INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1895
U.S. NAVAL WAR COLLEGE

Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?

Noam Lubell

89 INT'L L. STUD. 252 (2013)

Volume 89 2013

Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?

Noam Lubell[*]

I. INTRODUCTION

Most of the advanced and largest militaries in the world have, in recent years, devoted significant attention and resources to the development of the capacity to conduct—and defend against—cyber operations.[1] Indeed, cyber operations feature prominently in discussions over future conflicts and are expected to be an inherent and major component in the waging of war. But cyber operations are not usually conducted with the aim of straightforward material harm to a physical military object and their use

* Reader in Law, School of Law, University of Essex, United Kingdom. Thanks are due to Marty Ehlenbach for research assistance and to Audrey Guinchard for comments.

1. U.S. Department of Defense, Department of Defense Strategy for Operating in Cyberspace (2011), *available at* http://www.defense.gov/news/d20110714cyber.pdf; HM Government, Securing Britain in an Age of Uncertainty: UK Strategic Defence and Security Review (2010), *available at* http://www.cabinetoffice.gov.uk/sites/default/files/resources/strategic-defence-security-review.pdf; NATO Cooperative Cyber Defence Centre of Excellence, http://www.ccdcoe.org/; Jim Wolf, *China Cyber Capability Puts U.S. Forces at Risk: Report*, REUTERS (Mar. 8, 2012, 12:11 AM), http://www.reuters.com/article/2012/03/08/us-china-usa-cyberwar-idUSBRE8270AF20120308; Nick Hopkins, *Militarisation of Cyberspace: How the Global Power Struggle Moved Online*, GUARDIAN (Apr. 16, 2012, 10:00 AM), http://www.guardian.co.uk/technology/2012/apr/16/militarisation-of-cyberspace-power-struggle.

raises complex questions concerning the choice of targets. During armed conflict, international law provides detailed rules on targeting, most of which stem from the fundamental principle of distinction. At its most basic understanding, this rule requires that all things and people military must be distinguished from things and people civilian.[2] It governs questions of who and what may be attacked. It also influences other rules on how attacks may be carried out—prohibitions of indiscriminate attacks and concepts of proportionality would in most cases become meaningless without the distinction between military and civilian.[3] The principle of distinction is one of the foundations of the law of war. The International Court of Justice has described it as part of "[t]he cardinal principles contained in the texts constituting the fabric of humanitarian law."[4] As such, this principle should presumably hold true in any type of conflict. The cyber sphere, however, presents unique challenges to our ability to adequately distinguish between military and civilian and thereby adhere to this fundamental principle. Moreover, the nature of cyber operations is such that it does not neatly fit into the paradigm of hostilities around which the law of armed conflict (LOAC) is constructed. In fact, it has even been debated whether the LOAC rules on targeting would always apply to cyber operations, and whether the need to distinguish between military and civilian and the prohibition on attacking civilian targets are applicable to all forms of cyber operations or not.[5] This article will examine these questions in the following manner. Part II will address the question of the nature of cyber operations

---

2. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 48, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I].

3. *Id.*, art. 51 (protection of the civilian population).

4. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 78 (July 8) [hereinafter *Nuclear Weapons*]. Note also the International Committee of the Red Cross commentary on the rule, which states the rule of protection and distinction is

> the foundation on which the codification of the laws and customs of war rests: the civilian population and civilian objects must be respected and protected in armed conflict, and for this purpose they must be distinguished from combatants and military objectives. The entire system established in The Hague in 1899 and 1907 and in Geneva from 1864 to 1977 is founded on this rule of customary law.

COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, ¶ 1863 (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann eds., 1987) (footnotes omitted) [hereinafter COMMENTARY ON THE ADDITIONAL PROTOCOLS].

5. *See infra* pp. 254.

that are likely to take place. This will include an examination of cyber operations as fitting within the notion of attack. Part III will then turn to an analysis of the appropriate threshold of harm that would lead a cyber operation to be considered an attack under LOAC—and thus subject to the principle of distinction—with particular focus on destruction of data and harm that does not have direct physical manifestation.

II. THE CONCEPT OF ATTACK IN CYBER OPERATIONS

In order to examine what might be lawful targets in the context of cyber operations, we must first get an idea of what types of targets the parties to a conflict might seek to attack. Actual cyber operations in past years range from hacking into government or military networks, such as the "Titan Rain" incident in 2003 when U.S. Department of Defense facilities, NASA labs, Lockheed Martin and other systems were hacked into and lost many terabytes of information (Chinese sources were alleged to have been behind this operation)[6] through to more recent years and well-publicized cyber incidents directed against Estonia and Georgia, which included incidents described as denial of service attacks leading to severe disruption of media, government and banking systems.[7] The Stuxnet worm is alleged to have led to physical damage to centrifuges at the Iranian nuclear facilities.[8] Cyber operations have also been employed in tandem with kinetic attacks, as was said to have happened in the Israeli attack on an alleged nuclear development site in Syria.[9] Individuals with a personal agenda have demonstrated the dangerous potential for using computer networks to gain con-

6. RICHARD A. CLARKE & ROBERT KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 58, 125–26 (2010). There have been a number of other such incidents originating from various sources, including those known as "Solar Sunrise" and "Moonlight Maze," as well as Operation "Buckshot Yankee." For the latter, see Ellen Nakashima, *Cyber-Intruder Sparks Massive Federal Response—and Debate over Dealing with Threats*, WASHINGTON POST (Dec. 9, 2011), http://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html. For a detailed list of these and other cyber operation incidents, see H. HARRISON DINNISS, CYBER WARFARE AND THE LAWS OF WAR app. 1 (2012).

7. See the detailed discussion in ENEKEN TIKK, KADRI KASKA & LIIS VIHUL, INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS (2010).

8. David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, NEW YORK TIMES, June 1, 2012, at A1.

9. CLARKE & KNAKE, *supra* note 6, at 1–8.

trol of complex systems and unleash serious damage.[10] More generally, cyber attacks are described as operations seeking to accomplish a wide range of effects, including "[d]estroy data on a network or a system connected to the network"; [11] "[b]e an active member of a network and generate bogus traffic";[12] "[c]landestinely alter data in a database stored on the network";[13] and "[d]egrade or deny service on a network."[14]

One way of describing all of this is simply to say that targets in cyber operations are usually computer network systems. It is, however, also possible to create an element of differentiation between these potential targets. In certain operations, such as denial of service, it is the computer system itself that is the object of the operation and the direct objective is to shut down or prevent the system from functioning as designed.[15] Alternatively, it may be that the objective is the corruption of data on the system or the destruction of specific information data, in which case it might be more accurate to state that the target of the operation is not the system as a whole but rather the data.[16] Lastly, if an attack is designed to take control of a computer network in order to directly manipulate a physical object—for example, take control of a missile launch system or open the floodgates of a dam—then it might be more accurate to describe the computer network as part of the means and methods of attack, while the actual target is the physical object directly affected.

