANADIAN MILITARY MANUAL].

11. *See, e.g.*, Minority Rights Group International, *Peoples Under Threat 2019* (2019), https://minorityrights.org/wp-content/uploads/2019/06/PUT-2019-Briefing-with-spread.pdf; *see also* Graphika & the Stanford Internet Observatory, *More-Troll Kombat: French and Russian Influence Operations Go Head to Head Targeting Audiences in Africa* (2020), https://public-assets.graphika.com/reports/graphika_stanford_report_more_troll_kombat.pdf.

12. Irene Khan, Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *Report*, ¶ 12, U.N. Doc. A/77/288 (Aug. 12, 2022).

13. *Id.* ¶¶ 18–20; *see also* Minority Rights Group International, *supra* note 11.

14. Khan, *supra* note 12, ¶ 21.

15. *Id.* ¶¶ 24–25; *see also* Tilman Rodenhäuser et al., *Safeguarding Humanitarian Organizations from Digital Threats*, HUMANITARIAN LAW AND POLICY BLOG (Oct. 13, 2022), https://blogs.icrc.org/law-and-policy/2022/10/13/safeguarding-humanitarian-organizations-from-digital-threats/. Humanitarian organizations have observed that in times of armed conflict or other situations of violence, digital disinformation and hate speech can contribute to harassment, defamation, intimidation, social unrest, displacement, adverse effects on the operations of humanitarian organizations, or even physical violence against particular groups. *See* INT'L COMM. OF THE RED CROSS, *supra* note 7, at 11.

These operations have a particularly concerning impact if disinformation or hate speech is used in periods of instability (including armed conflicts) and if it coincides with pre-existing social tensions, low levels of digital literacy, or lack of trust or transparency in mainstream media or the authorities.[16] Such risks have increased over the past years through growing internet connectivity in all parts of the world, and technological evolution, in particular in relation to "deep fakes," will further increase the deceptive effect of information operations.[17]

Establishing causality between information or psychological operations and harm to humans can be challenging.[18] Nonetheless, experts have concluded that in several places affected by armed conflict, "the linkage between offline and online hate speech and real world acts of discrimination and violence is more than circumstantial"[19] and that "the consequences of online hate have manifested in offline violence."[20]

Against this background, this article analyzes the limits IHL sets on information or psychological operations during armed conflicts.[21] While other bodies of international law such as human rights law and international criminal law provide relevant rules, these rules, that also regulate information operations, have been examined elsewhere and are not the focus of this article.[22]

---

16. INT'L COMM. OF THE RED CROSS, *supra* note 7, at 18.

17. *See, e.g.*, Kelley Sayler & Laurie Harris, Cong. Rsch. Serv., IF11333, *Deep Fakes and National Security* (2021), https://crsreports.congress.gov/product/pdf/IF/IF11333.

18. The Independent International Fact-Finding Mission on Myanmar cautioned that whether online hate campaigns "have led or contributed to actual outbreaks of violence is difficult to establish" and needs further examination, while also noting that there is information suggesting that in some contexts "the linkage between offline and online hate speech and real world acts of discrimination and violence is more than circumstantial." Human Rights Council, *Report of the Detailed Findings of the Independent International Fact-Finding Mission on Myanmar*, ¶¶ 1325–26, U.N. Doc. A/HRC/39/CRP.2 (Sept. 17, 2018).

19. *Id.*

20. Khan, *supra* note 12, ¶ 31. With regard to incitement of genocide and crimes against humanity through the use of traditional media such as radio and newspaper, *see* Prosecutor v. Nahimana et al., Case No. ICTR-99-52-T, Trial Judgment, ¶ 949 (Dec. 3, 2003).

21. This article is written based on the position that IHL applies to the use of all means and methods of warfare during armed conflict. *See* INT'L COMM. OF THE RED CROSS, INTERNATIONAL HUMANITARIAN LAW AND CYBER OPERATIONS DURING ARMED CONFLICTS (Nov. 28, 2019), https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts.

22. For a recent overview of relevant rules of international law that regulate information operations, *see* Dapo Akande et al., *The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Information Operations and Activities*, https://www.elac.ox.ac.uk/the-oxford-process/the-statements-overview/the-oxford-statement-on-the-regulation-of-infor

## II. UNDER IHL, THE RIGHT TO RESORT TO INFORMATION OR PSYCHOLOGICAL OPERATIONS IS NOT UNLIMITED

Information or psychological operations during armed conflicts are not, as such, unlawful. Legal experts frequently remind us that "psychological operations directed at the civilian population have been a feature of warfare for centuries"[23] or recall that "propaganda, even disinformation" to "provoke the local (enemy) population to oust the enemy government" are unproblematic under IHL.[24] Some have concluded that "IHL takes a remarkably lenient approach" to disinformation during armed conflict.[25] Indeed, several military manuals expressly assert the permissibility of certain information or psychological operations, for example, disinformation or psychological warfare, as part of lawful ruses of war, in accordance with Article 37(2) of Additional Protocol I.[26] In addition, the United States Department of Defense *Law of War Manual* asserts that "in general, the use of propaganda is permissible under the law of war, even when it encourages acts that violate an enemy State's domestic law or is directed towards civilian or neutral audiences."[27] Likewise, an older version of the French military manual noted that "the law of armed conflict does not regulate psychological operations as

---

mation-operations-and-activities/ (last visited Sept. 5, 2023). For some analysis, *see* Khan, *supra* note 12; Eian Katz, *Liar's War: Protecting Civilians from Disinformation During Armed Conflict*, INTERNATIONAL REVIEW OF THE RED CROSS (Dec. 2021), https://international-review.icrc.org/articles/protecting-civilians-from-disinformation-during-armed-conflict-914.

23. Michael Schmitt, *France Speaks Out on IHL and Cyber Operations: Part II*, EJIL:TALK! (Oct. 1, 2019), https://www.ejiltalk.org/france-speaks-out-on-ihl-and-cyber-operations-part-ii/.

24. Marco Sassòli & Yvette Issar, *Challenges to International Humanitarian Law*, *in* 100 YEARS OF PEACE THROUGH LAW: PAST AND FUTURE 181, 219 (Andreas von Arnaud et al., eds. 2015).

25. Katz, *supra* note 22, at 663.

26. *See, e.g.*, the excerpts of the military manuals of Australia, Ivory Coast, Israel, Nigeria, South Africa, and the United States of America presented by the ICRC relating to its customary international humanitarian law Rule 57: Int'l Comm. of the Red Cross, International Humanitarian Law Databases, *Practice Relating to Rule 57: Ruses of War*, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule57 (last visited Sept. 5, 2023).

27. OFFICE OF THE GENERAL COUNSEL, U.S. DEPARTMENT OF DEFENSE, LAW OF WAR MANUAL § 5.26.1 (updated July 2023) [hereinafter U.S. DOD MANUAL].

such" and that "non-violent psychological operations are not prohibited and lawful even if targeted at civilians."[28]

Recalling the permissibility of certain information or psychological operations is, however, only part of the story. Importantly, many of the State militaries quoted above are also clear that information or psychological operations have well-established limits in existing rules of international law, especially IHL. For instance, already in the year 2000, the Russian Federation was clear that when conducting "military activity in the global information space . . . the Armed Forces of the Russian Federation follow the international humanitarian law."[29]

In broad terms, IHL contains two types of rules that address information or psychological operations during armed conflict. First, there are some rules that directly address certain forms of information or psychological operations. This category includes, for example, the mentioning of "misinformation" as a lawful ruse of war.[30] IHL also prohibits using "pressure or propaganda which aims at securing voluntary enlistment" of protected persons in occupied territories.[31] While during the drafting of the latter prohibition the inclusion of propaganda was controversial, the majority of States voted in favor, recognizing that there is a fine line between lawful propaganda and unlawful compulsion.[32] The second set of IHL rules does not explicitly address propaganda or other types of information or psychological operations; instead, they impose limits on the effects that may be caused. This includes at least five categories of basic rules that aim to prevent or mitigate harm against persons who do not, or no longer, participate in hostilities:

---

28. RÉPUBLIQUE FRANÇAISE, MINISTÈRE DE LA DÉFENSE, MANUEL DE DROIT DES CONFLITS ARMÉS 68 (2012) (translation by the author). Note that this statement is no longer included in the 2022 edition.

29. Ministry of Defence of the Russian Federation, The Russian Federation Information Security Doctrine approved by the President of the Russian Federation (Sept. 9, 2000), https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle (unofficial translation available at: Information Security Doctrine of the Russian Federation, INTERNATIONAL TELECOMMUNICATION UNION (Dec. 29, 2008), https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf).

30. Additional Protocol I, *supra* note 8, art. 37(2).

31. Convention (IV) Relative to the Protection of Civilian Persons in Time of War art. 51, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter GC IV].

