RETHINKING COMPUTER NETWORK "ATTACK": IMPLICATIONS FOR LAW AND U.S. DOCTRINE

Paul A. Walker

I. Introduction

The law is built on words. The meaning of words is often an integral part of legal analysis. Indeed, in our adversarial system, the parties to a lawsuit spend a great deal of time arguing for contrasting definition of key words. Even relatively mundane words get high-level treatment. The United States Supreme Court has recently reached for its dictionary to define such ordinary words as "arrange,"[1] "elect,"[2] and "deliver."[3] In international law cases, the Court has found itself looking

1 Burlington N. & Santa Fe Ry. v. United States, 129 S. Ct. 1870, 1879 (2009).
2 Atl. Sounding Co. v. Townsend, 129 S. Ct. 2561, 2570 (2009).
3 Gonzales v. Carhart, 550 U.S. 124, 152 (2007).

for the "ordinary meaning"[4] of such commonplace words as "accident"[5] and "event."[6] It is surprising, then, that so much current legal scholarship dealing with information-age warfare uses "attack" without defining it or examining the meaning given to "attack" under international humanitarian law (IHL).

Article 49 of Additional Protocol I to the 1949 Geneva Conventions defines "attack" in the following way: "acts of violence against the adversary, whether in offence or in defence."[7] That definition applies not only to the 169 State parties that have ratified Additional Protocol I, but should also be considered part of customary international law applying to all states involved in international armed conflict. The drafters of the *San Remo Manual on International Law Applicable to Armed Conflicts at Sea* took this position,[8] incorporating substantially the same definition in Article 13(b) of the Manual.[9] Likewise, the recently published *Manual on International Law Applicable to Air and Missile Warfare*, an effort to compile the existing rules of IHL for air and missile warfare, uses the same definition of "attack" as contained in the *San Remo Manual*.[10] In its 2005 study of customary international law applicable to armed conflicts, the International Committee of the Red Cross (ICRC) does not provide a definition of "attack," but the ICRC study repeatedly uses the term in rules dealing with protection of the civilian population.[11] Most of those rules are drawn either directly from Additional Protocol

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

5 Olympic Airways v. Husain, 540 U.S. 644, 651 n.6 (2004).

6 *Id.* at 655.

7 Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 49, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I].

8 San Remo Manual on International Law Applicable to Armed Conflicts at Sea 5 (Louise Doswald-Beck, ed., 1995) ("most of its provisions are considered to state the law which is currently applicable") [hereinafter San Remo Manual]; *see also* Louise Doswald-Beck, *The San Remo Manual on International Law Applicable to Armed Conflicts At Sea*, 89 Am. J. Int'l L. 192, 192 (1995) (stating that the Manual contains "international law currently applicable to armed conflicts at sea"). The Explanation to the Manual states that Manual's definition of "attack" was "inspired by" the definition contained in Additional Protocol I. San Remo Manual, *supra* note 8, at 86.

9 San Remo Manual, *supra* note 8, at 9 ("'attack' means an act of violence, whether in offence or defence"). The primary difference is the San Remo Manual's omission of the term "against the adversary," from its definition of attack. The Manual's Explanation attributes this omission to the fact that, unlike in land warfare, "it is lawful to carry out acts of violence against neutral shipping or neutral aircraft in certain limited situations." *Id.* at 87. For present purposes, this difference is not significant. The key term examined in this paper, "act of violence," is retained in the San Remo Manual formulation.

10 HPCR Manual on International Law Applicable to Air and Missile Warfare, Program on Humanitarian Policy and Conflict Research 1 (2009) [hereinafter Air and Missile Warfare Manual] (stating that attack "means an act of violence, whether in offence or in defence.").

11 For instance, the very first rule in the Study states: "Attacks may only be directed against combatants. Attacks must not be directed against civilians." Jean-Marie Henckaerts, *Study on Customary International Humanitarian Law: A Contribution to the Understanding and Respect for the Rule of Law in Armed Conflict*, 87 Int'l Rev. Red Cross 175, 198 (2005). The Annex to Henckaerts's article lists all 161 rules the ICRC study found to be "Customary Rules of International Humanitarian Law." *Id.* at 198–212. "Attack" is prominently featured in many of the first 24 rules listed in the ICRC study, dealing with the areas of distinction between civilians and combatants, distinction between civilian objects and military objectives, indiscriminate attacks, proportionality and precautions in attack, and precautions against the effects of attacks. *Id* at 198–200.

I, or echo its terms quite closely.

Although the United States has not ratified Additional Protocol I, it is a signatory to the Protocol and has long taken the position that many portions of the protocol are customary international law.[12] Viewing Article 49 as customary law is consistent with this approach, in particular because a number of subsequent articles that use "attack" are, according to the United States, reflective of customary international law.[13]

Specifically, the key principle that belligerents must distinguish between combatants and civilians and military and civilian objectives is embodied in Articles 51 and 52.[14] The key to understanding both articles, though, is their repeated use of the word "attack." It is "attack[s]" that cannot be directed against the civilian population or individual civilians.[15] Likewise, it is an "attack" that shall not be directed at civilian objects.[16] Article 51 also prohibits "indiscriminate attacks" against civilians,[17] while Article 52 requires "attacks" to be "limited strictly to military objectives."[18] But not every military operation or action is an "attack," as defined in Article 49 and used in these key provisions.[19] It is often the case that military operations have negative effects on a civilian population. For instance, the movement of armies prior to, or during an attack, often leads to large displacements of the population. For those that remain in place during such movements, daily life faces severe disruptions, including slowed or non-existent mail service and other forms of communication. IHL is not designed to eliminate all impacts on civilians and civilian objects, but to guard against the worst impacts resulting from the destructive force of military attacks.[20]

This article takes a very narrow approach to this area of IHL. It ignores the *jus ad bellum* concepts of "use of force" and self-defense in response to an "armed attack."[21] Instead, it assumes that a state of "armed conflict" under Common Article 2 of the Geneva Conventions exists in order to focus on the definition of an "attack." Rather than examining hypothetical scenarios, the methodol-

12 *See* Michael J. Matheson, *Session One: The United States Position on the Relation of Customary International Law to the 1977 Protocols Additional to the 1949 Geneva Conventions*, 2 Am. U.J. Int'l L. & Pol'y 419, 426 (1987).

13 *Id.* (pointing to portions of Articles 51 and 52 as containing such principles).

14 Additional Protocol I, *supra* note 7, arts. 51, 52.

15 *Id.* art. 51(2).

16 *Id.* art. 52(1).

17 *Id.* art. 51(4).

18 *Id.* art. 52(2).

19 Of course, "attack" is used in other parts of Additional Protocol I as well. *See, e.g.*, Additional Protocol I, *supra* note 7, art. 12 ("Protection of medical units"), art. 42 ("Occupants of aircraft"), art. 44 ("Combatants and prisoners of war"), art. 54 ("Protection of objects indispensable to the survival of the civilian population"), art. 56 ("Protection of works and installations containing dangerous forces"), art. 57 ("Precautions in attack").

20 *See* Michael N. Schmitt, *Wired Warfare: Computer Network Attack and Jus in Bello*, Int'l Rev. Red Cross 365, 373, 378 (2002).

21 As the San Remo Manual points out, "attack" is separately defined "to make it quite clear that references to 'attack' in humanitarian law are not to be confused with the concept of an armed attack as referred to in Article 2(4) of the United Nations Charter." San Remo Manual, *supra* note 8, at 86. For analysis of the *jus ad bellum* aspects of information-based actions, *see generally* Walter Gary Sharp, Sr., CyberSpace and the Use of Force (1999) and Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 Colum. J. Transnat'l L. 885 (1999).

ogy used to define an "attack" is then applied to known capabilities that may be (or, in some cases, have been)[22] used in information-based operations or actions by a State.[23] Such an examination is necessary not only because it is not well addressed by the legal literature,[24] but also because "attack" is so comprehensively overused throughout our internet society.[25] This is perhaps understandable in the media and the technical literature, which describes any adverse action against a computer or a computer network as an "attack." Unfortunately, this common use of "attack" has bled over into legal analysis and military doctrine, specifically into the *Air and Missile Warfare Manual* and the United States doctrine of "computer network attack."[26] When the meaning of "attack" is rigorously

22 Although the examples used to demonstrate these potential capabilities did not occur during periods of armed conflict (i.e., *jus ad bellum*, or use of force, principles would have applied to them at the time they occurred, with the possible exception of the information-based actions against Georgia discussed *infra* section III.A.), the analysis applied to these capabilities in this article assumes their use during an established international armed conflict (between two state actors) and assesses whether or not the use of such a capability during a period of armed conflict would amount to an "attack" under IHL (*jus in bello*).

