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

Cyber Attacks: Proportionality and Precautions in Attack

Eric Talbot Jensen

89 INT'L L. STUD. 198 (2013)

Volume 89 2013

Cyber Attacks: Proportionality and Precautions in Attack

Eric Talbot Jensen[*]

I. INTRODUCTION

When David Sanger[1] and Ellen Nakashima[2] officially broke the news that the United States and Israel had been involved in a long-term collaborative cyber operation focused on Iran and its nuclear development capabilities, they only confirmed what many had assumed for some time.[3] In

* Associate Professor, Brigham Young University Law School. The author wishes to thank Brooke Robinson and Brigham Udall for their exceptional research assistance.

1. David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, NEW YORK TIMES, June 1, 2012, at A1, *available at* http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0; *see also* DAVID E. SANGER, CONFRONT AND CONCEAL: OBAMA'S SECRET WARS AND SURPRISING USE OF AMERICAN POWER (2012).

2. Ellen Nakashima, Greg Miller & Julie Tate, *U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say*, WASHINGTON POST (June 19, 2012), http://articles.washingtonpost.com/2012-06-19/world/35460741_1_stuxnet-computer-virus-malware.

3. William J. Broad, John Markoff & David E. Sanger, *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, NEW YORK TIMES, Jan. 15, 2011, at A1, *available at* http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html; Tucker Reals, *Stuxnet Worm a U.S. Cyber-Attack on Iran Nukes?*, CBS NEWS (Sept. 24, 2010, 6:41 AM), http://www.cbsnews.com/8301-501465_162-20017507-501465.html; *A worm in the centri-*

fact, with the discovery of Stuxnet in 2010, many scholars and practitioners had speculated on whether the use of the Stuxnet malware, if State sponsored, amounted to a "use of force" or even an "armed attack" under the UN Charter paradigm.[4]

Some even began to consider the hypothetical legality of Stuxnet-type cyber actions within an armed conflict as opposed to a use of force or armed attack that would initiate an armed conflict. For these writers, the major issues revolved around the cyber tool's compliance with the law of armed conflict (LOAC) and principles such as discrimination and proportionality. For example, Jeremy Richmond analyzed Stuxnet in light of these principles and concluded that whoever designed the malware did so with the clear intent to comply with the LOAC.[5]

Even prior to the discovery of Stuxnet, a group of legal and technical experts[6] were gathered by the Estonian Cooperative Cyber Defence Centre of Excellence to draft a manual, known as the *Tallinn Manual on the International Law Applicable to Cyber Warfare*.[7] The *Manual* explores the international law governing the use of force—in both its *jus ad bellum* and *jus in bello* aspects[8]—as applied to cyber operations conducted by States and non-State actors. Several key principles arose during the *Manual* discussions in relation to the principles of proportionality and precautions in and against attack, including a number of challenging aspects in applying these principles

---

fuge, ECONOMIST, Oct. 2, 2010, at 63, *available at* http://www.economist.com/node/17147818.

4. Gary D. Brown, *Why Iran Didn't Admit Stuxnet Was an Attack*, JOINT FORCE QUARTERLY, Oct. 2011, at 70, *available at* http://www.ndu.edu/press/lib/images/jfq-63/JFQ63_70-73_Brown.pdf; Chance Cammack, Comment, *The Stuxnet Worm and Potential Prosecution by the International Criminal Court Under the Newly Defined Crime of Aggression*, 20 TULANE JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW 303, 320–23 (2011); John Richardson, *Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield*, 29 JOHN MARSHALL JOURNAL OF COMPUTER & INFORMATION LAW 1, 9–11 (2011).

5. Jeremy Richmond, Note, *Evolving Battlefields: Does STUXNET Demonstrate a Need for Modifications to the Law of Armed Conflict?*, 35 FORDHAM INTERNATIONAL LAW JOURNAL 842, 883–93 (2012).

6. The author was a member of the group.

7. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL].

8. The *jus ad bellum* regulates the laws of conflict management, or the laws governing going to war. The *jus in bello* regulates activities once armed conflict has begun. Though some terms are similar in both bodies of law, they are considered separate and distinct under the current armed conflict paradigm.

to cyber warfare. This article will discuss some of those interesting challenges.

Part II of the article will focus on the constant-care standard and how it applies to all cyber operations. Part III will look at the principle of proportionality with specific focus on the idea of indirect effects. Part IV analyzes the issue of feasibility with the precautionary standards. Part V analyzes State responsibilities under the obligation to take precautions against the effects of attacks. The article will conclude in Part VI.

A. Attack

Before embarkation on the above-mentioned analysis, some brief comments are necessary concerning the definition of "attack." With the exception of Part II, which deals with the constant-care standard, the legal standards discussed below apply to an "attack." Many LOAC principles apply only to situations of attack, such as the principle of proportionality. The idea of taking precautions in the attack assumes that there is an attack. The fundamental nature of "attack" underlies many of the LOAC principles that govern cyber warfare, making it important to come to some understanding of the meaning of the word.

