# *Wired warfare 3.0: protecting the civilian population during cyber operations*

Article

Accepted Version

**Wired Warfare 3.0:**
**Protecting the Civilian Population during Cyber Operations**

**Forthcoming: International Review of the Red Cross**

Michael N. Schmitt*

**Abstract**: *As a general matter, international humanitarian law is up to the task of providing the legal framework for cyber operations during an armed conflict. However, two debates persist in this regard, the resolution of which will determine the precise degree of protection the civilian population will enjoy during cyber operations. The first revolves around the meaning of the term "attack" in various conduct of hostilities rules, while the second addresses the issue of whether data may be considered an object such that operations destroying or altering it are subject to the prohibition on attacking civilian objects and that such effects need be considered when considering proportionality and the taking of precautions in attack. Even if these debates were to be resolved, the civilian population would still face risks from the unique capabilities of cyber operations. This article proposes two policies which parties to a conflict should consider adopting in order to ameliorate such risks. They are both based on the premise that military operations must reflect a balance between military concerns and the interest of States in prevailing in the conflict.*

**Keywords**. *Cyber, attack, data, civilian object, proportionality, precautions in attack, military necessity*

The refusal by Russia, China, and a number of other countries during the 2016-2017 United Nations Group of Governmental Exerts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) negotiations to expressly acknowledge the applicability of international humanitarian law (IHL) to cyber operations marked a major reversal in the effort to clarify how such operations are constrained by international law.[1] Their refusal was particularly stunning in light of the fact that two years earlier the previous UN GGE, which included both Russia and China as members, had characterized "the principles of humanity, necessity, proportionality and distinction" as "established international law principles," [2] a statement that can only be interpreted as agreement that IHL governs the conduct of cyber hostilities during armed conflicts.

As a matter of law, the refusal is puzzling. There is broad consensus that IHL applies to cyber operations during an armed conflict. This is the position of key countries wielding cyber capability,

*Member of the Editorial Board; Professor of International Law, University of Exeter; Charles H. Stockton Professor, U.S. Naval War College; Francis Lieber Distinguished Scholar, U.S. Military Academy at West Point; General Editor, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. The views expressed are those of the author in his personal capacity. The author is grateful to Lieutenant Colonel Jeffrey Biller (USAF) for his invaluable comments.

[1] Michael N. Schmitt and Liis Vihul, *International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms*, JUST SECURITY (June 30, 2017), https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.

[2] UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2015 Report, para. 28(d), UN Doc. A/70/174 (July 22, 2015) [hereinafter UN GGE 2015 Report].

such as the United States[3], international organizations like NATO and the European Union[4], the ICRC;[5] and most of the academic community. [6] The consensus is based in part on State practice that has long recognized that new means and methods of warfare are subject to the prohibitions, restrictions and requirements found in IHL's weapons law and conduct of hostility rules[7]. In its Nuclear Weapons Advisory Opinion, for instance, the International Court of Justice confirmed IHL's applicability to new weapons.[8] Furthermore, Article 36 of Additional Protocol I to the 1949 Geneva Conventions requires parties to "in the study, development, acquisition or adoption of a new weapon, means or method of warfare….determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law." [9] Even non-Party States to Additional Protocol I recognize the need to ensure new weapons, including cyber weapons, meet the requirements of extant IHL norms. [10] Finally, simple logic dictates that IHL must apply to novel ways of conducting hostilities, for almost every conflict brings with it new weapons, tactics and operational design. It would be absurd to hold that only means and methods of warfare that predated the adoption of a treaty or the crystallization of a customary law rule are subject to the principles and rules found therein.[11]

The question, therefore, is not whether IHL applies to cyber operations conducted during an armed conflict. Rather, it is how does it do so? In most cases, application is straightforward. It is hardly a jurisprudential epiphany, for example, to conclude that a lethal, injurious or destructive cyber operations directed at civilians not violates IHL,[12] but also constitute war crimes during both

[3] Brian J. Egan, Legal Adviser, U.S. Department of State, Remarks at Berkeley Law School on International Law and Stability in Cyberspace (Nov. 10, 2016), https://perma.cc/B6TH-232L. See also *Applicability of International Law to Conflicts in Cyberspace*, 2014 DIGEST OF UNITED STATES PRACTICE IN INTERNATIONAL LAW, ch. 18, sect. A(3)(b), at 737; Harold Koh, Legal Adviser, Department of State, Remarks at the U.S. Cyber Command Inter-Agency Legal Conference (Sept. 18, 2012). On the Koh statement, see Michael N. Schmitt, *International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*, 54 HARVARD JOURNAL OF INTERNATIONAL LAW ON-LINE 13 (2012).

[4] North Atlantic Council, *Wales Summit Declaration*, para. 72, Sept. 5, 2014, https://www.nato.int/cps/ic/natohq/official_texts_112964.htm. See also European Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Feb. 7, 2013, at 72.

[5] ICRC, *Cyberwarfare and International Humanitarian Law: The ICRC's Position*, June 2013, at page 2, https://www.icrc.org/eng/assets/files/2013/130621-cyberwarfare-q-and-a-eng.pdf.

[6] See, e.g., TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Cambridge U.P., Michael N. Schmitt gen. ed. 2013), rule 20; TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 168 (Cambridge U.P., Michael N. Schmitt gen. ed. 2017), rule 80.

[7] William H. Boothby, WEAPONS AND THE LAW OF ARMED CONFLICT (Oxford U.P. 2009), at 340-341; ICRC, A Guide to the Legal Review of New Weapons, Means and Methods of Warfare (January 2006), at 3-4.

[8] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J Rep. 226, paras. 85-86 (July 8).

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

[10] Office of the General Counsel, U.S. Department of Defense, Law of War Manual, para. 16.6 (revised edition, Dec. 2016); U.S. Air Force, Legal Review of Weapons and Cyber Capabilities, AF Instruction 51-402, July 27, 2011.

[11] For an excellent comprehensive survey of the IHL issues arising from cyber operations, see Cordula Droege, *Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians*, INTERNATIONAL REVIEW OF THE RED CROSS, vol. 94, no. 886 (2012), at 533.

[12] AP I, *supra* note 9, art. 51(2); I CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, rule 1 (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2005); Protocol Additional to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of Non-international Armed Conflicts art. 4(i), June 8, 1977, 1125 U.N.T.S. 609. See also Tallinn Manual 2.0, note 6, rule 94.

international and non-international armed conflict.[13] Similarly, cyber attacks are self-evidently limited by the rule of proportionality[14] and the requirement to take precautions in attack.[15]

A number of issues nevertheless remain unsettled. Lying at the heart of this gray area are two persistent debates, the resolution of which will have significant consequences for the civilian population. Both are definitional in character. The first deals with the scope of the term "attack". It is a determinative matter with respect to cyber operations because various IHL prohibitions, restrictions and requirements apply only to those meeting the definition of attack. [16] A second debate surrounds the meaning of the term "object." It bears on cyber operations by begging the question of whether a cyber operation that destroys or alters civilian data in a way that has no physical manifestation is a prohibited attack on a civilian object.[17]

I have addressed these issues in two earlier Review articles, *Wired Warfare* and *Rewired Warfare*.[18] In this piece, I move beyond the law itself in search of partial solutions to these quandaries. This requires a brief return visit to the debates. Therefore, in Part I of this article, I summarize the differing views as to where the threshold of "attack" lies, whereas in Part II I sketch out the current disagreement as to whether data is an object. It is not my intention to relitigate the sundry positions here; on the contrary, the discussion in these two Parts is offered solely to illustrate that the law is either unsettled in a way that places civilians at risk or fails to address currently lawful cyber operations that could nevertheless prove highly detrimental to the civilian population.

