International Review of the Red Cross (2014), **96** (893), 189–206.
Scope of the law in armed conflict
doi:10.1017/S1816383114000381

INTERNATIONAL REVIEW of the Red Cross

Rewired warfare: rethinking the law of cyber attack

Michael N. Schmitt*
Michael N. Schmitt is Charles H. Stockton Professor and Director of the Stockton Center for the Study of International Law, United States Naval War College; Professor of Public International Law at Exeter University; and Senior Fellow at the NATO Cyber Defence Centre of Excellence.

Abstract
The most significant debate regarding the applicability of international humanitarian law to cyber operations involves interpretation of the rules governing cyber "attacks", as that term is understood in the law. For over a decade, the debate has been a binary one between advocates of the "permissive approach" developed by the author and a "restrictive approach" championed by those who saw the permissive approach as insufficiently protective of the civilian population and other protected persons and objects. In this article, the author analyses that debate, and explains a third approach developed during the Tallinn Manual project. He concludes by suggesting that the Tallinn Manual approach best approximates the contemporary law given the increasing value which societies are attributing to cyber activities.

Keywords: cyber attack, cyber operations, data, functionality test.

* The views expressed are those of the author in his personal capacity and do not necessarily represent those of any organization with which he is associated. Email: schmitt@aya.yale.edu.

© icrc 2014. This is a work of the U.S. Government and is not subject to copyright protection in the United States

Cyber operations are fast becoming a fixture of modern warfare.[1] They first appeared overtly in the 2008 international armed conflict between Georgia and Russia,[2] were employed during the international and non-international armed conflicts in Afghanistan and Iraq,[3] figured in operations throughout the non-international armed conflicts in Libya and Syria,[4] and most recently played a bit part during the 2014 international armed conflict between Russia and Ukraine.[5] The United States has established US Cyber Command to conduct defensive and offensive cyber operations during armed conflicts, and other States, most notably China, are following suit by acquiring cyber capabilities and developing their force structures to leverage them.[6] The spread of cyber wherewithal is not limited to the regular armed forces and other organs of the State. Non-State actors have discovered the utility of cyber operations as a means of asymmetrical warfare when facing a State's superior conventional forces.[7] Cyber operations have already become an integral facet of command, control, communications, computer, intelligence, surveillance, and reconnaissance activities in the battlespace, and it is inevitable that they will soon play a central role in "attacking" one's enemy.[8]

1 Lt Gen Richard P. Mills, speech, AFCEA TechNet Land Forces East Chapter Lunch, 21 August 2012, available at: www.slideshare.net/afcea/afcea- technet-land-forces-east-aberdeen-chapter-lunch-ltgen-richard-p-mills-usmc.

2 Enekin Tikk, Kadri Kaska and Liis Vihul, *International Cyber Incidents: Legal Considerations*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2010, pp. 66–90. The 2007 cyber operations directed at Estonia did not occur in the context of an armed conflict.

3 Shane Harris, "The Cyber War Plan", *National Journal Online*, 14 November 2009, available at: www.nationaljournal.com/member/magazine/the- cyberwar-plan-20091114; Raphael Satter, "Afghanistan Cyber Attack: Lt. Gen. Richard P. Mills Claims to Have Hacked the Enemy", *The World Post*, 24 August 2012, available at: www.huffingtonpost.com/2012/08/24/afghanistan-cyber-attack-richard-mills_n_1828083.html; John Markoff and Thom Shanker, "Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk", *New York Times*, 1 August 2009, available at: www.nytimes.com/2009/08/02/us/politics/02cyber.html.

4 See, e.g., Eric Schmitt and Yhom Shankar, "U.S. Debated Cyberwarfare in Attack Plan on Libya", *New York Times*, 17 October 2011, available at: www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html?hp; Ivan Watson, "Cyberwar Explodes in Syria", *CNN*, 22 November 2011, available at: www.cnn.com/2011/11/22/world/meast/syria-cyberwar/; Eva Galperin, Morgan Marquis-Boire and John Scott-Railton, "Quantum of Surveillance: Familiar Actors and Possible False Flags in Syrian Malware Campaign", Electronic Frontier Foundation, 2013, available at: www.eff.org/files/2013/12/28/quantum_of_surveillance4d.pdf.

5 Most of the reliable material is classified and cannot be cited. For some public discussion, see Jarno Limnell, "Why Hasn't Russia Unleashed a Cyber Attack on Ukraine?", *CBS News*, 2 July 2014, available at: www.cbsnews.com/news/why-hasnt-russia-unleashed-a-cyber-attack-on-ukraine/.

6 David E. Sanger, "U.S. Tries Candor to Assure China on Cyberattacks", *New York Times*, 6 April 2014, available at: www.nytimes.com/2014/04/07/world/us-tries-candor-to-assure-china-on-cyberattacks.html?_r=0.

7 Gregory J. Rattray and Jason Healey, "Non-State Actors and Cyber Conflict", in Kristan M. Lord and Travis Sharp (eds), *America's Cyber Future: Security and Prosperity in the Information Age*, June 2011, pp. 65–86, available at: www.cnas.org/files/documents/publications/CNAS_Cyber_Volume%20II_2.pdf; Kenneth Geers, "Pandemonium: Nation States, National Security, and the Internet", Tallinn Paper No. 1, 2014, available at: www.ccdcoe.org/publications/TP_Vol1No1_Geers.pdf.