Paul Walker was one of the first to address this issue directly, in his article "Rethinking Computer Network 'Attack.'"[9] He notes that the word "attack" is defined in the 1977 Additional Protocol I (API) to the Geneva Conventions as "acts of violence" and states that this definition has become customarily binding even on non-parties to the Protocol.[10] As a result, Walker argues that very few activities in cyber warfare will actually amount to an attack and will therefore not be governed by the principles of attack, such as proportionality.

The meaning of "attack" was also vigorously debated by Michael Schmitt,[11] Chairman of the International Law Department of the U.S. Naval War College and leader of the *Tallinn Manual* project, and Knut Dörmann, representative of the International Committee of the Red Cross

9. Paul A. Walker, *Rethinking Computer Network "Attack": Implications for Law and U.S. Doctrine*, 1 NATIONAL SECURITY LAW BRIEF 33 (2011), *available at* http://digitalcommons.wcl.american.edu/nslb/vol1/iss1/3.

10. *Id.* at 34.

11. Michael N. Schmitt, *Wired Warfare: Computer Network Attack and* Jus in Bello, 84 INTERNATIONAL REVIEW OF THE RED CROSS 365, 374–79 (2002), *available at* http://www.icrc.org/eng/assets/files/other/365_400_schmitt.pdf.

(ICRC).[12] In Schmitt's view, an attack is something that results in death, damage, destruction or injury. Dörmann argued that anything that was aimed at civilians amounted to an "attack." These views tend to mark the extremes of the debate. The *Tallinn Manual* softened Schmitt's view somewhat by indicating that a cyber attack need not be characterized by the release of kinetic force.[13]

Resolving the debate on the definition of attack may need to wait for more State practice. It is enough for this article to state that most of the law discussed here presupposes an "attack," whatever that means. For example, in the absence of an attack, commanders are not required to apply the principle of proportionality.

B. State and Non-State Actors

In addition to the definition of "attack," another important consideration is the involvement of non-State actors in cyber operations. One of the most intriguing aspects of cyber operations is that they allow non-State actors to relatively easily harness State-level violence. This undermines the Westphalian monopoly on the use of violence as few other weapon systems have done.

Other articles in this volume will address this question more directly,[14] so little need be said here except to note that many of the standards discussed below only apply to States. To the extent that some organized armed groups might elect to be bound by LOAC principles, they would also be bound, but as a matter of law the majority of the discussion below applies to States.

12. KNUT DÖRMANN, APPLICABILITY OF THE ADDITIONAL PROTOCOLS TO COMPUTER NETWORK ATTACKS (2004), *available at* http://www.icrc.org/eng/assets/files/other/applicabilityofihltocna.pdf; Knut Dörmann, *The legal situation of "unlawful/unprivileged combatants,"* 85 INTERNATIONAL REVIEW OF THE RED CROSS 45, 46, 72–73 (2003), *available at* http://www.icrc.org/eng/assets/files/other/irrc_849_ dorman.pdf.

13. TALLINN MANUAL, *supra* note 7, rule 30.

14. For example, Michael Schmitt's article on the application of these principles to non-international armed conflict discusses non-State actors. Michael Schmitt, *Classification of Cyber Conflict*, 89 INTERNATIONAL LAW STUDIES ___ (forthcoming 2013).

II. THE "CONSTANT-CARE" STANDARD

Article 57 of Additional Protocol I is titled "Precautions in the Attack"[15] and is generally believed to be binding on States in both international armed conflict and non-international armed conflict.[16] However, the first subparagraph takes a much broader approach than just "attack." It states that "[i]n the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects."[17] The ICRC *Commentary* adds, "The term 'military operations' should be understood to mean any movements, manoeuvres and other activities whatsoever carried out by the armed forces with a view to combat."[18]

The term "military operations" is obviously meant to be much broader than the term "attack" and imposes a general legal requirement on militaries even when not attacking. The legal requirement is to exercise "constant-care," but that term is not defined either in Article 57, the ICRC *Commentary* or generally in the LOAC. While the exact application of this principle in a specific military operation must be left to the commander, it seems clear that exercising constant care would at least mean that a commander cannot ignore effects on civilian population.

In the context of cyber operations, constant care would likely require a commander to maintain situational awareness at all times, including all

---

15. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 57, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter API].

16. TALLINN MANUAL, *supra* note 7, rule 52; 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW rule 15, at 51 (Jean-Marie Henchaerts & Louise Doswald-Beck eds., 2005) [hereinafter ICRC CIL STUDY]; MICHAEL N. SCHMITT, CHARLES H.B. GARRAWAY & YORAM DINSTEIN, THE MANUAL ON THE LAW OF NON-INTERNATIONAL ARMED CONFLICT WITH COMMENTARY ¶ 2.1.2 (2006), *reprinted in* 36 ISRAEL YEARBOOK ON HUMAN RIGHTS (special supplement) (Yoram Dinstein & Fania Domb eds., 2006) [hereinafter NIAC MANUAL]; U.S. Navy, U.S. Marine Corps & U.S. Coast Guard, NWP 1-14M/MCWP 5-12.1/COMDTPUB P5800.7A, The Commander's Handbook on the Law of Naval Operations ¶ 8.1 (2007), *available at* http://www.usnwc.edu/getattachment/a9b8e92d-2c8d-4779-9925-0defea93325c/1-4M_(Jul_2007)_(NWP [hereinafter Commander's Handbook]; UNITED KINGDOM MINISTRY OF DEFENCE, THE MANUAL OF THE LAW OF ARMED CONFLICT ¶ 5.32 (2004) [hereinafter UK MANUAL]; COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, at 680 (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann eds., 1987) [hereinafter API COMMENTARY]. *See also id.* at 600 (explanation of the term "operations").