---

10. For example, see the case of an Australian individual who caused the dumping of sewage into rivers, leading to serious harm to the local environment. Robert O'Harrow Jr., *Search Engine Exposes Industrial-Sized Dangers*, WASHINGTON POST (June 4, 2012), http://www.washingtonpost.com/investigations/cyber-search-engine-exposes-vulnerabilities/2012/06/03/gJQAIK9KCV_story.html. In another case, a disgruntled employee disabled the system for detecting oil pipeline leaks off the Californian coast. David Kravets, *Feds: Hacker Disabled Offshore Oil Platforms' Leak-Detection System*, WIRED (Mar. 18, 2009, 3:47 PM), http://www.wired.com/threatlevel/2009/03/feds-hacker-dis/. *See also* Rebecca Allison, *Hacker Attack Left Port in Chaos*, GUARDIAN (Oct. 6, 2003), http://www.guardian.co.uk/technology/2003/oct/07/usnews.uknews.

11. Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 JOURNAL OF NATIONAL SECURITY LAW AND POLICY 63, 69–70 (2010).

12. *Id.*

13. *Id.*

14. *Id.*

15. For example, disrupting command and control systems, or communication networks.

16. See *infra* pp. 256 for an analysis of whether or not data should be considered as an object in the context of attacks.

Ultimately, since the world we actually live in is not the non-material cyber sphere, it is clear that any cyber operation is designed to lead—directly or indirectly—to a result which includes an effect in the physical world. Nonetheless, there is a qualitative difference between attacks designed to gain direct control of a physical object and cause it to act in a specific planned way, and attacks targeting the networks and data themselves, aiming for more generalized knock-on effects. In the former cases, such as using a computer network in order to gain control of an opposing party's missile system and cause it to fire upon itself, or a cyber operation designed to open a dam and unleash a flood, there is, of course, the need to assess the legality of these targets. For this determination of whether these are lawful targets under LOAC, such cyber operations may raise certain new aspects, but at the end of the day the legality question will in most cases not be unique to cyber operations.[17] It is in those circumstances in which the systems and data themselves are attacked where the more complex questions arise with regard to choice of target.

A number of legal concerns must be recognized. First and foremost is, of course, the question of whether certain computer network systems can be considered military objectives, and consequently lawful targets. Further challenges in this context concern the ability to take adequate precautions, avoid disproportionate effects, and not stray beyond lawful means and methods. These are all matters of vital importance, but are not within the scope of this article focused on lawful targets.[18] The issues addressed here

---

17. The LOAC rules most directly applicable include Article 56(1) of Additional Protocol I, which states that

> [w]orks or installations containing dangerous forces, namely dams, dykes and nuclear electrical generating stations, shall not be made the object of attack, even where these objects are military objectives, if such attack may cause the release of dangerous forces and consequent severe losses among the civilian population. Other military objectives located at or in the vicinity of these works or installations shall not be made the object of attack if such attack may cause the release of dangerous forces from the works or installations and consequent severe losses among the civilian population.

18. Cyber operations can present particular challenges in these areas due to characteristics such as their potential capacity to spread indiscriminately through the networks, and to have indirect effects that may be difficult to foresee. For a discussion of some of these issues, see Eric Talbot Jensen, *Unexpected Consequences from Knock-On Effects: A Different Standard for Computer Network Operations?*, 18 AMERICAN UNIVERSITY INTERNATIONAL LAW REVIEW 1145 (2003); KNUT DÖRMANN, APPLICABILITY OF THE ADDITIONAL PROTOCOLS TO COMPUTER NETWORK ATTACKS 2–3 (2004), *available at* http://www.icrc.org/eng/resources/documents/misc/68lg92.htm. For an example of a unique challenge arising from cyber operations, see the discussion of active defenses and use of "hack back" in

are concerned with questions relating to the nature of the objects attacked and whether they must be defined as military objectives in order to be lawful targets of cyber operations. In other words, we are currently examining *what* can be attacked rather than *how/with what*.

Before proceeding further, a preliminary matter must be clarified: the question of lawful targets in the *ius in bello* is separate from the questions of the *ius ad bellum*. While the need for maintaining a separation between these two areas of law has long been evident for a number of reasons,[19] the discussions surrounding cyber operations have on occasion muddied the waters. Much of this is due to the fact that cyber operations present equally vexing problems for both bodies of law and, moreover, many of these challenges in both the *ius ad bellum* and the *ius in bello* surround the notion of "attack."[20] As has been the subject of much discussion, there is a debate as to whether cyber operations against certain objects might be considered an armed attack, thereby triggering the right to self-defense under the *ius ad bellum*.[21] However, the response to that question does not provide us with an answer as to whether the object was a lawful target under the *ius in bello*; the debate over defining an attack as an armed attack under the *ius ad bellum* can exist regardless of the military nature of the object attacked. An event constituting an armed attack for the purpose of the *ius ad bellum* might include an attack against the military installation of another State, but equally if the attack was against a civilian target (e.g., bombing civilian areas of a city) this would also be an armed attack under the *ius ad bellum*. A determination of an armed attack having occurred tells us therefore nothing about the civilian or military nature of the object attacked—a criterion crucial to

---

David E. Graham, *Cyber Threats and the Law of War*, 4 JOURNAL OF NATIONAL SECURITY LAW AND POLICY 87, 101–2 (2010).

19. For example, the application of the *ius in bello* must not be linked to determinations under the *ius ad bellum* in order to ensure equal application of the *ius in bello* rules, thus alleviating the risk of dis-incentivizing one of the parties from adhering to the rules. It is also notoriously difficult to agree on violations of the *ius ad bellum*, making any reliance on *ius ad bellum* determinations for the purpose of *ius in bello* rules a sure recipe for disaster.

20. For attack in the context of the *ius in bello,* see the detailed discussion *infra* pp. 262. For the *ius ad bellum*, see the authorities *infra* note 21.

21. For discussion of the *ius ad bellum* in the context of cyber operations, *see*, *e.g.*, Matthew Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE JOURNAL OF INTERNATIONAL LAW 421 (2011); Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885 (1999); TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE ch. II (The Use of Force) (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL].

the determination of lawful targets under the *ius in bello*. Accordingly, the current focus is not on the *ius ad bellum*, but on the nature of lawful targets within the *ius in bello*.