23 One European commentator has reviewed distributed denial of service actions under "public international law," but assumed that such actions are a "major weapon of cyberwarfare" and did not examine such actions under Article 49 of Additional Protocol I. Stefan Kirchner, *Distributed Denial-of-Service (DDoS)-Attacks Under Public International Law: State-Responsibility in Cyberwar*, 8 ICFAI Univ. J. Cyber L. 10 (quoting from the abstract). Unfortunately, Kirchner incorrectly holds out the least destructive of information-based actions, denials-of-service, as the poster-child for all "cyberweapons," making unsupported assertions about possible consequences that could result from such actions, such as death, *id.* at 18 ("There is no information if ever anybody has been killed by a DDoS attack, but it *cannot be excluded completely* that this is a possibility") (emphasis added), and disruption of a nation's electric grid, *id.* at 15. Kirchner makes these claims despite accurately describing distributed denial-of-service actions and the fact that there are an estimated 10,000 such actions every day. *Id.* at 12. In fact, DDoS actions essentially effect affect traffic on the internet and at websites connected to the internet and affect computers connected to the internet only in their actions on the network and not their ability to be used for other functions, *see infra* notes 72–79, and accompanying text, especially if disconnected from the internet at the onset of a denial of service action. Although an electric company's website could be affected by a denial of service action, electrical company control systems generally operate separately from the internet, such that they cannot be affectedby denial of service actions, though they can definitely be impacted by viruses and other types of malicious software. *See generally* Eric J. Byres, *Cyber Security and the Pipeline Control System*, Pipeline & Gas J. 58–59 (Feb. 2009), *available at* http://www.oildompublishing.com/PGJ/pgjarchive/Feb09/cyber.pdff_ (describing the effects of malicious software, the Slammer worm, on control systems and highlighting the fact that the worm used at least five different pathways to get into the victimized control systems).

24 Only Professor Schmitt has examined Article 49's definition of "attack" in any significant detail, *see* Schmitt, *supra* note 20, at 376–77, and no one has applied the definition to the types of information-based capabilities that may be used in attacks during an armed conflict.

25 *See, e.g.*, Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, Wired, Aug. 21, 2007, *available at* http://www.wired.com/politics/security/magazine/15-09/ff_estonia; Kevin J. Houle & George M. Weaver, *Trends in Denial of Service Attack Technology*, CERT Coordination Center, 1 (Oct. 2001), *available at* http://www.cert.org/archive/pdf/DoS_trends.pdf. These are just two examples of sources used in this article, but every technical and media source cited refers to these actions as "attacks."

26 *See* Joint Chiefs of Staff, Joint Publication 3-13: Information Operations, at II-5 (2006), *available at* http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf (last accessed August 25, 2010) [hereinafter Joint Publication 3-13] defines computer network attack as "actions 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."

examined and applied to known action capabilities,[27] there are three clear implications. First, academic concerns about a distinction problem arising from the use of information-based capabilities are overblown. Second, and stemming from the first implication, is the conclusion that recent calls for new treaties or new "international law for information operations" are premature. Finally, the various permutations of "computer network attack" based on the United States' information operations doctrine[28] are legally unsound and should be revised. From a legal perspective the new *Air and Missile Warfare Manual* egregiously expands that definition[29] and unwisely portrays the problematic definition[30] that results as existing law.[31] These implications are particularly relevant at a time when the United States and Russia appear to be moving towards discussion of these issues.[32] In light of the differing Russian approach to "computer network attack,"[33] it is important that the terms and definitions used are grounded in the law and not derived from the popular mythology that surrounds notions of "cyberwar." The intent of this article is to begin that reappraisal by examining what constitutes an "attack" when the internet or computers and computer networks are involved.

Part II of this article examines the definition of "attack" under international humanitarian law and derives a methodology for applying that definition to the use of information-based capabilities. Part III then examines two specific capabilities: distributed denial of service (DDoS) actions and

27 "Capability" and "action" are used throughout this article in an effort to be terminologically precise. Such terms are also used to avoid referring to something as a "weapon" or an "attack" until it demonstrably is, or can be used as, a weapon or an attack. "Capability" is also appropriate because many of them are capable of being used as weapons, but also may be used in other ways. In this analysis, the use to which the capability is applied is key.

28 *See* Joint Publication 3-13, *supra* note 26 and accompanying text.

29 The AIR AND MISSILE WARFARE MANUAL incorporated essentially all of the U.S. doctrinal definition into its own definition of "computer network attack," as well as two additional, even more problematic concepts: manipulation and gaining control over the computer or computer network. AIR AND MISSILE WARFARE MANUAL, *supra* note 10, at 6 (defining "computer network attack" to mean "operations to *manipulate*, disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computer network itself, or to *gain control* over the computer or computer network") (emphasis added). It appears that the drafters of the AIR AND MISSILE WARFARE MANUAL have fully bought into the popular conception of what constitutes an "attack" on computers.

30 The AIR AND MISSILE WARFARE MANUAL definition is problematic because the additions it makes to the U.S. doctrinal definition, Joint Publication 3-13, *supra* note 26 and accompanying text, will encompass espionage activities that could legally occur in peacetime, outside the *jus in bello* setting of "armed conflict." In addition, the definition is problematic because its use of "attack" in the term "computer network attack" is completely and illogically disconnected from the Manual's own definition of "attack." The Commentary makes this clear: "The term 'attack' in 'computer network attack' is not meant to necessarily imply that all such operations constitute an attack as that term is used elsewhere in this Manual (see definition of 'attack' as set forth in Rule 1 (e)). Some CNA operations may rise to the level of an attack as defined in Rule 1 (e), whereas others will not." COMMENTARY ON THE HPCR MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE, PROGRAM ON HUMANITARIAN POLICY AND CONFLICT RESEARCH 34 (2010) [hereinafter AMW COMMENTARY]. For further discussion of these points, *see infra* Part IV.C.

31 AMW COMMENTARY, *supra* note 30, at 2 (describing the goal of the AIR AND MISSILE WARFARE MANUAL as "to present a methodical restatement of existing international law on air and missile warfare . . . to systematically capture in the text the *lex lata* as it is.").

32 *See* John Markoff and Andrew E. Kramer, *In Shift, U.S. Talks to Russia on Internet Security*, N.Y. TIMES, Dec. 13, 2009, at A1.

33 *See infra* note 182.

chip-level actions.[34] Though much about this area remains classified, there is a substantial body of technical literature available, especially with respect to DDoS, to understand the possible uses and potential effects of these capabilities. For each capability, this section of the article will also review known or suspected examples of state practice in employing such capabilities. Following the explication of each of these capabilities, the methodology developed in Part II will be applied to determine whether the use of each capability, or some uses, should be considered attacks under IHL. Because this analysis concludes that DDoS actions, and some uses of chip-level actions (and by implication, malicious software actions), are not attacks under IHL, the implications of these conclusions are addressed in Part IV. Finally, Part V concludes.

II. The Definition of "Attack" in International Humanitarian Law

The four Geneva Conventions concluded in 1949 use the word "attack" fourteen times without ever defining what constitutes an "attack."[35] Similarly, the body of treaties and international law that preceded the four seminal Geneva conventions sporadically referred to "attacks" or "attacking force" without further definition.[36] In some cases, the combination of "attack" with "bombardment" made it very clear that a specific type of attack was contemplated, either by land forces or sea-borne forces bombing land-based objects.[37] The lack of definitional precision is perhaps understandable, given the experiences of World War I and World War II that confronted the drafters. Especially in the aftermath of World War II, the drafters knew what attacks on the civilian population looked like: the bombing of London by the Luftwaffe in the Battle of Britain; the firebombings of Dresden, Stuttgart and numerous other German cities by the allies; and, of course, the first use of nuclear weapons against the Japanese cities of Hiroshima and Nagasaki. For the generation of post-World War international scholars, the definition of an attack was largely self-evident.