32. COMMENTARY TO GENEVA CONVENTION IV RELATIVE TO THE PROTECTION OF CIVILIAN PERSONS IN TIME OF WAR 293 (Jean Pictet ed., 1958).

- The prohibition of encouraging IHL violations;[33]
- The prohibition of perfidy and limits imposed on "ruses of war";[34]
- The prohibition of certain threats of violence and terror—against civilians and soldiers;[35]
- The prohibition of inhumane treatment, outrages against personal dignity, humiliating or degrading treatment, for instance, by exposing prisoners of war to public curiosity;[36]
- The obligation to respect and protect medical and humanitarian relief personnel, and to allow and facilitate humanitarian relief operations.[37]

As will be discussed below, it has also been suggested that information or psychological operations can amount to "attacks" (as defined in IHL) and would therefore be subject to all IHL principles and rules on the conduct of hostilities. Similarly, it may be asked whether they qualify as "military operations," in the course of which constant care shall be taken to spare the civilian population, civilians, and civilian objects and which, under Article 48 of Additional Protocol I, must only be directed against military objectives.[38]

These rules will be discussed in the following sections. It will be shown that on a number of issues, IHL provides well-established limits that apply to all methods of warfare, including digital ones. On other issues, however, further analysis and clarification is needed. Before delving into the substance

33. Article 1 common to the four 1949 Geneva Conventions, *e.g.*, Convention (I) for the Amelioration of the Condition of the Wounded and Sick in the Armed Forces in the Field art. 1, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31 [hereinafter GC I]; CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, *supra* note 8, r. 139, 144.

34. Additional Protocol I, *supra* note 8, art. 37; CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, *supra* note 8, r. 57, 65.

35. Additional Protocol I, *supra* note 8, arts. 51(2), 75(2); Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-international Armed Conflicts arts. 4(2), 13(2), 17, June 8, 1977, 1125 U.N.T.S. 609 [hereinafter Additional Protocol II]; CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, *supra* note 8, r. 2, 129; GC IV, *supra* note 31, art. 49.

36. Convention (III) Relative to the Treatment of Prisoners of War art. 13, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter GC III]; Article 3 common to the four 1949 Geneva Conventions; Additional Protocol II, *supra* note 35, art. 4; CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, *supra* note 8, r. 87.

37. CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, *supra* note 8, r. 25, 26, 31, 32, 55.

38. Additional Protocol I, *supra* note 8, arts. 48, 57(1); CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, *supra* note 8, r. 15.

of these rules, the next section provides a brief discussion on which actors are bound by IHL rules on information and psychological operations.

### *A. Who is Bound by IHL Rules on Information and Psychological Operations?*

IHL rules are primarily addressed to parties to armed conflicts, which can be State and non-State parties.[39] Depending on the circumstances, however, attributing authorship and responsibility for information operations is challenging, especially when they occur in the digital space. In some situations, actors might feel confident in spreading inflammatory information openly, even if that information may be said to amount to prohibited hate speech.[40] In contrast, if an actor aims to use information or psychological operations to disinform, influence, or mislead the target, the operation may also be designed in a way to obscure or falsify authorship. For example, when examining alleged French and Russian disinformation in the Central African Republic, Mali, and Libya, Facebook—one of the platforms on which disinformation was spread—found that "the people behind this activity used fake accounts . . . to pose as locals in the countries they targeted."[41] While this will make it difficult to attribute such operations to their original source, attribution might not be impossible. With regard to the allegedly French and Russian operations, Facebook stated: "Although the people behind this activity attempted to conceal their identities and coordination, our investigation found links to individuals associated with past activity by the Internet Research Agency (IRA) and previous operations we attributed to entities associated with Russian financier Yevgeniy Prigozhin"[42] as well as "individuals associated with French military."[43]

Attribution of responsibility is important for several reasons, including ensuring compliance with the applicable law. As the International Committee of the Red Cross (ICRC) has cautioned with regard to cyber operations,

---

39. The latter includes, first and foremost, non-State armed groups. It may, however, also include other entities, such as private military and security companies.

40. *See, e.g.*, *Report of the Detailed Findings of the Independent International Fact-Finding Mission on Myanmar*, *supra* note 18, ¶¶ 1310–60. Still, the mission cautioned that "it is difficult to establish a comprehensive picture of the originators and propagators of hate messages, especially online" and that "many messages are reportedly also shared through private communications means, such as Viber and Messenger, which are not accessible to the Mission." *Id.* ¶¶ 1311, 1320.

41. Graphika & the Stanford Internet Observatory, *supra* note 11, at 46.

42. *Id.* at 21.

43. *Id.* at 47.

if actors obscure or hide the origin of an operation, this "hampers the possibility to identify actors who violate IHL . . . and hold them responsible," which is "one way to ensure compliance with IHL."[44] While the perceived anonymity of cyberspace and the resulting accountability challenges pose serious issues, difficulties related to attribution do not present themselves to those conducting the operation. Necessarily, they will know all the facts to determine their obligations and ensuing responsibility.[45] Under international law, a State is responsible for internationally wrongful acts, including violations of IHL, that are committed by its organs; by persons or entities it empowered to exercise elements of governmental authority; by persons or groups acting in fact on its instructions, or under its direction or control; or by private persons or groups that it acknowledges and adopts as its own conduct.[46]

When misinformation, disinformation, or hate speech is spread in the context of an armed conflict, the authors might also be private individuals, meaning persons who are neither members of State armed forces, of non-State armed groups, nor of any other party to the armed conflict. Still, private persons have been considered directly bound by (at least some) IHL rules and can be prosecuted for violations of IHL amounting to a war crime. Already in 1952, Hersch Lauterpacht considered it a "principle, which has been gaining general recognition, that the law of war is binding not only upon states but also upon individuals i.e. both upon members of the armed forces and upon civilians."[47] This principle is also reflected in the ICRC's 1960 and

44. LAURENT GISEL & LUKASZ OLEJNIK, THE POTENTIAL HUMAN COST OF CYBER OPERATIONS 7 (May 2019), https://www.icrc.org/en/document/potential-human-cost-cyber-operations (reporting on the November 2018 meeting of experts organized by the ICRC to discuss the potential human cost of cyber operations).

45. *See also* Laurent Gisel, Tilman Rodenhäuser & Knut Dörmann, *Twenty Years On: International Humanitarian Law and the Protection of Civilians Against the Effects of Cyber Operations During Armed Conflicts*, 102 INTERNATIONAL REVIEW OF THE RED CROSS 287, 309 (2020).

46. *See* CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, *supra* note 8, r. 149; *see also* Int'l Law Comm'n, *Draft Articles on the Responsibility of States for Internationally Wrongful Acts with Commentaries*, 56 U.N. GAOR Supp. No. 10, arts. 4–11, U.N. Doc. A/56/10 (2001), *reprinted in* [2001] 2 YEARBOOK OF THE INTERNATIONAL LAW COMMISSION 26, U.N. Doc. A/CN.4/SER.A/2001/Add.1 (Part 2), https://legal.un.org/ilc/documentation/english/reports/a_56_10.pdf.

47. Hersch Lauterpacht, *The Problem of the Revision of the Law of War*, 29 BRITISH YEAR BOOK OF INTERNATIONAL LAW 360, 381–82 (1952).

1987 Commentaries on the Geneva Conventions and their Additional Protocols,[48] in other expert opinions,[49] and among scholars.[50] Moreover, international criminal tribunals have held individuals responsible for war crimes irrespective of whether they have "a specific link with one of the abovementioned Parties."[51] Thus, private individuals can be held responsible for violations of those rules of IHL that are criminalized as war crimes. As will be discussed below, private individuals may also be prosecuted for information or psychological operations that order, solicit, or induce the commission of war crimes, including through digital means.[52]

If information or psychological operations are conducted by non-State actors and not attributable to a party to an armed conflict, States are nonetheless obliged to take reasonable measures to ensure respect for IHL. This means that each State has "a general duty of due diligence to prevent and repress breaches of the Conventions by private persons over which a State exercises authority."[53] This positive obligation should be interpreted as requiring a State to take active and feasible measures to prevent or halt, for example, disinformation or hate speech by private actors within its territory

---

48. *See* COMMENTARY TO GENEVA CONVENTION II FOR THE AMELIORATION OF THE CONDITION OF THE WOUNDED, SICK, AND SHIPWRECKED MEMBERS OF ARMED FORCES AT SEA 34 (Jean Pictet ed., 1960); COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, ¶ 4444 (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann eds., 1987). These two Commentaries make this statement in the context of explaining why non-State armed groups are bound by IHL. The ICRC's 2016 Commentary furthermore points to specific IHL obligations that apply to civilians. INT'L COMM. OF THE RED CROSS, COMMENTARY ON THE FIRST GENEVA CONVENTION: CONVENTION (I) FOR THE AMELIORATION OF THE CONDITION OF THE WOUNDED AND SICK IN THE ARMED FORCES IN THE FIELD, ¶ 2779 (2016).