Another vital differentiation—and one which requires clarification—is the significance of using the word "attack." As noted above, under the *ius ad bellum*, the key is whether a specific event meets the threshold of an *armed* attack. This allows for perhaps a looser usage of the phrase "cyber attacks" in the knowledge that this phrase does not in itself contain a legal determination as to whether it constitutes an *armed* attack under the *ius ad bellum*. This, however, is not the case for *ius in bello*, where—as will be seen shortly—the very use of the word "attack" may in and of itself have significant legal repercussions, including for the issue of lawful targets during these operations. For the sake of legal clarity, it would therefore be advisable to utilize a more legally neutral (at least under the *ius in bello*) description and—unless intending to define an event as an attack under LOAC—to speak of cyber operations rather than cyber attacks.[22] This has not, unfortunately, been the case thus far. In fact, it appears that the term "cyber attack" has been used indiscriminately when discussing a wide range of operations, including activities such as hacking into Google servers or probing government computers,[23] and defacing websites.[24] Indeed, the U.S. Department of Defense defines the phrase "computer network attack" 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."[25] This definition—or

22. This is reminiscent of another area of LOAC in which terms are used without due regard to their legal implications, most notably in the inaccurate use of the term "combatant" to describe any fighter, even though the individual described might not meet the strict definition for being a combatant as set out in the law. For an examination of the difference between rhetoric, factual descriptions and legal terms in this latter context, see NOAM LUBELL, EXTRATERRITORIAL USE OF FORCE AGAINST NON-STATE ACTORS ch. 6 (2010).

23. Eric Talbot Jensen, *Cyber Warfare and Precautions against the Effects of Attacks*, 88 TEXAS LAW REVIEW 1533, 1536–42 (2010).

24. "The Federal Bureau of Investigation (FBI) reports that cyberattacks attributed to terrorists have largely been limited to unsophisticated efforts such as e-mail bombing of ideological foes, denial-of-service attacks, or defacing of websites." CATHERINE A. THEOHARY & JOHN ROLLINS, CONGRESSIONAL RESEARCH SERVICE, R41674, TERRORIST USE OF THE INTERNET: INFORMATION OPERATIONS IN CYBERSPACE 5 (2011), *available at* http://assets.opencrs.com/rpts/R41674_20110308.pdf.

25. *Computer Network Attack*, *in* DOD DICTIONARY OF MILITARY AND ASSOCIATED TERMS (Nov. 8, 2010), http://www.dtic.mil/doctrine/dod_dictionary/.

similar versions—has also been used by commentators writing on the topic.[26] Notably, it is a wide definition that can encompass a vast array of cyber operations with many different types of targets and varying degrees of effects. Moreover, it includes cyber operations designed to damage data, not just physical destruction.[27]

The dangerous ease with which we use the word "attack" causes us to unwittingly slide into an assumption that all these so-called attacks require an analysis under LOAC. But this is not always the case. There can be plenty of cyber operations that occur outside the context of an armed conflict, such as certain types of cyber espionage between supposedly friendly countries to which the law of armed conflict would not apply.[28] The inapplicability of LOAC in many situations is a crucial matter which must not be cast aside without consideration. Once the LOAC framework enters the stage, the legal regulation of operations takes on a new dimension that has significant repercussions for all concerned.[29] This is not an exhortation to never apply LOAC, but simply a reminder that it does not become applicable purely because we use the word "attack." LOAC can only apply within situations that qualify as an armed conflict. There is a complex debate as to whether stand-alone cyber operations between two parties—devoid of the kinetic actions usually associated with hostilities—can ever be considered an armed conflict.[30] This, however, becomes less of an obstacle if the cyber

26. DINNISS, *supra* note 6, at 4. Having used this definition, Dinniss later in the same book notes two different concepts of attack: "the question is raised as to when a computer network attack becomes an attack for the purposes of international humanitarian law." *Id.* at 179. *See also* Lin, *supra* note 11, at 63.

27. This point will be returned to later in the examination of data as an "object" of attack.

28. *See infra* notes 81–88 and accompanying text for mention of other relevant bodies of law which may regulate cyber operations outside of armed conflict.

29. For example, it can permit attacks that lead to civilian casualties that might otherwise have been unlawful. Equally, however, if violating the LOAC rules, those conducting the attacks will be open to charges under international criminal law.

30. This will largely depend on the manifestation and consequences of the cyber operations. See discussion in Noam Lubell, *Cyber Warfare as Armed Conflict*, *in* BRUGES COLLOQUIUM, TECHNOLOGICAL CHALLENGES FOR THE HUMANITARIAN LEGAL FRAMEWORK 41 (College of Europe & International Committee of the Red Cross eds., 2011), *available at* http://www.coleurope.eu/sites/default/files/uploads/page/collegium_41_0.pdf; Michael N. Schmitt, *Cyber Operations and the* Jus in Bello*: Key Issues*, *in* INTERNATIONAL LAW AND THE CHANGING CHARACTER OF WAR 89, 102–6 (Raul A. "Pete" Pedrozo & Daria P. Wollschlaeger eds., 2011) (Vol. 87, U.S. Naval War College International Law Studies); DÖRMANN, *supra* note 18, at 2–3. At least in theory, the possibility does exist as "the International Group of Experts unanimously concluded that cyber operations alone

operations are conducted alongside traditional methods of warfare.[31] The current focus of this article is on circumstances in which cyber operations take place between parties to an existing armed conflict and in which, therefore, LOAC has already been triggered.

The need for concern over the correct use of the term "attack" becomes evident when considering the repercussions of cyber operations that take place during armed conflict but might not, arguably, constitute an "attack" under the *ius in bello*. The key issue here is whether defining these operations as not being attacks can thereby expand the choice of lawful targets beyond the sphere of military objectives. For example, does a denial of service operation against a website constitute an attack? If so, then clearly the categorization of the website attacked as a legitimate military objective—or not—will be a vital concern. But what if denial of service is not an "attack" as understood in LOAC, and how might this affect the legality of directing a cyber operation against the website? In other words, does the nature of the targeted website even matter? Can one engage in cyber operations against non-military targets by claiming that the said cyber operations do not come under the definition of attacks? The *Tallinn Manual*, for example, unequivocally states that the prohibition on attacking civilian objects only applies to cyber operations that qualify as "attacks."[32] These questions are therefore of crucial significance.