8 See, generally, Chairman of the Joint Chiefs of Staff, Information Operations, Joint Publication 3–13, 27 November 2012; United States Air Force, Cyberspace Operations, Air Force Doctrine Document 3–12, 30 November 2011; United States Army, Cyber Electromagnetic Activities, Field Manual 3–38, February 2014.

This emergent reality begs the question of how to treat cyber operations in the context of international humanitarian law (IHL). This is an essential query not only from the perspective of persons and objects protected by IHL during armed conflict, but also from that of States, which are currently in the process of acquiring cyber capabilities, developing the tactics, techniques and procedures for their use, and crafting cyber-specific rules of engagement. Lying at the heart of the matter is a decade-old dispute over when cyber operations directed against protected persons and objects are prohibited. In particular, the debate circulates around the scope of the concept of "attack" under IHL, a normatively critical notion in light of the fact that most of the law regulating the conduct of hostilities is framed in terms of attacks.

The debate was engaged soon after the turn of the millennium. Two approaches emerged, one permissive (in the sense of allowing a wider range of cyber operations against the civilian population) and the other restrictive (restricting cyber operations as a matter of law). In order to qualify as an attack by the former, the cyber operation had to result in injury to persons or physical damage to objects. Accordingly, for instance, cyber operations directed at civilian cyber infrastructure that did not cause damage were not barred by the prohibition on attacking civilian objects because the operations did not qualify as an attack. By contrast, the latter extended the concept of attack, and prohibited operations more broadly, to cyber operations that caused certain harmful effects without necessarily resulting in injury or damage; no bright-line test was offered to identify prohibited cyber actions. I was the progenitor of the permissive approach, with my views best captured in a 2002 article in this journal entitled "Wired Warfare: Computer Network Attack and *Jus in Bello*".[9] My friend, and presently head of the Legal Division of the International Committee of the Red Cross (ICRC), Knut Dörmann, originated the restrictive approach. An early exposition of his position was set forth in the article "Applicability of the Additional Protocols to Computer Network Attack", published in the proceedings of a 2004 conference in Sweden that we both attended.[10]

The debate proved relatively static until the North Atlantic Treaty Organization (NATO) Cyber Defence Centre of Excellence in Tallinn, Estonia, launched a major project to examine the implications of cyber warfare under *jus ad bellum* and *jus in bello*, for which I served as director. Twenty distinguished international scholars and practitioners with extensive IHL expertise participated in their personal capacities (the "International Group of Experts"), supported by a team of cyber experts. The ICRC, NATO and US Cyber Command provided observers who participated fully in all deliberations. The result of that effort was

9 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.

10 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 2011, p. 139, Swedish National Defence College, 2005, reprinted at: www.icrc.org/eng/resources/documents/misc/68lg92.htm.

the publication of the *Tallinn Manual on the International Law Applicable to Cyber Warfare* in 2013.[11]

Importantly, the Tallinn Manual raised the prospect of a third approach to the issue at hand, one focusing on the functionality of an object that has been targeted by a cyber operation. In my view, the so-called "functionality test" appropriately addresses fair criticism that the permissive approach fails to adequately constrain the effects of cyber operations on the civilian population. At the same time, it adds a degree of clarity as to where the threshold of attack lies that is missing in the restrictive approach.

It must be cautioned that the issue has not been definitively resolved. As the project was under way, the ICRC published a position on the matter in its 2011 report to the 31st Conference of the Red Cross and Red Crescent, entitled *International Humanitarian Law and the Challenges of Contemporary Armed Conflict*.[12] An important recent article by an ICRC legal adviser, Cordula Droege, entitled "Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians", has further sharpened the dialogue.[13]

Swayed by the logic of Dörmann, Droege and the ICRC, although not necessarily their precise legal argumentation, and influenced by the sophisticated discussions that took place during the three years of the Tallinn Manual process, my thinking on the topic has evolved. It is therefore appropriate to "rewire" my original approach. I will begin by outlining the competing permissive and restrictive approaches that prevailed prior to publication of the Tallinn Manual. I will then describe the legal reasoning of the majority of the experts that participated in that project, and explain why I now find their functionality test persuasive. The article will conclude with my thoughts on how this issue may continue to evolve over time.

The permissive approach

Article 48 of the 1977 Additional Protocol I to the 1949 Geneva Conventions (AP I)[14] sets forth the principle of distinction:

> In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects

11 Michael N. Schmitt (gen. ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Cambridge, 2013 (Tallinn Manual).

12 ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, official working document of the 31st International Conference of the Red Cross and Red Crescent, 28 November–1 December 2011, Doc. 31IC/11/5.1.2, pp. 36–38.

13 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, pp. 533–578.

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

> and military objectives and accordingly shall direct their operations only against military objectives.

Distinction, which has been labelled a "cardinal" principle of IHL by the International Court of Justice,[15] is universally acknowledged as a norm of customary law binding on all States during both international and non-international armed conflicts. This is the case regardless of their being parties to AP I.[16]

Textually, it might appear that the provision prohibits any *operation* conducted by the armed forces against civilians and civilian objects. However, State practice, including by States party to AP I, demonstrates that such an interpretation is overbroad. For instance, psychological and civil-military operations intended to influence the civilian population are key elements of contemporary military campaigns, especially during counter-insurgency conflicts such as those that have taken place, and continue, in Afghanistan and Iraq.[17] Although military operations, they are not prohibited under IHL because, as we shall see, they do not qualify as "attacks".