Since this situation is unlikely to be resolved as a matter of law any time soon, in Part III, I offer two policy proposals to address the shortfalls in civilian protection vis-a-vis cyber operations. They are meant to be applied by the State conducting a cyber operation when that State concludes that the operation either does not qualify as an attack or is not subject to the prohibition on attacking civilian objects because data is being targeted and, in its view, data is not an object. Although the proposals are intended to enhance the protection of the civilian population, they remain sensitive to the need of

---

[13] See, e.g., Rome Statute of the International Criminal Court arts. 8(2)(b)(i), 8(2)(c)(i), July 17, 1998, 2187 U.N.T.S. 90.
[14] AP I, *supra* note 9, arts. 51(5)(b), 57(2)(a)(iii), 57(2)(b); Customary IHL Study, *supra* note 12, rule 14; Tallinn Manual 2.0, *supra* note 6, rule 113.
[15] AP I, *supra* note 9, art. 57; Customary IHL Study, *supra* note 12, chapter 5; Tallinn Manual 2.0, *supra* note 6, rules 114-120. See also Eric Jensen, *Cyber Attacks: Proportionality and Precautions in Attack*, 89 INTERNATIONAL LAW STUDIES 198 (2012).
[16] See generally AP I, *supra* note 9, part IV, sect. I. Some scholars would extend application of the rules beyond attacks despite the use of the term in the rules themselves. See, e.g., Nils Melzer, Cyberwarfare and International Law, UNIDIR Resources Paper, 2011, p. 27, http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf (arguing that applicability depends on whether the cyber operations constitute "hostilities"); Heather Harrison Dinniss, CYBER WARFARE AND THE LAWS OF WAR, at 196-202 (Cambridge University Press, 2012) (focusing on the reference to "military operations" in Article 48 of AP I).
[17] AP I, *supra* note 9, art. 52(1); Customary IHL Study, *supra* note 12, rule 7; Tallinn Manual 2.0, *supra* note 6, rule 99.
[18] Michael N. Schmitt, *Wired Warfare: Computer Network Attack and Jus in Bello*, INTERNATIONAL REVIEW OF THE RED CROSS, Vol. 84, No. 846, 2002, p. 365; Michael N. Schmitt, *Rewired Warfare: Rethinking the Law of Cyber Attack*, INTERNATIONAL REVIEW OF THE RED CROSS, Vol. 96, No. 893, 2014, p. 189. See also Knut Dörmann, *Applicability of the Additional Protocol to Computer Network Attack*, in Karin Bystrom (ed.), PROCEEDINGS OF THE INTERNATIONAL EXPERT CONFERENCE ON COMPUTER NETWORK ATTACKS AND THE APPLICABILITY OF INTERNATIONAL HUMANITARIAN LAW, Stockholm, 17–19 November 2004, p. 139, Swedish National Defence College, 2005, https://www.icrc.org/eng/resources/documents/misc/68lg92.htm. See also Michael N. Schmitt, *"Attack" as a Term of Art in International Law: The Cyber Operations Context,* PROCEEDINGS OF THE 4TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT (Christian Czosseck, Rain Ottis & Katharina Ziolkowski eds., NATO Cooperative Cyber Defence Centre of Excellence, 2012), p. 283.

States to conduct their wartime operations effectively. Thus, the proposals are designed to reflect the balance between humanitarian considerations and military necessity that undergirds international humanitarian law and other norms of warfare.[19]

It must be cautioned that I am not asserting that the two proposals represent *lex lata*; in my view they do not, although I concede that others may disagree. Instead, I am proposing a policy-driven, militarily realistic, humanitarian safety net that States can adopt for situations in which they conclude an operation during an armed conflict falls outside the strictures of IHL. Over time, the legal issues that are described below may be resolved, thereby strengthening the influence of IHL over cyber operations. But in the interim, the international community needs a practical solution that addresses these gray areas in the law of cyber targeting.

## I. Issue One: Meaning of "Attack"

As noted, key IHL prohibitions, restrictions and requirements found in treaty and customary law, or both, are framed in terms of "attacks." For instance, it is prohibited to directly attack civilians or civilian objects;[20] conduct indiscriminate [21] or perfidious attacks [22]; or attack, with various exceptions and qualifications, specified persons or objects enjoying special protection (such as medical units, [23] objects indispensable to the survival of the civilian population;[24] the environment,[25] works and installations containing dangerous forces,[26] non-defended localities,[27] and combatants who are hors de combat[28]). Attacks are subject to the rule of proportionality, which prohibits "an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to concrete and direct military advantage anticipated."[29] Additionally, a party to the conflict that is mounting an attack must take certain feasible precautions to minimize harm to the civilian population.[30]

The interpretation and customary status of some of these rules, especially with respect to cyber operations, are the subject of controversy. The point, however, is that whether they apply in the cyber context depends on the scope of the term "attack."[31] Should a cyber operation not qualify as such, the

---

[19] Jean Pictet, DEVELOPMENT AND PRINCIPLES OF INTERNATIONAL HUMANITARIAN LAW (Martinus Nijhoff Publishers 1985), at 61-63. On my approach to this balancing, see Michael N. Schmitt, *Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance,* 50 VIRGINIA JOURNAL OF INTERNATIONAL LAW 795 (2010).
[20] AP I, *supra* note 9, arts. 51(2) and 52(1). On their customary status, see Customary IHL Study, *supra* note 12, rules 1 and 7.
[21] AP I, *supra* note 9, art .51(4); Customary IHL Study, *supra* note 12, rule 11.
[22] AP I, *supra* note 9, art. 37(1); Customary IHL Study, *supra* note 12, rule 65. On the use of the term with respect to misuse of enemy emblems of nationality, see AP I, *supra* note 9, art. 39(2); Customary IHL Study, supra note 12, rule 62.
[23] AP I, *supra* note 9, art. 12(1); Customary IHL Study, supra note 12, rule 28. On the use of the term with respect to attacking medical aircraft, see AP I, *supra* note 9, arts. 27(2), 31(2).
[24] AP I, *supra* note 9, art. 54(2); Customary IHL Study, *supra* note 12, rule 54.
[25] AP I, *supra* note 9, art. 55(2). The customary status of this rule is unsettled.
[26] AP I, *supra* note 9, art. 56(1). The customary status of this rule is unsettled.
[27] AP I, *supra* note 9, art. 59(1); Customary IHL Study, *supra* note 12, rule 37.
[28] AP I, *supra* note 9, art. 41(1); Customary IHL Study, *supra* note 12, rule 47. On the prohibition on attacking persons parachuting from aircraft in distress, see AP I, *supra* note 9, art. 42.
[29] AP I, *supra* note 9, arts. 51(5)(b), 57(2)(a)(iii), 57(2)(b); Customary IHL Study, *supra* note 12, rules 14, 19.
[30] AP I, *supra* note 9, art. 57; Customary IHL Study, *supra* note 12, rule 15.
[31] For an excellent summary regarding the issue of cyber attacks, see William H. Boothby, THE LAW OF TARGETING (Oxford U.P., 2012).

rules are inapplicable, although other rules of IHL may nevertheless prohibit or restrict the cyber operation.[32]

Article 49(1) of Additional Protocol I defines attacks as "acts of violence against the adversary, whether offense or in defense." It is well accepted that conducting an act of violence against civilians or civilian objects also qualifies as an attack. [33] Drawing on this definition, the experts who produced the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* concluded that a cyber attack includes any "cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects." [34] This is so irrespective of whether the harm is caused to the target of the attack or collaterally.[35] There would appear to be no meaningful objection to characterizing cyber operations having these results as attacks.

What is often missed is that the experts did not limit the concept of "cyber attack" to physically destructive or injurious cyber operations. A majority of them concurred that "interference with functionality qualifies as damage if restoration of functionality requires replacement of physical components."[36] Thus, a cyber operation resulting in cyber infrastructure's loss of functionality would amount to a cyber attack.