The first matter that must be examined in order to answer these questions is whether the principle of distinction is limited only to attacks or whether it covers a wider range of operations. If it is primarily attacks that are covered, then it will be necessary to examine whether cyber operations might constitute attacks as understood in LOAC. Article 48 of Additional Protocol I sets out the following underlying "basic rule": 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 and military objectives and accordingly shall direct their operations only against military objectives."[33]

This appears to cast a wide net that could include most cyber operations. However, it has been noted by Schmitt that most of the specific rules

---

might have the potential to cross the threshold of international armed conflict." TALLINN MANUAL, *supra* note 21, cmt. to rule 22, ¶ 15.

31. DÖRMANN, *supra* note 18, at 2; Schmitt, *supra* note 30, at 102.

32. TALLINN MANUAL, *supra* note 21, rule 37, cmt. to rule 37, ¶ 2.

33. Additional Protocol I, *supra* note 2, art. 48.

within the relevant section of the Protocol speak not of any operations, but of attacks.[34] There is a debate as to the ways in which the reference to military "operations"—as opposed to a potentially narrower concept of "attack"—provides protection to the civilian population in the cyber context.[35] Notwithstanding that debate, the current analysis focuses on the applicability of the concept of attack to cyber operations because of its paramount importance in the specific rules on targeting and military objectives. In the context of lawful targets, Article 52 states that "[c]ivilian objects shall not be the object of *attack* or of reprisals" and that "[a]*ttacks* shall be limited strictly to military objectives."[36] This too appears to confine the rule to attacks, rather than any operations. This line of reasoning by Schmitt also notes that there are forms of operations, such as psychological operations conducted by militaries, which do not amount to attacks and which may proceed even if targeted at the civilian population.[37]

Article 49 of the Protocol defines "Attacks" as "acts of violence against the adversary, whether in offence or in defence."[38] The reference to violence is also included in the *Commentary* to the Protocol, in relation to the concept of military operations.[39] This leads Schmitt to note the following:

> That Additional Protocol I and its official commentary define both operations and attacks by reference to the notion of violence further strengthens the conclusion that application of the principle of distinction generally depends on an attack having occurred and that an attack is an action during armed conflict that is violent in nature.[40]

Where does this leave cyber operations—might they be considered attacks, and, if not, are they exempt from the principle of distinction, leaving a free choice of targets? One argument, proposed by Dörmann, is that

---

34. Schmitt, *supra* note 30, at 91–93.

35. See the examination of this issue in DINNISS, *supra* note 6, at 196–202.

36. Additional Protocol I, *supra* note 2, art. 52 (emphases added).

37. "[U]nless they cause physical harm or human suffering." Schmitt, *supra* note 30, at 91.

38. Additional Protocol I, *supra* note 2, art. 49(1).

39. "Finally, 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." COMMENTARY ON THE ADDITIONAL PROTOCOLS, *supra* note 4, ¶ 1875.

40. Schmitt, *supra* note 30, at 93.

> [t]he 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]

But this approach has been countered by Schmitt, noting that the definition of military objectives, from which the neutralization possibility is taken, applies in the context of an attack, and if the cyber operation is not an "attack" as understood in the *ius in bello* then there is actually no need to reach for the military objective definition at all.[42] Although according to this view the requirement for a violent component would rule out certain cyber operations, it would not exclude them all. For an act to be violent in this context, it does not necessarily require a physically violent means of delivery: "'Violence' merely constituted useful prescriptive shorthand for use in rules designed to shield the population from harmful effects. Despite being styled as act-based norms (violence), they are in fact consequence-based."[43] Indeed certain cyber operations—such as in the earlier mentioned examples of taking over missile control systems or dams—can lead to violent effects, and there should be no doubt as to the inclusion of such operations in the rules on attacks. However, this position would exclude many other types of cyber operations from the rules on attacks if their effects do not include casualties or physical damage to objects. Otherwise, it is argued, we could end up ruling that any inconvenience to civilians is prohibited.[44] Cyber operations are thereby presented as often more akin to psy-

---

41. DÖRMANN, *supra* note 18, at 6.

42. Schmitt, *supra* note 30, at 95–96.

43. *Id.* at 93. The *Tallinn Manual* addresses this point as follows:

> "Acts of violence" should not be understood as limited to activities that release kinetic force. This is well settled in the law of armed conflict. In this regard, note that chemical, biological, or radiological attacks do not usually have a kinetic effect on their designated target, but it is universally agreed that they constitute attacks as a matter of law.

TALLINN MANUAL, *supra* note 21, cmt. to rule 30, ¶ 3 (citing Prosecutor v. Tadić, Case No. IT-94-1-l, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, ¶¶ 120, 124 (Int'l Crim. Trib. for the former Yugoslavia Oct. 2, 1995)). *See also Nuclear Weapons, supra* note 4.

44. State practice provides no support for the notion that causation of inconvenience is intended to be prohibited in [international humanitarian law]. On the contra-

chological operations that do not have violent effects, and which would then be permissible even when directed at the civilian networks.[45]

In principle, this analysis is sound and on solid ground. Clearly there are some cyber operations with effects that are equal to any other attack and must therefore be conducted within the LOAC rules on lawful targets. It is equally evident that there may be cyber operations that have no real harmful effect even if directed at civilian networks. There is however, room for significant debate as to where the dividing line lies between these two descriptions and what is the threshold of harm that leads us into the former, requiring adherence to the principle of distinction in choosing targets. In particular, there is a question over the use of physical harm as the threshold.

First, however, a note of caution is perhaps warranted with regard to the analogy between cyber operations and psychological operations, such as disseminating propaganda. The latter operations might be directed at the civilian population by, for example, issuing calls attempting to convince them to abandon support for their leadership:

> The mission of PSYOP is to influence the behavior of foreign target audiences (TAs) to support U.S. national objectives. PSYOP accomplish this by conveying selected information and/or advising on actions that influence the emotions, motives, objective reasoning, and ultimately the behavior of foreign audiences.[46]

Such operations are not considered to be ones that cause direct harm to the civilian population and, as such, can be excluded from certain restrictions placed on attacks.[47] They are therefore a very useful demonstration of how certain types of operations might target the civilian population and remain lawful. But it is less clear that they are the most adequate analogy for cyber operations. The nature of such psychological operations is to convince rather than to create pressure through harm, other than perhaps lowering morale. Cyber operations are, in contradistinction, more often designed

---

> ry, inconvenience and interference with the daily lives of civilians are a frequent result of armed conflict and psychological operations directed against the civilian population are common.

Schmitt, *supra* note 30, at 95.

45. *Id.* at 92.

46. Headquarters, Department of the Army, FM 3-05.30, MCRP 3-40.6, Psychological Operations (2005), *available at* http://www.fas.org/irp/doddir/army/fm3-05-30.pdf.