In "Wired Warfare", I argued that Article 48 reflects a general principle of IHL that is operationalized in a number of specific IHL rules. Most notable among these are Article 51(2) ("the civilian population as such, as well as individual civilians, shall not be the object of attack") and Article 52(1) ("civilian objects shall not be the object of attack"). These two rules suggest that the essence of Article 48 is a prohibition on *attacking* civilians and civilian objects, not on targeting them in a manner that does not qualify as (or is not integrally related to) an attack. Repeated reference to attacks throughout the subsequent rules supports this interpretation. For instance, although Article 51(1) provides that "[t]he civilian population and individual civilians shall enjoy general protection against dangers arising from military operations", it goes on to explain that "[t]o give effect to this protection, the following rules … shall be observed in all circumstances." Each of the "following rules" in the article refers to attacks – indiscriminate attacks are forbidden,[18] attacks must comply with the rule of proportionality,[19] and reprisal attacks are outlawed.[20] Similarly, Article 57(1) provides that "in the conduct of military operations, constant care shall be taken to spare the civilian population, civilians, and civilian objects." Despite the

15 International Court of Justice, *Military and Paramilitary Activities in and against Nicaragua* (*Nicaragua* v. *United States of America*), Judgment, *ICJ Reports 1986*, para. 78.

16 ICRC, *Customary International Humanitarian Law,* Vol. 1: *Rules*, Jean-Marie Henckaerts and Louise Doswald-Beck (eds), Cambridge University Press, Cambridge, 2005, Rule 1.

17 According to NATO, "in complex political and social contexts where the will of the indigenous population becomes the metaphorical vital ground (i.e. it must be retained or controlled for success), there is a requirement to influence and shape perceptions through the judicious fusion of both physical and psychological means". Allied Joint Doctrine, AJP-01(D), December 2010, pp. 2–10. See also, generally, NATO, Allied Joint Doctrine for Civil-Military Cooperation, AJP-3.4.9, February 2013; Allied Joint Doctrine for Psychological Operations, AJP-3.10.1(A), October 2007.

18 AP I, Art. 51(4).

19 *Ibid*., Art. 51(5)(b).

20 *Ibid*., Art. 51(6).

chapeau reference to operations, the article sets forth its various requirements in terms of attacks. Other AP I articles relevant to targeting also typically frame their operative provisions in the context of attack. Thus "attacks shall be limited strictly to military objectives",[21] reprisal attacks against the natural environment are prohibited,[22] works or installations containing dangerous forces may not be attacked except under specified circumstances,[23] precautions against the effects of attack should be taken,[24] non-defended locations may not be made the object of attack,[25] and so on.

The repeated reference to attacks begs the question of how these prohibitions and restrictions relate to cyber operations. AP I defines attacks in Article 49(1): "'Attacks' means acts of violence against the adversary, whether in offence or defence."[26] Similarly, the ICRC Commentary to Article 48 explains the reference to operations in terms of violence:

> The word "operations" should be understood in the context of the whole of the Section; it refers to military operations during which violence is used, and not to ideological, political or religious campaigns. For reasons which have nothing to do with the discussions in the Diplomatic Conference, the adjective "military" was not used with the term "operations", but this is certainly how the word should be understood. According to the dictionary, "military operations" refers to all movements and acts related to hostilities that are undertaken by armed forces.[27]

Although clear with respect to classic kinetic operations, Article 48's plain text and the Commentary's reference to the use of violence might seem problematic when applied to cyber operations since they are not violent *per se*. However, there appears to be widespread agreement that the matter is resolved by looking to the object and purpose of the various attack rules, especially Article 48.[28] State practice demonstrates that the article was designed to encompass acts having violent *consequences*, in addition to those that are violent in the kinetic sense. For instance, States have always treated chemical or biological operations, which had already occurred before the drafting of AP I, as attacks, even though they release no kinetic force.

Critics of the permissive approach sometimes cite the final sentence of the Commentary set forth above.[29] They also point to Article 51's Commentary, which

21 *Ibid*., Art. 52(2).
22 *Ibid*.
23 *Ibid*., Art. 56(1).
24 *Ibid*., Arts 57 and 58.
25 *Ibid*., Art. 59.
26 The term "attack" in IHL must be distinguished from "armed attack" in the *jus ad bellum*. The latter term refers to the condition precedent for the exercise of self- (or collective) defence pursuant to Article 51 of the UN Charter and customary international law.
27 Yves Sandoz, Christophe Swinarski and Bruno Zimmerman (eds), *Commentary on the Additional Protocols*, ICRC, Geneva, 1987, para. 1875.
28 Vienna Convention on the Law of Treaties, 23 May 1969, 1155 UNTS 331 (entered into force 27 January 1980), Art. 31(1).
29 C. Droege, above note 13, p. 556.

describes military operations as "all the movements and activities carried out by the armed forces related to hostilities",[30] and the Commentary on Article 57, which explains that military operations "should be understood to mean any movements, manoeuvres and other activities whatsoever carried out by the armed forces with a view to combat".[31] Doing so ignores the opening sentence of the quoted paragraph, which unambiguously notes that the relevant section of AP I deals with operations during which violence is used, as well as the fact that the Commentary to Article 51 contains a footnote referring back to Article 48's Commentary, and thus incorporates the condition of violence by reference.[32] And, of course, the term "combat" in the Article 57 Commentary is self-explanatory.