17. API, *supra* note 15, art. 57.1.

18. API COMMENTARY, *supra* note 16, at 680.

phases of the operation. When employing a cyber tool or conducting cyber operations, the commander would need to maintain oversight of the tool and be ready to adjust operations if the tool or operation began to have effects that the commander determined would have an illegal impact on civilians. This might be especially difficult in the cyber domain since virtually every cyber operation will traverse, affect, employ or damage civilian cyber infrastructure of some kind.[19]

A contemporary application of this standard occurred in the case of the infamous Stuxnet malware.[20] Evidently, it was discretely targeted at Iranian nuclear facilities, but reports show that it spread much wider than that, presumably wider than the United States and Israel[21] intended it to disseminate, which may have led to its discovery. Though no other damage was reported, the unintended spread of the virus at least implicates the constant-care standard and informs State practice on the issue.

Additionally, it appears that the Stuxnet malware was used in conjunction with another malware that has been termed "Flame." Flame was "designed to secretly map Iran's computer networks and monitor the computers of Iranian officials, sending back a steady stream of intelligence used to enable an ongoing cyberwarfare campaign."[22] Flame was discovered by Iranian officials when Israeli government hackers were carrying out operations against Iranian oil ministry and export facilities.[23]

Similar situations might lead a commander to argue that he cannot continue to monitor the network in order to exercise constant care for fear of being discovered. The LOAC allows no such exception in this case, though it does in others.[24] Therefore, it seems unlikely that a commander could

---

19. Michael McConnell, Former Director of National Intelligence, Keynote Address at the Texas Law Review Symposium: Law at the Intersection of National Security, Privacy, and Technology (Feb. 4, 2010) [hereinafter McConnell], *referred to in* Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks,* 88 TEXAS LAW REVIEW 1533, 1534 (2010).

20. Nicolas Falliere, Liam O Murchu & Eric Chien, W32.Stuxnet Dossier, Version 1.4, (Feb. 2011), http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

21. Sanger, *supra* note 1.

22. Nakashima, Miller & Tate, *supra* note 2.

23. *Id.*

24. For example, the Hague rules require the attacker to "do all in his power to warn the authorities" unless the attack is an "assault." Regulations Respecting the Laws and Customs of War on Land, annexed to Convention No. IV Respecting the Laws and Customs of War on Land art. 26, Oct. 18, 1907, 36 Stat. 2227, *available at* http://www.icrc.org/ihl.nsf/FULL/195?OpenDocument; *see also* TALLINN MANUAL, *supra* note 7, rule 58.

argue that he was relieved of his legal duty to maintain constant care for fear it might lead to discovery. Rather, commanders and all persons conducting cyber operations must recognize and accept the legal obligation to exercise constant care in all military operations, including cyber operations.

III. PROPORTIONALITY AND INDIRECT EFFECTS

The principle of proportionality is found in Article 51(5)(b) of API:[25]

> 5. Among others, the following types of attacks are to be considered as indiscriminate:
>
> . . .
>
> (b) an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.

This principle is generally accepted as customary international law in international and non-international armed conflicts and is analyzed elsewhere in great length[26] so it needs no further discussion here.

Few would argue that the principle of proportionality does not apply to cyber warfare; instead the controversy centers on its application to specific cyber operations.[27] While all cyber operations are governed by the constant-care standard, the principle of proportionality will only apply to those cyber operations that amount to an "attack." For those operations where the principle of proportionality does apply, two specific aspects of the rule deserve more detailed analysis: the understanding of "damage" and the problem of indirect effects.

---

25. *See also* Amended Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices art. 3(3), May 3, 1996, 2048 U.N.T.S. 93, 1342 U.N.T.S. 168; Second Protocol to the Hague Convention of 1954 for the Protection of Cultural Property in the Event of Armed Conflict art. 7, Mar. 26, 1999, 2253 U.N.T.S. 212.

26. *See, e.g.*, Eric Talbot Jensen, *Unexpected Consequences from Knock-On Effects: A Different Standard for Computer Network Operations?*, 18 AMERICAN UNIVERSITY INTERNATIONAL LAW REVIEW 1145, 1170–75 (2003); Richmond, *supra* note 5, at 889–93.

27. *See generally* TALLINN MANUAL, *supra* note 7, rule 51 (discussing the application of proportionality to cyber warfare).