47. TALLINN MANUAL, *supra* note 21, cmt. to rule 31, ¶ 5 and associated footnotes.

with some form of harmful effect in mind (including relatively low levels of harm, such as denial of service operations to disable a website), even if not always measurable in casualties. There is a difference between morale and harm. Outside of propaganda, what type of analogy might we make with cyber operations directed at civilian networks? If they are designed to change the behavior of the civilian population through adverse pressure, then anything that actively targets civilian networks will likely be causing some type of harm, which may cause it to cross the threshold into what we consider attacks. Other types of operations directed at civilian networks will need to be examined individually and their expected effects must be assessed before making any determination. In other words, it is not that cyber operations are akin to psychological operations because of the cyber format; rather, it is that some specific cyber operations are analogous because their method and produced effect are no more harmful than psychological propaganda operations (for example, during the Russia-Georgia conflict Georgian websites were defaced and made to portray images of President Saakashvili together with a range of dictators).[48] This type of cyber operation has been described as follows: "Another use of cyber war is to send propaganda out to demoralize the enemy, distributing emails and other Internet media in place of the former practice of dropping pamphlets."[49] But this is not true of all cyber operations; therefore a general analogy between cyber operations and psychological ones is too sweeping a generalization that risks minimizing the need to examine the effects of the cyber operations.

III. THE THRESHOLD OF HARM

What then is the threshold of harm that would lead cyber operations to be categorized as attacks subject to the LOAC principle of distinction? There appears to be wide agreement that cyber operations that result in casualties or physical property damage may be categorized as attacks.[50] There is, however, strong reason to question whether physical damage is the most appropriate threshold. Even if such an approach adheres to a stricter reading of the violence requirement, it should be noted that the concept of vio-

48. *See* TIKK, KASKA & VIHUL, *supra* note 7, at 71.

49. CLARKE & KNAKE, *supra* note 6, at 11. The authors also describe the case of the U.S. military sending e-mails to Iraqi officers prior to the U.S. invasion, urging them to abandon their posts and equipment, which many then duly did. *Id.* at 9–10.

50. TALLINN MANUAL, *supra* note 21, rule 30, cmt. to rule 30.

lence is not only physical, but can, for example, include mental suffering.[51] This is well documented in other areas, such as the prohibition of torture, where a wide range of non-physical actions are said to cross the boundary into prohibited torture and ill-treatment due to their severe adverse mental effects.[52] Of course, this is not presented here in order to argue that all cyber operations would fall within this area; it is hardly the case that cutting off the civilian population from their e-mail access would cause mental distress at the level of ill-treatment (although that might be true for some of us). Nevertheless, it serves to demonstrate that when looking at the possible violent effects of a cyber operation in order to ascertain whether it should be considered an attack, we do need to look wider than physical casualties and destruction. In other words, the dividing line is neither the format of the attack nor the physical violence involved, but rather the level of harm caused. It must be stressed at this point that the argument here is not that absolutely any harm would render an operation as being within the definition of attacks. It is clear that there is a threshold that must be crossed, but there is good reason to question whether physical damage is the only possible test for crossing the threshold.

We return, therefore, to the questions surrounding the qualification of cyber operations as attacks—or not—on the basis of their effects. An interesting debate in this regard has emerged through the process surrounding the drafting of the *Tallinn Manual*. There appears to be an emerging view among experts that one of the defining criteria could be the level of effect on the functionality of the targeted object. According to this approach, if the functionality is impaired to the point that it requires replacement of physical components, then this would constitute damage as envis-

51. "While the notion of attack extends to injuries and death caused to individuals, it is, in light of the law of armed conflict's underlying humanitarian purposes, reasonable to extend the definition to serious illness and severe mental suffering that are tantamount to injury." *Id.*, cmt. to rule 30, ¶ 8.

52. This can include mock executions, threats of physical violence, exploitation of the phobias of detainees, and more. The prohibition on causing serious mental suffering or psychological violence has been affirmed in a number of cases at the European, Inter-American and UN human rights bodies, as well as the International Criminal Tribunal for the former Yugoslavia. See analysis and cases cited in NIGEL S. RODLEY & MATT POLLARD, THE TREATMENT OF PRISONERS UNDER INTERNATIONAL LAW 140–43 (3d ed. 2009).

aged in the concept of attack.[53] This approach is not so much a compromise between the earlier mentioned views, but more of a fine-tuning of the idea that for an operation to be an attack, it must cause casualties or damage—and in this case allowing for functionality to be a test for damage or property destruction. If the test still requires there to be physical components that must be replaced, then it ultimately remains very much tied in to the notion of physical property damage.

This insistence on remaining focused on physical property is, however, a position that may require rethinking. A functionality test that requires physical effects would include as an attack a cyber operation that damages a computer system that can be repaired in under an hour by replacing one part, but it would exclude a cyber operation that incapacitates a whole system for two days if there is no physical damage or repair other than waiting for the operation to be over. Moreover, consider this: insisting on physical damage means that blocking enemy communications by physically sabotaging the lines or bombing the telephone or fiber-optic cables would be an attack, but blocking the same communications through cyber operations causing data corruption that does not physically damage property or require replacement of parts is not an attack. What is the basis for this differentiation? The objective sought, the military advantage gained and the effects of the operations will be almost identical. Surely it is not because one requires physically repositioning a telephone pole and the other does not? This seems like an arbitrary distinction that does not take account of modern reality.

This issue is also linked to another question which we face when looking at the definition of military objectives, as it appears in the first Additional Protocol:

> Attacks shall be limited strictly to military objectives. In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.[54]

---

53. TALLINN MANUAL, *supra* note 21, rule 30, cmt. to rule 30, ¶ 10. There was also a subgroup of experts who held the view that this should include loss of functionality that can be restored through reinstalling an operating system.