The ineluctable conclusion is that the prohibitions and restrictions set forth in the relevant provisions of AP I generally apply to targeting operations that qualify as attacks and that attacks are acts that have violent consequences. I therefore concluded in "Wired Warfare":

> It is clear that what the relevant provisions hope to accomplish is shielding protected individuals from injury or death and protected objects from damage or destruction. … Significant human physical or mental suffering is logically included in the concept of injury; permanent loss of assets, for instance money, stock, etc., directly transferable into tangible property likewise constitutes damage or destruction. The point is that inconvenience, harassment or mere diminishment in quality of life does not suffice; human suffering is the requisite criterion.[33]

The text of various articles in AP I supports the focus on damage, destruction, injury and death. In particular, Article 51 notes that the "civilian population and individual civilians enjoy general protection against *dangers* arising from military operations" and prohibits "acts or threats of *violence* the primary purpose of which is to spread terror among the civilian population".[34] The environmental provisions refer to *damage* being widespread, long-term and severe,[35] whereas the article addressing restrictions on attacking dams, dykes and nuclear electrical generating stations speaks of "*losses* among the civilian population".[36] Most importantly, the rule of proportionality is framed in terms of "*loss* of civilian life, *injury* to civilians, *damage* to civilian objects, or a combination thereof".[37] Since this rule lies at the heart of targeting, it is difficult to convincingly extend the notion of attack beyond the types of harm specified therein. After all, it would be incongruent to suggest, on the one hand, that a cyber operation against civilian cyber infrastructure that did not cause loss, injury or damage constituted a prohibited

30 Y. Sandoz *et al.*, above note 27, para. 1936.
31 *Ibid.*, para. 2191.
32 *Ibid.*, para. 1936, footnote 8.
33 M. Schmitt, above note 9, p. 337.
34 AP I, Arts 51(1) and 51(2) (emphasis added).
35 *Ibid.*, Arts 35(3) and 55(1).
36 *Ibid.*, Art. 56(1) (emphasis added).
37 *Ibid.*, Arts 51(5(b), 57(2)(a)(iii) and 57(2)(b) (emphasis added).

attack, but, on the other, that the same harm caused incidentally to the same infrastructure during a cyber attack on a military objective need not be considered in the proportionality analysis.

The implications of the permissive approach must be grasped. Cyber operations directed against civilians, civilian objects and other protected persons and objects do not violate IHL prohibitions or restrictions framed in terms of attacks unless they result in death, injury, physical damage or destruction. But, as I noted in 2002, "the advent of [computer network attack] reveals a normative lacuna that, unless filled, will inevitably result in an expansion of war's impact on the civilian population".[38] The restrictive approach championed by Dörmann responded to this concern.

The restrictive approach

At the 2004 conference in Sweden, Knut Dörmann set forth an alternative, more restrictive approach to the issue of how IHL governs cyber targeting. Although we generally came to similar conclusions regarding cyber operations during armed conflicts,[39] we differed on the matter of whether physical consequences are conditions precedent to activation of the prohibitions and restrictions on targeting.[40] Our two competing approaches would shape the debate for over a decade.

Dörmann pointed to the definition of military objectives as demonstrating the flaw in the permissive approach I was advocating.

> The fact that CNA [computer network attack] does not lead to the destruction of the object attacked is irrelevant. In accordance with Art. 52 (2) of AP I only those objects, which make an effective contribution to military action and whose total or partial destruction, capture or neutralization offers a definite military advantage, may be attacked. By referring not only to destruction or capture of the object but also to its neutralization the definition implies that it is irrelevant whether an object is disabled through destruction or in any other way.[41]

In 2011, the ICRC affirmed this position in its report to the 31st International Conference of the Red Cross and Red Crescent, asserting that:

> It is sometimes claimed that cyber operations do not fall within the definition of "attack" as long as they do not result in physical destruction or when its effects

38 M. Schmitt, above note 9, p. 379.

39 We agreed, for example, that cyber operations are fully subject to IHL, in particular the principle of distinction and its various derivative rules such as the prohibition on attacking people other than combatants, civilians directly participating in hostilities, and military objectives.

40 On this issue, see also Nils Melzer, "Cyberwarfare and International Law", UNIDIR Resources Paper, 2011, p. 27, available at: www.unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf; Heather Harrison-Diniss, *Cyber Warfare and the Laws of War*, Cambridge University Press, Cambridge, 2012, pp. 196–202.

41 K. Dörmann, above note 10, p. 6.

> are reversible. If this claim implies that an attack against a civilian object may be considered lawful in such cases, it is unfounded under existing law in the view of the ICRC. Under IHL, attacks may only be directed at military objectives, while objects not falling within that definition are civilian and may not be attacked. The definition of military objectives is not dependent on the method of warfare used and must be applied to both kinetic and non-kinetic means; the fact that a cyber operation does not lead to the destruction of an attacked object is also irrelevant. Pursuant to article 52 (2) of Additional Protocol I, only objects that make an effective contribution to military action and whose total or partial destruction, capture or neutralization offers a definite military advantage, may be attacked. By referring not only to destruction or capture of the object but also to its neutralization the definition implies that it is immaterial whether an object is disabled through destruction or in any other way.[42]

I have become increasingly sympathetic to the concerns expressed by Dörmann and reflected in the ICRC report. That said, the legal logic underpinning the restrictive approach remains elusive for me. The concept of attack does not rely in any way on the definition of military objectives. On the contrary, directing injurious or harmful operations against civilians, civilian objects and other protected persons or objects is no less an attack than directing the same operations against combatants, civilians directly participating in hostilities, or military objectives. It is only once an operation qualifies as an attack (or even a "military operation" for those taking the restrictive approach) that the issue of whether the target is a military objective arises. For example, military forces often conduct intelligence, surveillance and reconnaissance (ISR) operations against both civilian and military activities – the former to develop pattern of life assessments that will facilitate compliance with the proportionality rule and the requirement to take precautions in attack, the latter in order to gather information to effectively strike the target. The question of whether the ISR is directed at a military objective is irrelevant since the operation does not qualify as one to which attack restrictions or prohibitions apply.