By the late 1970s, however, the need for a definition of attack emerged and was codified in Article 49 of Additional Protocol I. That article defines an "attack" as "acts of violence against the adversary, whether in offence or in defence,"[38] and provides the best starting point to understand

34 The use of malicious software could also have been chosen for examination. However, the variety of malicious software, along with the variety of propagation methods and the many (non-state) examples of worms and viruses, make it somewhat difficult to focus the analysis. Because there are many different consequences that can result from the different varieties of malicious software, the legal analysis for this capability is basically the same as for chip-level actions, whose modalities and consequences can also vary greatly, as can be seen in the text accompanying, *infra* notes 130–134.

35 Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31 [hereinafter Geneva I] (using "attack" six times); Geneva Convention for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85 [hereinafter Geneva II] (using "attack" four times); Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287[hereinafter Geneva IV] (using "attack" four times). The third Geneva Convention relating to Prisoners of War does not use the word "attack."

36 *See, e.g.*, Convention Respecting the Laws and Customs of War on Land and its Annex: Regulations Concerning the Laws and Customs of War on Land arts. 25, 26, Oct. 18, 1907.

37 *See* Geneva II, *supra* note 35, art. 23.

38 Additional Protocol I, *supra* note 7, art. 49(1).

whether an action taken by a state actor against an information system or computer network is considered an attack under international humanitarian law.

This section of the article is broken into two subsections. The first addresses the plain language of the definition and considers the amplifying comments addressed in the commentary to Protocol I. After concluding that additional analysis is required to apply the definition in the context of modern-day warfare against information systems and networks, the second section addresses three interpretive theories that are available to understand what constitutes an "act of violence" that equates to an "attack" under international humanitarian law. This section concludes that a consequences-based determination best comports, not only with the text of Article 49, but also with the underlying objectives of international humanitarian law.

A. "Acts of Violence"

At the outset, it is important to understand that there are three elements to the definition provided in Article 49: (1) acts of violence (2) against the adversary (3) in offense or defense. This section focuses on the first element as the core of the definition of attack. The second and third elements are peripheral to the extent that they are contextual in nature. In other words, once an act of violence is going to be committed, then the commission of that action against an "adversary" is an attack,[39] regardless of whether the act of violence is committed in an offensive or a defensive manner. The predicate question, though, is whether or not the contemplated action is, in fact, an "act of violence."

At the first and easiest level, an attack must be an affirmative step, because, in its ordinary sense, an "act" is "the doing of a thing," usually voluntarily.[40] In the case of an "attack," what is done is "violence," or an "exertion of physical force so as to injure or abuse."[41] A party must do something prior to an attack. In conventional kinetic operations, this act could be pulling a rifle trigger, dropping a bomb from an aircraft, or initiating the launch sequence for nuclear weapons, all of which result in the use of physical force to cause injury. In the context of information weapons, the analogous "act" usually involves a computer, keyboard, and usually some type of software program, though the analysis below will also examine a hardware-based action against information systems.[42] But, as with the pulling of a trigger, the act of pressing a button on a keyboard only initiates the intended action. In the case of a rifle, the resulting action is a violent one; the bullet exits the barrel

39 As previously discussed, in the context of air and sea warfare, an "act of violence" does not have to be against an adversary to be considered an "attack." *See supra* notes 9–10 and accompanying text.

40 Merriam-Webster's Online Dictionary: Act, http://www.merriam-webster.com/dictionary/act (last visited 15 November 2009).

41 Merriam-Webster's Online Dictionary: Violence, http://www.merriam-webster.com/dictionary/violence (last visited 15 November 2009). This is the primary definition provided for "violence." Other dictionaries take a similar approach. *See, e.g.*, The Oxford Dictionary and Thesaurus 1717 (American ed. 1996) (defining "violence" as "the quality of being violent" and "violent" as "involving or using great physical force").

42 *See infra* section III.B, Part III.B.

at high velocity and causes injury or death if it hits a person, or physical damage if it hits an object.[43]

In the example of the rifle, then, the outcome of the act of pulling the trigger satisfies the portion of the definition that requires the act to be a violent one. In a rifle attack, the desired result – stopping the immediate threat from an enemy soldier, for instance—occurs as the result of a violent consequence—his injury or death. The problem that arises with pushing the button on a keyboard is that usually the outcome that directly results is inherently non-violent in that pushing the button may start a distributed denial of service against a website, launch a computer worm program, or send a command to activate a software program stored in the computer of an adversary State. All of those outcomes that could result from pushing the keyboard button, while not inherently violent in and of themselves,[44] effect action of one sort or another against an information system or computer network. Those actions have consequences that may or may not be the desired result of the button pusher.[45]

The question then arises as to whether those often inherently non-violent actions are "attacks." The easy answer, of course, is to say that they are not. But to do so would be to overlook the

43 Even a rifle that is not aimed at a person or an object has the potential to culminate in an act of violence. *See, e.g.*, John Futty, *A Bullet from the Sky*, The Columbus Dispatch (Jul. 10, 2009), *available at* http://www.dispatch.com/live/content/ local_news/stories/2009/07/10/falling_bullet.ART_ART_07-10-09_A1_VVEEBLV.html. *See generally* Wikipedia, Celebratory Gunfire, http://en.wikipedia.org/wiki/Celebratory_gunfire (last visited Nov. 25, 2009).

44 Yet, each of these actions, while not using force to cause injury, could easily fit within the expansive definition of "computer network attack" in that denials of service can be used to disrupt websites or even to deny access to those websites, albeit only on a temporary basis. *See infra* notes 85–92 and accompanying text. Likewise, computer worms also often cause disruptions during the course of their transmission and often cause significant degradation in system performance. *See infra* note 97 and accompanying text. Finally, implanted software can be used for a variety of functions that could be classified as manipulation or gaining control over a computer, but remain inherently non-violent. For instance, programs can be activated that search the targeted computer or network for information and then clandestinely communicate that information to someone outside the network. *See* Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities 150–51 (William A. Owens, Kenneth W. Dam, & Herbert S. Lin, eds., 2009) [hereinafter Technology, Policy, Law] (describing examples of data exfiltration from an adversary's network). In this case, the manipulation is the use of the software to acquire the information and the control over the system comes from the ability to use the communication mechanism without the authorization of a user or the system's administrator.

45 It is precisely because the outcome of an initiating act is not usually inherently violent that this article has consistently used "actions" when discussing the application of various information capabilities against information systems or computer networks. Such terminological precision is not only necessary in an article that defines such a basic term as "attack," but is necessary in all areas of this emerging warfare area. One of the primary implications of the analysis contained in this article is that terminological imprecision by following the lead of the hacker community and using "attack" indiscriminately undermines much of modern scholarship in this area, *see infra* Part IV.A. The same problem occurs in United States doctrine, with the result that the definition of "computer network attack" used by the United States is legally unsound and risks expansion of customary international law in a direction not favorable to U.S. interests, *see infra* Part IV.B.

tremendous amount of doctrinal development by the world's armed forces in this area.[46] Even a modest review of American, Chinese and Russian doctrine reveals the common belief that actions against information systems and computer networks is a new mode of warfare, though they may differ on the specifics and whether or not these are stand-alone capabilities or must be integrated with conventional military force to be fully effective.[47]

Unfortunately, the Commentary to Additional Protocol I does not provide additional assistance in determining when an action against an information system or computer network constitutes an "attack." Although the Commentary makes it clear that the intent of the drafters was to provide a broad definition of "attack,"[48] the breadth of the definition is in no way tied to the phrase "act of violence." In fact, the Commentary does not attempt to define or describe what it means by "violence." Instead, the Commentary's "wider scope" primarily stems from the inclusion of defensive measures in the definition of "attack," rather than being limited to the concept of hostile action that one initiates against another.[49] The Commentary goes on to characterize this offensive and defensive back and forth as "combat action,"[50] a term that itself requires definition and is far less specific than the actual phrase used in the text of Article 49: "acts of violence." The reason for broadening the definition in this way, according to the Commentary, is that both offensive and defensive acts "can affect the civilian population."[51] As the Commentary makes clear, although the definition of "attack" was to be applied to all uses of the word in Protocol I,[52] the definition was specifically excluded from Article 2 and placed in the section on protections for civilians to give it "special significance" with respect to defining attacks against civilians for the purposes of distinction and proportionality.[53]

---

46 *See generally* Joint Publication 3-13, *Information Operations*, Feb. 13, 2006; Information Operations: Warfare and the Hard Reality of Soft Power 189–201, 207–11 (Leigh Armistead, ed., 2004) [hereinafter Information Operations] (reviewing Russian and Chinese doctrine); *see also* Dorothy E. Denning, *Assessing the Computer Network Operations Threat of Foreign Countries*, *in* Information Strategy and Warfare: A Guide to Theory and Practice 187–210 (John Arquilla & Douglas A. Borer, eds., 2007) (describing a methodology developed to examine a nation's capacity for "computer network operations" and applying the methodology to the countries of Iran and North Korea, finding indications of a developed capacity for "computer network operations" in each).