49. INT'L COMM. OF THE RED CROSS, INTERNATIONAL HUMANITARIAN LAW AND THE CHALLENGES OF CONTEMPORARY ARMED CONFLICT 25 (2007).

50. *See, e.g.*, Jan K. Kleffner, *Scope of Application of International Humanitarian Law*, *in* THE HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW 55 (Dieter Fleck ed., 3d ed. 2013). *But see* Sassòli, who finds "it is unclear whether individuals, especially those who do not represent a party to the conflict, are bound by all rules of IHL that are not criminalized for behaviour that has the necessary nexus to the armed conflict." MARCO SASSÒLI, INTERNATIONAL HUMANITARIAN LAW: RULES, CONTROVERSIES, AND SOLUTIONS TO PROBLEMS ARISING IN WARFARE 199 (2019).

51. *See, e.g.*, Prosecutor v. Akayesu, Case No. ICTR-96-4-A, Judgment on Appeal, ¶¶ 437, 444 (June 1, 2001).

52. *See* Rome Statute of the International Criminal Court art. 25(3)(b), July 17, 1998, 2187 U.N.T.S. 90.

53. COMMENTARY ON THE FIRST GENEVA CONVENTION, *supra* note 48, ¶ 150; *See also* SASSÒLI, *supra* note 50, at 126.

that encourages or incites IHL violations—a duty that may also derive from international human rights law.[54]

## III. INFORMATION OR PSYCHOLOGICAL OPERATIONS MUST NOT ENCOURAGE IHL VIOLATIONS

The prohibition against encouraging IHL violations—irrespective of the means that is employed—derives from a State's obligation to respect and to ensure respect for IHL under Article 1 common to the four Geneva Conventions and its customary IHL equivalent, which binds all parties to armed conflicts.[55] This rule requires all parties to armed conflicts to "ensure respect for international humanitarian law by its armed forces and other persons or groups acting in fact on its instructions, or under its direction or control."[56] This means, first and foremost, that the civilian or political leadership of a party to an armed conflict must not order or encourage IHL violations by their own forces. In addition, the International Court of Justice found that a party to an armed conflict must "not encourage persons or groups engaged in the conflict . . . to act in violation of the provisions of [IHL]."[57] This finding was made with regard to a manual on "Psychological Operations in Guerrilla Warfare," which the United States provided to a non-State armed group in Nicaragua and which the Court found to encourage IHL violations.[58]

---

54. *See, e.g.*, International Covenant on Civil and Political Rights art. 2, Dec. 16, 1966, T.I.A.S. 92-908, 999 U.N.T.S. 171, which requires States to ensure the Covenant rights to all persons under its jurisdiction. *See also* Human Rights Comm., 80th Sess., *General Comment No. 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant*, CCPR/C/21/Rev.1/Add.13 (May 26, 2004).

55. Article 1 common to the four 1949 Geneva Conventions; CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, *supra* note 8, r. 139, 144.

56. CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, *supra* note 8, r. 139; *see also* GC I, *supra* note 33, art. 1; COMMENTARY ON THE FIRST GENEVA CONVENTION, *supra* note 48, ¶¶ 143–49.

57. Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 220 (June 27). As the International Court of Justice found that the obligation "not to encourage persons or groups" to violate IHL derives "from the general principles of humanitarian law" applicable in non-international armed conflict, this obligation applies to State and non-State parties to armed conflicts.

58. *Id.* ¶ 256. While some have disagreed with the Court's finding that the obligation to "ensure respect" forms part of customary IHL, they nonetheless concluded that a prohibition against encouraging IHL violations can be derived from the general principles of "good

It is widely recognized that this obligation imposes limitations on information or psychological operations: whatever method is applied, no party to an armed conflict may use communication tools—offline or online—to "encourage," "incite," or "instigate" IHL violations, including by others (i.e., not the party's own forces).[59] In some military manuals, States use different terms to describe the prohibited encouragement of IHL violations, including "incitement" or "instigation." In this respect, it should be recalled that the prohibition against encouraging IHL violations is significantly broader than the criminalization of ordering, soliciting, or inducing the commission of war crimes.[60]

First, while the Rome Statute of the International Criminal Court criminalizes acts that order, solicit, or induce the commission of war crimes—i.e., violations of only a limited number of IHL rules—IHL prohibits the encouragement of *any* IHL violation.

Second, while under international criminal law the ordering, soliciting, or inducing of war crimes can only be prosecuted if such a crime "in fact occurs or is attempted," IHL prohibits the act of encouragement and does not require that such encouragement results in an IHL violation.[61]

Third, operations prohibited as encouragement of an IHL violation are different from conduct that can qualify as soliciting or inducing war crimes. Encouraging someone is generally understood as "giving support" or to "help or stimulate" a desired conduct.[62] The International Court of Justice used "encouragement" interchangeably with the "incitement" of an IHL violation in "circumstances where the commission of such acts was likely or

---

faith" and "*pacta sunt servanda*." *See* Theodore Meron, *The Geneva Conventions as Customary Law*, 81 AMERICAN JOURNAL OF INTERNATIONAL LAW 348, 354–55 (1987).

59. *See* GERMAN MILITARY MANUAL, *supra* note 10; FRENCH MILITARY MANUAL, *supra* note 2; CANADIAN MILITARY MANUAL, *supra* note 10; U.S. DOD MANUAL, *supra* note 27; 4 NEW ZEALAND DEFENCE FORCE, DM (2 ed), MANUAL OF ARMED FORCES LAW: LAW OF ARMED CONFLICT § 8.10.27 (2019) [hereinafter NEW ZEALAND MILITARY MANUAL].

60. *See, e.g.*, Rome Statute of the International Criminal Court, *supra* note 52, art. 25(3)(b). This difference is due, in large parts, to the different ways in which State responsibility and individual criminal responsibility are reflected in international law.

61. *Id.* In other words, while the instigation of acts that would amount to war crimes is not an inchoate crime under international criminal law, such act would nonetheless be an IHL violation. For further discussion on instigation under international criminal law, *see* Wibke Timmermann, *Incitement in International Criminal Law*, 88 INTERNATIONAL REVIEW OF THE RED CROSS 823 (2006); Gregory Gordon, *Formulating a New Atrocity Speech Offense: Incitement to Commit War Crimes*, 43 LOYOLA UNIVERSITY CHICAGO LAW JOURNAL 281 (2012).

62. *Encouraging*, CONCISE OXFORD ENGLISH DICTIONARY 470 (12th ed. 2012).

foreseeable."[63] In contrast, the international criminal law notions of "inducing" or "soliciting" a war crime are understood as " 'instigating' or 'prompting another person to commit a crime' in the sense that they refer to a form of conduct by which a person exerts psychological influence on another person as a result of which the criminal act is committed."[64] Jurisprudence has consistently held that for an act of instigation, inducing, or soliciting to amount to an international crime, the act must have a direct or causal effect[65] on the commission of the offense or has made a substantial contribution to, or had a substantial effect on, the perpetrator's conduct.[66]

As a result, while the encouragement of IHL violations, including by information or psychological operations, may amount to the soliciting or inducing of war crimes, the encouragement of IHL violations is prohibited in circumstances where such violations are likely or foreseeable, even if it cannot be shown that the encouragement has a direct effect on the person committing the IHL violations.

## IV. INFORMATION OR PSYCHOLOGICAL OPERATIONS BETWEEN LAWFUL RUSES OF WAR AND PROHIBITED ACTS OF PERFIDY

IHL treaties recognize that ruses of war are not prohibited and list "misinformation" as an example of such ruses.[67] Ruses of war are defined as "acts which are intended to mislead an adversary or to induce him to act recklessly,"[68] which can be achieved, for example, by "circulating misleading

63. Military and Paramilitary Activities in and against Nicaragua, *supra* note 57, ¶¶ 255–56.

64. Prosecutor v. Bemba, ICC-01/05-01/13, Judgment Pursuant to Article 74 of the Statute, ¶ 73, ICC-01/05-01/13 (Oct. 16, 2016) (footnote omitted).

65. *See, e.g.*, *id.* ¶ 81.; Prosecutor v. Gbagbo, ICC-02/11-01/11-656-Red, Decision on the Confirmation of Charges, ¶ 244 (June 12, 2014).