Cordula Droege has responded to this analysis. She argues that:

> This criticism fails to acknowledge that "neutralization" was meant to encompass "an attack for the purpose of denying the use of an object to the enemy without necessarily destroying it". This shows that the drafters had in mind not only attacks that are aimed at destroying or damaging objects, but also attacks for the purpose of denying the use of an object to the enemy without necessarily destroying it. So, for instance, an enemy's air defence system could be neutralized through a cyber operation for a certain duration by interfering with its computer system but without necessarily destroying or damaging its physical infrastructure.[43]

42 ICRC, above note 12, p. 37.
43 C. Droege, above note 13, p. 558.

The ICRC Commentary to Article 52(2) unfortunately sheds no light on the meaning of the term "neutralization". Moreover, Droege's reference to the extract concerning the drafter's intent, drawn from the unofficial commentary by Bothe *et al.*,[44] misconstrues the concept of neutralization, a common one in military tactics. Most military operations are designed to generate particular "effects"; indeed, today, "effects-based operations" are the norm.[45] The reference to neutralization must be evaluated from this perspective.[46]

To illustrate, if the effect sought is to "neutralize" an enemy airfield, one need not attack the entire airfield or, indeed, attack the airfield at all. It might be sufficient to attack a taxiway or off-base POL (petroleum, oil, lubricants) storage facility to neutralize the airfield and its operations. Similarly, one can destroy cyber infrastructure in order to neutralize enemy command, control and communications (C3) facilities without attacking the C3 facility itself. The point is that in military parlance, the term "neutralize" has never been an antonym for physical damage. On the contrary, "neutralization fire" is a term of art that refers to "[f]ire which is delivered to render the target ineffective".[47] Moreover, in light of the military technology available at the time the Additional Protocols were negotiated, which only included first-generation electronic warfare equipment and not cyber systems, it is unlikely that the drafters were contemplating non-kinetic operations when referring to neutralization, rather than its classic military meaning.

Although the neutralization argument is counter-factual, the result it achieves better approximates what I believe has become the prevailing understanding of the concept of attack in the cyber context. Since my initial "Wired Warfare" analysis was designed to capture the *lex lata* and not the *lex ferenda*, my position demands "rewiring". The interpretive journey commenced during the Tallinn Manual process.

The Tallinn Manual deliberations

Among the areas with which the International Group of Experts struggled during the Tallinn Manual project was the application of targeting rules under IHL to cyber operations. The binary debate described above loomed large throughout the

44 Michael Bothe, Karl Josef Partsch and Waldemar A. Solf, *New Rules for Victims of Armed Conflicts: Commentary to the Two 1977 Protocols Additional to the Geneva Conventions of 1949*, Martinus Nijhoff, Dordrecht, 1982, p. 325.

45 "Targeting systematically analyzes and prioritizes targets and matches appropriate lethal and nonlethal actions to those targets to create specific desired effects that achieve the JFC's objectives, accounting for operational requirements, capabilities, and the results of previous assessments." US Chairman, Joint Chiefs of Staff, Joint Publication 3–60, Joint Targeting, January 2013, Appendix A at p. I-5 ("JP 3-60").

46 For instance, US Joint Doctrine provides that "[t]he CONOPS [concept of operations] provides more detail on what and where *fires* effects are desired by phase (e.g., deny, disrupt, delay, suppress, neutralize, destroy, corrupt, usurp, or influence)": *ibid.*, p. I-10 (emphasis added).

47 US Chairman, Joint Chiefs of Staff, Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms (as amended through April 2012), p. 226. "Fires" is defined as "[t]he use of weapon systems to create specific lethal or non-lethal effects on a target": *ibid.*, p. 119.

proceedings. Eventually, the experts agreed on Rule 30: "A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[48] The rule does not necessarily exclude cyber operations that do not manifest in injury or physical damage from the ambit of attack. Rather, since the rules required unanimity, Rule 30 represented a least common denominator upon which all the experts could agree.[49]

The notion of "attack"

A major breakthrough in the dialogue occurred in the project's final year with the development of what has become known as the "functionality test". Although a few supporters of the permissive approach remained firmly entrenched, the majority of the International Group of Experts eventually agreed that the concept of "cyber attacks" should not be limited to injurious or physically damaging operations. For them, a cyber operation that interfered with the functionality of cyber infrastructure such that it was, in a sense, "broken" would also qualify as damaging.[50] This was crucial, considering the relationship between the reference to damage in the rule of proportionality and the definition of attack: an operation that "damages" an object is logically an attack. I believe this new approach accurately reflects the current state of the law for reasons that I will set forth in the next section.

