2012 4th International Conference on Cyber Conflict
C. Czosseck, R. Ottis, K. Ziolkowski (Eds.)
2012 © NATO CCD COE Publications, Tallinn

"Attack" as a Term of Art in International Law: The Cyber Operations Context

Michael N. Schmitt
International Law Department
United States Naval War College
Newport, U.S.A.
schmitt@aya.yale.edu

Abstract: This article examines the meanings of "attack" in international law. It points out that the term is used in two distinct bodies of that law. First, the term "armed attack" appears in the *jus ad bellum*, which governs when a State may resort to force as an instrument of its national policy. In that context, it serves as a condition precedent to the resort to force in self-defence pursuant to Article 51 of the UN Charter and customary international law. Second, in the *jus in bello* attack refers to a particular type of military operation to which various prohibitions and restrictions apply. The *jus in bello*, or international humanitarian law, establishes rules as to how operations may be conducted during an armed conflict. The article examines and analyses these usages both to distinguish them from each other and to better inform the non-legal community as to their legal significance.

Keywords: *jus ad bellum, jus in bello, international humanitarian law, armed attack, self-defence, attack, distinction*

1. INTRODUCTION

The U.S. Department of Defense's *Dictionary of Military Terms* defines "computer network attack" (CNA) as "[a]ctions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[1] NATO adopts this definition in its *Glossary of Terms*, but adds the parenthetical that "[a] computer network attack is a type of cyber attack."[2] Curiously, it does not define "cyber attack" and the reference contains the sole mention of "cyber" in the document.

The term "computer network attack" is adequately descriptive for non-legal use. For instance, it usefully distinguishes such operations from computer network defence, computer network

1 U.S. Department of Defense, Dictionary of Military and Associated Terms, Joint Publication 1-02, Nov. 8, 2010, as amended through Feb. 15, 2012, available at http://www.dtic.mil/doctrine/dod_dictionary/.
2 NATO Standardization Agency, NATO Glossary of Terms and Definitions (AAP-6) (2010), at 2-C-12.

exploitation and other cyber activities.[3] Despite practical utility, its use causes measurable disquiet among lawyers, for "attack" is a legal term of art that has specific meaning in the context of two very different bodies of international law governing State behaviour in times of crisis or conflict. In both cases, the term represents a consequential threshold that delineates the legality of particular cyber operations, and, in some cases, the lawfulness of responses thereto.

This article seeks to bridge the terminological gap between the legal and non-legal communities by examining and explaining the significance of the word "attack" in international law. Hopefully, doing so will imbue policy makers, cyber operators and technical experts with greater sensitivity to the legal dimensions of the verbiage they employ when addressing cyber matters. Although the two communities may not speak the same language, members of both benefit from being bilingual.

2. THE LEGAL ARCHITECTURE

The international law governing conflict consists of two distinct bodies of law: the *jus ad bellum* and the *jus in bello*. *Jus ad bellum* norms govern when States, as an instrument of their national policy, may resort to force. They address, inter alia, the prohibition of the use of force by States and the exceptions thereto, most notably the right of self-defence and authorization or mandate by the UN Security Council.[4] The *jus in bello*, by contrast, deals with how the military and other armed actors may employ force, including who and what may be targeted.

These norms, also labelled the "law of armed conflict" or "international humanitarian law" (the latter term adopted in this article), apply in situations of "armed conflict" irrespective of whether the State or armed actor in question has resorted to force in compliance with the *jus ad bellum*. Differing objects and purposes animate the two bodies of law and explain the impenetrable barrier between them. The *jus ad bellum* seeks to maintain peaceful relations within the community of nations by setting strict criteria as to when States may move beyond non-forceful measures such as diplomacy, economic sanctions and counter-measures.[5] Of particular note is the right to do so in self-defence when either facing an "armed *attack*" or coming to the aid of another State which is defending itself (collective self-defence). By

3 Computer network operations comprise "computer network attack, computer network defense, and related computer network exploitation enabling operations. DoD Dictionary of Military Terms, *supra* note 1. Computer network defense is defined as "[a]ctions taken to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks," whereas computer network exploitation encompasses "[e]nabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks." *Id.*