66. *See, e.g.*, Prosecutor v. Semanza, Case No. ITCR-97-20-T, Judgment, ¶ 379 (May 15, 2003); Prosecutor v. Ngirabatware, Case No. ICTR-99-54, Judgment, ¶ 1291 (Dec. 20, 2012). As Coco points out, the way the ICC has applied the direct effect requirement until now "does not signal any practical difference with the 'substantial effect' requirement as applied by the ad hoc Tribunals." Antonio Coco, *Instigation*, *in* MODES OF LIABILITY IN INTERNATIONAL CRIMINAL LAW 257, 270 (Jérôme de Hemptinne et al. eds., 2019).

67. Additional Protocol I, *supra* note 8, art. 37(2); Regulations Respecting the Laws and Customs of War on Land art. 24, annexed to Convention No. IV Respecting the Laws and Customs of War on Land, Oct. 18, 1907, 36 Stat. 2227, T.S. No. 539 [hereinafter Hague Regulations]; CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, *supra* note 8, r. 57.

68. Additional Protocol I, *supra* note 8, art. 37(2).

messages."[69] Accordingly, it would not be prohibited to design false messages—including on social media—to mislead an adversary about an imminent attack or the delay of an attack, in order to shield the real intent and operation of one's forces, or to hack into the adversary's command system and spread "bogus orders purporting to have been issued by the enemy commander."[70]

While the lawfulness of spreading disinformation as a ruse of war opens the door to a variety of information or psychological operations, IHL imposes explicit limits: ruses of war must be intended to affect the adversary (meaning soldiers or fighters and not the civilian population), they must "infringe no rule of international law applicable in armed conflict," and they must not be perfidious (see below).[71] These explicit limitations are important because, in the history of armed conflict, "the ruse of war has many times served as a pretext for pure and simple violations of the rules in force."[72]

Lawful ruses of war are often contrasted with prohibited acts of perfidy. Perfidy is defined as "Acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under

---

69. COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977, *supra* note 48, ¶ 1516. The Canadian Military Manual provides the following acts as lawful ruses of war: "transmitting bogus signal messages, and sending bogus dispatches and newspapers with a view to their being intercepted by the enemy." CANADIAN MILITARY MANUAL, *supra* note 10, ¶ 602(3)(g).

70. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS r. 123 cmt. ¶ 2 (Michael N. Schmitt gen. ed., 2017) [hereinafter TALLINN MANUAL 2.0].

71. Additional Protocol I, *supra* note 8, art. 37(2); CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, *supra* note 8, r. 57. Moreover, examining IHL treaty law and the ICRC's 1987 Commentary on it, Geiss and Lahmann have suggested that ruses of war are only those practices "that have at least a nexus to the military operations" and that,

> it is not clear that corroding a civilian information space with the aim to spread confusion and uncertainty among the civilian population and without any direct link to combat activity—e.g. by manipulating content in all major online newspapers in a given country—should automatically qualify as a permissible ruse of war.

Robin Geiss & Henning Lahmann, Protecting the Global Information Space in Times of Armed Conflict 11 (Geneva Acad., Working Paper, Feb. 2021), https://www.geneva-academy.ch/joomlatools-files/docman-files/working-papers/Protecting%20the%20Global%20information%20space%20in%20times%20of%20armed%20conflict.pdf.

72. COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977, *supra* note 48, ¶ 1512.

the rules of international law applicable in armed conflict, with intent to betray that confidence."[73] Perfidy is prohibited if used to "kill, injure, or capture an adversary."[74] This rule would prohibit, for example, an information or psychological operation spreading a social media message that feigns an intent to negotiate under a flag of truce or to surrender to subsequently betray the adversary's confidence and attack. Similarly, an information operation would be prohibited if spreading fabricated images pretending that a military post (which will be used in a surprise attack against the adversary) is a medical or other civilian installation.

## V. INFORMATION OR PSYCHOLOGICAL OPERATIONS MUST NOT SPREAD CERTAIN FORMS OF FEAR, BE DESIGNED PRIMARILY TO SPREAD TERROR AMONG THE CIVILIAN POPULATION, OR CAUSE UNLAWFUL DISPLACEMENT

IHL imposes further limitations on whether and how information or psychological operations—online or offline—may be used to spread fear or terror among both belligerents and the civilian population.[75] This is explicitly recognized in several military manuals.[76]

With regard to combatants or other persons actively participating in hostilities, IHL prohibits orders or threats that no quarter will be given, including through information or psychological operations.[77] While a commonly proclaimed objective of information or psychological operations is causing defection, mutiny, or rebellion within the armed forces of an adversary,[78] such operations may not threaten that hostilities will be conducted in a way that there shall be no survivors.[79] This long-standing rule of IHL aims not only to prevent IHL violations, such as disregarding the obligation to care

73. Additional Protocol I, *supra* note 8, art. 37(1)

74. *Id.*; *see also* CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, *supra* note 8, r. 65. There is some debate on whether the customary IHL prohibition of perfidy includes the capture of an adversary or is limited to injuring and killing. *See, e.g.*, TALLINN MANUAL 2.0, *supra* note 70, r. 122 cmt. ¶ 2.

75. See discussion and accompanying text, *supra* notes 58, 62, 69.

76. See discussion and accompanying text, *supra* notes 59, 63.

77. Hague Regulations, *supra* note 67, art. 23(d); Additional Protocol I, *supra* note 8, art. 40; Additional Protocol II, *supra* note 35, art. 4; CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, *supra* note 8, r. 46.

78. *See, e.g.*, GERMAN MILITARY MANUAL, *supra* note 10; CANADIAN MILITARY MANUAL, *supra* note 10; U.S. DOD MANUAL, *supra* note 27.

79. *See, e.g.*, U.S. DOD MANUAL, *supra* note 27, § 5.26.1.3.

for the wounded and sick and to protect the life and dignity of those who surrender, but also to prevent "terrorising the adversary" with such a threat.[80]

IHL further prohibits threats of violence, where the primary purpose is to spread terror among the civilian population,[81] including when issued through information or psychological operations.[82] While there is no doubt that armed conflicts will almost inevitably "give rise to some degree of terror among the population and sometimes also among the armed forces," this rule prohibits threats of violence that are primarily designed to spread terror among civilians.[83] During the drafting of the provision, several States stressed that "the prohibition of spreading terror among the civilian population should also extend to psychological or propaganda warfare."[84] Accordingly, the prohibition of threats of violence prohibits online propaganda or a mass email campaign that would, for instance, threaten the annihilation of civilian populations[85] or threaten civilian populations with ill-treatment in

---

80. Additional Protocol I, *supra* note 8; COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977, *supra* note 48, ¶ 1591.

81. Additional Protocol I, *supra* note 8, art. 51(2); Additional Protocol II, *supra* note 35, art. 13(2); CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, *supra* note 8, r. 2; *see also* GC IV, *supra* note 31, art. 33 ("all measures of intimidation or of terrorism are prohibited").

82. *See* MINISTÈRE DE LA DÉFENSE (CÔTE D'IVOIRE), DROIT DE LA GUERRE, MANUEL D'INSTRUCTION, LIVRE I: INSTRUCTION DE BASE, at 41, 45 (Nov. 2007) (excerpt on "ruses of war" available on the ICRC website, https://ihl-databases.icrc.org/en/customary-ihl/v2/rule57 (last visited Sept. 5, 2023)); NEW ZEALAND MILITARY MANUAL, *supra* note 59, § 8.10.27; U.S. DOD MANUAL, *supra* note 27, § 5.26.1.1. TALLINN MANUAL 2.0, *supra* note 70, r. 98 cmt. ¶ 6.

83. COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977, *supra* note 48, ¶ 1940. As Gasser has pointed out:

> The *intention* to spread terror among civilians is a necessary element for defining acts of terrorism, for the simple reason that in war any use of deadly force may create fear among bystanders, even though the attack may be directed at a lawful target (e.g. aerial bombardment of a military target close to a civilian area).

Hans-Peter Gasser, *Acts of Terror, "Terrorism" and International Humanitarian Law*, 84 INTERNATIONAL REVIEW OF THE RED CROSS 547, 556 (2002).

84. Statement of Mr. Dixit, Representative of India, *reprinted in* 14 OFFICIAL RECORDS OF THE DIPLOMATIC CONFERENCE ON THE REAFFIRMATION AND DEVELOPMENT OF INTERNATIONAL HUMANITARIAN LAW APPLICABLE IN ARMED CONFLICTS, GENEVA (1974–1977), at 67 (1978); *see also id.* at 52 (statement of Mr. Crabbe, Representative of Ghana, seeking to "prevent the use of propaganda as a means of spreading terror among the civilian population").