There were differences of opinion among the experts as to what qualified as interference with functionality. Some members took the position that "interference with functionality qualifies as damage if restoration of functionality requires replacement of physical components".[51] Others included simple reinstallation of the operating system in the notion of repair, while a few argued that "interference with functionality that necessitates data restoration, while not requiring physical replacement of components or reinstallation of the operating system, qualifies as an attack".[52]

A common factor among all these positions is that the object in question is unusable for its intended purpose, at least until some form of repair is undertaken. During their deliberations, the experts discussed the treatment of cyber operations that do not cause physical or functionality damage, but which result in particularly detrimental consequences for the civilian population. These would typically involve denial (and distributed denial) of service operations that interfere with the use of a system without affecting the system itself. An example cited in the Tallinn Manual commentary is "blocking email communications throughout the country (as distinct

48 Tallinn Manual, above note 11, p. 106.
49 Similarly, the experts participating in the HPCR AMW Manual could not achieve consensus on this point. Harvard Program on Humanitarian Policy and Conflict Research, *Manual on International Law Applicable to Air and Missile Warfare*, Cambridge University Press, Cambridge, 2013, pp. 12–13 and 20–21.
50 Tallinn Manual, above note 11, commentary accompanying Rule 30, para. 10.
51 *Ibid.*, commentary accompanying Rule 30, para. 10.
52 *Ibid.*, commentary accompanying Rule 30, para. 11.

from damaging the system on which transmission relies)".[53] Most of the experts agreed that while "there might be logic in characterizing such activities as an attack, the law of armed conflict does not presently extend this far".[54]

Interpreting data as an "object" under IHL

A related issue that surfaced during the Tallinn Manual deliberations involved the treatment of data, and more specifically, the question of whether it qualifies as an "object" in IHL terms. If it does, then cyber operations that destroy or alter data are attacks, and those directed against civilian and other protected data are unlawful. Of course, if an attack on data directly causes injury to individuals (as in alteration of data in a water treatment plant that causes illness) or damages objects (as with manipulation of air traffic data that causes aircraft to crash), the operation is an attack. Similarly, destruction or alteration of data that causes a loss of functionality may also qualify as an attack. But is an operation targeting data an attack irrespective of the physical or functional consequence?

The majority of the International Group of Experts were unwilling to extend the concept of "object" to data as such. These experts found the ICRC Commentary on Article 52 – the prohibition on attacking civilian objects – to be particularly persuasive:

> 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.[55]

They concluded that since data is neither tangible nor visible, it is not an object benefiting directly from the various IHL protections that certain objects enjoy.[56]

Moreover, the majority also took notice of Article 31(1) of the Vienna Convention on the Law of Treaties, which provides that "[a] treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose".[57] In the view of these experts, the ordinary meaning of object does not include data. For example, the Merriam-Webster dictionary defines an object as "something material that may be perceived by the senses".[58] Data is unperceivable by any of the senses.

53 *Ibid*., commentary accompanying Rule 30, para. 12.
54 *Ibid*., commentary accompanying Rule 30, para. 12.
55 Y. Sandoz *et al*., above note 27, paras. 2007–2008.
56 Tallinn Manual, above note 11, commentary accompanying Rule 38, para. 5.
57 Vienna Convention, above note 28, Art. 31(1).
58 "Object", *Merriam-Webster Dictionary*, available at: www.merriam-webster.com/dictionary/object.

Some experts nevertheless took the contrary position that data *per se* is to be treated as an object, such that it would be prohibited to direct cyber operations against it absent its qualification as a military objective. They argued that

> failure to do so would mean that even the deletion of extremely valuable and important civilian datasets would potentially escape the regulatory reach of the law of armed conflict, thereby contradicting the customary premise of that law that the civilian population shall enjoy general protection from the effects of hostilities, as reflected in Article 48 of Additional Protocol I.[59]

Most, however, rejected this argument as reflecting *lex ferenda*, not *lex lata*.

Wired warfare rewired

The functionality test developed during the Tallinn Manual project comports with contemporary understandings of how IHL governs targeting in cyberspace. In this regard, it must be emphasized that IHL represents a delicate balancing act between two competing interests: military necessity and humanitarian concerns.[60] The former reflects the interest of States in being able to fight effectively during armed conflicts, unhampered by excessive legal strictures. The latter signals the interest of States in protecting their citizenry from harm, minimizing harm to their soldiers and, for some, pursuing worthy moral ends. The paradigmatic example is the rule of proportionality, which permits incidentally harming or even killing innocent civilians in order to achieve a worthy military goal, so long as the attack in question is not expected to result in excessive incidental civilian harm.[61]

When the military necessity–humanitarian considerations balance changes, a corresponding evolution in the law can be expected. To illustrate, attacks using common World War II-era bombs and aircraft would be deemed indiscriminate today because of advances in precision warfare. Given these advances, the military utility of the outdated weapons has plummeted, while increased colocation of civilians, civilian objects and military objectives has heightened humanitarian concerns. As a result, the balance has shifted such that contemporary application of the IHL rule prohibiting indiscriminate attack demands far greater precision than was previously the case.[62]

In an ever more "wired" world, the societal value attributed to activities in cyberspace is constantly rising. At the same time, the wired and networked nature of modern militaries makes it ever more important to preserve the legal manoeuvre room necessary to conduct militarily important cyber operations. These trends will influence how States perform the military necessity–humanitarian concerns

59 Tallinn Manual, above note 11, commentary accompanying Rule 38, para. 5.
60 My views on the operation of this balance are set forth in 10 Michael N. Schmitt, "Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance", *Virginia Journal of International Law*, Vol. 50, 2010, p. 795.
61 AP I, Arts 51(5(b), 57(2)(a)(iii) and 57(2)(b).
62 *Ibid*., Art. 51(4)(a).

balancing act as they interpret and apply IHL norms vis-à-vis cyber operations. One thing is certain: the strict permissive approach no longer comports with the contemporary significance of cyber systems and activities.