4 U.N. Charter, arts. 2(4), 42 & 51.

5 Countermeasures are "measures that would otherwise be contrary to the international obligations of an injured State vis-à-vis the responsible State, if they were not taken by the former in response to an internationally wrongful act by the latter in order to procure cessation and reparation." Draft Articles on Responsibility of States for Internationally Wrongful Acts, Report of the International Law Commission on the Work of its 53rd sess., UNGAOR, 56th sess., sup. No. 10 (A/56/10), ch. IV.E.1, at p. 128, *available at* http://untreaty.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [hereinafter Articles of State Responsibility]. Note that Article 50 of the Articles of State Responsibility provides that countermeasures cannot amount to a use of force. However, this position, which the author accepts, was challenged by Judge Simma in the Oil Platforms case, where he argued that countermeasures could involve force when in response to an act that itself amounted to a use of force, but did not qualify as an armed attack. Oil Platforms (Islamic Republic of Iran v. U.S.), 2003 I.C.J. 161, ¶¶12-13 (Nov. 6) (separate opinion of Judge Simma).

contrast, international humanitarian law seeks to minimize harm during an armed conflict that is either unnecessary to effectively accomplish legitimate military aims or excessive relative to them. It does so most directly by establishing legal boundaries for the conduct of "*attacks*." Ignoring "right or wrong" under the *jus ad bellum* optimizes this purpose.

Since the term "attack" applies in separate bodies of law with discrete objects and purposes, it is unsurprising that its meaning differs depending on its source. In the *jus ad bellum*, it appears in Article 51 of the United Nations Charter: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security." Article 51, recognized as reflective of customary international law by the vast majority of legal scholars, is an express exception to Article 2(4) of the Charter, which provides that "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." Taking the Articles together, a State may "use force" without violating Article 2(4) when it is the victim of an "armed attack", as that term is envisaged in Article 51. Self-defence requires no *ex ante* authorization from the Security Council, States alone enjoy the right of self-defence, and the right only attaches to armed attacks with a transnational element.[6]

In international humanitarian law, "attack" refers to a particular category of military operations. Article 49(1) of the 1977 Additional Protocol I to the 1949 Geneva Conventions defines "attacks" as "acts of violence against the adversary, whether in offence or in defence."[7] It is a neutral term in the sense that some attacks are lawful, whereas others are not, either because of the status of the object of the attack or how the attack is conducted. Neutral though it may be, "attack" is operatively a key threshold concept in international humanitarian law because many of its core prohibitions and restrictions apply only to acts qualifying as such.

It is important to bear in mind that this notion only attains relevance once an "armed conflict" is underway. Like "attack", "armed conflict" is a legal term of art referring to two types of conflicts: 1) international armed conflicts, which are between States; and 2) non-international armed conflicts, which are conflicts at a certain level of intensity and organization between a State and an organized armed group or between organized armed groups.[8] Absent a situation qualifying as one of these conflicts, domestic and human rights law, not humanitarian law, governs the activities in question.

6 In the cyber context, the meaning of the term "use of force" is highly unsettled. See Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual), (Michael N. Schmitt et al. eds., Cambridge University Press, forthcoming 2013) [hereinafter Tallinn Manual].

7 Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, art. 49.1, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP I].

8 For the thresholds applicable to international and non-international armed conflict, see common articles 2 and 3 respectively to the four Geneva Conventions. Note that in addition to situations involving hostilities, the applicability of humanitarian law extends to those in which there has been a declaration of war or occupation, even when hostilities have not broken out. Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31; Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85; Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135; Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287.

To summarize, an "armed attack" is an action that gives States the right to a response rising to the level of a "use of force," as that term is understood in the *jus ad bellum*. By contrast, the term "attack" refers to a particular type of military operation during an armed conflict to which particular international humanitarian law norms apply. The general outline fashioned, it is apropos to examine the terms as they apply in the cyber environment.