54. Additional Protocol I, *supra* note 2, art. 52(2).

The problem that arises, which is relatively unique to cyber operations, is whether data can be considered an object. While there is no definitive answer to this question, the currently prevailing view among LOAC experts appears to hold that in most cases data, for the purposes of LOAC targeting, should not be considered an object.[55] This reasoning is said to be supported by well-established interpretations of LOAC, as found in the International Committee of the Red Cross's *Commentary* to the Protocol.[56] According to this *Commentary*, the term "object" refers to something which is "visible and tangible."[57] This, *prima facie*, certainly does not seem to include data. But there is good reason to consider this issue further, and raise the possibility that data may nevertheless be akin to an object in this context. The reference to "visible and tangible" is not part of the Protocol definition, but rather the understanding given to it at a particular point in time and in a specific context. These must be examined more closely to see whether the same reasoning applies to our current situation. At the time of drafting it is unlikely that the drafters would have considered the possibility of data destruction separate from physical damage. Destroying data at the time would have meant physically damaging the storage method, such as the paper files. Today, however, it is perfectly possible to destroy vast quantities of vital data without physically destroying the computers on which they are stored. To place this in context, it raises the question whether a kinetic attack that results in the setting on fire of five hundred mailbags is any more harmful than a cyber operation that permanently deletes five million e-mails. This is a scenario that could hardly have been contemplated when the *Commentary* made the reference to objects being "visible and tangible." Looking beyond this specific phrase into the explanation surrounding its use further reveals why it might not exclude data. While the phrase "visible and tangible" is used to discuss what was being included, it is equally important to see what it was that was being excluded. In fact, the reference to tangible objects is made in order to distinguish ob-

---

55. "The majority of the International Group of Experts agreed that the law of armed conflict notion of object should not be interpreted as including data." TALLINN MANUAL, *supra* note 21, cmt. to rule 38, ¶ 5. Relatively uncontroversial exceptions include cases where the attack on data leads to casualties or physical damage—in which case it can be said that the object of attack was that which was ultimately harmed. *See id.*, cmt. to rule 30, ¶ 6. Schmitt recognizes certain exceptions, but argues that "[g]enerally, data should not be characterized as an object in itself." Schmitt, *supra* note 30, at 96.

56. TALLINN MANUAL, *supra* note 21, cmt. to rule 38, ¶ 5.

57. "It is clear that in both English and French the word means something that is visible and tangible." COMMENTARY ON THE ADDITIONAL PROTOCOLS, *supra* note 4, ¶ 2008.

jects from the very different concept of "general objective (in the sense of aim or purpose) of a military operation."[58] Consequently, it is, therefore, at least arguable that computer data is closer to what the drafters wanted to include as objects than to the notion of what they wanted to exclude as aim or purpose. Indeed, domestic legal systems have demonstrated the ability to evolve beyond physical conceptions of damage to recognize that, rather than physical damage to a computer system, the focus should be on the harm to the contents of the system—data included.[59]

The question of destroying data raises a further matter, the relevance of existing backup data. It might be argued that one of the reasons to exclude data from the rules on attacks is that damage has not occurred if the data can be retrieved. First, however, it should be noted that if this is the argument against viewing data as an object, it does, in fact, allow for *irretrievable* data to be classified as within the rules on attacks. Second, one may question whether potential restoration capability is the correct test for determining the nature of the object and the lawfulness of targeting it. This is not the test we use for physical property. In fact, most physical property is not irretrievable—buildings can be rebuilt, cars can be remanufactured; it is often just a question of cost. Restoration of complex digital data might be restorable from a backup, but this too has a cost. Why is causing one costly act more lawful than the other, and is it just a question of the degree of time and money involved? Perhaps the key here is that data can be backed up so that there are multiple copies, in which case it might be claimed that destroying one copy is not really harmful or damaging since copies exist elsewhere. But how is the attacker to know this? If this is the argument, would the rules on taking precautions require verification of the existence of backup copies?[60] Moreover, once again it is useful to compare this sce-

58. *Id.*, ¶ 2010. See a similar analysis by Dinniss of what the commentators meant to exclude, leading her to note that "any computer program, database, system or virtual network would still be a legitimate target if it meets the above definition, regardless of whether it has a tangible component or exists purely as lines of code." DINNISS, *supra* note 6, at 185.

59. This is evident from the wording of the Computer Misuse Act, 1990, c. 18 (Eng.) and the Police and Justice Act, 2006, c. 48 (Eng.). *See also* R. v. Victor Lindesay, [2001] EWCA (Crim) 1720; R. v. Simon Lee Vallor, [2003] EWCA (Crim) 2288; Regina v. Steven Parr-Moore, [2002] EWCA (Crim) 1907.

60. Additional Protocol I, *supra* note 2, art. 57. Note that this creates an additional problem, since if this argument claims that data destruction is not an attack, one might then say that the rules on precautions in attack do not apply, which would in turn leave us without the rules on verification.

nario to a non-data situation: if a paper document facility or a library is destroyed, do we say it was not an attack because there are copies of the same books in another facility or library? Why treat computer data differently?

Notwithstanding the above, this argument will take on a different shape in the context of cultural objects. It is possible that digital archives might be considered cultural property,[61] and as such benefit from added protections to objects of this type.[62] In this context, backup copies may well play a role, since the uniqueness of an object will often be one of the reasons behind its cultural property protection. If, therefore, it is verifiable and known that additional and equal copies exist and that they will remain unharmed, it may be that a digital item might not benefit from the special protection.[63] But the relevance of backup copies is considered here only in the context of the applicability of extra protections for unique items of cultural value; the general rules on attacking objects should not—as demonstrated above—be affected by this.

There are, of course, limits to the analogies that can be made between the cyber sphere and the physical world. For example, just as we hold discussions of data as objects, some might also question whether computer network systems are considered to be part of the infrastructure of a State; this in turn may lead to a claim that taking over the network infrastructure of a State is akin to taking over its territory.[64] Considering that we have already seen arguments being made in the context of Gaza that a State should be considered an occupying power due to control exerted from the outside and without boots on the ground,[65] might we one day see arguments calling for the obligations stemming from the laws of occupation to be applied to occupation through control of network infrastructure? This

---

61. See examples in the TALLINN MANUAL, *supra* note 21, cmt. to rule 82, ¶ 5.

62. Convention for the Protection of Cultural Property in the Event of Armed Conflict, May 14, 1954, 249 U.N.T.S. 240; Second Protocol to the Hague Convention of 1954 for the Protection of Cultural Property in the Event of Armed Conflict art. 22, Mar. 26, 1999, 2253 U.N.T.S. 212.

63. See discussion in TALLINN MANUAL, *supra* note 21, cmt. to rule 82, ¶ 6.

64. *But see id.*, ch. VI, ¶ 3 ("[C]yber operations cannot alone suffice to establish or maintain the degree of authority over territory necessary to constitute an occupation.").

65. The debate over the status of Gaza contains some genuinely complex questions as to the definition, nature and purpose of the laws of occupation. For an examination of some of these issues, see, e.g., Yuval Shany, *Faraway, So Close: The Legal Status of Gaza after Israel's Disengagement*, 8 YEARBOOK OF INTERNATIONAL HUMANITARIAN LAW 2005, at 369–83 (2005). See also the opinions expressed in SARI BASHI & KENNETH MANN, DISENGAGED OCCUPIERS: THE LEGAL STATUS OF GAZA (2007), a*vailable at* http://www.gisha.org/UserFiles/File/Report%20for%20the%20website.pdf.

sounds extremely far-fetched, and probably rightly so. As the *Tallinn Manual* correctly points out, "[t]here is no legal notion of occupation in cyberspace."[66] The creation of such a notion is *not* an argument being proposed or supported here; its possibility is simply being raised as a warning sign of things to come.