Preliminarily, it is important to keep in mind that civilians can never be made the object of attack[28] and that the principle of proportionality limits commanders when, as the result of a lawful attack, civilians or civilian objects may be harmed. In order for such an attack to be lawful, the commander must determine that the death, injury and damage are not "excessive in relation to the concrete and direct military advantage anticipated." Though cyber attacks will inevitably have the ability to kill and injure civilians, the vast majority of known cyber operations have focused on or resulted in damage, hence the focus on the damage element of the legal standard.

Additionally, the requirement that the damage occur to civilian objects should be understood broadly. The vast majority of the Internet, including the cables, servers and routers, consists of civilian objects, which are owned, operated and maintained by civilians. Any damage to these elements of the Internet infrastructure would be considered civilian damage for purposes of the proportionality analysis.

Finally, although the drafters of 1977 Additional Protocol I certainly did not anticipate cyber warfare, they did recognize that electronic advances in technology would affect the way wars would be fought and their potential impacts on civilians. In the *Commentary*, the ICRC notes, "It was also pointed out that modern electronic means made it possible to locate military objectives, but that they did not provide information on the presence of civilian elements within or in the vicinity of such objectives."[29] Though perhaps not entirely true in cyber warfare, this idea certainly impacts the application of proportionality to cyber attacks.

A. Damage to Civilian Objects

When considering kinetic weapons that result in heat, blast and fragmentation, the issue of defining damage is less controversial. However, when cyber tools are used to conduct an attack, determining what cyber actions amount to damage becomes more problematic. There are several approaches in determining what equates to damage in the cyber domain.

One approach would be to analogize from a kinetic attack and argue that if what occurs from a cyber operation would have been considered damage if accomplished by kinetic means, then the attack amounts to dam-

28. API, *supra* note 15, art. 48.

29. API COMMENTARY, *supra* note 16, at 625.

age. The advantage to this approach is that it places commanders in a comfortable position to apply known factors. Commanders have been applying the proportionality analysis to kinetic attacks their entire careers and will likely feel quite comfortable with this analysis.

However, there are many cyber actions that would not look at all like the results of a kinetic attack. For example, simply closing a computer's specific communication port normally used to communicate with another computer, while leaving the rest of the computer function untouched, is not a similar effect to what might be caused by a kinetic attack. Using the kinetic analogy approach, an extremely limited number of cyber attacks would cause damage.

Alternatively, one could take the view that any unauthorized intrusion into a computer or computer system results in a change to the computer or system and therefore equates to damage.[30] In other words, the digital changes required to allow penetration into a computer would be damage under the principle of proportionality. This view would require a commander to essentially consider any effects on a computer system in his proportionality analysis.

This seems to go too far. The principle of proportionality was clearly not designed to exclude the possibility of any civilian casualties or damage, but only that which was excessive.[31]

Finally, some have taken the view that damage also encompasses serious interruptions in functionality, such as would require replacing parts or reloading software systems. For example, in the kinetic analogy used above where a cyber attack shut down a communication port but left the rest of the computer unaffected, the computer would still turn on but its actual functionality might be seriously affected. If functionality is considered when determining damage, the kinetic analogy would be of limited value.

---

30. WALTER GARY SHARP SR., CYBERSPACE AND THE USE OF FORCE 140 (1999) (where the author argues that "any computer network attack that intentionally causes any destructive effect within the sovereign territory of another state is an unlawful use of force that may constitute an armed attack prompting the right to self-defense"); TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 253–54 (William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., 2009) (which states "actions that significantly interfere with the functionality of that infrastructure can reasonably be regarded as uses of force, whether or not they cause immediate physical damage").

31. Walter Gary Sharp Sr., *Operation Allied Force: Reviewing the Lawfulness of Nato's Use of Military Force to Defend Kosovo*, 23 MARYLAND JOURNAL OF INTERNATIONAL LAW AND TRADE 295, 313 (1999); *see also* Commander's Handbook, *supra* note 16, ¶ 8.1.2.1.

The functionality approach seems to be the best application of the proportionality rule to the cyber realm as it takes into account the unique aspects of cyber operations, without going so far as to make the proportionality analysis unwieldy for commanders to apply. Armed conflict has always included effects on civilians that have caused inconvenience, irritation, stress and fear, but these have traditionally not been part of the commander's analysis of damage required by the proportionality analysis.[32] By focusing on functionality, the commanders can easily understand the legal standard and apply it to modern cyber operations.

B. Indirect Effects

Gauging indirect effects in cyber warfare may prove to be one of the most difficult issues in applying proportionality. It is clear that a commander must consider the direct effects of his cyber attack. These direct effects are defined as the "immediate, first order consequences, unaltered by intervening events or mechanisms."[33] In the cyber domain, this would include the effects on a computer that is shut down by a cyber attack or the damage to the centrifuges caused by the Stuxnet malware.