3. CYBER "ARMED ATTACKS" UNDER THE JUS AD BELLUM

Before turning to the possible qualification of cyber operations as armed attacks, it is important to grasp the related point that there are no unique restrictions on the resort to defensive cyber operations in response to kinetic operations that qualify as an armed attack. On the contrary, they mirror those applying to kinetic defensive actions. For instance, cyber operations have to comply with the *jus ad bellum* principle of necessity, by which force may only be employed defensively to the extent non-forceful measures are unlikely to suffice. They equally have to comport with the *jus ad bellum* principle of proportionality, allowing only that degree of force required for an effective defence.[9] Cyber uses of force in the face of an armed attack must further meet the related requirements of imminency and immediacy, which limit, respectively, responses in anticipation of, and subsequent to, an attack. These and other questions, in particular the legal meaning of the phrase "use of force", are dealt with at length in the forthcoming *Tallinn Manual*.[10]

The question at hand, however, is when does a cyber operation qualify as an armed attack, that is, when does an action against a State legally merit a response with either cyber or kinetic actions that are at the level of a use of force?[11] The challenge lies in interpreting the adjective "armed." "Armed" is not to be equated with "force" in the sense of Article 2(4). The International Court of Justice recognized this normative "gap" in the *Nicaragua* Judgement when it found that there are "measures which do not constitute an armed attack but may nevertheless involve a use of force" and distinguished "the most grave forms of the use of force from other less grave forms."[12] The Court cited supplying weapons and providing logistical support to a rebel group in another State as an example of a use of force that did not amount to an armed attack against that State.[13] This gap makes sense in light of the central object and purpose of the United Nations Charter – to craft a system that effectuates a strong presumption against the use of force in international relations and favours collective responses to threats to (or breaches of) the peace over unilateral ones.

The result is a normative schema in which all armed attacks are uses of force, but not all uses of force are armed attacks. As a consequence, States may face cyber operations constituting a use of force, but be unable to respond in kind because the offending operations fall within the

9 Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶¶ 176,194 (June 27); Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 41 (July 8); Oil Platforms, *supra* note 5, ¶¶43, 76.

10 Tallinn Manual, *supra* note 6.

11 Cyber operations at the use of force level that do not qualify as an armed attack may nevertheless justify countermeasures (see Tallinn Manual).

12 Military and Paramilitary Activities, *supra* note 9, ¶¶ 191 & 210. See also Oil Platforms, *supra* note 5, ¶ 51.

13 Military and Paramilitary Activities, *supra* note 9, ¶ 195.

gap − they are uses of force, but not sufficiently severe to qualify as an armed attack. When this happens the victim-State may resort to either lawful responses, such as diplomatic protests or economic sanctions, or to cyber or kinetic actions short of uses of force that would otherwise be unlawful, but which qualify as lawful "counter measures" in the circumstances.[14] Of course, the victim-State can also refer the matter to the Security Council, which enjoys the authority to act forcefully in the face of any "threat to the peace, breach of the peace, or act of aggression".[15]

Use of the term "armed attack" in lieu of Article 2(4)'s "use of force" verbiage constructs the gap. Note how Article 51 adopts an "act-based" threshold using a specified type of action (armed attack) rather than one based on particular consequences. This approach tracks that taken in Article 2(4), with its prohibition on uses of force. In 1945, an act-based threshold made sense, for the action to which States were most unwilling to completely defer forceful responsive measures to the Charter's new collective security system was an attack by the armed forces of another State. Thus, the term armed attack represented an elegant balancing of the general apprehension about States using force unilaterally, on the one hand, and the fear of States about being defenceless in the face of attacks should the international community fail to act, on the other. This mechanism worked well when the threats that inspired the acceptance of a self-defence exception to the prohibition on the use of force consisted of classic military operations.

The advent of cyber operations challenged this presupposition because dire consequences could now be caused by operations that did not fit neatly into the notion of an attack that was "armed" in the kinetic sense. While the International Court of Justice had opined in its *Nuclear Weapons* advisory opinion that the type of weapon used is immaterial to the application of Articles 2(4) and 51,[16] cyber operations seemed distant from the concept of "armed." Traditional weapons were not employed, they did not require the supporting elements typically associated with military assaults and, most importantly, their direct destructive effect did not result from a release of kinetic force.