However, just as the attempts to apply the law to cyber realities might be stretched beyond credibility, equally, attempts to resist updated interpretations will result in stagnant and even obsolete rules. To avoid both misapplication and obsolescence, we must accept that the law cannot forever be interpreted and applied in exactly the same manner, lock, stock and barrel. If we wish to ensure the relevance of the rules to the twenty-first century, it is vital that they are interpreted in light of modern reality. Proposing new interpretations is not the same as saying the law itself is inadequate to deal with new challenges. While there are times that new laws are deemed necessary to confront contemporary battlefield realities,[67] at other times we may be able to rely on the existing body of international law for many of the current and future challenges, just as its general principles have been deemed applicable to numerous technological advances during the past century:

> Indeed, nuclear weapons were invented after most of the principles and rules of humanitarian law applicable in armed conflict had already come into existence; the Conferences of 1949 and 1974–1977 left these weapons aside, and there is a qualitative as well as quantitative difference between nuclear weapons and all conventional arms. However, it cannot be concluded from this that the established principles and rules of humanitarian law applicable in armed conflict did not apply to nuclear weapons. Such a conclusion would be incompatible with the intrinsically humanitarian character of the legal principles in question which permeates the entire law of armed conflict and applies to all forms of warfare and to all

66. TALLINN MANUAL, *supra* note 21, ch. VI, ¶ 3.

67. A clear example of these is the adoption of the 1977 Additional Protocols to the 1949 Geneva Conventions, which contained rules designed to cover developments on the battlefield in relation to means, methods and participants in combat. *See also Nuclear Weapons*, *supra* note 4, ¶ 76 ("Since the turn of the century, the appearance of new means of combat has—without calling into question the longstanding principles and rules of international law—rendered necessary some specific prohibitions of the use of certain weapons, such as explosive projectiles under 400 grammes, dum-dum bullets and asphyxiating gases. Chemical and bacteriological weapons were then prohibited by the 1925 Geneva Protocol.").

> kinds of weapons, those of the past, those of the present and those of the future.[68]

There should be no doubt that existing law can apply to the cyber sphere, but there must be room for new approaches and interpretations that might differ from the manner in which the same law was read in the past.[69] The earlier discussion of considering data as an object for the purpose of targeting rules is a case in point. The law itself does not exclude the possibility; rather, those who exclude data do so by relying on past interpretations of the law that were necessarily wedded to the time.[70] Instead, it is perfectly possible to remain true to the object and purpose of the law—and indeed to the letter of the law itself—by interpreting it in light of the modern-day context in which it is being implemented.[71] This is therefore a call for new interpretations in light of reality, and not a call to overhaul the law itself.[72] In the context of cyber operations, this requires rethinking the nature of harm required for crossing the threshold into actions that are regulated by the rules on attacks. Rather than focus on the *type* of harm, the focus should be on the *level* of harm, regardless of whether or not the effects are caused through physical destruction. Massive deletion of data from institutional archives (e.g., educational institutions, local councils, government offices) is an example of an act which can cause a significant

---

68. *Id.*, ¶ 86.

69. See, for example, the White House International Strategy for Cyberspace:

> The development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace. Nonetheless, unique attributes of networked technology require additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them.

THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 9 (2011), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

70. *See, e.g.*, referring to objects as "visible and tangible." *See supra* text accompanying note 57.

71. The first rule on the interpretation of treaties states 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*." Vienna Convention on the Law of Treaties art. 31.1, May 23, 1969, 1155 U.N.T.S. 331 (emphasis added).

72. There are, however, also arguments being made for creating new laws to regulate cyber operations. See, e.g., the call for a new framework of "international law for information operations" in Duncan B. Hollis, *Why States Need an International Law for Information Technology*, 11 LEWIS & CLARK LAW REVIEW 1023 (2007).

level of harm without leading to physical destruction or casualties. These should at the least be considered as having crossed the threshold so as to be regulated by the rules on attacks, and subject to the principle of distinction with regard to choice of targets.

The above questions on the categorization of operations as attacks must also be viewed in light of the underlying concerns behind some of the positions. Much of this debate is occurring in the context of excluding certain operations from the definition of attacks so that they will not be hampered by the restrictions placed in LOAC, and so that we do not end up describing any disruption to civilian networks as unlawful.[73] But this concern is, to a certain extent, misplaced. Note that we are seeking to examine the categorization of operations *directed* against civilian networks, and *not* about operations against so-called dual-use networks.[74] *Directing* operations against civilian networks *intending* to cause negative effects for the civilian population should not be an encouraged military activity, and by ensuring that these operations are considered attacks, we can afford better protection to civilians. At the same time, having a lower threshold of toleration for operations against pure civilian networks should not have a detrimental effect on military needs—it does *not* prevent attacks on dual-use networks, which could be legitimate military objectives.[75] If the primary concern is the latter, then this debate is misplaced since defining the operation as an attack would still allow for the target to be a legitimate military objective. The primary concern would then be the separate matter of indiscriminate attacks or collateral damage, and whether the harm caused to the civilians is acceptable disruption or rises to the level of damage that tips the balance in the proportionality formula—but these are separate questions from our current focus on the lawfulness of choosing a particular target.[76]

A final point on whether cyber operations are "attacks" is a reminder that in other contexts States have rightly clarified that when analyzing the legality of an attack, one must look at the attack as a whole,[77] recognizing

---

73. Schmitt, *supra* note 30, at 95.

74. Note that under LOAC there is no specific rule for categorizing objects as dual-use. They are either a military objective or not. The fact that a military objective may be used for civilian purposes does not remove its status as a military objective, but will have consequences with regard to the precautions, and means and methods employed, which can then in turn determine the lawfulness of the attack.

75. Schmitt, *supra* note 30, at 96.

76. For issues relating to how an attack may be carried out, see *supra* note 18.

77. For example, see the statement of the United Kingdom on Articles 51 and 57 upon ratification of Additional Protocol I that "the military advantage anticipated from an

that a specific operation might be "part of the complex mosaic of a bigger integrated operation."[78] To apply this to the question at hand, if a cyber operation that alone might not have been described as an attack is, in fact, an inherent component in a collection of operations that form a single attack, then this cyber operation must be assessed within the laws applicable to attacks,[79] including the question of its target. For example, disabling a communications network for a few hours might not seem to cause serious harm, but if this is carried out in order to mask other activity that enables a devastating attack to occur while the enemy cannot communicate then clearly the cyber operation was part of the attack.[80] Again, as noted in the previous point, this does not place undue restrictions on the cyber operation if its target is indeed a military communications system.