In contrast to direct effects, indirect effects are "the delayed and/or displaced second-, third-, and higher-order consequences of action, created through intermediate events or mechanisms."[34] In the cyber domain, this would include damage that was not the intent of the attack, but that resulted from elements of the attack. In the case of Stuxnet, the malware infected many computers beyond its intended targets within Iran. Whatever damage might have resulted from these unintended infections might have been indirect effects. Another example might be a targeted attack on a military computer system that would shut the system down, but, because of the linkages between military and civilian systems, the malware is also likely to spread to the civilian systems and shut them down as well. Resulting indi-

32. Geoffrey S. Corn & Gary P. Corn, *The Law of Operational Targeting: Viewing the LOAC Through an Operational Lens*, 47 TEXAS INTERNATIONAL LAW JOURNAL 337, 364–66 (2012); Jensen, *supra* note 26, at 1170–71; Michael N. Schmitt, *Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance*, 50 VIRGINIA JOURNAL OF INTERNATIONAL LAW 795, 826 (2010).

33. Chairman, Joint Chiefs of Staff, Joint Publication 3-60: Joint Targeting, at I-10 (2007), *available at* http://www.bits.de/NRANEU/others/jp-doctrine/jp3_60(07).pdf.

34. *Id.*

rect effects are generally accepted as being included in the proportionality analysis.[35]

Even in the cases mentioned above, for the damage to be considered in the proportionality analysis, it must have been expected. Indirect effects which were not expected to be excessive are not factored into the analysis.[36] In other words, this standard does not anticipate that a reviewer can come after the fact and assess the reasonableness of the commander's decision on the excessiveness of the indirect effects. Rather, any reviewer must assess the reasonableness of the commander's decision based on what the commander reasonably expected the effects to be, given the information he had at the time.[37]

Considerations of expected effects have already affected known military operations. In the 2003 U.S. attacks on Iraq, cyber attackers for the United States considered attacking Saddam Hussein's financial accounts in an attempt to pressure him. The attacks were called off, however, when it was determined that the attacks would probably affect the European banking system and have negative repercussions.[38]

Similar considerations would have to be made in the case that a prospective malware targeting military objectives was to be implemented via a portable storage device. The commander would have to determine whether or not the potential transfer of that same malware to civilian systems was expected, and then consider how much damage it was expected to cause. On the other hand, if that same malware was unexpectedly transferred into civilian systems, the commander would not be responsible for having misapplied the principle of proportionality.

A commander's ability to properly apply this rule is obviously tied back to the earlier discussion on constant care. Unless a commander is constant-

35. Commander's Handbook, *supra* note 16, ¶ 8.11.4.

36. *Id.* (which states that "indirect effects of an attack may be one of the factors included when weighing anticipated incidental injury or death to protected persons").

37. Prosecutor v. Stanislav Galic, Case No. IT-98-29-T, Judgment, ¶ 58 (Int'l Crim. Trib. for the former Yugoslavia Dec. 5, 2003) (where the Trial Chamber held "[i]n determining whether an attack was proportionate, it is necessary to examine whether a reasonably well-informed person in the circumstances of the actual perpetrator, making reasonable use of the information available to him or her, could have expected excessive civilian casualties to result from the attack").

38. John Markoff & Thom Shanker, *Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk*, NEW YORK TIMES (Aug. 1, 2009), http://www.nytimes.com/2009/08/02/us/politics/02cyber.html?_r=0.

ly mapping and monitoring the targeted computer or network, he will not be able to make a reasonable assessment of what effects are expected.

IV. FEASIBILITY

The legal standard of feasibility appears in several places in the "Precautions in Attack" section of API[39] and applies to most types of attacks.[40] In various provisions, a commander must do "everything feasible"[41] or "take all feasible precautions."[42] During the ratification process, there was great debate about the term "feasible" and what it meant.[43] A number of representatives to the negotiating convention made specific comments about the meaning "feasible" was to have when applied as a legal standard. John Redvers Freeland, the head of the United Kingdom delegation, through several sessions stated that the words "to the maximum extent feasible" related to what was "workable or practicable, taking into account all the circumstances at a given moment, and especially those which had a bearing on the success of military operations."[44] Similarly, S.H. Bloembergen, a delegate from the Netherlands, stated that "feasible" should be "interpreted as referring to that which was practicable or practically possible, taking into account all circumstances at the time."[45] As a result, "feasible" is generally understood to mean that which is "practicable or practically possible, taking into account all circumstances ruling at the time."[46]

---

39. API, *supra* note 15, arts. 57.2(a)(i)–(ii), 58.

40. *Id.*, art. 57.4; API COMMENTARY, *supra* note 16, at 704; TALLINN MANUAL, *supra* note 7, sec. 7.

41. API, *supra* note 15, art. 57.2(a)(i).

42. *Id.*, art. 57.2(a)(ii).

43. 14 Official Records of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts 199 (1978) [hereinafter Official Records].

44. 6 *id.* at 214; Jensen, *supra* note 19, at 1548.

45. 6 *id.* at 214; Jensen, *supra* note 19, at 1549.