The resulting shift will be subtle, but certain. It will progressively, albeit cautiously, afford greater protection to civilian cyber activities than would the strict injury, death, damage or destruction test that I had previously maintained. However, in terms of the legal rationale for this evolutionary progression, I remain unconvinced by arguments based on a nuanced reference to the term "neutralization" in the definition of military objectives. Such an interpretation deviates from traditional military usage of the term. At the operational level, the argument also runs counter to how the military thinks about targeting by placing, if you will, the cart (military objective) before the horse (attack). And theoretically, it makes little sense to define an act by reference to the entities that are protected against it.

I am nevertheless now persuaded by the foundational premise of the restrictive approach – that is, that the notion of cyber attacks cannot be limited to injurious or physically destructive cyber operations. My rationale is that States are no longer likely to adopt this rigid position. The legal basis for my revised interpretation of the law focuses on the rule of proportionality and its sharp articulation of the genre of harm against which the civilian population is protected. If civilians and civilian objects are protected against *incidental* consequences of a specified nature, they (and other protected persons and objects) must equally enjoy protection against an operation *directed* at them causing the same consequences. This being so, an attack is an operation that causes, borrowing from the text of the proportionality rule, loss of life, injury or damage.

The key is the contemporary understanding of damage. IHL has traditionally been framed in terms of physical damage, for that is the type of harm typically associated with warfare and the kinetic weaponry used to conduct it. Only limited means and methods were available for disabling systems and equipment non-kinetically. This explains the various AP I and AP Commentary references to danger, violence, combat and hostilities cited above. War was about physical destruction.

That reality has changed dramatically. In contemporary warfare, systems and equipment, whether civilian or military, can be more susceptible to being rendered inoperative by cyber than kinetic means. For instance, it may be impossible to target an object kinetically because it is hardened, difficult to locate, or situated in the proximity of civilians or civilian objects such that there is a risk of violating the rule of proportionality. Yet, depending on the circumstances, such factors may be no hindrance to cyber operations. Moreover, for the military and for civilians, it makes little difference whether a computer system or an object relying on computers fails to function because it is disabled kinetically or non-kinetically. It simply does not work. In the cyber context, therefore, the logic underpinning the requirement for injury or physical damage breaks down.

The functionality test elegantly addresses this new perspective in a way that does not exacerbate State concerns about overly restrictive norms that fail to

acknowledge the military advantage component of IHL's balancing act. It shifts attention away from the means of achieving an effect (physical damage/injury) to the effect itself (taking a targeted system out of play). After all, it is not the fact that an object is physically damaged that matters, but rather the fact that it is no longer completely suitable for its intended purpose. This is so regardless of whether one is a military commander attacking an enemy military objective or a civilian that relies on the object.

Of course, the civilian consequences of an attack were always what mattered; IHL is generally anthropocentric. The prohibition on attacking a civilian residence, for example, exists not because of the intrinsic value of the residence, but rather to protect its utility. In the past, the means of threatening that utility were kinetic and thus expressed in kinetic terms. Now that it is possible to threaten utility non-kinetically, it makes sense to reinterpret damage as the loss of functionality that permanently renders the object inoperable or that necessitates some form of repair.

As noted above, members of the International Group of Experts who supported the functionality test differed over the extent of repair necessary to qualify as a loss of functionality. The continuum ranged from physical replacement of components to reloading data. In my own view, the loss of functionality would include situations requiring reloading of the operating system or any software essential to operation, but would not include replacing data that was merely stored on the system.

Because reinterpretation is usually evolutionary, not revolutionary, I believe States would presently be uncomfortable extending the notion of damage to operations that temporarily interfere with functioning but require no repair or other remedial action, as in a distributed denial of service (DDoS) operation. Such operations are more akin to communications jamming, which is not an attack as a matter of law unless it results in harm qualifying as damage or injury. This is, obviously, a somewhat circular analysis. However, States make, interpret and apply IHL, and there appears to be no appetite for extending the concept of damage this far.[63]

The importance of the "functionality test" cannot be overestimated. To the extent that it accurately reflects the contemporary *lex lata*, a proposition by no means settled, it establishes substantial common ground between the permissive and restrictive approaches. The grace of the test is that it extends humanitarian protection well beyond the permissive approach without sacrificing meaningful military advantage. Thus, it plays well to the military advantage–humanitarian considerations balance that permeates IHL.

63 Cordula Droege has usefully cited certain activities, the cyber equivalent of which would not be considered attacks. These include espionage, dissemination of propaganda, non-physical psychological and economic warfare, and embargoes. See C. Droege, above note 13, p. 559. While I agree with her on every count, the question remains of how to articulate a norm of general applicability that does not rely on individual *ad hoc* determinations.