At that point, consensus among the experts broke down, for they took various positions with respect to the meaning of "loss of functionality." Whereas some would limit loss of functionality to situations in which physical components of targeted cyber infrastructure need to be repaired or replaced, others were willing to extend the notion to those in which regaining functionality requires reinstallation of the operating system or of bespoke data upon which the system relies to perform its intended function. A number of them went so far as to argue that it is immaterial how the loss of functionality occurs. The mere fact that the system no longer works as designed is sufficient.[37]

A further grey area of the law involves cyber operations that do not result in injury or damage, but nevertheless cause adverse consequences for the civilian population, such as "disrupting all email communications throughout the country." [38] Most of the *Tallinn Manual* experts, despite recognizing the extent to which cyber operations of this nature might disrupt civilian life, were of the view that there is as yet no legal basis for treating such operations as an attack.[39] Nevertheless, all of the experts agreed that cyber operations causing mere inconvenience or irritation do not rise to the level of a cyber attack.[40]

---

[32] See, e.g., DoD Manual, *supra* note 10, para 16.5.2.
[33] Nils Melzer, Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law (ICRC 2009), at 49.
[34] Tallinn Manual 2.0, *supra* note 6, rule 92.
[35] Tallinn Manual 2.0, *supra* note 6, at 419.
[36] Tallinn Manual 2.0, *supra* note 6, at 417. See also Droege, *supra* note 11, at 560-561.
[37] Tallinn Manual 2.0, *supra* note 6, at 417-418. On the loss of functionality, see Boothby, Law of Targeting, *supra* note __, at 386-387.
[38] Tallinn Manual 2.0, *supra* note 6, at 418.
[39] Tallinn Manual 2.0, *supra* note 6, at 418.
[40] Tallinn Manual 2.0, *supra* note 6, at 418. See also ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, Oct. 2015, at 41-42, https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts.

The ICRC addressed the issue in both its 2011 and 2015 *IHL Challenges* reports. [41] In the latter, the organization noted that "the manner in which the notion of cyber 'attack' is defined under the rules governing the conduct of hostilities…will greatly influence the protection that IHL affords to essential civilian infrastructure."[42] It went on to zero in on the decisive question of the point at which loss of functionality renders a cyber operation an attack. In particular, the ICRC concluded that "an operation designed to disable an object – for example a computer or a computer network – constitutes an attack under the rules on the conduct of hostilities, whether or not the object is disabled through kinetic or cyber means."[43] The report correctly observed that "an overly restrictive understanding of the notion of attack would be difficult to reconcile with the object and purpose of the rules on the conduct of hostilities, which is to ensure the protection of the civilian population and civilian objects against the effects of hostilities."[44]

Sagaciously, the ICRC used the report to highlight the ambiguity in the concepts surrounding qualification as an attack. For example, with respect to the exclusion of cyber operations that merely cause inconvenience, the ICRC pointed out that "what is covered by 'inconvenience' is not defined and this terminology is not used in IHL."[45] But like the *Tallinn Manual 2.0* experts, the ICRC recognizes that, to an extent, the nature of consequences, and not necessarily their severity, matters when qualifying a cyber operation as an attack. In particular, the report excluded espionage *per se* as an attack and noted that "the jamming of radio communications or television broadcast has not traditionally been considered an attack in the sense of IHL."[46]

By these mainstream approaches, it is possible to definitively characterize destructive or injurious cyber operations as attacks and exclude those at the low-end of the effects spectrum. Yet, most cyber operations are unlikely to be physically destructive or injurious and many will not affect the targeted cyber infrastructure's functionality in a manner that would be clearly cross whatever the appropriate threshold might be for loss of functionality.

This is troubling on two accounts. First, many cyber operations that might be directed at civilian infrastructure or otherwise have serious adverse consequences for the civilian population would arguably not qualify as cyber attacks, and accordingly lie beyond the reach of IHL's rules on attack. Second, uncertainty with respect to the loss of functionality threshold leaves the legal characterization of certain cyber operations directed at or affecting the civilian population ambiguous. A party to the conflict could exploit such uncertainty to avoid consensus condemnation as unlawful of cyber operations that are directed at or otherwise affect civilian cyber infrastructure. From a humanitarian perspective, this situation is untenable.

## II. Issue Two: Data as Objects

[41] ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, Oct. 2011, at 38, https://www.icrc.org/eng/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf; 2015 IHL Challenges Report, *supra* note 40, at 41-42

[42] 2015 IHL Challenges Report, *supra* note 40, at 41.

[43] 2015 IHL Challenges Report, *supra* note 40, at 41.

[44] 2015 IHL Challenges Report, *supra* note 40, at 41.

[45] 2015 IHL Challenges Report, *supra* note 40, at 42.

[46] 2015 IHL Challenges Report, *supra* note 40, at 41-42.

A second dilemma posing particular risk for the civilian population surrounds the question of whether the notion of "objects" extends to data, such that civilian data would enjoy the protection of the prohibition on attacking civilian objects.[47] This question is independent of the issue of the definition of attack, for if data is an object, the deletion or alteration of the targeted data would plainly comprise the damage that is necessary to qualify the cyber operation as an attack. And if data is not an object, the prohibition does not attach.[48]

Two views dominate the discourse. A majority of the *Tallinn Manual* experts agreed that the term "object" should not be interpreted as encompassing data. [49] They based their conclusion on the fact that data neither falls within the "ordinary meaning" [50] of the term "object" because it is intangible, nor "comports with the explanation of it offered in the ICRC Additional Protocols 1987 commentary."[51]

The other experts replied that adopting this approach "would mean that even the deletion of essential civilian datasets such as Social Security data, tax records, and bank accounts would potentially escape the regulatory reach of the law of armed conflict, thereby running counter to the principle that the civilian population enjoys general protection from the effects of hostilities." They looked to the object and purpose of the prohibition on attacking civilian objects to conclude that the essential factor is the "severity of the operation's consequences, not the nature of harm." For these experts, "civilian data that is 'essential' to the well-being of the civilian population is encompassed in the notion of civilian objects and protected as such."[52]

In its *2015 IHL Challenges* report, the ICRC made a similar observation. Noting that "deleting or tampering with [certain] data could quickly bring government services and private businesses to a complete standstill, and could cause more harm to civilians than the destruction of physical objects,"[53] the organization opined that "[t]he conclusion that this type of operation would not be prohibited by IHL in today's ever more cyber-reliant world – either because deleting or tampering with such data would not constitute an attack in the sense of IHL or because such data would not be seen as an

[47] It must be cautioned that the debate does not extend to a cyber operation directed at data when that operation has knock-on destructive or injurious effects. Consider a cyber operation that deletes or manipulates data in an air traffic control system and thereby risks the crash of aircraft. There is broad consensus that such an operation would be an attack. The data issue only arises in situations in which a cyber operation against data does not risk having consequences that otherwise would qualify it as an attack.

[48] Operations directed against certain data are prohibited by other IHL rules. See, e.g., Tallinn Manual 2.0, *supra* note 6, rule 132 and discussion at 515 (medical data) and rule 142 and discussion at 535-536 (some experts extend protection to cultural property in data form).

[49] Tallinn Manual 2.0, *supra* note 6, at 437.

[50] Vienna Convention on the Law of Treaties, 23 May 1969, 1155 U.N.T.S. 331 (entered into force 27 January 1980), art. 31(1).