47 *Compare* Information Operations, *supra* note 46, at 191 (describing Russian beliefs that military objectives are easier to accomplish without loss of life using "information superiority") and 196–197 (describing Russian reliance on "informational-psychological components" of Information Operations as possible stand-alone capabilities) *with* Information Operations, *supra* note 46, at 208 (providing a description of warfare by Chinese Lieutenant General Huai Guomo that contemplates extensive use of information warfare in advance of a conventional military attack).

48 Int'l Comm. of the Red Cross, Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, at 603 (Yves Sandoz, Christophe Swinarski & Bruno Zimmerman eds. 1987) [hereinafter ICRC Commentary] (citing Shorter Oxford Dictionary 127 (1978) (defining "attack" as "to set upon with hostile action")).

49 *Id.*

50 *Id.*

51 *Id.*

52 Including articles that precede it in numeric order, *see* Additional Protocol I, *supra* note 7, art. 12 ("Protection of Medical Units"), art. 39 ("Emblems of Nationality") and art. 41 ("Safeguard of an Enemy Hors de Combat").

53 ICRC Commentary, *supra* note 48, at 603.

B. Determining Whether an "Act of Violence" Exists

Given the fact that the Commentary is focused on the third element of the definition of "attack" contained in Article 49 and the facial inability to apply the term "act of violence" to most actions against information systems and computer networks, the line between something that is an "attack" and something that is not an attack must be sought elsewhere. The next section examines three methodologies to determine whether such an action constitutes an attack under international humanitarian law: actor-based, results-based, and consequences- (or, effects-) based.

1. Actor-Based Methodology

An actor-based methodology for determining when an "act of violence" has occurred is suggested by the Commentary to Article 49 of Protocol I. The Commentary is focused on the back and forth between military forces: offensive and defensive actions; attack and counter-attack. At its broadest, and most out of context,[54] the statement in the Commentary that "the term 'attack' means 'combat action'," can be taken to mean any action occurring between two forces engaged in combat. Under such a view, all actions taken by a military force engaged in combat would need to be reviewed to determine their impacts on the civilian population. This would be so, even if it is not an inherently violent action. Under this methodology, every action against an adversary's information systems or computer networks would constitute an "attack."

While there may be many that would applaud such a black and white rule and probably do so because of, rather than in spite of, such a rule's overinclusive nature, it is not one that states will agree to accept. Regardless of whether they are parties to Protocol I, current state practice is to apply the IHL principles of proportionality, necessity, and distinction to weapons and uses of weapons, and not to non-violent operations. For instance, as Professor Michael Schmitt points out, "psychological operations directed against the civilian population that cause no physical harm are entirely permissible, so long as they are not intended to terrorize."[55]

Using an actor-based methodology would also seriously jeopardize long-held notions regarding the distinction between espionage and attacks, especially where computers and computer networks are involved. In the modern information age, the gathering of intelligence may often encompass actions, such as the installation of monitoring programs or other types of computer subroutines, against adversary computer systems and networks.[56] When these actions are used to gather information for analysis and production as intelligence, permissible espionage is occurring. But using an actor-based methodology would mean that computer-based espionage carried out by military personnel would equate to an "attack" during an armed conflict, subject not to the rules of espionage, but to the principles of proportionality, necessity, and distinction. Although such an outcome may not matter during an armed conflict because an act of espionage presumably would not encounter

54 *See supra* notes 39–40 and accompanying text.

55 Schmitt, *supra* note 20, at 378.

56 Technology, Policy, Law, *supra* note 44, at 190–92.

any difficulty in meeting those principles, there is a greater danger. Viewing computer-based espionage techniques as an "attack" during an armed conflict could negatively affect the use of such techniques in peacetime if there is a spillover effect so that the techniques are viewed as a use of force for purposes of *jus ad bellum*. Most, if not all, states have a decided interest in keeping the permissive international legal regime on espionage in place and would reject any legal rule that improperly hindered that activity. Thus, because an actor-based methodology would blur the lines between espionage and attacks, it is a methodology that is not likely to be accepted by States.

2. Results-Based Methodology

In making a case for why a new treaty is needed to govern what he terms "information attack," Davis Brown suggests a "results-oriented approach" to determinewhether IHL applies "to any given situation."[57] Simply put, according to Brown's formulation, IHL applies "if an information attack achieves the same result that could have been achieved with bombs or bullets."[58] There are a number of reasons that Brown's formulation is not the correct solution for determining either the existence of "armed conflict" under Common Article 2 of the Geneva Conventions or defining "attack" under Protocol I.

First, in the specific context of defining "attack," using Brown's approach would ignore the plain text of Article 49 of Protocol I because the approach only focuses on the result of the action in question and not the nature of the action. Nor does Brown limit his approach to violent results. In fact, he uses an example of a denial of service action that causes no physical damage to the recipient computer system, but is successful in temporarily shutting down its transmission capability.[59] Because the same "objective and result" could previously only have been accomplished with kinetic weapons, Brown considers this action to be of the same character as if it had been carried out kinetically.[60] The danger of such a "but for" test is that it equates an information-based action with a kinetic action without recognizing valid distinctions and differences between the two. In fact, many commentators have recognized that information-based warfare has the potential to dramatically lessen the human coston battlefields precisely because information-based actions can accomplish the

57 Davis Brown, *A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict,* 47 HARV. INT'L L.J. 179, 187 (2006).

58 *Id.*

59 *See id.* at 188.

60 *See id.*

same or similar results without the destruction resulting from a kinetic strike.[61] To equate the two, as Brown's results-based approach does, would be to constrain these humanitarian ends by limiting the ability to use information-based actions under international humanitarian law.[62]

The second problem with Brown's approach is one of derivation. In *International Law and the Use of Force by States*, Ian Brownlie addressed the particular problem posed for the use of force analysis by chemical and biological "devices" because they "do not involve any explosive effect with shock waves and heat."[63] Brownlie goes on to find such "devices" to constitute a "use of force" not only because the military agencies called them "weapons,"[64] but primarily because "these weapons are employed for the destruction of life and property."[65] In other words, the use of chemical and biological weapons resulted in consequences that were violent in nature. Brownlie then went on to find it "difficult to regard" as a use of force deliberate action releasing "large quantities of water down a valley."[66] Although citing to Brownlie's work to support his results-based approach, Brown takes the opposite view of the same scenario if the deliberate action occurs as the result of an "informa-

61 *See, e.g.*, Brian T. O'Donnell & James C. Kraska, *Humanitarian Law: Developing International Rules for the Digital Battlefield*, 8 J. Conflict & Sec. L. 133, 134 (2003) (stating that "[c]omputer network warfare may reduce the" humanitarian impacts caused by the "blunt instrument" of military power); Eric Talbot Jensen, *Unexpected Consequences from Knock-On Effects: A Different Standard for Computer Network Operations?*, 18 Am. U. Int'l L. Rev. 1145, 1166 (2003) (stating "the use of CNA as an alternative to traditional kinetic weapons presents an often more humane method of accomplishing the same overall objective"); Schmitt, *supra* note 20, at 394 (stating that "[t]he availability of computer network attack actually increases the options for minimizing collateral damage and incidental injury," and proceeding to discuss the benefits of simply "turning off" or interrupting target operations during an assault, including the availability of dual-use facilities to the populace post-hostilities). The conclusions are correct, but for the wrong reasons. Instead of relying without question on the U.S. military's definition of "computer network attack," analysis using IHL's definition of "attack" reveals that many common information-based actions are more humane because they simply are not attacks and the effort to shoehorn coverage of IHL over such actions is not grounded in law, but sounds in doctrine or policy.