Notwithstanding all the above, and while it has been argued above that there is a need to reconsider the threshold of harm in light of the potential for serious non-physical harm, by definition having a threshold means that there will be a possibility for certain circumstances to remain below it. Accordingly, there will be certain cyber operations that do not reach the required threshold (e.g., cyber operations that are propaganda/psychological operations) and which would not constitute an "attack" as defined in the law. If so, then the law of armed conflict might not prohibit such an operation even if directed at a civilian network. We should, however, remember that the law of armed conflict is far from being the only legal framework in existence. Such operations would not take place in a legal black hole; indeed, much attention has been given in recent years to the risks created by claiming legal vacuums.[81] Depending on the precise circumstances, a host of other laws might apply, ranging from telecommunication laws,[82] princi-

attack is intended to refer to the advantage anticipated from the attack considered as a whole and not only from isolated or particular parts of the attack." International Committee of the Red Cross, Reservation/Declaration Text, http://www.icrc.org/ihl.nsf/NORM/0A9E03F0F2EE757CC1256402003FB6D2?OpenDocument%20 (last visited Nov. 19, 2012).

78. Stefan Oeter, *Methods and Means of Combat*, *in* THE HANDBOOK OF HUMANITARIAN LAW IN ARMED CONFLICTS 105, 162 (Dieter Fleck ed., 1995).

79. TALLINN MANUAL, *supra* note 21, cmt. to rule 30, ¶ 16.

80. For an example of combining cyber operations as an element leading to physical attack, see the description of the Israeli attack on the Syrian alleged nuclear facility in CLARKE & KNAKE, *supra* note 6, at 1–8.

81. Most notably in the debates surrounding the applicability of international humanitarian law and human rights law to actions taken in the "war on terror."

82. International Telecommunication Convention, Nov. 6, 1982, S. TREATY DOC. NO. 6, 99th Cong., 1st Sess. (1985); Optional Protocol on the Compulsory Settlement of

ples of non-intervention,[83] outer space treaties[84] and human rights law[85] to domestic criminal law or international agreements on cyber crime.[86] The applicability of these branches of law will vary from case to case based on the precise circumstances, and they may themselves be subject to debate (an obvious example of debate is the disagreement over extraterritorial applicability of international human rights law).[87] However, they cannot be ignored and their applicability must at least be considered. This is, in fact, not only the case when LOAC does not apply to the operations; indeed, some of these branches of law may well apply also during armed conflict, though once again this will depend on the specific branch of law under discussion, and the interplay between it and LOAC will need to be taken into account.[88]

Disputes Relating to the Constitution of the International Telecommunication Union, to the Convention of the International Telecommunication Union and to the Administrative Regulations, Dec. 22, 1992, S. TREATY DOC. NO. 104-34, 104th Cong., 2nd Sess. (1996).

83. For example, under the Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, G.A. Res. 2625, Annex, U.N. GAOR, 25th Sess., Supp. No. 28, U.N. Doc. A/8028, at 121 (Oct. 24, 1970).

84. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, Jan. 27, 1967, 610 U.N.T.S. 205. See discussion of applicability of outer space treaties in James P. Terry, *The Lawfulness of Attacking Computer Networks in Armed Conflict and in Self-Defense in Periods Short of Armed Conflict: What Are the Targeting Constraints?*, 169 MILITARY LAW REVIEW 70, 87–88 (2001).

85. International Covenant on Civil and Political Rights, G.A. Res. 2200A (XXI), U.N. Doc. A/6316 (Dec. 16, 1966), 999 U.N.T.S. 171; International Covenant on Economic, Social and Cultural Rights, G.A. Res. 2200A (XXI), U.N. Doc. A/6316 (Dec. 16, 1966), 993 U.N.T.S. 3.

86. Convention on Cybercrime, Nov. 23, 2001, Europ. T.S. No. 185.

87. LUBELL, *supra* note 22, ch. 8.

88. The interplay between the law of armed conflict and international human rights law has been subjected to extensive scrutiny, albeit not yet resolved. *See, e.g.*, Cordula Droege, *The Interplay Between International Humanitarian Law and International Human Rights Law in Situations of Armed Conflict*, 40 ISRAEL LAW REVIEW 310 (2007); Nancie Prud'homme, Lex Specialis: *Oversimplifying a More Complex and Multifaceted Relationship?,* 40 ISRAEL LAW REVIEW 356 (2007); Françoise J. Hampson, *Is Human Rights Law of Any Relevance to Military Operations in Afghanistan?*, *in* THE WAR IN AFGHANISTAN: A LEGAL ANALYSIS 485 (Michael N. Schmitt ed., 2009) (Vol. 85, U.S. Naval War College International Law Studies); Noam Lubell, *Challenges in Applying Human Rights Law to Armed Conflict*, 87 INTERNATIONAL REVIEW OF THE RED CROSS 737 (2005); U.N. Econ. & Soc. Council, Comm'n on Human Rights, Subcomm. on the Promotion & Protection of Human Rights, Françoise J. Hampson & Ibrahim Salama, *Administration of Justice, Rule of Law and Democracy:*

IV. CONCLUSION

Cyber operations taking place during armed conflict can present a number of challenges in discerning the correct legal framework for their regulation. Notably, they are an awkward fit for the rubric of laws relating to attacks, as these were clearly designed with the primary focus on kinetic attacks. In particular, there is the possibility that excluding cyber operations from the notion of attack would thereby release these operations from the requirement to adhere to the principle of distinction in the choice of targets—one of the fundamental principles at the heart of the law of armed conflict. Clearly, cyber operations that lead to direct physical damage or casualties must be considered attacks. Likewise, those cyber operations that amount to no more than propaganda and cause no actual harm might lie outside the notion of attacks. This article has argued, however, that the dividing line between these two poles cannot rely on the physical nature of the harm caused. Rather, the key criteria for the threshold at which an operation must be regarded as an attack under the law of armed conflict must rest on the level of harm caused, and this can include non-physical damage. Such an understanding does not require new laws, but can be a legitimate interpretation of the current law, in line with both its object and purpose, and a better reflection of modern reality.

Working Paper on the Relationship Between Human Rights Law and International Humanitarian Law, 57th Sess., U.N. Doc. E/CN.4/Sub.2/2005/14 (June 21, 2005).