[51] Yves Sandoz, Christophe Swinarski and Bruno Zimmerman (eds), C OMMENTARY ON THE ADDITIONAL PROTOCOLS, ICRC, Geneva, 1987, paras. 2007- 2008: 'The English text uses the word "objects", which means "something placed before the eyes, or presented to the sight or other sense, an individual thing seen, or perceived, or that may be seen or perceived; a material thing". … The French … text uses the word "biens", which means "chose tangible, susceptible d'appropriation." It is clear that in both English and French the word means something that is visible and tangible.'. It must be acknowledged that the context in which the explanation was offered is not directly on point; however, the Tallinn Manual 2.0 experts nevertheless found it helpful in their deliberations.

[52] Tallinn Manual 2.0, *supra* note 6, at 437.

[53] 2015 IHL Challenges report, *supra* note 40, at 43.

object that would bring into operation the prohibition of attacks on civilian objects – seems difficult to reconcile with the object and purpose of this body of norms."[54] I agree in principle.

Various other approaches have been suggested to deal with the matter. One differentiates between so-called operational and content level data. [55] The former denotes data upon which the functioning of cyber infrastructure is reliant, whereas the latter simply represents information in data form, such as the data upon which this article is based. Dealing only with operational level data, the approach rejects the criterion of tangibility and instead concentrates its attention on whether the data qualifies as a military objective.[56] In doing so, it implicitly adopts an absolutist view of operational level data as an object. A somewhat broader approach is to simply treat data as an object. In one example thereof, the proponent supports doing so by "means of a textual, systematic and teleological interpretation of the definition of military objectives found in treaty and customary law." [57] He concludes that "if the law of armed conflict is to retain its relevance, it ought to reflect this change. That is why, it is submitted, in 2015 computer data are objects under international humanitarian law."[58]

None of the aforementioned approaches is entirely satisfactory. The restrictive approach adopted by the majority of the *Tallinn Manual* experts is under inclusive in a practical sense, for it leaves data open to destruction or alteration that could have extremely serious, even if not destructive or injurious, consequences for the civilian population. This would, as its critics allege, run counter to the IHL's object and purpose.

By contrast, the argument, however arrived at, that data *per se* qualifies as an object is over inclusive. Militaries have long conducted information operations against the enemy population, for instance to undercut support for the government or its policies. [59] Doing so is especially alluring during counter-insurgencies.[60] With the advent of cyber capabilities, such operations have been carried out by cyber means.[61] Cyber psychological operations, as an example, can include the destruction or alteration of data, as with disrupting civilian media activities.

The severity approach advocated by the minority during the *Tallinn Manual* process, as well as by the ICRC, is the most viscerally appealing. Unfortunately, no legal justification beyond the rather general claim of compliance with object and purpose has been offered to support it. Nor has useful, granular guidance explicating its implementation been set out. Moreover, it glosses over the fact that the issue at hand is a definitional one. This begs the question of the normative logic of characterizing certain data as an object based on severity of the consequences, but not doing so vis-à-vis other data when

---

[54] *Id.*
[55] Heather A. Harrison Dinniss, *The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives*, 48 ISRAEL LAW REVIEW 39 (2015).
[56] *Id.* at 41-49.
[57] Kubo Macak, *Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law*, 48 ISRAEL LAW REVIEW 55 at 55 (2015). I responded to both approaches in *The Notion of 'Objects" during Cyber Operations: A Riposte in Defence of Interpretive Precision*, 48 ISRAEL LAW REVIEW 81 (2015).
[58] Macak, *supra* note 57, at 80.
[59] See generally, e.g., U.S. Joint Chiefs of Staff, INFORMATION OPERATIONS, Joint Publication 3-13, as amended Nov. 20, 2014.
[60] See, e.g., U.S. Army, COUNTERINSURGENCY, Field Manual 3-24, Dec. 2006, paras. 5-19 to 5-34.
[61] The U.S. military is carefully assessing the use of such capabilities. See, e.g., Liston Wells II, *Cognitive-Emotional Conflict: Adversary Will and Social Resilience*, 7:2 P RISM 5 (2017). Prism is published by the US National Defense University. The emphasis on such operations is evidenced by establishment of the College of Information and Cyberspace at National Defense University (see http://cic.ndu.edu/).

the consequences of damaging or altering it are less serious. It might make sense to draw a transactional legal line on the basis of consequences caused, as is done with the rule of proportionality, but the same reasoning does not apply when merely defining a term.

The debate will not be resolved in the near future, for adopting an approach by which data either is or is not an object leads to results that are unsatisfactory and impractical. And although considering the severity of consequences for the civilian population seems to reflect the foundational purposes of IHL, the lack of a clear legal basis for the position renders it *lex ferenda*, rather than *lex lata*.

## III. What is to be done?

What is to be done in the face of this troubling situation? In my view, the answer lies in looking to the spirit, since the letter falls short, of IHL to inform policy choice. I therefore offer two policy recommendations in that spirit, both of which focus on the severity of effects caused for the civilian population, rather than the type (as in physical damage) of the harm resulting.

The spirit of international humanitarian law is found in its delicate balancing act between the interests of States in effectively conducting military operations and the suffering it causes to both combatants and the civilian population. This balancing has been repeatedly recognized in the key IHL treaties and State guidance. For instance, the 1863 Lieber Code, which set forth instructions for the Union Army during the U.S. Civil War, provided,

> Military necessity does not admit of cruelty – that is, the infliction of suffering for the sake of suffering or for revenge, nor of maiming or wounding except in fight, nor of torture to extort confessions. It does not admit of the use of poison in any way, nor of the wanton devastation of a district. It admits of deception, but disclaims acts of perfidy; and, in general, military necessity does not include any act of hostility which makes the return to peace unnecessarily difficult.[62]

Five years later, the St. Petersburg Declaration similarly emphasized the need to "fix[] the technical limits at which the necessities of war ought to yield to the requirements of humanity."[63] Balancing also animated the 1907 Hague Peace Conference, as is apparent in Hague Convention IV, which noted that the instrument, one that since has been recognized as having a customary character,[64] was "inspired by the desire to diminish the evils of war, as far as military requirements permit."[65] The

[62] U.S. Department of War, Instructions for the Government of Armies of the United States in the Field, General Orders No. 100, Apr. 24, 1863 (Lieber Code), art. 16.

[63] Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight, preamble, Nov. 29, 1868, 18 Martens Nouveau Recueil (ser. 1) 474

[64] Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136 at 172 (July 9); Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226 at 257 (July 8). The Nuremberg Tribunal also found the rules set forth in Hague IV to reflect customary law. 1 Trial of the Major War Criminals before the International Military Tribunal 254 (1947).

[65] Convention Respecting the Laws and Customs of War on Land (Hague Convention IV), preamble, Oct. 18, 1907, 36 Stat. 2277, 207 Consol. T.S. 277. See also Convention with Respect to the Laws and Customs of War on Land, preamble, July 29, 1899, 32 Stat. 1803, 26 Martens Nouveau Recueil (ser. 2) 949. The 1899 and 1907 Hague Regulations, in Article 22 of the annex to both treaties, also noted, "[t]he right of belligerents to adopt means of injuring the enemy is not unlimited." For the modern expression of this principle, see AP I, supra note 9, art. 35(1) (adding a reference to "methods" of warfare).

instrument likewise set out the "Martens Clause", which reappeared seven decades later in Additional Protocol I:

> Until a more complete code of the laws of war has been issued, the High Contracting Parties deem it expedient to declare that, in cases not included in the Regulations adopted by them, the inhabitants and the belligerents remain under the protection and the rule of the principles of the law of nations, as they result from the usages established among civilized peoples, from the laws of humanity, and the dictates of the public conscience.[66]

These examples exemplify the International Court of Justice's observation in *Corfu Channel*, its first case, that "elementary considerations of humanity" infuse international law.[67]

Cyber operations are a game changer in terms of achieving the sought-after balance informing IHL. International humanitarian law was crafted in the context of means and methods of warfare, the effects of which were to damage, destroy, injure or kill. While the civilian population might suffer as a result of military operations that do not cause these consequences, the threat of harm was overwhelmingly from such effects. Thus, IHL rules are grounded in shielding civilians and civilian objects from them, at least to the extent possible without depriving States of their ability to conduct essential military operations.[68]

Unlike kinetic means and methods of warfare, however, cyber operations can severely disrupt civilian life without necessarily running afoul of such physicality-based rules. This is because the vast majority of the operations, being neither damaging nor injurious, do not fit neatly into the extant normative architecture meant to protect the civilian population. This predicament cannot be alleviated by treating civilian data as a protected civilian object, for doing so would be legally controversial at best and almost certainly prove unacceptable to many States.