The dilemma was that despite these qualitative differences cyber operations could theoretically prove monumentally destructive, in many cases more so than kinetic ones. Accordingly, it was self-evident that some of them were surely encompassed within the ambit of armed attacks. After all, the Charter scheme would make no sense if it prohibited States from responding to devastating attacks merely because such attacks were not in the drafters' contemplation decades before they became technically possible. Such legal formalism would take strict constructionism to absurd ends. Clearly, the advent of cyber operations necessitated a reconceptualization of the notion of "armed attack". To date, the international community has failed to achieve consensus on this critical issue.

The solution to the quandary lies in a realization that the act-based threshold of Article 51 is but cognitive shorthand for a consequence-based legal regime. Reduced to basics, law is about avoiding particular deleterious consequences (or achieving certain positive ones). So the right to resort to force in the face of an armed attack can best be appreciated as a right to do so when States face particular consequences that are severe enough to merit setting aside international

14 On the criteria for, and limitations on, countermeasures, see Articles on State Responsibility, *supra* note 5, ch. 2.

15 U.N. Charter, arts. 39, 42.

16 Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. ¶ 39 (July 8).

law's prohibition on the use of force. By this logic, "armed attack" in the cyber context can be interpreted as encompassing any acts that result in consequences analogous to those caused by the kinetic actions originally envisaged by the term "armed attack."

But what are those consequences? Three points bear on this determinative question. First, as noted, since they are the product of an armed attack, the actions causing them lie above Article 2(4)'s "use of force" threshold. Second, recall the Charter presumption against the use of unilateral force. This too points to a fairly restrictive understanding of armed attack, for it is the point at which States may use force without Security Council authorization. Finally, treaties "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."[17] The ordinary meanings of the term "armed" are "equipped with or carrying a weapon or weapons," "involving the use of firearms," and "prepared to activate or explode."[18] This suggests that the term implies the sort of consequences that are incident to the use of weapons, an interpretation strengthened by the deliberate omission of the adjective "armed" with respect to "use of force" in Article 2(4). Taken together, a defensible interpretation of the phrase is any action that causes death or injury (including illness and severe suffering) to individuals or damage or destruction of objects.

Some controversy exists over the degree of harm necessary to qualify consequences as an armed attack. The International Court of Justice addressed this matter in the *Nicaragua* case. There it found that an armed attack must have certain "scale and effects," citing the case of a "mere frontier incident" as insufficiently grave.[19] Unfortunately, the Court failed to set forth criteria against which to judge a particular action or incident, an omission for which it has been roundly criticized.[20] In this author's view, it is therefore more useful and appropriate to focus on the qualitative nature of an action's consequences than on any ill-defined quantitative standards; hence the standard proposed.

A recurring question in the cyber context is whether the damage or destruction or manipulation of data that does not generate such consequences is capable of qualifying as an armed attack. Generally it does not, for so qualifying such action would dramatically lower the threshold at which States would enjoy a right to forcefully respond to actions directed at them. This would contravene international law's general presumption against the resort to force in the absence of authorization by the Security Council.

In light of the ever-increasing reliance of society on computers and computer networks, many readers, like the author, will find the "physical consequences" standard too narrow. But it does represent the lex lata, that is, the law that presently exists. For those who share this concern, solace can be found in the fact that international law is not static. As experience with cyber operations grows, the international community may embrace more nuanced understandings of the extant legal standard, or even adopt new legal interpretations thereof. In particular, the law's qualitative focus on the type of harm may yield somewhat to a quantitative analysis such that

17 Vienna Convention on the Law of Treaties art. 31(1), May 23, 1969, 1155 U.N.T.S. 331.

18 The New Oxford American Dictionary, *available at* http://www.oxfordamericandictionary.com/LOGIN?sessionid=35340fb16f7eef9ffa3d1efc76377df8&authstatuscode=400.

19 Military and Paramilitary Activities, *supra* note 9, ¶ 195.

20 And in the later *Platforms* case, it held that the mining of even a single ship could rise to the level of an armed attack. Oil Platforms, *supra* note 5, ¶ 72; see also William H. Taft IV, Self-Defense and the Oil Platforms Decision, 29 Yale Journal of International Law 295, 300 (2004).

a cyber operation causing serious consequences, such as severe economic effects or significant disruption of societal functions, may be characterized as armed attack even if it does not cause death, injury, damage or destruction. Time will tell.