46. Reservation Letter from Christopher Hulse, Ambassador from the United Kingdom to Switzerland, to the Swiss Government (Jan. 28, 1998), *available at* http://www.icrc.org/ihl.nsf/NORM/0A9E03F0F2EE757CC1256402003FB6D2?OpenDocument (listing the United Kingdom's reservations and declarations to Additional Protocol I, and explaining in paragraph (b) that "[t]he United Kingdom understands the term 'feasible' as used in the Protocol to mean that which is practicable or practically possible, taking into account all circumstances ruling at the time, including humanitarian and military considerations"). *See also* UK MANUAL, *supra* note 16, ¶ 5.32; ICRC CIL STUDY, *supra* note 16, at 54.

A. "Practicable or Practically Possible"

During the API negotiations mentioned above, the national representatives were anxious to set a standard that would require diligence on the part of the commander, but would not be one with which it was beyond his capability to comply. The resulting language of practicality was the eventual resolution, which seems to be a workable standard in applying precautions in the attack.

The application of "feasibility" to cyber attacks seems ultimately tied to technology. As a commander contemplates a potential cyber attack, his "feasible precautions" should require him to sufficiently map the networks to determine the effects of the attack, particularly on civilians and civilian objects. This is much like the duty of constant care, but should carry a heightened specificity when planning a specific attack.

If in the process of preparing a cyber attack, the commander is unable to determine the extent of the attack's effects, he cannot launch an attack that would otherwise be considered indiscriminate. Or, if an attacker is unable to gather sufficient information as to the nature of a proposed target system, he should limit the attack to only those parts of the system for which he does have sufficient information to verify their status as lawful targets. In other words, the feasibility limitation should not be used as a justification for conducting an attack.

B. Circumstances Ruling at the Time

Without detracting from the duty of constant care previously discussed, the commander's duty to do what is feasible is limited by his circumstances. This limitation on commanders' liability stems from the post-World War II prosecution of German general Lothar Rendulic.[47] General Rendulic conducted a scorched-earth policy in Finnmark to slow what he thought were swiftly advancing Russian troops. In the end, the Russians were not coming as quickly as Rendulic had thought and the destruction proved to be unnecessary. However, the Military Tribunal determined that the legal standard was "consideration to all factors and existing possibilities" as they "appeared to the defendant at the time."[48]

---

47. *See* United States v. Wilhelm List and others, XI Trials of War Criminals Before the Nuernberg Military Tribunals Under Control Council Law No. 10, at 1295 (1950) [hereinafter Hostage Judgment]; *see also* Jensen, *supra* note 26, at 1181–83.

48. Hostage Judgment, *supra* note 47, at 1296.

This same standard should apply to the understanding of "feasibility" in cyber attacks. While commanders are required to do everything practicable, the responsibility is limited to the circumstances as the commander knows them at the time. For example, if a commander has used his best technology to map a network and exercises continuous monitoring in preparation for the attack, he has not violated the law if, during the course of the attack, the malware spreads unexpectedly to a civilian network that the commander did not know was linked to the military system.

V. PRECAUTIONS AGAINST THE EFFECTS OF ATTACKS

In addition to considering precautions when conducting attacks, nations have an obligation to take precautions against the potential effects of attacks.[49] Unlike the provisions discussed above that govern the conduct of attacks, this standard is not only a wartime standard. Rather, it is a standard that applies to nations during peacetime, in anticipation that armed conflict might arise in the future that would affect civilians and civilian objects.

Article 58 reads:

> The Parties to the conflict shall, to the maximum extent feasible:
>
> (a) Without prejudice to Article 49 of the Fourth Convention, endeavour to remove the civilian population, individual civilians and civilian objects under their control from the vicinity of military objectives;
> (b) Avoid locating military objectives within or near densely populated areas;
> (c) Take the other necessary precautions to protect the civilian population, individual civilians and civilian objects under their control against the dangers resulting from military operations.[50]

This provision of the law is binding on nations only in international armed conflict, and is considered part of customary international law.[51] The

49. *See generally* TALLINN MANUAL, *supra* note 7, rule 59 (discussing precautions against the effects of attacks in relation to cyber operations).

50. API, *supra* note 15, art. 58.

51. ICRC CIL STUDY, *supra* note 16, at 68–69, 71, 74; NIAC MANUAL, *supra* note 16, ¶ 2.3.7; YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT 145 (2d ed. 2010).

cyber aspects of Article 58 have been thoroughly discussed recently.[52] It is sufficient here to say that it establishes two layers of responsibility. Initially, a nation has the obligation to segregate its military objectives from civilians and civilian objects. Second, for those military objectives that it cannot segregate, the nation has a responsibility to protect the civilians and civilian objects from the anticipated effects of attacks.