The first step in remedying the situation is to recognize that, as illustrated, the international community generally accepts the principle that the suffering afflicted on the civilian population by warfare should be minimized to the extent possible in the attendant circumstances. There is no reason to limit application of this humanitarian principle to the province hard law. On the contrary, most IHL norms were either adopted in treaty form or crystallized into customary law only after the international community found the actions to which they apply unacceptable or inappropriate in the circumstances. Humanitarian policies and perspectives have often matured into law over time.

---

[66] 1907 Hague Convention IV, *supra* note 65, preamble; AP I, *supra* note 9, art. 1(2). The clause has been cited by the International Court of Justice. Legality of the Threat or Use of Nuclear Weapons, *supra* note 64, at 257.

[67] Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4 at 22 (Apr. 9).

[68] This cognitive paradigm of physicality finds expression, for example, in the general principle that the "civilian population and individual civilians shall enjoy general protection against *dangers* arising from military operations" (AP I, *supra* note 9, art. 51(1)); the reference to *violence* in the definition of attack (art. 49(1)); the limitation in the application of the rule proportionality and certain precautions in attack to "incidental *loss of civilian life, injury to civilians, [and] damage* to civilian objects" (arts. 51(5)(b), 57(2)(a)(ii), 51(2)(a)(iii), 51(2)(b)); and the prohibition of "acts or threats of *violence* the primary purpose of which is to spread terror among the civilian population" (art. 51(2)). Indeed, in explicating the principle of distinction, which requires that parties to a conflict "at all time distinguish between the civilian population combatants and between civilian objects and military objectives and accordingly…direct their operations only against military objectives" (art. 48), the ICRC *Commentary* to the Additional Protocols defines military operations as those "during which *violence* is used" (Additional Protocols Commentary, *supra* note 51, para. 1875).

Therefore, I propose that States adopt two humanitarian policy norms to address the gaps and uncertainty identified above. Some States may be of the view that elements thereof already reflect IHL. However, because consensus is lacking, it is necessary to style them as policy mandates, at least for States that do not hold that position.

*a. Policy One: Essential Civilian Functions*

The first proposal is to *accord special protection to certain "essential civilian functions or services" by committing to refrain from conducting cyber operations against civilian infrastructure or data that interfere with them*. I raised the notion in a 2014 article,[69] where I suggested that over time States might "simply begin to treat operations against essential civilian services and data as attacks by refraining from conducting them and condemning those who do, thereby creating the State practice upon which an evolution in meaning can be based."[70] That proposal was misguided in the sense that I confused adaptation of the meaning of a term – "attack" – with what is effectively a special protection. Therefore, I am now recasting the idea in the guise of a special protection based in policy to be adopted by States that do not already see it as a legal requirement.[71]

Note that the proposal is to safeguard functions and services rather than specified categories of civilian (that is, not qualifying as a military objective) cyber infrastructure or data. This is meant to avoid disagreement over whether specific infrastructure or data falls within the protected category. By focusing on functions or services, protection is extended to any infrastructure or data that might degrade them irrespective of the nature or category of infrastructure or data involved. Such an approach is not unprecedented in IHL. For instance, interference by cyber means with medical functions[72] or, under certain circumstances, the provision of humanitarian assistance [73] is prohibited. The proposal takes the same tack, albeit from a policy perspective.

---

[69] Michael N. Schmitt, *The Law of Cyber Warfare: Quo Vadis?,* 25 STANFORD LAW AND POLICY REVIEW 269 (2014).
[70] Schmitt, Quo Vadis, *supra* note 69, at 296.
[71] For an early proposal along these lines, see Adam Segal, 'Cyber space governance: the next step', Council on Foreign Relations, Policy Innovation Memorandum No. 2, 14 November 2011, p. 3, www.cfr.org/cybersecurity/cyberspace-governance-next-step/p24397. A number of authors have expressed skepticism about its prospects. Droege, *supra* note 11, at 577; Robin Geiss and Henning Lahmann, 'Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space', in Israeli Law Review, Vol. 45, No. 3, November 2012, p. 394. I am less pessimistic than them about the prospect of States issuing such declarations or policies regarding so-called "digital safe havens," but believe the proposal, which encompassed both *jus ad bellum* and *jus in bello* issues, requires greater legal granularity.
[72] Tallinn Manual 2.0, *supra* note 6, rule 131 (duty to "respect" is "breached by actions that impede or prevent medical or religious personnel, units, or medical transports from performing their medical or religious functions." Id. at 514). For the obligations generally, see Convention (I) for the Amelioration of the Condition of the Wounded and Sick in the Armed Forces in the Field arts. 19, 24, 25, 35-36, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31; Convention (II) for the Amelioration of the Condition of the Wounded, Sick, and Shipwrecked Members of Armed Forces at Sea arts. 22, 24, 25, 27, 36-39, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85; Convention (III) Relative to the Treatment of Prisoners of War art. 33, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135; Convention (IV) Relative to the Protection of Civilian Persons in Time of War arts. 18-22, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287; AP I, *supra* note 9, arts. 12, 15, 21-24, 26; Protocol Additional to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of II, *supra* note 12, art. 9.
[73] Tallinn Manual 2.0, *supra* note 6, rule 145 For the obligation generally, see GC IV, *supra* note 72, arts. 23 and 59; AP I, *supra* note 9, arts. 69-70.

In its *2015 IHL Challenges* report, the ICRC similarly highlighted the need for protection of essential civilian infrastructure and civilian data, particularly in light of uncertainty in the law.[74] It observed,

> With regard to data belonging to certain categories of objects that enjoy specific protection under IHL, the protective rules are comprehensive. For example, the obligation to respect and protect medical facilities must be understood as extending to medical data belonging to those facilities. However, it would be important to clarify the extent to which civilian data that does not benefit from such specific protection, such as social security data, tax records, bank accounts, companies' client files or election lists or records, is already protected by the existing general rules on the conduct of hostilities.

While I agree with the ICRC, clarification could result in a finding that IHL does not fully protect key data affecting the civilian population. The proposed policy would lower that risk, for if clarification found data not to be protected by IHL, it would nevertheless enjoy protection based on the policy. Additionally, the policy could operate until the matter of data, as well as the threshold of attack, is settled.

The devil is in the details, specifically, identifying the functions and services that qualify as essential. There is certain to be disagreement in this regard, as already evidenced by the long-running debates over designating systems as "critical infrastructure." [75] As an example of possible disagreement, note how the ICRC highlighted data affiliated with bank accounts and election records in the extract above. I suspect that many States would be unwilling to completely take such data off the table. For instance, a cyber operation blocking access to the bank accounts of an enemy dictator's cronies or senior members of her political party might well be an attractive option during an armed conflict. Similarly, disrupting her reelection by manipulating election returns might appeal to the enemy State. This point is made not to express disagreement, but rather to underline that it will be difficult to forge broad consensus as to which civilian functions and services are essential and merit protection.