62 To the extent that enhancing humanitarian ends rather than constraining them is itself a policy choice, it is one that appears to be strongly encouraged by IHL. For instance, Article 27 of the Geneva Convention Relative to the Protection of Civilian Persons in Time of War states that civilians "shall at all times be humanely treated, and shall be protected especially against all acts of violence or threats thereof." Geneva IV, *supra* note 35, at art. 27. Likewise, Additional Protocol I echoes this mandate in Article 51: "The civilian population and individual civilians shall enjoy general protection against dangers arising from military operations." Additional Protocol I, *supra* note 7, at art. 51(1). It is this latter proscription that applies to information-based actions that do not rise to the level of an "attack" under IHL as such actions are military operations even though not attacks. Applying Article 51 to such information-based actions is beyond the scope of this article. Suffice to say that such information-based actions (not rising to level of an attack under IHL) are not subject to the principles of proportionality, necessity and distinction, but should be treated as any other military operation that is itself not an attack.

63 Ian Brownlie, International Law and the Use of Force By States 362 (1963).

64 An example of how classifying a device or object as a "weapon" may be used or cited as a determinative state practice by international law commentators seeking to discern the formulation of customary international law.

65 Brownlie, *supra* note 63, at 362–63.

66 *Id.* at 362–63.

tion attack,"[67] where the resulting "physical damage could not otherwise be accomplished without conventional munitions."[68] But this misapprehends Brownlie's point, which looked at the consequences of an action in the absence of what traditionally constituted a use of force and not through the prism of whether traditional means would have caused the same result. This is borne out by his physical damage examples (such as releasing water from a dam down a valley and "spreading of fire through a built up area or woodland across a frontier"), which Brownlie finds not to be a use of force, but under Brown's formulation would be "armed conflict" because conventional weapons would normally be needed to cause such damage.

Finally, the above discussion also highlights another problem with Brown's approach: what if a particular result could also have been achieved without the use of "bombs or bullets"? For instance, in the example of water released from a dam, such a result could just as easily have resulted from an agent planted into the facility committing an act of sabotage, as from a bomb dropped from an airplane. The same could be said of power plants, air traffic control towers and many other potential targets. To the extent there are plausible, alternative means of reaching a result not involving kinetic means, Brown's theory does not adequately address the classification of information actions to accomplish a result that could be achieved by both kinetic and non-kinetic means. Not only is there a great deal of ambiguity present in the use of such a standard, but its attempted sweep is easy to avoid,[69] rendering it underinclusive and ineffective.

3. Consequence-based Methodology

Professor Michael Schmitt has proposed the use of a consequence-based methodology for determining whether information-based actions[70] rise to the level of a "use of force" under article 2(4) of the United Nations Charter, as well as when the use of such actions may give rise to an "armed

67 Brown, *supra* note 57, at 187 ("Similarly, it is sometimes possible to inflict physical damage on objects via information attack, such as releasing flood waters by remotely opening a dam, causing a meltdown at a nuclear power plant, or rupturing an oil pipeline.").

68 *Id.*

69 For instance, it is not hard to make the argument that if kinetic means (Brown's "bombs or bullets") are not needed to achieve a certain result, then using an information action to accomplish the same result is, in fact, a substitution for the non-kinetic means of achieving that result and could potentially have the same legal effect of the alternate, non-kinetic means. This is a tremendously large loophole for well-trained lawyers to exploit in this methodology.

70 Professor Schmitt actually uses the term "Computer Network Attack," or "CNA" in his writings, but for consistency's sake, I have opted to replace those terms (when not directly quoting) with the neutral, non-circularity inducing term, "action," that has been used throughout this article.

conflict" under Common Article 2.[71] In both cases, he was building a case for why IHL applied to information-based actions, despite the fact that such actions do not fit traditional notions of "force" or "armed conflict." What he found dispositive in each case was the fact that information-based actions can lead to the types of consequences that international humanitarian law is designed to protect: "[a]s for the protection [civilians, civilian objects, persons *hors de combat*, or medical personnel] are entitled to, it is usually framed in terms of injury or death or, in the case of property, damage or destruction."[72]

Given that, Schmitt found that some information-based actions can amount to a prohibited use of force under the Charter, especially when an information-based action is taken with a specific intent to directly cause death, injury, or physical damage to property.[73] Schmitt addressed indirect consequences by providing six factors to be used to determine whether the consequence of an information-based action "more closely approximate consequences of the sort characterizing armed force or whether they are better placed outside the use of force boundary."[74] Importantly, according to Schmitt's formulation, the consequences of the information-based action must be reasonably foreseeable.[75]

In examining the second-level issue of an "armed conflict," Schmitt's six factors were significantly reduced as the issue was no longer one of a prohibition on the use of force, but whether international humanitarian law would apply. In other words, because the motivation for the action or its legitimacy or wrongfulness is irrelevant, Schmitt reached a narrower, more cogent formulation for the *jus in bello* problem of when an information-based action constitutes "armed conflict": "when a group takes measures that injure, kill, damage or destroy. The term also includes actions intended to cause such results or which are the foreseeable consequences thereof."[76]

---

71 To best understand this section of the paper, it is helpful to think of three levels, or planes, of analysis. The first level, or international plane, deals with defining and understanding what constitutes "use[s] of force" that are prohibited by the United Nations Charter. The second level, or state-to-state plane, deals with what constitutes an "armed conflict" between states party to the Geneva Conventions such that those conventions, and the attendant rules of international humanitarian law, apply to the conflict. This level of analysis concerns the state of affairs between state parties. Once it is resolved that the nature of affairs between the parties is an "armed conflict," then the third level of analysis takes over and the question of whether an action is an attack or not comes into play. In other words, attacks occur within armed conflicts (though "armed conflicts" may or may not result from a technical "use of force."). In dealing with the first two, Schmitt is actually engaged in an exercise to determine at what point an information-based action constitutes a use of force or gives rise to an armed conflict. As part of the latter analysis, he draws from the definition of "attack" in Article 49 to essentially derive the types of violent consequences that would need to occur before a state of armed conflict would come into being. This Article takes the latter analysis and applies it to the third level of analysis, information-based actions occurring during an acknowledged armed conflict, to determine whether or not such actions should be considered attacks necessitating application of the IHL principles of proportionality, necessity and distinction.

72 Schmitt, *supra* note 20, at 373.

73 Schmitt, *supra* note 21, at 913.

74 *Id.* at 915. The factors are: severity, immediacy, directness, invasiveness, measurability, and presumptive legitimacy. *Id.* at 914–15.

75 *Id.* at 916

76 Schmitt, *supra* note 20, at 373. Here, based on Schmitt's earlier discussion of the protections to which civilians and other protected entities are entitled, he clearly means damage to property. *See supra* text accompanying note 742.

Schmitt then goes on to consider whether Article 48's statement that "[p]arties to the conflict . . . shall direct their operations only against military objectives" means that no non-military objective could be the object of a military operation, including an information-based action.[77] Relying on the fact that the specific prohibitions in subsequent articles use the word "attack," he concludes that Article 48's "prohibition is not so much on targeting non-military objectives as it is on *attacking* them, specifically through the use of violence."[78] This brings him squarely to Article 49 and the question of whether an inherently non-violent information-based action can be considered an "act of violence" such that it is an "attack." Schmitt again applies the same methodology, focusing not on the nature of the act, but on the nature of the consequences: an information-based action with violent consequences is an "attack."[79] Those violent consequences are exactly the kinds that are contemplated in other provisions of Additional Protocol I: "shielding protected individuals from injury or death and protected objects from damage or destruction."[80] He adds, "that inconvenience, harassment or mere diminishment in quality of life does not suffice; human suffering is the requisite criterion."[81] "Human suffering" stems from the violent consequences of death or injury[82] to people and damage or destruction of property,[83] including "permanent loss of [financial] assets."[84] Significantly, then, information-based actions that only result in "inconvenience, harassment or mere diminishment in quality of life" are not "attacks" under this methodology because these consequences do not cause sufficient human suffering to be considered violent under Schmitt's methodology. Although unstated by Schmitt, as with the second-level "armed conflict" analysis, the violent consequences must be reasonably foreseeable from the information-based action in question in order for its use to constitute an attack.