85. *See also* NEW ZEALAND MILITARY MANUAL, *supra* note 59, § 8.10.27.

order to make them leave an area.[86] Similarly, information operations falsely raising alerts of air raids in order to spread fear amongst the civilian population would be unlawful.[87] In contrast, experts have concluded that mis- or disinformation that conveys harmful information but does not threaten an attack (that is, threaten an act of violence) does not fall under this prohibition.[88] Concretely, this means that this rule of IHL may not prohibit, for example, the spread of disinformation "sent out in order to cause panic, falsely indicating that a highly contagious and deadly disease is spreading rapidly throughout the population."[89] In contrast, the IHL rule against terrorizing civilian populations would prohibit a party to the conflict from threatening that it will spread such disease among civilians.

Linked to these provisions is also the prohibition of threatening persons who do not participate in hostilities (i.e., civilians and non-combatant military personnel) and those who no longer participate in hostilities (such as detainees or the wounded and sick) with acts of violence (Fourth Geneva Convention)[90] or violence to their life, health, or physical or mental well-being (First and Second Additional Protocols).[91] An explicit prohibition of threats of such acts was included in both Additional Protocols because "the use of threats will generally constitute violence to mental well-being," and in practice, such threats "may in themselves constitute a formidable means of pressure and undercut the other prohibitions."[92] Thus, information and psychological operations are prohibited if threatening violence to the life and person of all those who do not, or no longer, directly participate in hostilities.[93] For instance, this would be the case if a party to a conflict used social media channels to threaten those who collaborate with the adversary with ill-treatment, sexual violence, or other IHL violations.

---

86. *See* FRENCH MILITARY MANUAL, *supra* note 2, at 225.

87. Such operation may not, however, be unlawful if aimed to misdirect the adversary's armed forces and qualifying as a ruse of war.

88. TALLINN MANUAL 2.0, *supra* note 70, r. 98 cmt. ¶ 3.

89. *Id.* Note, however, that it may be unlawful under international human rights law (IHRL). *See* Marco Milanovic & Michael Schmitt, *Cyber Attacks and Cyber (Mis)information Operations During a Pandemic*, 11 JOURNAL OF NATIONAL SECURITY LAW & POLICY 247 (2020).

90. GC IV, *supra* note 31, art. 27(1).

91. *See* Additional Protocol I, *supra* note 8, art. 75(2); Additional Protocol II, *supra* note 35, art. 4(2).

92. COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977, *supra* note 48, ¶ 4543.

93. *See also* FRENCH MILITARY MANUAL, *supra* note 2, at 225.

It may further be asked whether the IHL rule prescribing that "parties to a non-international armed conflict may not order the displacement of the civilian population, in whole or in part, for reasons related to the conflict, unless the security of the civilians involved or imperative military reasons so demand" imposes limits on online or offline information or psychological operations.[94] Consider a scenario in which a party to an armed conflict spreads disinformation designed to spread fear among civilians with the objective of making them flee a location. The wording of relevant IHL provisions seems to limit the prohibition against forced displacement in non-international armed conflict to "ordering" such displacement, which would exclude the present scenario from this prohibition.[95] Yet, experts have argued—based on the object and purpose of IHL, subsequent State practice, and the drafting history of Additional Protocol II—that "ordering in this context is to be construed broadly, interpreted in the sense of a deliberate action on the part of the relevant party."[96] Otherwise, "parties would be in a position to avoid their responsibilities by deliberately creating a climate of terror, leaving the civilian population with no other choice but to leave and then claiming that no order was ever given."[97] Going in a similar direction, the International Criminal Tribunal for the Former Yugoslavia interpreted the crime against humanity of "forcible displacement" as to include displacement that is caused by "threats or the use of force, fear of violence, and illegal detention," meaning situations in which "the displacement takes place under coercion."[98] Interestingly, during the drafting of the two Additional Protocols of the Geneva Conventions, States considered "threats aimed at

94. CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, *supra* note 8, r. 129; Additional Protocol II, *supra* note 35, art. 17.

95. *See, e.g.*, Cantor, stressing that "the prohibition actually applies only to a relatively narrow form of action, namely the 'order' to displace," emphasizing further that "displacement incidental to the conflict clearly falls outside the scope of this rule." David Cantor, *Does IHL Prohibit the Forced Displacement of Civilians During War?*, 24 INTERNATIONAL JOURNAL OF REFUGEE LAW 840, 845 (2012).

96. SANDESH SIVAKUMARAN, THE LAW OF NON-INTERNATIONAL ARMED CONFLICTS 285–86 (2012). Sivakumaran flags that the important point is to distinguish such deliberate action from "voluntary movement on the part of the civilian population." *See also* Jan Willms, *Without Order, Anything Goes? The Prohibition of Forced Displacement in Non-International Armed Conflict*, 91 INTERNATIONAL REVIEW OF THE RED CROSS 547, 550 (2009).

97. MÉLANIE JACQUES, ARMED CONFLICT AND DISPLACEMENT: THE PROTECTION OF REFUGEES AND DISPLACED PERSONS UNDER INTERNATIONAL HUMANITARIAN LAW 62 (2012).

98. Prosecutor v. Blagojević & Jokić, Case No. IT-02-60-T, Judgment, ¶ 596 (Int'l Crim. Trib. for the former Yugoslavia Jan. 17, 2005).

forced movement or migration of individuals or groups of the population" to be unlawful based on the prohibition of threatening certain acts of violence.[99] As a result, there are strong legal arguments supporting the view that IHL prohibits parties from employing information or psychological operations designed to threaten or coerce civilians to flee their homes or that may be expected to result in displacement unless the security of the civilians involved or imperative military reasons so demand.

## VI. INFORMATION OPERATIONS MUST NOT AMOUNT TO INHUMANE TREATMENT

The obligation to treat humanely persons who do not or no longer participate in hostilities is "the 'leitmotiv' of the four Geneva Conventions."[100] The obligation is found—in general terms—in treaty and customary IHL and is also reflected in several more specific IHL rules.[101]

One of these rules—which is especially pertinent to information or psychological operations—is that "prisoners of war must at all times be protected . . . against insults and public curiosity."[102] Over the past decades, there have been several instances in which technological developments have presented new ways in which prisoners of war have become exposed to public curiosity, including on the internet.[103] Thus, the ICRC has found that,

> in modern conflicts, the prohibition [of exposing prisoners of war to public curiosity] also covers [subject to certain exceptions] the disclosure of photographic and video images, recordings of interrogations or private conversations or personal correspondence or any other private data, irrespective of which public communication channel is used, including the internet.[104]

---

99. COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977, *supra* note 48, ¶ 3058.

100. COMMENTARY TO GENEVA CONVENTION IV, *supra* note 32, at 204.

101. For the general obligation of humane treatment, *see* GC III, *supra* note 36, art. 13; GC IV, *supra* note 31, art. 27; Additional Protocol I, *supra* note 8, art. 75; Common Article 3 of the four 1949 Geneva Conventions; Additional Protocol II, *supra* note 35, art. 4; CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, *supra* note 8, r. 87.

102. GC III, *supra* note 36, art. 13(2). *See, e.g.*, NEW ZEALAND MILITARY MANUAL, *supra* note 59, § 8.10.27e.

103. INT'L COMM. OF THE RED CROSS, COMMENTARY ON THE THIRD GENEVA CONVENTION: CONVENTION (III) RELATIVE TO THE TREATMENT OF PRISONERS OF WAR ¶ 1622 (2021).

104. *Id.* ¶ 1624.

As a result, using photographs or videos of prisoners of war in information or psychological operations would, for example, be contrary to this rule, irrespective of whether such an operation is designed to influence military personnel or civilians.

The Fourth Geneva Convention, which aims to protect civilians in times of war, imposes further limits on information and psychological operations. The treaty provides that,

> protected persons are entitled, in all circumstances, to respect for their persons, their honour, their family rights, their religious convictions and practices, and their manners and customs. They shall at all times be humanely treated, and shall be protected especially against all acts of violence or threats thereof and against insults and public curiosity.[105]

Importantly, these rules protect "protected persons," meaning persons who "find themselves, in case of a conflict or occupation, in the hands of a Party to the conflict or Occupying Power of which they are not nationals."[106] While this includes, for example, most persons living in occupied territory as well as nationals of one party to the conflict who find themselves in the territory of an adverse party to the conflict, it does generally not include information operations conducted by State A targeted at nationals of State B living in a non-occupied part of State B.[107] In other words, IHL rules that protect the honor, family rights, religion, manners, or customs of "protected people" will not protect enemy populations who are not under the control of the party conducting such operations, which makes the question of whether such operations are restricted by the conduct of hostility rules even more important (see Part VII below).[108]

Still, where applicable, these protections are rather broad: they can be interpreted as imposing a range of limits on disinformation operations that

---

105. GC IV, *supra* note 31, art. 27(1)–(2).

106. *Id.* art. 4.