Nevertheless, certain functions would seem to clearly fall within the category's boundaries. For instance, the delivery of social services to the disabled, young, poor and elderly would do so. So too would primary and secondary education. Indicators of the propriety of inclusion of a function or service in the category could include the fact that interference therewith would likely cause significant mental anguish amongst the civilian population. To illustrate, I have suggested elsewhere that "the integrity of data of financial institutions and the availability of critical financial systems" should be afforded special protection as a matter of policy.[76]

Another indicator might be that a cyber operation affecting a particular function of service would have consequences extending well beyond the close of hostilities. A prime example would be impeding the overall functioning of a country's university system, although this protection would not extend to individual cyber infrastructure at a university qualifying as a military objective, as in the case of that used to conduct weapons or other military-related research.

---

[74] 2015 Challenges Report, *supra* note 40, at 42-43.

[75] See, e.g., John Moteff, Claudia Copeland, and John Fischer, Critical Infrastructures: What Makes an Infrastructure Critical? (Congressional Research Service Report, Jan. 29, 2003).

[76] Michael N. Schmitt and Tim Maurer, *Protecting Financial Data in Cyberspace: Precedent for Further Progress on Cyber Norms?* JUST SECURITY (August 26, 2017), https://www.justsecurity.org/44411/protecting-financial-data-cyberspace-precedent-progress-cyber-norms/. That proposal does not encompass such activities as blocking access to data for a limited period of time or intruding into confidential data.

*b. Policy Two: Balancing Negative Civilian Effects and Benefits Related to the Conflict*

The second proposed policy would apply in situations not encompassed in the first (or until agreement is reached regarding designated functions and services). Unlike the first, which is absolute in character, this commitment is a relative in that it is based on a balancing of humanitarian considerations and a State's interest in prevailing in the armed conflict. By it, States would commit, as a matter of policy, to *refrain from conducting cyber operations to which the IHL rules governing attacks do not apply when the expected concrete negative effects on individual civilians or the civilian population is excessive relative to the concrete benefit related to the conflict that is anticipated to be gained through the operation*.[77]

Drawing on the controversies set forth above, IHL inapplicability could result from a State's conclusion that the operation is not an attack under IHL or by its taking of a position that data is not an object. Importantly, the perspective on the applicable interpretation of the law would be that of the State conducting the operation. In other words, by this proposal a State would agree to apply the policy whenever it concludes that an operation is not subject to the IHL rules on the conduct of hostilities. Another State might come to a different conclusion with respect to an analogous operation; in that case, it would follow guidance found in that law.

The commitment merits careful parsing. To begin with, it encompasses operations targeting cyber infrastructure and data that are either military objectives or civilian objects. An interesting point in this regard highlighted by the *2015 IHL Challenges* report involves so-called "dual-use" objects, that is, those used for both military and civilian purposes. The prevailing position among IHL experts is that any military use of a civilian object, including cyber infrastructure, renders the object a military objective, with the exception of those aspects thereof that are clearly separate and distinct components.[78] The report expresses apprehension about this standard should it be applied in the cyber context.

> A strict application of this understanding could lead to the conclusion that many objects forming part of the cyberspace infrastructure would constitute military objectives and would not be protected against attack, whether cyber or kinetic. This would be a matter of serious concern because of the ensuing impact that such a loss of protection could have in terms of disruption of the ever-increasing concomitant civilian usage of cyber space.[79]

---

[77] IHL's focus on physicality poses particular challenges with respect to cyber operations that *do* amount to an attack. In particular, the collateral damage that factors into the proportionality analysis and the requirement to take feasible precautions in attack is textually limited to injury, death, or damage. Although damage can reasonably be understood to include loss of functionality (wherever that threshold might lie), it does not include other forms of harm. For example, a proportionality analysis of an attack on dual-use cyber infrastructure would not need, as a matter of law, to account for the temporary disruption or loss of civilian services that depend on it unless that loss placed civilians at risk of physical harm or civilian objects at risk of damage. While this is also the case with the kinetic strikes, as with an attack on a store that is being used to stash weapons, networking and other forms of connectivity exacerbate the knock-on non-destructive or non-injurious effects of cyber attacks. This article does not address that reality as it is limited to cyber operations falling beyond the reach of IHL, but it is a cyber-specific phenomenon that merits serious attention.

[78] Tallinn Manual 2.0, *supra* note 6, rule 101; Harvard Program on Humanitarian Policy and Conflict Research, Manual on International Law Applicable to Air and Missile Warfare 119 (2013); Nils Melzer, INTERNATIONAL HUMANITARIAN LAW: A COMPREHENSIVE INTRODUCTION 92 (ICRC, 2016). For a discussion of the distinctness of part of a targeted object, see Michael N. Schmitt and John J. Merriam, *The Tyranny of Context: Israeli Targeting Practices in Legal Perspective*, 37 U NIVERSITY OF PENNSYLVANIA JOURNAL OF INTERNATIONAL LAW 53 (2015), at 119-123.

[79] 2015 Challenges report, *supra* note 40, at 42.

I share the concern. Whether such cyber infrastructure should be considered a military objective is an issue that is beyond the scope of this article; I take the prevailing view. But even if this stance was to shift over time and certain dual-use cyber infrastructure began to be characterized as civilian in character, it would nevertheless be lawful to conduct cyber operations against it, including operations having severe consequences for the civilian population, so long as those operations did not rise to the level of an attack, in particular by being destructive or injurious. The proposed policy would in part ameliorate this dilemma.

Certain terms contained in the policy were cautiously selected to make particular points and hopefully will serve as the fulcrum around which subsequent discussions occur. "Negative effects" is meant to be all-encompassing. It includes any effect on the civilian population that does not qualify the cyber operation as an attack and therefore subject it to application of the rules on attack. Although limited to effects on persons as distinct from objects, it extends to those consequences for civilians that result from an operation's effect on the targeted infrastructure. To take a simple example, a denial of service attack on a bank's computer system would deprive customers of their ability to withdraw currency; the customers have been affected and the policy applies.

The focus on effects also signals that the type of a cyber operation has no bearing on applicability of the proposal. For instance, a denial of service attack or an operation that causes a cyber system to slow would be no less governed by the policy than one resulting in the system operating improperly. Instead, the key factor is that the civilian population is somehow affected in a manner that is not addressed, at least in the opinion of the State conducting the operation, by the rules of IHL.

Although the *Tallinn Manual* experts agreed that inconvenience is not sufficiently severe to reach the attack threshold, there is no reason to draw a line of that nature in the case of the proposed policy. This is because it would only prohibit a cyber operation when the negative civilian effects thereof are excessive relative to the conflict-related benefits that are anticipated to result. As a matter of policy, there is rationale for excluding inconvenience or irritation as a prohibitive consequence if the party conducting the cyber operation cannot proffer a sufficient reason to outweigh it. Expecting to cause inconvenience or irritation that would be excessive in light of the anticipated benefits of the cyber operation, which presumably would be trifling, would smack of mere maliciousness. The United States Department of Defense commendably appears to have accepted this approach as a matter of policy.[80]

In terms of balancing humanitarian considerations with a State's conflict-related interests, the proposed policy adopts the rule of proportionality's excessiveness test. The *Harvard Manual on the International Law Applicable to Air and Missile Warfare*, prepared by a distinguished group of international law practitioners and scholars, took the reasonable position that excessiveness is characterized by a situation in which "there is a significant imbalance between the military advantage anticipated, on the one hand, and the expected collateral damage to civilians and civilian objects, on the other." [81] This standard accommodates IHL's foundational principle of military necessity. After all, it would be

[80] DoD Manual, *supra* note 10, para. 16.5.2 ("For example, even if a cyber operation is not an 'attack' or does not cause any injury or damage that would need to be considered under the principle of proportionality in conducting attacks, that cyber operation still should not be conducted in a way that unnecessarily causes inconvenience to civilians or neutral persons.").
[81] HARVARD MANUAL, *supra* note 78, at 92; N ILS MELZER, TARGETED KILLINGS IN INTERNATIONAL LAW 344 and 360 (2008).

impractical to apply a strict "51-49" balancing test with respect to two values – collateral damage and military advantage – that are so dissimilar, especially when the consequence of a slight perceived imbalance in favor of the former would be an absolute bar to striking a valid military objective. Sensitivity to this dynamic is also reflected in the Rome Statute's application of the proportionality rule only when expected collateral damage is "clearly" excessive to the anticipated "overall" military advantage.[82]

Given that the cyber operations encompassed by the policy include those directed against military objectives, albeit in situations that do not rise to the level of an attack, it would make no sense to lower the excessiveness bar. If a lower bar were to be suggested, States would harbour the same concern that animated the decision to adopt the excessiveness standard vis-à-vis proportionality. Indeed, the argument for a high threshold is actually stronger with respect to the policy because the harm, which is generally non-destructive and non-injurious, is of a less severe nature.