Importantly, those who wrote this provision of API discussed in some detail the difficulty of accomplishing this standard. The inclusion of the caveat "to the maximum extent feasible" was the basis of much discussion and was purposely added in a way to apply to the entire provision, meaning that both the segregate and protect requirements are limited by the feasibility of any required actions.[53] This is also reflected by the ICRC in the *Commentary*, which states that "it is clear that precautions should not go beyond the point where the life of the population would become difficult or even impossible."[54]

One more important point is worth noting before discussing the obligations in detail. The title of Article 58 specifically refers to "attacks"; however, Article 58(c) refers to "operations," which cover a much broader spectrum of cyber activities. There is no doubt that the provisions discussed below, even those under the heading of "Protect," apply to precautions against potential cyber attacks, but the extent to which these provisions apply to operations is unclear, particularly for State parties to API. For nations like the United States who are not parties and are only bound by this article to the extent that it reflects customary international law, it seems clear that the customary aspect of this rule applies only to "attacks" and not all operations. The news is replete with examples of attacks on military objectives that impact civilian infrastructure and systems, and no States appear to have accepted the obligation to protect these targets.[55]

---

52. *See generally* Jensen, *supra* note 19.

53. Official Records, *supra* note 43, at 199.

54. API COMMENTARY, *supra* note 16, at 692.

55. *Security experts admit China stole secret fighter jet plans*, THE AUSTRALIAN, Mar. 12, 2012, World at 9, *available at* http://www.theaustralian.com.au/news/world/security-experts-admit-china-stole-secret-fighter-jet-plans/story-fnb64oi6-1226296400154; Press Release, Permanent Select Committee on Intelligence, Statement by Chairman Rogers on Senate Cybersecurity Legislation (Aug. 2, 2012), *available at* http://intelligence.house.gov/press-release/statement-chairman-rogers-senate-cybersecurity-legislation; Alexander Melnitzky, *Defending America Against Chinese Cyber Espionage Through the Use of Active Defenses*, 20 CARDOZO JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW 537 (Winter 2012).

A. Segregate

It is clear that this rule was originally written with a very "geographic" focus that is hard to translate to the cyber domain. Segregating a military armaments storage facility is geographically easier than segregating digital military communications. In fact, estimates of the U.S. Department of Defense digital traffic that traverses civilian-owned and -operated infrastructure are between 90 and 98 percent.[56] There is certainly still a geographic aspect to the rule, even in the cyber domain, but there is also a virtual location aspect to the provision.

The distinction between the virtual and geographic natures of this rule in its application to cyber operations is exemplified by the difference between cyber infrastructure and digital communications. A nation can comply with the geographic nature of the requirement by positioning servers and other military cyber equipment away from civilian areas. Similarly, a nation could conceivably create a separate cyber infrastructure backbone upon which its military cyber communications would traverse, effectively segregating it from civilian infrastructure. This has obviously not been the practice of States to this point.

Rather, the ubiquitous nature of the cyber domain has made it almost impossible to segregate potential military objectives from civilian objects even in a geographic sense. Consider air traffic control centers and other major civilian transportation control centers, as well as power generation facilities. All of these serve both civilian and military purposes and are clearly cyber targets, but they are also virtually impossible to segregate. State practice in this area has at least demonstrated that nations have not found such segregation to be feasible.

In fact, many militaries seem to be moving in the exact opposite direction and co-locating an ever greater percentage of their cyber infrastructure with civilian infrastructure. A good example of this is the movement of military and government data to the "cloud."[57] While this move is heralded as providing great financial savings, it is unclear whether the legal obliga-

56. *See* McConnell, *supra* note 19.

57. CHIEF INFORMATION OFFICER, DEPARTMENT OF DEFENSE, CLOUD COMPUTING STRATEGY (2012), *available at* http:/www.defense.gov/news/DoDCloudComputing Strategy.pdf; John Keller, *U.S. Military Begins Moving Its Information Technology (IT) Infrastructure to Secure Cloud Computing*, MILITARY & AEROSPACE ELECTRONICS (July 29, 2012), http://www.militaryaerospace.com/articles/2012/07/dod-cloud-computing.html.

tion of segregation of military objectives was ever considered as part of the decision to use the cloud.

B. Protect

Given the difficulty of segregating military objectives from civilians and civilian objects in the cyber domain, the subsequent duty to protect civilians and civilian objects from the indirect effects of attacks on non-segregable military objectives becomes very important. The caveat of feasibility applies equally to this portion of the legal obligation, but the descriptive wording of "maximum extent" must also be allowed to have some meaning or the provision carries no legal weight at all.

1. "Dangers"

The requirement to protect does not encompass every potential cyber inconvenience or irritation. Rather, it applies only to "dangers" that might result from military operations. While this term is not defined in API, it seems reasonable to equate this standard to that used in the proportionality analysis discussed above, i.e., death or injury to civilians and damage to civilian objects.

Therefore, the protection obligation would not apply to cyber operations such as a denial of service attack that prevents access to a website or the altering of a website to change its appearance or connecting links. Instead, the obligation to protect should be understood to protect civilians and civilian objects from death or injury and destruction, such as shutting down air traffic control systems or power systems, which would result in serious effects on civilians.

2. "Under Their Control"

Another aspect of this rule that limits its general application is the use of the words "under their control." The plain reading of the obligation makes it clear that governments are not expected to protect all civilians and civilian objects from the effects of attacks, but only those which fall under the government's control.