The road ahead

This is an area of the law that will remain in flux for some time. The vector of evolutionary reinterpretation of extant norms is likely to be in the direction of greater protection of civilian cyber activities. As societies become ever more dependent on cyberspace, humanitarian considerations will loom larger in the balance, thereby increasingly offsetting military necessity factors. For instance, it is by no means certain that a decade from now the functionality test will be limited to permanent disablement or system incapacitation requiring repair. The argument that it makes no difference whether a cyber operation disables a system in a manner requiring repairs taking one day or simply shuts that system down for the same period is compelling. Along the same lines, why should targeting cyber infrastructure in a way that necessitates a day's repairs qualify as an attack, but not a DDoS operation against the same system that takes it offline for a week?

Similarly, the unwillingness to treat data as an object because it is not tangible, which I believe presently reflects *lex lata*, is unlikely to survive for long. Loss of data can produce effects that are far more deleterious than kinetic attack. For instance, altering financial system data in a manner that undercuts confidence in a nation's economic system is more detrimental to the civilian population than a kinetic attack on a single bank. It will prove increasingly difficult in cyber-reliant societies to maintain a normative distinction between harm caused to physical objects and that caused to data.

The question remains as to how the evolution towards greater protection for civilian cyber activities will unfold. One possibility is a shift in interpretive emphasis from nature to severity of harm. In the past, nature generally served as effective cognitive shorthand for severity. For instance, the rule of proportionality's reference to death, injury and damage made sense because harm of that nature was typically more severe than, say, inconvenience or disruption; congruity between the severity of consequences and the nature of harm set forth in the rule existed in most cases. Precisely the same result attended the definition of attack's reference to acts of "violence".

Yet, as the aforementioned examples illustrate, cyber operations disrupt that congruency dramatically. Therefore, a trend in interpretation that plays directly to the core concern of the severity of consequences, rather than their nature, when defining attack and applying the rule of proportionality and requirement to take precautions in attack should be expected. The reinterpretation of damage by the Tallinn Manual experts to include significant interference with functionality is illustrative. A similar reinterpretation might extend the notion of "injury" to actions that dramatically disrupt daily life for civilians, or of "violence" to include the same disruptive effect. Even the mere denial of some services could, in theory, eventually be characterized as damage. Of course, these prospects raise difficult questions. Would denial of service operations that, for instance, merely cause inconvenience or irritation be excluded? How would the threshold be expressed and how would legal logic justify a distinction between lawful and unlawful denial of service attacks?

An alternative approach might be to expand the scope of protected persons, objects or activities. As suggested, the obvious candidate for reinterpretation is the notion of "object" with respect to data, although this possibility begs the question of how to avoid making the interpretation overbroad. Should such a reinterpretation occur, it would raise anew the question of "damage". Would data have to be destroyed, as in erased? Would it suffice to alter the data or even to simply make it inaccessible?

The scope of protected objects could also be expanded through reinterpretation of the "use" criterion in the definition of military objectives. Presently, the use of civilian objects, however slight, renders them military objectives.[64] When this transformation occurs, any residual protection enjoyed by the object (for example, because it can be subdivided into distinct civilian and military components) and nearby civilian objects resides in the rule of proportionality and the requirement to take precautions in attack.

Yet the criterion of "use" is problematic in the cyber context because so much civilian cyber infrastructure also serves military purposes. To accommodate this situation, "use" could be reinterpreted through State practice to require, for example, "substantial" or "predominant" military use, such that cyber operations directed at cyber infrastructure that was only marginally utilized for military purposes would not be lawful. Of course, the same practical result with regard to dual-use cyber infrastructure might be obtained if non-physical effects counted as "damage" for the purpose of the proportionality rule and requirement to take precautions in attack.

A final possibility is the provision of special protection to particular cyber infrastructure, such as that associated with, for the lack of an accepted term, "essential civilian functions". In fact, protection could also be extended to those functions directly. As an illustration, special protection for cyber infrastructure and functions could be crafted analogously to that presently existing for objects indispensable to the civilian population or for civil defence activities.[65] Doing so would likely require adoption of new treaty law in the form of, for example, a further additional protocol to the Geneva Conventions. Since the path to conduct of hostilities treaty law is usually an arduous one, reinterpretation of existing law to accord with the emergence of cyber operations is far more likely.

Concluding remarks

It has become fashionable to bemoan the inadequacy of IHL in the face of novel technologies. Such criticism undersells the law's inherent flexibility and vitality. In fact, after an initial shock to the system, IHL, including the interpretation thereof, tends to respond rather comfortably to new weapon systems.

64 See discussion at Tallinn Manual, above note 11, Rule 39 and accompanying commentary.
65 AP I, Arts 54 and 61–67.

This has been the case with cyber operations. Those early participants in the examination of IHL's application to cyber operations who argued that the law applied fully, such as Knut Dörmann and myself, have prevailed. Very few pundits, and no serious ones, continue to claim the inapplicability of IHL to this form of warfare. The next hurdle is determining *how* it applies. The differences between the two points of view that surfaced early on regarding the notion of cyber operations (and attack) have, over the ensuing decade, slowly but unremittingly narrowed. That trend is certain to continue as further State practice and *opinio juris* exposes common ground.

There are, accordingly, grounds for optimism. Cyber operations do not exist in a normative void and do not constitute a method of warfare that is so fundamentally different that it renders application of the law forbiddingly complex, and the international legal community is actively engaged in searching for common ground on IHL's application to cyber operations. The trick will be to remain objective and open-minded about how best to balance military necessity and humanitarian considerations with respect to this new form of warfare.