107. A notable exception would be obligations of an invading power during the "invasion phase," during which different views exist on which legal obligations apply. *See* TRISTAN FERRARO, INT'L COMM. OF THE RED CROSS, OCCUPATION AND OTHER FORMS OF ADMINISTRATION OF FOREIGN TERRITORY, REPORT OF THE EXPERT MEETING 25–26 (2012), https://www.icrc.org/en/doc/assets/files/publications/icrc-002-4094.pdf.

108. The extraterritorial effects of such operations would also raise important questions on whether human rights law would impose any restrictions. For discussion of this issue, *see* Milanovic & Schmitt, *supra* note 89.

would insult or humiliate protected persons, for instance, by ridiculing their beliefs, manners, customs, or religious practices.[109] In fact, when the Geneva Conventions were negotiated, the provision was understood as being broad enough to proscribe acts that would amount to "slander, calumny, insults or any other action impugning [the] honour or affecting [the] reputation [of a protected person]."[110]

In non-international armed conflict, humane treatment is likewise a foundational obligation, albeit not elaborated in the same amount of detail as found in the rules protecting prisoners of war or protected persons in international armed conflict. IHL, applicable in non-international armed conflict, prohibits "outrages upon personal dignity, in particular, humiliating and degrading treatment" against persons who do not or no longer participate in hostilities.[111] Additional Protocol II prescribes that these persons "are entitled to respect for their person, honour and convictions and religious practices," whether or not their liberty has been restricted.[112] Some States have taken the view that, for example, "propaganda may not be used to subject a detainee to public curiosity or other humiliating or degrading treatment."[113] It may be asked whether information operations that, for example, spread disinformation about the beliefs and customs of an ethnic or religious group, or aim to defame the political supporters of an adversary by publishing fabricated humiliating information about such persons, could amount to "outrages upon personal dignity." If IHL rules applicable in non-international armed conflict, in particular those of Additional Protocol II, were interpreted in analogy to the Fourth Geneva Convention as discussed above, these questions would be answered positively. In fact, some States consider such operations prohibited because they are "intended to harm individual civilians or the civilian population."[114] The bottom line is that the prohibition

109. COMMENTARY TO GENEVA CONVENTION IV, *supra* note 32, at 201–4.

110. *Id.* at 202.

111. IHL applicable in NIAC prohibits inhuman treatment and outrages upon personal dignity, in particular humiliating and degrading treatment. Common Article 3 of the four 1949 Geneva Conventions; CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, *supra* note 8, r. 87, 90.

112. Additional Protocol II, *supra* note 35, art. 4.

113. U.S. DOD MANUAL, *supra* note 27, § 5.26.1.3.

114. *See* NEW ZEALAND MILITARY MANUAL, *supra* note 59, § 8.10.27a.

of "outrages upon personal dignity" does not require an information operation to cause severe mental or physical pain; however, it must have a certain severity in order "to be distinguished from a mere insult."[115]

In the context of international criminal law, however, the threshold for acts that amount to "outrages upon personal dignity" is rather high, potentially higher than under IHL. For instance, the "Elements of Crimes" of the International Criminal Court require that the "severity of the humiliation, degradation or other violation was of such degree as to be *generally recognized* as an outrage upon personal dignity."[116] Until now, it appears that war crimes trials have only found violations of that rule in a limited set of cases, usually concerning the protection of detainees against sexual violence (including forced nudity) or other acts that cause a real and serious degradation or humiliation,[117] including creating the constant fear of being subjected to physical, mental, or sexual violence.[118] As a result, while it cannot be excluded that certain information or psychological operations could meet the rather high threshold of the war crime of humiliating and degrading treatment against those targeted, jurisprudence suggests that this will rather be the exception than the rule.

## VII. INFORMATION OR PSYCHOLOGICAL OPERATIONS MUST NOT HARM SPECIFICALLY PROTECTED ACTORS

For humanitarian and healthcare actors, online misinformation, disinformation, and hate speech are a growing concern. In places affected by armed conflict, tensions are high, rumors spread easily, and false information falls on fertile ground. Yet, the trust of all warring parties and communities is essential for healthcare facilities and humanitarian organizations to do their job safely. If the perception of their work changes, fueled by online or offline disinformation, their ability to operate will likely be affected. For example, a changing security situation can quickly inhibit humanitarian personnel from leaving their offices, distributing live-saving assistance, visiting detainees, or bringing news to people who have lost contact with a family member.

115. COMMENTARY ON THE THIRD GENEVA CONVENTION, *supra* note 103, ¶ 703 (commentary on common article 3).

116. INT'L CRIMINAL COURT, ELEMENTS OF CRIMES 33 (2013), https://www.icc-cpi.int/sites/default/files/Publications/Elements-of-Crimes.pdf (emphasis added).

117. COMMENTARY ON THE FIRST GENEVA CONVENTION, *supra* note 48, ¶¶ 666, 672.

118. Prosecutor v. Kvočka et al., Case No. IT-98-30/1-T, Judgment, ¶ 173 (Int'l Crim. Trib. for the former Yugoslavia Nov. 2, 2001).

In practice, misinformation that undermines their acceptance and work—or causes objection and violence against them—may unfold organically, for instance, as the result of a misunderstanding or dissatisfaction with the humanitarian services. Neither healthcare actors nor impartial humanitarian organizations are legally protected against criticism or the expression of anger of authorities or beneficiaries; to the contrary, they must welcome constructive feedback and be accountable to affected populations. In other cases, however, humanitarian or healthcare personnel have become the target of disinformation or intentionally defamatory social media campaigns.[119]

While IHL protects healthcare and humanitarian personnel and facilities as civilians and civilian objects, it also provides specific protection for these actors.

Regarding medical personnel, IHL requires belligerents to respect and protect medical facilities and personnel at all times.[120] The obligation to respect medical facilities and personnel is understood as a prohibition not only against attacking but also against "harm[ing] them in any way. This means that there should be no interference with their work (for example, by preventing supplies from getting through) or preventing the possibility of continuing to give treatment to the wounded and sick who are in their care."[121]

---

119. *See* INT'L COMM. OF THE RED CROSS, *supra* note 7, at 12; *see also Security Media Trends: Democratic Republic of the Congo*, INSECURITY INSIGHT (Apr. 2020), http://insecurityinsight.org/wp-content/uploads/2020/04/Bulletin-4-Security-Media-Trends-in-DRC.pdf.

120. *See, e.g.*, GC I, *supra* note 31, art. 19; Convention (II) for the Amelioration of the Condition of the Wounded, Sick, and Shipwrecked Members of Armed Forces at Sea art. 12, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85 [hereinafter GC II]; GC IV, *supra* note 31, art. 18; Additional Protocol I, *supra* note 8, art. 12; Additional Protocol II, *supra* note 35, art. 11; CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, *supra* note 8, r. 25, 28, 29; TALLINN MANUAL 2.0, *supra* note 70, r. 131–32. Protection of medical facility and personnel ceases only if they commit, or are used to commit, outside their humanitarian duties, acts harmful to the enemy. Protection may, however, cease only after a due warning has been given, naming, in all appropriate cases, a reasonable time limit and after such warning has remained unheeded. *See* GC I, *supra* note 31, art. 21; GC II, *supra* note 120, art. 34; GC IV, *supra* note 31, art. 19; Additional Protocol I, *supra* note 8, art. 13; Additional Protocol II, *supra* note 35, art. 11(2); CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, *supra* note 8, r. 25, 28, 29; TALLINN MANUAL 2.0 *supra* note 70, r. 134.

121. COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977, *supra* note 48, ¶ 517. *See also* COMMENTARY ON THE FIRST GENEVA CONVENTION, *supra* note 48, ¶ 1799; Dapo Akande et al., *supra* note 22:

> 5. During armed conflict, international humanitarian law requires that medical units, transport and personnel must be respected and protected at all times. Accordingly, parties to armed conflicts: must not disrupt the functioning of health-care facilities through cyber

The obligation to protect medical personnel and facilities also entails positive steps, namely an obligation to actively take measures to protect them against harm to the extent feasible.[122] Applied to information or psychological operations, this means that conducting such operations that harm medical services or disrupt their work is prohibited. Moreover, parties to the conflict must take active and feasible measures to prevent or halt, for example, disinformation or hate speech against medical personnel or facilities. Depending on the circumstances, this can mean prohibiting or countering such information or exercising influence on potential perpetrators of harm to protect medical facilities.