As with the general rule, this particular provision was originally conceived territorially. In the drafting debates, the Canadian representative, Brigadier General Wolfe, argued to change the originally proposed lan-

guage of "authority" to "control" to make clear the de facto nature of the obligation.[58] The change was accepted and the obligation amended. In the cyber context, the de facto nature of the rule has significant impact. A government might claim that it does not have authority over most of the cyber infrastructure due to the various legal regimes that exist within the nation. However, under the de facto standard, if the party can dictate the operations of a civilian computer system, it is under the control of that party and the duty to segregate or protect applies.

3. Specific Measures

The ICRC *Commentary* to Article 58 suggests examples of specific measures that a nation could take to fulfill its obligations under the rule, including providing well-trained civil defense forces, systems for warnings of impending attacks, and responsive fire and emergency services.[59] Analogizing these suggestions to the cyber world would suggest actions such as providing or requiring protective software products, monitoring networks and systems and providing warnings of impending or ongoing attacks, and providing technical assistance to repair networks or reroute them to alternative systems that continue to maintain functionality.

The U.S. government has already started to take some of these actions, though the extent to which it is taking them as a result of its legal obligation is unclear. For example, the United States has recently started the Defense Industrial Base Pilot Program, which is now expanding.[60] Under the program, specific industries providing defense services that make them legitimate targets in an armed conflict must meet certain cybersecurity requirements in order to do business with the government. Additionally, they receive some cyber assistance as a result of their membership in the program.

Additionally, the U.S. government recently stated that it will warn industries when they appear to be the target of an attack in an attempt to put

58. 14 Official Records, s*upra* note 43, at 198–99 (where it states, "[T]he use of the word 'control' would impose obligations on the parties which would not necessarily be implied by the use of the word 'authority.' It referred to the de facto as opposed to the de jure situation.").

59. API COMMENTARY, *supra* note 16, at 694–95; *see also* ICRC CIL STUDY, *supra* note 16, at 70.

60. News Release, U.S. Department of Defense, DOD Announces the Expansion of Defense Industrial Base (DIB) Voluntary Cybersecurity Information Sharing Activities (May 11, 2012), http://www.defense.gov/releases/release.aspx?releaseid=15266.

them on notice so they can increase their security posture.[61] Interestingly, the cyber giant Google has also recently announced that it will provide warnings to clients that appear to be the target of "State" hacking operations.[62] While Google certainly does not have any legal obligation under Article 58 to do so, it is interesting to note the sense that there is a need for such warnings.

Finally, the recent coordination between Google and the National Security Agency after the former was the victim of attacks from the Chinese government[63] may foreshadow an emerging cyber era where the government not only provides warning information, but then works closely to remediate and potentially retaliate for State-sponsored cyber activities that affect key civilian industries.

As a closing point to this part, it is important to note that a nation's inability or failure to fulfill its obligations under Article 58 does not affect an adversary's legal ability to conduct cyber attacks, so long as those attacks comply with the applicable rules of the LOAC.

VI. CONCLUSION

Cyber warfare is governed by the LOAC, and the LOAC does a generally good job of regulating cyber operations. In most cases, the existing law provides a clear paradigm to govern cyber activities; however, there are several areas where governments and military operators might question how to apply the LOAC to a specific cyber operation. This article has highlighted a few areas where additional clarity would be useful, such as in the cases of the definition of attack, the details of applying constant care, and

---

61. Lolita C. Baldor, *Pentagon Warns Public About Cyber Attacks by China*, BOSTON.COM (Aug. 20, 2010), http://www.boston.com/news/nation/washington/articles/2010/08/20/pentagon_warns_public_about_cyber_attacks_by_china/; Michael Finnegan, *US Government Warns over Gas Pipeline Cyberattacks*, TECHEYE.NET (May 9, 2012, 3:14 PM), http://news.techeye.net/security/us-government-warns-over-gas-pipeline-cyberattacks.

62. Hayley Tsukayama & Ellen Nakashima, *Google to alert users about state-sponsored cyberattacks*, WASHINGTON POST, June 6, 2012, at A5, *available at* http://www.washingtonpost.com/business/economy/google-to-alert-users-about-state-sponsored-attacks/2012/06/05/gJQA.zS8GV_story.html.

63. Ellen Nakashima, *Google to enlist NSA to help it ward off cyberattacks*, WASHINGTON POST, Feb. 4, 2010, at A1, *available at* http://www.washingtonpost.com/wp-dyn/content/article /2010/02/03/AR2010020304057.html; *see also* Stephanie A. DeVos, Note, *The Google-NSA Alliance: Developing Cybersecurity Policy at Internet Speed*, 21 FORDHAM INTELLECTUAL PROPERTY, MEDIA AND ENTERTAINMENT LAW JOURNAL 173 (2010).

the required precautions against the effects of attacks. As the discussion on these issues increases, particularly spurred by the *Tallinn Manual*, and as State actions in cyberspace inevitably increase, State practice will provide nuance to the application of the LOAC that will allow clearer definition on the use of cyber operations in armed conflict.