Schmitt's application of his consequence-based methodology to the definition of "attack" is secondary to his larger point regarding armed conflict, but it is the correct one to apply. In fact, of the three levels of Schmitt's analysis discussed in this section, the consequence-based methodology is probably most applicable and most appropriately applied at this narrow, relatively well-defined level of analysis. One of the main advantages of Schmitt's consequence-based methodology is that it provides relatively clear guidance as to when an information-based action should be considered at

77 Schmitt, *supra* note 20, at 375–76, quoting Additional Protocol 1, *supra* note 11, art. 48.

78 Schmitt, *supra* note 20, at 376 (emphasis in the original).

79 *See id.* at 377.

80 *Id.*

81 *Id.*

82 "Injury" includes "significant human physical or mental suffering," according to Schmitt's conception of violent consequences. *Id.*

83 As this Article was undergoing final revisions, in March 2010, the Commentary to the Air and Missile Warfare Manual was published and takes the same approach to non-kinetic attacks, such as CNA, stating that "[t]he definition of 'attacks' also covers 'non-kinetic' attacks . . . that result in *death, injury, damage or destruction of persons or objects*." AMW Commentary, *supra* note 30, at 28 (emphasis added).

84 Schmitt, *supra* note 20, at 377. For instance, damage or destruction of property also encompasses stock or money that can be converted into property. *Id.* Schmitt goes on to conclude that "a major disruption of the stock market or banking system" would be an attack under IHL if it collapsed the economy and led to "widespread unemployment, hunger, mental anguish, etc." *Id.*

attack. It also has the advantage of not being over-inclusive.. Unlike Brown's results-based methodology, not every action that yields a result that previously could only have occurred by kinetic means equates to an attack. As a result, use of the consequence-based methodology is likely to lead to increased adherence to IHL protective norms, as Commanders will have incentive to use information-based actions, but without the violent consequences often incurred through kinetic means.

III. Capabilities Used in Information-based Actions

This section examines the characteristics of two specific information-based capabilities and reviews known, or suspected, state practice in using these capabilities. For each capability, the consequence-based methodology established above will be used to determine whether these capabilities, or the types of actions that can stem from the employment of these capabilities, are attacks as defined in international humanitarian law. The two specific capabilities that will be examined in some detail are distributed denial of service (DDoS) actions and chip-level[85] actions.

A. Distributed Denial of Service Actions

Computers and networks are finite resources. Even the internet, which is comprised of many networks connected together, does not have an infinite amount of resources. This finiteness of resources is the primary vulnerability that gives rise to denial of service actions against websites, computers, or even entire networks.[86] At the macro level, the action consists of directing a large number of activity requests, for instance, requests for a page view of a website, at the subject system with the result that it is overwhelmed.[87] The result, effectively, is to stop the system from being able to respond to any of the activity requests. When the subject is a website, the result is that the website is not able to be viewed by those not taking part in the denial of service action.[88] When the subject is a computer or a network, the denial of service acts to prevent that computer or network from

85 This specific term comes from a recent *Foreign Affairs* article that identifies microchips as the "soft spot" in hardware-based information systems. Wesley K. Clark & Peter L. Levin, *Securing the Information Highway: How to Enhance the United States' Electronic Defenses*, Foreign Aff., Nov.-Dec. 2009, at 2. The manipulation of microchips for malicious purposes has previously been described in information security literature as "chipping." See Dorothy Denning, Information Warfare and Security 266 (1999), (citing to Winn Schwartau, Information Warfare 254–68 (2d ed. 1996)). It is often little-discussed. Denning's seminal work in this area contains only one paragraph on "chipping," concluding that "[t]here are no substantiated reports of chipping." Denning, *supra*, at 266. In fact, this turns out not to be the case, as the Central Intelligence Agency conducted a microchip action against the Soviet Union in the 1980s, with some of the details declassified in 1996. *See* Gus W. Weiss, *The Farewell Dossier: Duping the Soviets*, 39 Studies in Intelligence (Cent. Intelligence Agency) (1996), *available at* https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm; Thomas C. Reed, At the Abyss: An Insider's History of the Cold War 266–70 (2004); *see also infra* text accompanying notes 152-160.

86 *See* Houle & Weaver, *supra* note 25, at 1.

87 *Id.* at 2; *see also* Ramneek Puri, *Bots & Botnet: An Overview*, SANS Institute InfoSec Reading Room, 1–2 (Aug. 8, 2003); http://www.sans.org/reading_room/whitepapers/malicious/bots_and_botnet_an_overview_1299.

88 Allen Householder et al., *Managing the Threat of Denial-of-Service Attacks*, CERT Coordination Center, 2 (Oct. 2001) [hereinafter Householder]; http:// www.cert.org/archive/pdf/Managing_DoS.pdf - 2008-07-31.

communicating with legitimate activity requests coming over the internet, effectively stopping that computer or system's contact with the rest of the internet until the denial of service action stops or the system administrator is able to mitigate the effect of the action.[89] Because a denial of service action uses a considerable amount of available bandwidth, such an action also causes a slowdown or stoppage in the flow of information packets in the vicinity of the denial of service action.[90] This may lead to a complete halt in email communications, either as an intended result of the action or, more often, as an unintended byproduct.[91] Significantly, a DDoS action does not cause any physical damage to the targeted system or network.[92] The servers and computers may need to be restarted in order to clear buffers or reset the system, but the physical hardware remains intact. In addition, the information contained within the network is also usually not directly impacted by a DDoS action.[93]

Although a denial of service action can be initiated by a single computer connected to the internet, it is the use of a large number of such computers that gives a DDoS action its increased effectiveness.[94] Control over the required number of computers is accomplished in a variety of ways.[95] Multiple individuals can cooperate, either formally or informally, to share "attack" scripts for DDoS actions, often for political or activist reasons.[96] It is also possible for a single individual, or group, to gain control over the computers of unsuspecting internet users and use them to initiate a DDoS action.[97] Such control may be achieved by using a worm to carry the DDoS software as a "payload" that is left on every computer infected by the worm; by luring visitors to tainted websites, which load the DDoS malware on the unsuspecting visitor; and by social engineering techniques that are designed to trick a computer's unsuspecting owner to load the DDoS software on his own system, often by opening an email or clicking on an email attachment.[98] Widespread growth of internet "chat" technology has greatly increased the ability of DDoS initiators to control large numbers of disparately situated computers for such actions, forming them into BOTNETs that are controlled

89 *See generally id.* at 4–16 (discussing responses to denial of service actions available to system administrators and methods to mitigate the effects of such actions on computer systems and resources).

90 *See* Larry Rogers, What is a Distributed Denial of Service (DDoS) Attack and What Can I Do About It?, http://www.cert.org/homeusers/ddos.html (last visited Nov. 29, 2009).

91 *See* Householder, *supra* note 88, at 2 ("For example, the direct target of a DoS attack may not be the only victim. An attack against one site may affect network resources that serve multiple sites."). For a real-world example which discusses the impacts of a well-coordinated DDoS on the email and phone systems of Georgia, see John Bumgarner & Scott Borg, *Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008*, A US-CCU Special Report, Aug. 2009, at 6 [hereinafter US-CCU Overview], http://www.registan.net/wp-conten/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf.

92 Instead, the "primary goal" of a denial of service action "is to deny the victim(s) access to a particular resource," and is often indistinguishable from heavy, legitimate loads on a network. Householder, *supra* note 87, at 2.

93 It is possible that a DDoS action may serve to distract attention from a more nefarious action such as using a backdoor to place a virus or other malicious code in the system. *See* US-CCU Overview, *supra* note 91, at 6.

94 *See* Puri, *supra* note 87, at 1–2.

95 *See* Investigative Research for Infrastructure Assurance Group, *Diversification of Cyber Threats*, Inst. Security Tech. Studies, Dartmouth College, 5–10 (May 2002) [hereinafter IRIA Diversification Study].