4. CYBER "ATTACKS" UNDER INTERNATIONAL HUMANITARIAN LAW

The notion of armed attacks under the *jus ad bellum* must not be confused with international humanitarian law's usage of the term "attack". In the latter body of law, an "attack" triggers a wide array of legal protections. These prohibitions and restrictions generally derive from the principle of distinction, which requires the parties to a conflict to "at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly direct their operations only against military objectives."[21]

Although the principle of distinction is framed in terms of "military operations," it is clear that not all military operations are contemplated by the norm. For instance, longstanding State practice demonstrates that non-destructive psychological operations directed at the civilian population, such as dropping leaflets, broadcasting to the enemy population, or even jamming enemy public broadcasts, are lawful as long as no physical consequences attend them. Rather, the principle is primarily meant to address "attacks", as that term is understood in the law.

Various facts support this contention. Note how the principle of distinction is set forth in Article 48 of Additional Protocol I. That article appears in the Chapter on "Basic Rule and Field of Application" of the treaty's conduct of hostilities section. Since the only other article in the Chapter is Article 49, which defines attacks, this placement implies that the military operations referred to in Article 48 are primarily attacks.

Further review of the section reveals a constant and pervasive emphasis on "attacks". Article 51 is illustrative. It begins by noting that the "civilian population and individual civilians shall enjoy general protection against dangers arising from military *operations*," but operationalizes the provision by noting that "to give effect to this protection" it is prohibited to attack individual civilians or the civilian population, conduct an attack that is not directed at a military objective, engage in reprisal attacks against civilians, launch attacks in which the expected collateral damage is excessive relative to anticipated military advantage, treat multiple military objectives during an attack as a single one when they are clearly separated and distinct in a concentration of civilians, and use a method or means of warfare during an attack that is either incapable of distinguishing lawful from unlawful targets or has effects that cannot be controlled.[22] Subsequent articles are likewise framed in terms of prohibitions and restrictions on attacks. The most important of these prohibit attacks on civilian objects and mandate various precautions that must be taken during an attack to avoid harming the civilian population and civilians. Simply put, the prohibition on directing military operations against civilians, civilian objects

21 AP I, *supra* note 7, art. 48. The provision is generally deemed reflective of customary international law and the International Court of Justice has cited it as one of international humanitarian law's "cardinal" principles. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 78 (July 8).

22 AP I, *supra* note 7, art. 51(4). The emphasis in this and all other treaty extracts is the author's and does not appear in the original.

and other protected persons and objects must be understood as essentially a prohibition on *attacking* them. Conducting military operations that do not qualify as attacks against them is, in a general sense, lawful (absent a specific prohibition to the contrary[23]).

This conclusion raises the question of which acts qualify as an attack. The reference to acts of violence against the adversary, whether in offence or defence, in Article 49 is the key to the answer.[24] It should be cautioned that mention of the "adversary" does not imply that only violent operations against enemy forces qualify. On the contrary, the prohibition on attacking civilians irrefutably confirms that the *sine qua non* criterion is violence, not the individual or entity that is the object of an attack.

The definitional centrality of violence is well supported. For example, the Bothe, Partsch and Solf commentary on Additional Protocol I explains that "[t]he term 'acts of violence' denotes physical force. Thus, the concept of 'attacks' does not include dissemination of propaganda, embargoes, or other non-physical means of psychological or economic warfare."[25] Their commentary is particularly authoritative given that all three were active participants at the Diplomatic Conference that negotiated the treaty. The official International Committee of the Red Cross (ICRC) Commentary similarly explains that "the term 'attack' means 'combat action.'"[26]

The cognitive dilemma is that cyber operations do not directly involve the release of violent forces. This begs the questions of whether and when cyber operations qualify as attacks under international humanitarian law such that its prohibitions and restrictions thereon apply.