The term "concrete benefit related to the conflict" in the proposed policy must be distinguished from "concrete and direct military advantage" found in the rule of proportionality. All of the adjectives reflect the military necessity component of the balancing that I contend should inform every military decision affecting the civilian population. However, as will be explained, the deletion of the word direct is meant to broaden the scope of the policy beyond that which applies in the case of proportionality.

According to the ICRC *Commentary* to the Additional Protocols, "the expression 'concrete and direct' was intended to show that the advantage concerned should be substantial and relatively close, and that advantages which are hardly perceptible and those which would only appear in the long term should be disregarded."[83] The term was also explained in the unofficial, although authoritative (in light of the authors' participation in the Diplomatic Conference that produced the Additional Protocols) Bothe, Partsch and Solf commentary on the Protocol. It notes that "concrete" means "specific, not general; perceptible to the senses," and equated it to the term "definite" in the definition of military objective, which denotes an advantage that is not hypothetical or speculative.[84] By contrast, the authors explained "direct" as meaning "'without intervening condition of agency.'"[85]

There is no logical basis for holding that the benefits to be considered when applying the proposed policy need not be concrete. To suggest that speculative benefits related to the conflict would ever suffice to justify actual negative expected consequences for the civilian population would effectively be to ignore humanitarian considerations altogether. However, the same logic does not apply to the qualifier "direct." States would likely object to imposing the proportionality requirement of direct causal nexus between the operation and benefit that applies to cyber or other forms of attack. Consider the case of operations designed to undercut civilian support for involvement in the conflict. Such influence campaigns typically involve a chain of causation consisting of more than a single step. The information operation in question may be designed to shift civilian attitudes towards the government and to the conflict over time, perhaps by encouraging engagement by civil society or the media. As

---

[82] Rome Statute, *supra* note 13, art. 8(2)(b)(iv).

83. Additional Protocols Commentary, *supra* note 51, para. 2209.

84. Michael Bothe, Karl Josef Partsch & Waldemar A. Solf, NEW RULES FOR VICTIMS OF ARMED CONFLICTS: COMMENTARY ON THE TWO 1977 PROTOCOLS ADDITIONAL TO THE GENEVA CONVENTIONS OF 1949, at 407 (2d ed. 2013). *See also* United Kingdom Ministry of Defence, THE MANUAL OF THE LAW OF ARMED CONFLICT, para. 5.33.3 (2004).

[85] Bothe, Partsch & Solf, *supra* note 84, at 407.

long as there is a causal nexus that is not so attenuated that it becomes speculative, it would, under the proposal, be appropriate for consideration in the balancing process.

Precisely the same logic, albeit turned on its head, supports the limitation of negative effects for the civilian population to those that are concrete. To suggest a party to the conflict should have to forego an operation that would likely yield valid benefits related to the conflict on the basis of speculation as to possible negative effects on the civilian population would be to inappropriately skew the desired balance in the opposite direction.

The other significant difference between the proposed policy and the rule of proportionality is substitution of the term "military advantage" with the phrase "benefit related to the conflict." Military advantage is a concept that is narrowly construed in IHL. For instance, the *Harvard Manual* provides:

> Military advantage refers only to advantage which is directly related to military operations and does not refer to other forms of advantage which may in some way relate to the conflict more generally. Military advantage does not refer to advantage which is solely political, psychological, economic, financial, social, or moral in nature. Thus, forcing a change in the negotiating position of the enemy only by affecting civilian morale does not qualify as military advantage.[86]

The policy would not limit the advantage attained by cyber operations to that which is purely military. Taking the example cited above, it would be acceptable to consider conducting cyber operations intended to alter the enemy's negotiating position, even by affecting civilian morale. States already plan cyber operations not amounting to an attack, including those altering or deleting data, that have effects that are not strictly military. In light of the predictable resistance from them to imposing a standard that requires a military benefit, the proposal dispenses with the term military. [87]

It must be emphasized that advantage typically refers to an attacking party's military gain at the tactical or operational levels of war, but not at the strategic, in the sense of political, level. [88] In other words, the advantage must have an impact on the battlefield or the campaign in question that is not overly attenuated.[89] For example, the advantage of causing enemy military leaders to rethink involvement in the conflict, as in the case of attacks against their personal property or investments, would not qualify

---

[86] Harvard Manual *supra* note 78, at 36.

[87] As noted in the U.K. declaration on ratification of Additional Protocol I, "the military advantage anticipated from an attack is intended to refer to the advantage anticipated from the attack as a whole and not only from isolated or particular parts of the attack." UK Additional Protocol Ratification Statement, para. (i), available at http://www.icrc.org/applic/ihl/ihl.nsf/Notification.xsp?actionopenDocument&document Id0A9E03F0F2EE757CC1256402003FB6D2.

[88] "Tactical level of warfare — The level of warfare at which battles and engagements are planned and executed to achieve military objectives assigned to tactical units or task forces." U.S. Department of Defense, DICTIONARY OF MILITARY AND ASSOCIATED TERMS 226 (current as of March 2018); "Operational level of warfare — The level of warfare at which campaigns and major operations are planned, conducted, and sustained to achieve strategic objectives within theaters or other operational areas." *Id.* at 173; "Strategic level of warfare — The level of warfare at which a nation, often as a member of a group of nations, determines national or multinational (alliance or coalition) strategic security objectives and guidance, then develops and uses national resources to achieve those objectives." *Id.* at 219.

[89] UK Manual, *supra* note 84, para. 5.33.5; Harvard Manual, *supra* note 78, at 36-37; Tallinn Manual 2.0, *supra* note 6, at 442. See also Ian Henderson, THE CONTEMPORARY LAW OF TARGETING (Martinus Nijhoff Publishers 2009), at 199-202 (providing a more detailed discussion of why military advantage may be measured at the operational as opposed to the tactical level, and why measuring military advantage at the strategic level is generally not appropriate).

those targets as military objectives nor justify collateral damage to them when engaging in the proportionality analysis.

However, States do seek strategic level advantage that does not bear on battlefield operations and under IHL are permitted to conduct military operations falling short of an attack in order to attain it. Thus, to be palatable to States, the proposed policy permits concrete benefits at any level of war to be factored into the assessment of whether the cyber operation may be launched. By way of illustration, blocking the ability of the enemy to disseminate conflict-related propaganda to the population through denial of service operations against media facilities would qualify as a benefit to be weighed in the balance.

Despite this widening of scope relative to the proportionality rule's standard, the policy limits benefits to those regarding which a clear nexus to the conflict exists. Although doing so might spark allegations of being overly restrictive, the intent of the policy is to enhance protection against disruption of the civilian population during what is likely to already be a dreadful situation – armed conflict. Malicious or vindictive cyber operations directed at civilians or the civilian population should be prohibited.