96 *See id.*

97 *See id.*

98 *See id.*

via Internet Relay Chat protocols and communications links.[99] This dispersion of effort is the primary reason that it is difficult to attribute DDoS actions to the perpetrators.[100] Often the computers actually carrying out the actions may belong to innocent parties, who remain blissfully unaware that their computer is being used to carry out such actions.[101]

No State has yet admitted to conducting a DDoS action. In 2007, there was much speculation that Russia was behind DDoS actions directed at many systems in Estonia,[102] and in August 2008, a DDoS action was directed against Georgian government sites at the same time Russian military forces were entering Georgia in a conflict over the Georgian territory of South Ossetia.[103] In both instances, it appeared that the actions were carried out by networks of Russian citizens and, in the Georgian case, perhaps elements of organized crime, but with no direct Russian government involvement. Because the DDoS action against Georgia occurred during a time of acknowledged armed conflict between Russia and Georgia, it is an example that is very relevant to the purpose of this article and bears closer scrutiny.

The DDoS actions against Georgia bear the hallmarks of what in the United States is known as a covert action[104]: private individuals acting in such way as to carry out objectives of direct benefit to a State's political and military policy, and done in such a way that State involvement can be denied.[105] A review of the actions against Georgia by the United States Cyber Consequences Unit (US-CCU) determined that "cyber attacks against Georgian targets were carried out by civilians with little or no direct involvement on the part of the Russian government or military."[106] US-CCU also concluded, however, that the organizers of the DDoS actions "had advance notice of Russian military intentions, and they were tipped off about the timing of the Russian military operations while these operations were being carried out."[107] Reports at the time indicated that the DDoS action preceded the Russian military advance by as much as twenty-four hours.[108] Such "close cooperation"[109] apparently occurred well before the actual military action was initiated, because the actions were not pre-

99 *See id.*

100 *See id.*

101 *See id.*

102 *See, e.g.*, Arthur Bright, Estonia Accuses Russia of "Cyberattack," CHRISTIAN SCI. MONITOR, May 17, 2007.

103 *See infra* notes 104–124 and accompanying text.

104 *See* 50 U.S.C. §413b(e) (2009) (defining "covert action" as "an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly . . . .").

105 For instance, during the Vietnam War, the CIA sponsored and paid for its own army of Hmong Tribesmen to interdict the Ho Chi Minh Trail running through Laos. *See* TIM WEINER, LEGACY OF ASHES 253, 301 (2009). The CIA also covertly funded Radio Free Europe and Radio Liberty for decades without the knowledge of most of the station staff members. *See* WEINER, *supra*, at 125, 129–30; A. John Radsan, *An Overt Turn on Covert Action*, 53 ST. LOUIS U. L.J. 485, 494–95 (2009).

106 US-CCU Overview, *supra* note 91, at 2.

107 *Id.* at 3.

108 *Cyber Attack Casts New Light on Georgia Invasion*, THE FIRST POST, Aug. 15, 2008, http://www.thefirstpost/co.uk/45135,news-comment,news-politics,cyber-attack-casts-new-light--on-georgia-invasion (last visited Nov. 28, 2009) [hereinafter News and Comment].

109 US-CCU Overview, *supra* note 91, at 3.

ceded by the usual level of reconnaissance and mapping required to shut down the Georgian sites as quickly and effectively as the DDoS action did.[110] In addition, US-CCU also concluded that "the signal to go ahead [with the DDoS action] had to have been sent before the news media and general public were aware of what was happening militarily."[111]

The DDoS actions were also effectively targeted and designed to produce specific benefits for the Russian military advance, largely by preventing the use of communications systems for coordinating an effective response.[112] BOTNETS and servers associated with Russian organized crime organizations were used in the first wave of DDoS actions, with the BOTNETS used to conduct focused and constant actions against a narrow list of eleven target websites.[113] These actions were directed at government and news media websites, causing significant disruption to the Georgian government's ability to get information about the invasion and to disseminate information about what was happening to the Georgian populace and to the outside world.

A second wave of DDoS actions was carried out against forty-three websites by hackers that were recruited to the cause by postings in hacker-affiliated websites. No special expertise was needed to deploy the posted capabilities, as the scripts were pre-written and pre-loaded with the list of websites to be subjected to the DDoS action.[114] These second wave actions occurred after Russian troops took positions inside Georgia,[115] which again indicated a level of cooperation with Russian authorities that is suggestive of the invisible hand of state action exercised covertly. This second wave of DDoS actions was directed at "many more government websites, Georgian financial institutions, business associations, educational institutions, more news media websites, and a Georgian hacking forum."[116] These actions sowed considerable confusion, prevented the organization of an effective response by the government, and disrupted patterns of civilian communications and normal business operations.[117]

---

110 *Id.* At least one news site, though, has pointed to a DDoS attack on the website of the Georgian president the month before (July) as a "practice attack" or "dry run" for the full-scale "attack" in August, 2008. News and Comment, *supra* note 107. US-CCU also stated that some of the material used in the campaign against Georgia was prepared at least two years before. Specifically, the graphic art used in one of the website defacements was prepared in March, 2006, at a time of previous tensions between Russia and Georgia. US-CCU Overview, *supra* note 91, at 5.

111 US-CCU Overview, *supra* note 91, at 3..

112 *Id.* at 6 ("The targets for attack were nearly all ones that would produce benefits for the Russian military.").

113 *Id.* at 4.

114 *Id. See also* Evgeny Morozov, *An Army of Ones and Zeros: How I Became a Soldier in the Georgia-Russia Cyberwar*, SLATE, Aug. 14, 2008, http://www.slate.com/id/2197514 (describing his effort to "enlist" in the cyberwar in order to illustrate the media fallacy describing the hand of Russia behind the action and relating his experience of, within an hour, finding three separate methods that could be used against Georgia, two of them fairly simple to use and at least one from a Russian hacker website).

115 US-CCU Overview, *supra* note 91, at 5.

116 *Id.* Although no reason is provided, it seems clear that a DDoS action specifically against a hacking forum frequented by Georgian hackers is an effort by Russian civilian hackers to preempt similar action from being taken by their Georgian counterparts in retaliation for the cyber actions against Georgia.

117 *Id.*

Significantly, the DDoS actions did not cause physical damage[118] and they ended soon after the completion of Russian military activity.[119] What the DDoS actions did, though, was substantial in terms of what the actions accomplished in support of the military operation. The net result of the sustained DDoS actions was described in the US-CCU Overview:

> The high volume of cyber attack traffic jammed many general communications links. The channels of communication that were seriously disrupted during parts of the cyber campaign included e-mails, land-line phone calls, and cell phones. The National Bank of Georgia was forced to severe (*sic*) its internet connection for ten days, stopping most of the financial transactions dependent on that institution. The economic disruptions and other uncertainties may have slowed activities where the Georgian government was dependent on private sector businesses.[120]

But, significantly, these results were achieved without a single bomb—and the attendant risk of collateral damage—dropping on a communication facility, cell phone tower, satellite dish, or news media building, as has occurred in other conflicts, most notably the controversial bombing of Serbia's state-owned television station by North Atlantic Treaty Organization (NATO) forces during the conflict over Kosovo.[121] In fact, if the hand of Russia was, indeed, behind the denial of service actions against Georgia, such actions stand as a silent, unacknowledged rebuttal to NATO's attack, which resulted in sixteen deaths and only kept the television station off-air for six hours.[122]

---

118 US-CCU points out that "a number of Georgian critical infrastructures were accessible over the internet" at the time of the Russian military action and they "would have been vulnerable to cyber attacks causing physical damage." *Id.* These types of attacks did not occur, however, despite the initiators "considerable technical expertise" indicated by the sophisticated and narrowly-tailored manner the DDoS and website defacements were carried out. US-CCU concludes that "[t]he fact that physically destructive cyber attacks were *not* carried out against Georgian critical infrastructure industries suggests that someone on the Russian side was exercising considerable restraint." *Id.*

119 *Id.* at 6.

120 *Id.*

121 BBC News, *Bombed Serb TV Back on Air*, BBC Online, April 23, 1999, http://news.bbc.co.uk/2/hi/europe/326339. US-CCU assumes that the effectiveness of the DDoS action meant there was no need to bomb those facilities. US-CCU Overview, *supra* note 90 at 6 ("the news media and communications facilities, which would ordinarily have been attacked by missiles or bombs during the first phase of an invasion were spared physical destruction, presumably because they were being effectively shut down by cyber attacks."). If this assumption is correct, this appears to be an example of how cyber action can be used to accomplish the same result as a bomb without the same type of physical destruction and possible loss of human life that implicates the principles of distinction and proportionality under IHL. *See also* Jensen, *supra* note 61 and accompanying text.