IHL also prescribes that humanitarian personnel and relief consignments must be respected and protected.[123] By analogy to the obligation to respect and protect medical personnel and facilities, the relevant rules should also be understood as prohibiting attacks against humanitarians as well as "other forms of harmful conduct outside the conduct of hostilities" targeted at humanitarians or that unduly interfere with their work.[124] Moreover, parties to armed conflicts are required to agree, allow, and facilitate humanitarian relief operations.[125] Thus, information or psychological operations that aim to incite violence against humanitarian personnel or relief consignments are prohibited. Moreover, operations that aim to interfere with their humanitarian relief work are unlawful if, for instance, they instigate protests to block roads and hinder humanitarians from reaching affected populations. Moreover, information operations aimed at undermining trust in the work of impartial humanitarian organizations and thereby impacting their ability to operate

---

> operations; must take all feasible precautions to avoid incidental harm caused by cyber operations, and; must take all feasible measures to facilitate the functioning of health-care facilities and to prevent their being harmed, including by cyber operations.

*Id.*; TALLINN MANUAL 2.0, *supra* note 70, r. 131 cmt. ¶ 5.

122. COMMENTARY ON THE FIRST GENEVA CONVENTION, *supra* note 48, ¶¶ 1805–8; TALLINN MANUAL 2.0, *supra* note 70, r. 131 cmt. ¶ 6.

123. Additional Protocol I, *supra* note 8, arts. 70(4), 71(2); CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, *supra* note 8, r. 31, 32.

124. COMMENTARY ON THE FIRST GENEVA CONVENTION, *supra* note 48, ¶¶ 1358, 1799. Along the same lines, the group of experts that prepared the *Tallinn Manual 2.0* identified an IHL rule requiring: "Cyber operations shall not be designed or conducted to interfere unduly with impartial efforts to provide humanitarian assistance." TALLINN MANUAL 2.0, *supra* note 70, r. 145. Such cyber operations are prohibited "even if they do not rise to the level of an 'attack.'" *Id.* r. 80 cmt. ¶ 4.

125. *See, e.g.*, GC IV, *supra* note 31, art. 59; Additional Protocol I, *supra* note 8, arts. 69–70; CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, *supra* note 8, r. 55.

safely and efficiently would be difficult to reconcile with the obligation to facilitate humanitarian relief operations. In fact, parties to armed conflicts have an obligation to take feasible measures to prevent or halt such operations, including if led by private actors or companies.

## VIII. INFORMATION OR PSYCHOLOGICAL OPERATIONS AND IHL RULES ON THE CONDUCT OF HOSTILITIES

In some circumstances, information or psychological operations may amount to attacks as defined in IHL and therefore be subject to the IHL principles and rules on the conduct of hostilities. For instance, the French military manual states that if a psychological operation "could lead indirectly to the neutralization of the targeted person, for instance through internal sanctions by the enemy, the process normally applied to kinetic targeting must be applied."[126] Likewise, the Norwegian military manual states that certain psychological operations are prohibited, such as "PSYOPS directed solely or partly at the civilian population that may cause injury or damage to civilians or civilian objects, as such PSYOPS would constitute an attack."[127] Furthermore, Michael Schmitt has argued that "psychological operations . . . are generally deemed lawful [even if directed at civilian populations] unless they *cause* physical harm or human suffering," which could be read as suggesting that certain psychological operations do amount to attacks and therefore are subjected to relevant rules on the conduct of hostilities.[128]

IHL defines attacks as "acts of violence against the adversary, whether in offence or in defence."[129] It is well-established that the notion of "violence" in this definition can refer to either the means of warfare or their effects, meaning that an operation that may be expected to cause violent effects is an attack, even if the means used to cause those effects are not

126. FRENCH MILITARY MANUAL, *supra* note 2, at 225 (translation by the author). A previous edition of the manual stated that if a psychological operation "amounts to an attack, the means employed are limited and such operations must not be directed against civilians, persons hors de combat, or be perfidious." MANUEL DE DROIT DES CONFLITS ARMÉS, *supra* note 28, at 68.

127. NORWEGIAN MILITARY MANUAL, *supra* note 2, at 200.

128. Michael Schmitt, *Cyber Operations and the Jus in Bello: Key Issues*, 87 INTERNATIONAL LAW STUDIES 89, 91 (2011) (emphasis added).

129. Additional Protocol I, *supra* note 8, art. 49.

violent as such.[130] Accordingly, for the purpose of cyber operations, the *Tallinn Manual 2.0* defines the notion of "attack" as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[131] Note that in this context, experts concluded that "injury" includes "serious illness or severe mental suffering that are tantamount to injury."[132] This focus on the effects of an operation, instead of the means employed, is also appropriate in the context of information or psychological operations, which may apply non-kinetic means but may cause violent effects.

Until now, the question of whether information or psychological operations can amount to an attack has not received much attention from IHL experts. This might be explained by the common understanding of the notion of attack. During the drafting of Additional Protocol I, the ICRC stated: "the author of an *attack* is he who . . . starts a *military operation involving the use of arms*."[133] The Bothe et al. commentary states that "the concept of 'attacks' does not include dissemination of propaganda, embargoes or other *non-physical means of psychological*, political or economic warfare."[134] Similarly, experts involved in the *Tallinn Manual* concluded that "non-violent operations, such as psychological cyber operations and cyber espionage, do not qualify as attacks."[135] The exclusion of "non-physical" or "non-violent" information or psychological operations from the notion of attack is also found in other expert commentary.[136] This, of course, poses the question of what a "violent" psychological operation would be, which, *a contrario*, could amount to

130. *See* Cordula Droege, *Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians*, 94 INTERNATIONAL REVIEW OF THE RED CROSS 533, 557 (2012) ("it is uncontroversial that the use of biological, chemical, or radiological agents would constitute an attack, even though the attack does not involve physical force"); *see also* WILLIAM BOOTHBY, THE LAW OF TARGETING 384 (2012).

131. TALLINN MANUAL 2.0, *supra* note 70, r. 92.

132. *Id.* r. 92 cmt. ¶ 8.

133. INT'L COMM. OF THE RED CROSS, COMMENTARY ON THE DRAFT ADDITIONAL PROTOCOLS TO THE GENEVA CONVENTIONS OF AUGUST 12, 1949, at 54 (1973) (emphasis added).

134. MICHAEL BOTHE ET AL., NEW RULES FOR VICTIMS OF ARMED CONFLICTS: COMMENTARY ON THE TWO 1977 PROTOCOLS ADDITIONAL TO THE GENEVA CONVENTIONS OF 1949, at 329 (2013) (emphasis added).

135. TALLINN MANUAL 2.0, *supra* note 70, r. 92 cmt. ¶ 2.

136. *See, e.g.*, YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT 3 (3d ed. 2016) ("Thus, non-violent recourse to psychological warfare; disruption of enemy communications; issuing false orders or using other

an attack. It is uncontroversial that applying overwhelming kinetic force with a "shock and awe" psychological effect will constitute an attack. But what about spreading information, such as disinformation or hate speech, that is reasonably expected to result in physical violence or severe mental suffering?

Two scenarios might help to analyze the issue further. In the first scenario, an information operation is used to influence a third party to conduct violence; in the second scenario, an information operation is used to cause an effect on the targeted people without the intervention of a third party.

In scenario one, consider that the encouragement of acts of violence are reasonably expected to cause injury or death of a third person or damage to an object, namely an information operation encouraging community A to attack community B. If the *Tallinn Manual* definition of attack is applied, one may conclude that encouragement can be reasonably expected to cause violent effects and thus qualifies as an attack. However, it may also be argued that such an interpretation is too broad because the causation between the encouragement and the harm is too remote. It seems well-accepted that an attack need not cause harm immediately or with absolute certainty (for instance, the laying of a landmine is generally considered an attack "whenever a person is directly endangered by a mine laid," not only at the moment it explodes).[137] Encouraging another person—who will take an independent decision—to conduct violence could be seen as interrupting the causation chain that is normally required for an attack. Traditionally, attacks seem to consist of acts or operations that cause harm without needing to rely on or convince another actor—who is not under the command and control of the attacking party—to conduct an act of violence.

In scenario two, consider deceiving or misleading a person into adopting a behavior they do not realize is harmful to themselves or others. For instance, consider an information operation sending disinformation by text message (SMS, WhatsApp, Facebook) to civilians fleeing hostilities that deliberately directs them into a minefield or another environment that may reasonably be expected to cause them harm. Or an information operation by State A disseminating false instructions on the handling of a weapon system to soldiers of State B that may reasonably be expected to cause these soldiers to mishandle and accidentally detonate ammunition, resulting in injury,

---

ruses . . . ; sleep-depriving sonic booms; airdropping of leaflets calling for surrender, etc., do not count as attacks").

137. COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977, *supra* note 48, ¶ 1881.

death, and destruction.[138] Compared to the first scenario, in this second scenario, the causation is more direct because it involves only one step: actor A is causing harm to actor B without needing to convince a third actor to take action. When the reasonably expected effect of an information or psychological operation is similar to a kinetic attack (i.e., injury, death, damage) and only the method to deliver the effect is different (in this case deceiving or misleading the targets into adopting a behavior that they are unaware will actually harm themselves or others), it is difficult to see why such difference should have relevance under IHL. For instance, the Norwegian *Manual* considers in the context of information operations and the notion of attack that an example of an "unlawful PSYOPS is distributing information with the aim of misleading civilians to cause them injury."[139]

While the notion of attack is today understood as including operations that employ non-violent means but can reasonably be expected to result in violent effects, only a few States and experts have expressed views on whether information operations that may be expected to lead to injury or death to humans or damage to objects could be considered attacks, and if yes, which ones. Legally speaking, the crux of the matter is whether the link between an information operation and the resulting harm can be sufficiently direct to be considered an attack.[140] Looking at the two types of operations discussed above from a humanitarian point of view, the issue is especially important regarding scenario two. While in the encouragement case (scenario one) the incitement of violence against civilians, civilian objects, or other protected actors and objects will likely be prohibited as an encouragement of IHL violations, irrespective of whether it amounts to an attack, this is not the case in scenario two. In that case, the legal classification of the information operation as an attack under IHL would be legally sound and operationally significant: IHL does not prohibit directing such attacks against members of the adversary's armed forces. However, State A would have to comply with a stricter set of rules and principles, notably distinction, proportionality, and precautions, in order to prevent, or at least minimize, their

138. Geiss and Lahmann have provided the example of disinformation spread by State A among soldiers (and eventually civilians) of State B about inhaling methanol to combat a respiratory disease, which is designed to, and actually causes, death among the addressees. Geiss & Lahmann, *supra* note 71, at 4.

139. NORWEGIAN MILITARY MANUAL, *supra* note 2, at 200.

140. *See also* Geiss & Lahmann, *supra* note 71, at 17 (suggesting a "causation" standard in analogy to the standard employed in international criminal law in the context of the instigation of crimes).

effects on civilian populations. In fact, recognizing that "non-lethal actions, such as an information operation or PSYOPS can lead to violent riots resulting in people being killed or harmed," NATO doctrine emphasizes generally that conducting information operations alongside kinetic ones "demands closer adherence to NATO policies that ensure the protection of civilians and the avoidance of collateral damage."[141]

### *A. Are Information or Psychological Operations "Military Operations" Under IHL?*

If an information or psychological operation does not amount to an attack subject to IHL rules on the conduct of hostilities because it cannot be considered as amounting to an act of violence, it needs to be asked whether such an operation may be considered a military operation under IHL and therefore subject to at least some rules governing the conduct of hostilities. Under Additional Protocol I, State parties "shall direct their *operations* only against military objectives";[142] "[t]he civilian population and individual civilians shall enjoy general protection against dangers arising from *military operations*";[143] and "[i]n the conduct of *military operations*, constant care shall be taken to spare the civilian population, civilians and civilian objects."[144] The latter rule forms part of customary IHL, applicable to all parties to armed conflicts. If information or psychological operations were considered to qualify as military operations in the IHL sense, the idea that non-violent psychological operations are lawful, if targeted at civilians, would seem difficult to reconcile with Article 48 of Additional Protocol I (for State parties to that Protocol), or at least would need to be carefully articulated.[145]

When Additional Protocol I was negotiated, military operations were understood as "any movements, manoeuvres and other activities whatsoever

141. NATO, Allied Joint Publication 3.9, Allied Joint Doctrine for Joint Targeting, at 1-3, 1-22 (ed. B, ver. 1, Nov. 2021).

142. Additional Protocol I, *supra* note 8, art. 48 (emphasis added).

143. *Id.* art. 51(1) (emphasis added).

144. *Id.* art. 57(1) (emphasis added); *see also* CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, *supra* note 8, r. 16 ("Each party to the conflict must do everything feasible to verify that targets are military objectives"). For a discussion of the notion of "military operation," *see, e.g.*, Droege, *supra* note 130, at 556; Geiss & Lahmann, *supra* note 71, at 15–16.

145. Gisel et al., *supra* note 45, at 3.

carried out by the armed forces with a view to combat" or "related to hostilities."[146] The ICRC Commentary points out that such operations do not include "ideological, political or religious campaigns."[147] Accordingly, it has been argued that "operations such as propaganda, espionage, or psychological operations will not fall under the concepts of hostilities or military operations and are therefore not governed by the principles of distinction, proportionality, and precaution, even if they are carried out by the armed forces."[148] In other words, while information operations may be conducted by the military, they would not be considered military operations for the specific legal purposes of IHL.

In contrast, others have suggested that "those communicative acts by armed forces that aim at furthering military objectives could be considered 'military operations'" under IHL.[149] While this interpretation would diverge from the traditional understanding of the term under IHL, it would arguably be in line with its natural meaning and the object and purpose of relevant rules.[150] For proponents of this view, at least the obligation to take constant care to spare the civilian population would have to be respected when conducting information or psychological operations.[151] The view that information or psychological operations are military operations is taken, for instance, by the U.S. DoD *Law of War Manual*. However, the *Manual* asserts that "the principle that military operations must not be directed against civilians does not prohibit military operations short of violence that are militarily necessary. For example, such operations may include . . . seeking to influence enemy civilians with propaganda."[152]

---

146. COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977, *supra* note 48, ¶¶ 2191, 1936, 1875. In the same vein, *see* Bothe et al., *supra* note 134, art. 48 ¶ 2.3, art. 57 ¶ 2.8.2. For State and expert views, *see* Gisel et al., *supra* note 45, n.172.

147. COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977, *supra* note 48, ¶ 1875.

148. Droege, *supra* note 130, at 556.

149. Geiss & Lahmann, *supra* note 71, at 13.

150. *Id.*

151. To reconcile such operation with Article 48 of Additional Protocol I, Schmitt has argued that Article 48 "must be interpreted as bearing on a particular type of operation, an attack" and that "operations not amounting to an attack, such as psychological operations, are generally accepted as lawful." Schmitt, *supra* note 128, at 92. *See also* DINSTEIN, *supra* note 136, at 143.

152. U.S. DOD MANUAL, *supra* note 27, § 5.2.2.1.

In the absence of additional views by States and experts, it is difficult to draw strong conclusions on whether information or psychological operations are governed by IHL rules applicable to military operations other than attacks. The views of some States suggest that directing such information or psychological operations against civilians is lawful, provided all other rules and principles of IHL are respected. This necessarily implies that either these operations are not military operations in the legal sense of the term, or that neither the principle of distinction nor the obligation of constant care apply to them. In either case, this position is difficult to maintain if such operations may be expected to put civilians in danger or cause them harm.

## IX. CONCLUSION

As digital technologies are prevalent in environments affected by armed conflicts and used by belligerents to achieve their objectives, digital forms of information or psychological operations risk being employed to cause violence against civilians, to spread fear and terror, to cause displacement, or to hinder medical and humanitarian services. While such risks have long existed irrespective of which vector is used to conduct an information or psychological operation, digital technologies enable such operations at unprecedented speed and scale.

There is general agreement that many forms of information or psychological operations—online or offline—are either not regulated by or not in violation of IHL. For instance, States did not define any rules on the regulation of political propaganda—including disinformation—to boost the morale of their own population or armed forces, to undermine support for the adversary, or to make their case in the court of public opinion. Moreover, certain forms of disinformation to mislead an adversary are recognized as lawful ruses of war. Yet, it would be wrong to infer that the use of online non-violent information or psychological operations during armed conflict is unconstrained under existing rules of IHL or that disinformation should, per se, be considered a lawful ruse of war. Ruses of war are only lawful if they "infringe no rule of international law applicable in armed conflict."[153] While only very few rules of IHL address such operations explicitly, there are several that impose limits on the conduct of belligerents irrespective of which means or methods are used. Most importantly, the International Court of Justice has found that parties to armed conflicts must "not encourage

153. Additional Protocol I, *supra* note 8, art. 37(2).

persons or groups engaged in the conflict . . . to act in violation of the provisions of [IHL]."[154] This prohibition applies irrespective of which communication vector is used. Moreover, belligerents are prohibited from threatening that no quarter will be given to surrendering enemy soldiers, from spreading fear and terror among civilian populations, or from using information operations to effect unlawful displacements. When information or psychological operations are used to undermine the morale of adversary soldiers or civilians, they must not amount to outrages against the dignity of either civilians or captured soldiers, for instance, by publishing pictures of prisoners of war. Moreover, if information operations can be reasonably expected to result in injury or death to humans, or damage to objects, their employment should comply with the rules and principles on the conduct of hostilities. And the list goes on.

In simple terms, while IHL permits information and psychological operations that are militarily necessary as part of military operations, it imposes limits, in particular, on those that are directed against either civilians or military personnel *hors de combat* and can be reasonably expected to cause harm.

154. Military and Paramilitary Activities in and against Nicaragua, *supra* note 57, ¶ 220.