The requirement must not be confused with application of the principle of military necessity. According to some interpretations of the principle, "only that degree and kind of force, not otherwise prohibited by the law of armed conflict, that is required in order to achieve the legitimate purpose of the conflict, namely the complete or partial submission of the enemy at the earliest possible moment with the minimum expenditure" is permitted. [90] Applying this principle would not suffice to address the problems at hand.

First, as set forth, the principle of military necessity only applies to a use of force; the proposed policy addresses cyber operations that are not easily described as such. Second, while it is addressed to necessity based on "military" considerations, the term "related to the armed conflict" in the policy is broader. Third, and most significantly, there is opposition to treating the principle of military necessity as a primary rule of international law that operates independently of other primary rules of international law. This issue was in part responsible for opposition to the *ICRC's Interpretive Guidance on the Notion of Direct Participation*, [91] and is viewed with suspicion by some in the field. [92] My own view is that military necessity is a foundational principle of international humanitarian law, but not a primary rule.[93] Whatever the correct interpretation, the principle of military necessity cannot accomplish the ends sought through adoption of the proposed policy.

---

[90] UK Manual, *supra* note 84, para. 2.2.

[91] Opposition to Chapter IX of the Interpretive Guidance, *supra* note 33, arose when some experts participating in the project objected to what they considered use of the principle as a primary rule of law. See, e.g., W. Hays Parks, *Part IX of the ICRC "Direct Participation in Hostilities" Study: No Mandate, No Expertise, and Legally Incorrect*, 42 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLITICS 769 (2010), at 802-810. But see the reply by Nils Melzer, then of the ICRC's legal division, who led the project. Nils Melzer, *Keeping the Balance between Military Necessity and Humanity: A Response to Four Critiques of the ICRC's Interpretive Guidance on the Notion of Direct Participation in Hostilities*, 42 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLITICS 831 (2010), at pp. 892-912.

[92] Interestingly, see DoD Manual, *supra* note 10, para. 16.5.2. (operations not qualifying as attacks nevertheless "must not be directed against enemy civilians or civilian objects unless the operations are militarily necessary."). This discussion has been criticized, and rightly so. William H. Boothby and Wolff Heintschel von Heinegg, THE LAW OF WAR: A DETAILED ASSESSMENT OF THE DEPARTMENT OF DEFENSE LAW OF WAR MANUAL (Cambridge U.P. 2018).

[93] Schmitt, Military Necessity, *supra* note 19.

Finally, like the rule of proportionality, the test proposed in the policy is applied *ex ante*, not *post factum*; the policy uses of the terms "anticipated" and "expected" drawn from the former. Thus, those applying the policy will be judged against the facts as they reasonably believed them to be at the time the cyber operation was planned, approved, and executed.

## IV. Concluding Reflections

The current state of the international humanitarian law governing cyber operations is not fully satisfactory. Lack of clarity as to which cyber operations qualify as an attack at best leaves civilians at risk when they otherwise should not be and at worst opens the door to States wishing to exploit the ambiguity in order to mount highly disruptive cyber operations against the civilian population. Moreover, some cyber operations that would clearly not qualify as an attack could nevertheless create chaos among the civilian population.

The issue of whether data is an object complicates this situation. On the one hand, if it is, many cyber operations presently conducted by States would be barred. Laudable though their intent may be, advocates of this view are naïve in believing the interpretation will prove acceptable to States that wield cyber capabilities.[94] But on the other hand, failing to treat some civilian data as a civilian object that benefits from IHL's protective umbrella undervalues the humanitarian considerations that underpin the prohibition on attacking civilian objects. In terms of finding an appropriate balance of humanitarian considerations and military necessity, arguments on both sides of the fence fall short.

The proposed policies are designed to address these realities. Initially, States may react negatively to them. This is often the reaction when academics and nongovernmental organizations seek to limit their discretion on the battlefield; in many such cases, that reaction is justified. However, in these cases, States should bear the following in mind.

First, in my discussion with cyber operators, it would appear that some elements of the policies already take the form of rules of engagement, other guidance or simply accepted practice. More importantly, Article 57(1) of Additional Protocol I requires parties to a conflict to take the possibility of negative consequences for the civilian population and/or civilian objects into consideration during military operations, including but not limited to attacks. I believe the requirement is reflective of customary IHL and groups of experts and military manuals confirm that this "constant care" provision is meant to impose an affirmative duty, albeit one that is general and poorly defined.[95] All the proposed policies do is provide some guidance as to measures to be taken in response to that assessment.

---

[94] Interesting work in this regard is being done by Lieutenant Colonel Bart van den Bosch (Netherlands Army) in a University of Amsterdam PhD ("Waging War Without Violence") under the direction of Professor Terry Gill and Brigadier General Paul Duchiene.

[95] *See* U.K. Manual *supra* note 11, para. 5.32.1 ("So 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."); Harvard Manual, *supra* note 10, at 142 ("'Constant care' means that there are no exceptions from the duty to seek to spare the civilian population, civilians and civilian objects."); TALLINN MANUAL 2.0, *supra* note 6, at 477 (noting the "broad general duty to 'respect' the civilian population, that is to consider deleterious effects of military operations on civilians"). Further, the Tallinn Manual 2.0 states, "the duty of constant care requires commanders and all others involved in the operations to be continuously sensitive to the effects of their activities on the civilian population and civilian objects, and to seek to avoid any unnecessary effects thereon." *Id.*

In this regard, it might be suggested that the work of the policies is already accomplished through application of the Martens Clause because the situations highlighted are ones that should be subject to the "laws of humanity" and the "dictates of the public conscience." Yet, States and experts disagree over the means by which the clause is to be implemented and whether it imposes specific binding rules of law on the parties to the conflict. Irrespective of where one stands on these issues, the Martens Clause is notable for its vagueness and its paucity of application in practice. This being so, the policies provide a degree of practical clarity and direction that can operate to provide actual protection to the civilian population.

Second, prohibiting attacks against cyber infrastructure or data that would interfere with essential civilian functions or services is consistent with the general premise that there are certain activities, functions and objects that deserve special protection from the harmful effects of warfare. The proposal merely acknowledges that the existing universe thereof should expand in response to the unique and sometimes severe risks for the civilian population that are associated with cyber operations. Moreover, the policy leaves it to States to determine which functions and services qualify as essential and are accordingly deserving of special protection, at least as a matter of policy.

Third, perceptive readers will have noticed that the second policy mandating balancing is more restrictive with respect to operations not qualifying as attacks against military objectives than those that qualify as attacks. The rule of proportionality applicable in cyber attacks only requires consideration of damage (including, presumably, loss of functionality), injury or death. By contrast, the proposed policy encompasses all negative effects on the civilian population. This might seem counterintuitive.

Nevertheless, the result is compensated for by the fact that the policy is more permissive in terms of what the party conducting the cyber operation may consider when balancing against those negative effects. The rule of proportionality is limited to concrete and direct military advantage. By contrast, the policy allows consideration of benefits that are neither direct nor military in character, and those benefits may accrue at the strategic level of warfare. Thus, the proposed policy achieves a fair balance between humanitarian considerations and the interest of the State. States can find further solace in the policy's adoption of the excessiveness standard. That standard affords parties to the conflict a significant margin of appreciation when applying the policy.

The proposals are not panaceas with respect non-destructive and non-injurious harm to the individual civilians or the civilian population from cyber operations. Much such harm would remain unaddressed, as in the case of application of the proportionality rule to cyber attacks, for that rule only applies to collateral damage, injury or death. Nevertheless, the time for States and international community to address humanitarian issues is always before they have manifested tragically on the battlefield. In this case, that time is now.