As with the UN Charter, actions that can cause harm without the immediate release of violent kinetic forces were beyond the contemplation of the drafters of Additional Protocol in 1977. Yet, by then, an implicit recognition existed that the violence of an act itself was not the crux of the norms in question. Over a half-century earlier, employment of chemical and biological weapons was already considered an attack, as evidenced, *inter alia*, by the outlawing of their use for Parties to the 1925 Gas Protocol.[27] They were outlawed because they were instrumentalities that caused particular harmful consequences that international humanitarian law sought to avoid. By the same logic, "acts of violence" are merely instrumentalities that cause consequences with which the law concerns itself.

Moreover, as noted, treaties must be interpreted in "context and in light of object and purpose." A careful reading of Additional Protocol I's prohibitions and restrictions on attacks discloses that the concern was not so much with acts which were violent, but rather with those that have harmful consequences (or risk them), in other words, violent consequences. In great part, the treaty's object and purpose is to avoid, to the extent possible in light of military necessity, those very consequences. For instance, civilians "enjoy general protection against *dangers* arising

23 As with the requirement to "respect and protect" medical units in addition to the prohibition on attacking them. AP I, *supra* note 7, art. 12.

24 See text accompanying note 7.

25 Michael Bothe et al., New Rules for Victims of Armed Conflicts 289 (1982).

26 Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, ¶ 1880 (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann, eds., 1987)

27 1925 Geneva Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, June 17, 1925, 26 U.S.T. 571, T.I.A.S. No. 8061.

from military operations."[28] Acts intended to *terrorize* the civilian population are prohibited.[29] The rule of proportionality assesses an act in light of the "incidental *loss* of civilian life, *injury* to civilians, *damage* to civilian objects, or a combination thereof" expected to be caused by an attack.[30] Precautions that are required to be taken when conducting an attack are meant to "*spare*" the civilian population.[31] They include selecting weapons and tactics "with a view to avoiding, and in any event to minimizing, incidental *loss* of civilian life, *injury* to civilians and *damage* to civilian objects"; refraining from launching, suspending, and cancelling attacks that would likely cause excessive "incidental *loss* of civilian life, *injury* to civilians [or] *damage*"; issuing warnings when feasible if an attack will "*affect* the civilian population"; choosing among comparable targets "which may be expected to cause the least *danger* to civilian lives and to civilian objects"; and, in air and sea operations, taking precautions "to avoid *losses* of civilian lives and *damage* to civilian objects".[32] Defenders must similarly take measures to protect civilians and civilian objects from "*danger*".[33] The same consequence-based approach applies to specially protected objects, as in the restrictions on conducting attacks against dams, dykes and nuclear generating stations when "*severe losses*" among the civilian population might result[34] and the prohibition on using methods or means of warfare likely to cause "*widespread, long-term and severe damage*" to the natural environment and thereby "prejudice the *health or survival* of the population."[35]

It is apparent that international humanitarian law, despite adopting an instrumentality-based definition of attack, takes a consequence-based approach to it normative prescriptions when operationalizing that term. The Bothe, Partsch and Solf commentary to Article 49 supports this conclusion by noting that attack refers to "those aspects of military operations that *most directly affect* the safety of the civilian population and the integrity of civilian objects."[36]

Through the process of induction, it is possible to derive a general principle regarding the notion of attack that has meaning within the cyber context. Attacks can be redefined as operations that result in, or if unsuccessful were originally expected to result in, death or injury of individuals or destruction or damage of objects. The notion of injury includes illness that might result from a cyber operation, as in the case of attacking a water treatment plant in order to contaminate drinking water. It is also sensible, based for example on the prohibition of terror attacks and starvation[37], to extend the concept to acts producing serious suffering not otherwise justified by the notion of military necessity. Destruction includes operations that, while not causing physical damage, nevertheless "break" an object, rendering it inoperable, as in the case of a cyber operation that causes a computer reliant system to no longer function unless repaired. Thus, the legal analysis of attack in the international humanitarian law context leads to roughly the same conclusion as arrived at with respect to the *jus ad bellum*. However, the reader must understand that since they derive from different bodies of law, their precise parameters are nuanced in ways beyond the capability of this article to address.[38]

28 AP I, *supra* note 7, arts. 51(2).
29 *Id*., art. 51(3).
30 *Id*., arts. 51(5)(b) & 57(2)(a)(iii).
31 *Id*., art. 57(1).
32 *Id*., art. 57.
33 *Id*., art. 58.
34 *Id*., art. 56(1).
35 *Id*., art. 55(1).
36 Bothe, *supra* note 26, at 325.
37 AP I, *supra* note 7, arts. 51(2) & 54.
38 These nuanced are explored in the forthcoming Tallinn Manual, *supra* note 6.

The consequence of this conclusion for cyber operations is significant. It means that cyber operations can be directed at civilian systems so long as the requisite type of harm is not triggered and no other specific international humanitarian law prohibition (such as those attending medical operations) applies.

At the 37th International Conference of the Red Cross and Red Crescent Society in 2011, the ICRC circulated a background paper articulating a different approach.[39] It began by noting that Article 49's reference to "acts of violence […] denotes physical force." Accordingly, "cyber operations by means of viruses, worms, etc., that result in physical damage to persons, or damage to objects that goes beyond the computer program or data attacked could be qualified as 'acts of violence', i.e. as an attack in the sense of IHL." There is universal agreement on this point.

However, the document then took issue with the general approach set forth (except for reversibility) in this article, that is, 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 are reversible." According to the ICRC paper,

> "[i]f 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."[40]

The ICRC's references to international humanitarian law comments reflect the state of the law. There is no doubt that an attack against a civilian object is unlawful. Nor is there any doubt that the methods or means of attack have no bearing whatsoever on the legal character of a targeted object as either a civilian object or a military objective. And the reference to "neutralization" properly confirms that the military advantage required for qualification as a military objective need not stem from physical damage to the target. These are binding norms not only for Parties to Additional Protocol I, but for also for other Stats since they reflect customary international law.[41]

But the organization's conclusion misses the mark. The question at hand is whether a cyber operation qualifies as an attack in the first place. Only when it does is the issue of the target's

39 International Committee of the Red Cross, 31st International Conference of the Red Cross and Red Crescent, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, Report 31IC/11/5.1.2, Oct. 2011.

40 *Id.* at 37.

41 See, e.g., Department of the Navy et al., The Commander's Handbook on the Law of Naval Operations (NWP 1-14M/MCWP 5-12/COMDTPUB P5800.7A), chapter 8 (2007).

status raised, for only then do international humanitarian law prohibitions and restrictions as to attacks come into play. Consequently, once a cyber operation qualifies as an attack, Article 52(2)'s criteria for qualification as a military objective apply…and not before that determination is made. Should an object not constitute a military objective, a prospective attack thereon is prohibited. If it does, the object may, as a military objective, be attacked by any method or means of warfare that otherwise complies with the rule of proportionality, the requirement to take precautions in attack and other applicable standards. For instance, even when cyber operation can be employed to neutralize a military objective, an attacker may elect to bomb it doing so is not expected to exacerbate incidental harm to civilians, civilian objects and other protected persons and places.

Admittedly, the conclusions reached in this article regarding the meaning of "attack" in international humanitarian law may seem unsatisfactory. Non-destructive attacks and those that do not place individuals or objects at physical risk can have severe consequences. Yet, the interpretation advanced in this article represents the extant law, that is, the *lex lata*. Assertions to the contrary are, in the author's estimation, merely *lex ferenda*. Of course, as with the term "armed attack" in the *jus ad bellum* context, the meaning of a legal term may shift over time through adoption of new treaty law, creation of new customary norms through State practice, or the emergence of new understandings in the face of the changing context of conflict to which it applies.

5. CONCLUDING THOUGHT

This article has attempted to clear some of the terminological dissonance that exists between the policy/technical/operational and legal communities regarding the term "attack." The former must be sensitive to the fact that legal meaning also attaches when the term is used in its colloquial sense. Complicating matters is the fact that the term inhabits two separate and distinct areas of the law. The risk of creating confusion as to precise policy parameters is accordingly high when using the term without care. For its part, the legal community must be alert to the possibility that its legal advice may not be fully grasped by their clients when the term attack is used *stricto sensu*. Unfortunately, the dearth of systematic interaction between the respective cyber communities has resulted in the emergence of two patois that are sometimes unintelligible to each other. It is hoped that this book, and the conference upon which it is based, will serve to narrow the gap between them.