122 BBC News, *supra* note 121. Even before the events in Georgia, one legal commentator presciently noted that prevention of loss of life was a potential benefit of using a "cyber weapon" instead of bombs against the Serbian television station. *See* Jeffrey T.G. Kelsey, Note, *Hacking Into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare*, 106 MICH. L. REV. 1427, 1440 (2008). However, Kelsey then proceeds to draw the wrong conclusion from this insight, stating that a "belligerent is more likely to engage in attacks that violate the principle of distinction using cyber warfare than when using conventional attack methods since it can do so without incurring the political cost associated with civilian casualties." *Id.* Instead, using the analysis presented here, because the use of a denial of service action is not an attack under IHL, there is no violation of the principle of distinction. This is a good example of a situation where the proper initial analysis will lead a commander to take an action designed to advance the overall objective of IHL–protection of civilians–without having to make a choice between violating the principle of distinction (using Kelsey's flawed analysis) or the principle of proportionality (that is undertaken when kinetic weapons are used).

The Georgians were able to mitigate some of the effects of the DDoS action by transferring some of their websites to servers outside the country, mostly to Estonia and the United States,[123] specifically Google.[124] While this served to increase communications to the outside world, it did not affect the communications disruptions that were occurring within Georgia as a result of the DDoS actions.

Using the consequence-based methodology, a denial of service action is not an attack under IHL. An attack is an action that results in violent consequences, such as death, injury, or property damage or destruction, with the resultant consequences either specifically intended or reasonably foreseeable. Even the most sophisticated DDoS action—the Russian-supported actions against Georgia previously discussed—did not yield such consequences. The economic disruptions that resulted were temporary in nature and did not result in the kind of permanent economic damage that results in human suffering. There were also no reports of violent consequences that were indirectly attributable to the denial of service action. Similar disruptions without violent consequences occurred in the earlier denial of service actions against Estonia in 2007, actions more tenuously connected to Russia than the actions against Georgia.[125]

The conclusion that IHL does not apply to even very sophisticated, targeted denial of service actions is not surprising. After all, denial of service events are probably the most commonly occurring adverse event on the internet, often occurring daily without any violent consequences.[126] Such actions, while disruptive to targeted businesses and websites, are generally viewed as temporary annoyances, rather than serious threats causing violent consequences.[127] Denial of service and website defacement actions are used by hackers and internet activists, known as "hacktivists," to make political statements or as forms of protest against actions taken by businesses, organizations, and governments.[128] Denial of service actions are properly viewed as harassments, and not attacks, under international humanitarian law.[129]

B. Chip-Level Actions

123 US-CCU Overview, *supra* note 91, at 7.

124 Clark &Levin, *supra* note 84, at 3.

125 *See* Bright, *supra* note 101.

126 One technical study found an average of 2,000 to 3,000 active denial of service actions per week over a three-year period (2001-2004). David Moore et al., *Inferring Internet Denial-of-Service Activity*, 24 ACM Transactions on Computer Sys. 115, 116 (2006), *available at* http://www.caida.org/publications/papers/2006/backscatter_dos/backscatter_dos.pdf.

127 *See* Dorothy E. Denning, *A View of Cyberterrorism Five Years Later*, *in* Internet Security: Hacking, Counterhacking, and Society (Kenneth Himma, ed., 2007) (stating that "the worst denial-of-service attacks have generally been conducted to extort money from victims, put competitors out of business, and satisfy the egos and curiosity of young hackers," and that most political and social "attacks" "have generally not been intimidating").

128 *See generally* Dorothy E. Denning, *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, 16 Computer Sec. J. 15 (2000), *available at* http://faculty.nps.edu/dedennin/publications/Activism-Hacktivism-Cyberterrorism.pdf.

129 The Commentary to the Air and Missile Warfare Manual agrees with this conclusion, stating "There was agreement among the Group of Experts that the term 'attack' does not encompass CNAs that result in an inconvenience (such as temporary denial of internet access)." AMW Commentary, *supra* note 30, at 28.

One of the oldest forms of actions against information systems and networks is also one of the least discussed, in both the legal and information security literature. A recent article by Wesley K. Clark and Peter L. Levin in *Foreign Affairs*, however, has highlighted the dangers of compromised microprocessor chips.[130] Clark and Levin point out that, as early as 1982,[131] the United States Central Intelligence Agency (CIA) carried out a cyber-operation that placed faulty chips and software in the Trans-Siberian natural gas pipeline. The result, according to Clark and Levin, was a claimed "three-kiloton explosion."[132]

Chip-level actions against the hardware component of an information system or computer network have certain advantages over software- or externally-based actions, such as worms/viruses or denials of service. Unlike the in-your-face nature of denial of service actions, chip-level actions are much more subtle, usually unknown until their intended action occurs. And, unlike software-based actions, chip-level actions are not vulnerable to detection by anti-virus software that is constantly updated with the newest software-based security threats.[133] Assuming accurate and actionable intelligence support, then, chip-level actions have the capacity to be very effective against information systems or networks.[134]

Chip-level actions occur in two ways. First, a microchip can act as a "kill switch," either by turning off the system in which it is installed or causing that system to malfunction, either randomly or at a set time.[135] The easiest way to accomplish this is to physically damage an existing chip by slightly nicking a wire, which later causes the chip to fail.[136] Second, a chip can be altered by adding extra logic to the chip itself. This creates a backdoor that allows someone from outside the targeted system to enable (or disable) specific functions. This addition could occur either by adding extra transistors to the chip during the 400-step manufacturing process[137] or by incorporating extra tran-

130 CLARK & LEVIN, *supra* note 85, at 4.

131 In contrast, the first internet "worm" to have widespread effect on even the limited version of the internet then in existence was the "Morris worm," which was designed as a proof-of-concept experiment that went awry in 1988, landing its creator in criminal trouble. *See* United States v. Morris, 928 F.2d 504 (2d Cir. 1991).

132 CLARK & LEVIN, *supra* note 85, at 4. Although Clark & Levin impliedly link the failed chips with the pipeline explosion, the underlying sources indicate that, in reality, the pipeline explosion was attributable to either flawed turbines or tainted software, while faulty chips were introduced into Soviet military equipment. *See infra*, notes 152-160 and accompanying text. The mistake makes for a useful hypothetical, though.

133 *Id.* at 5. *See also* MARTIN C. LIBICKI, CONQUEST IN CYBERSPACE: NATIONAL SECURITY AND INFORMATION WARFARE 20-21 (2007) (pointing out that efforts to destroy or degrade information are easily defeated by aggressive uses of file backup systems).

134 Although the examples used to demonstrate the viability of chip-level actions, including "kill switches," occurred outside the setting of an armed conflict, the legal analysis assumes their use inside armed conflict when considering the question of whether a specific use constitutes an "attack" under IHL.

135 Sally Adee, *The Hunt for the Kill Switch*, IEEE SPECTRUM, http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch/0, at 7 (explaining the chip fails "due to electromigration: as current flowed through the wire, eventually the metal atoms would migrate and form voids," causing the wire to break).

136 *Id.*

137 CLARK &LEVIN, *supra* note 85, at 5.

sistors into the design-stage of the chip manufacturing process.[138]

The chip alterations, whether implemented physically or by design, are extremely difficult to detect.[139] Because it is possible for a chip to hold up to a billion transistors,[140] most chip-testing programs only test for specific functionality.[141] If the chip is to be installed in a cell phone, then "the chip maker will check to see whether all the phone's various functions work. Any extraneous circuitry that doesn't interfere with the chip's normal functions won't show up in these tests."[142] If the chip contained a backdoor, it might then be possible to override any encryption used on the phone, , and obtain access to the conversation "in the clear."[143] Or the chip may make it easier to track the location of the cell phone and its owner, leading to the possible use of kinetic weapons, should the owner be a viable target under international humanitarian law.[144] As these examples make clear, the possibilities for using a backdoor into a system are many and varied.

The uses of "kill switches" are also similarly varied. A chip altered in such a way could be set to malfunction, or "kill", a system when a specified circumstance occurs. For instance, in a missile system, an altered chip might disable "the fire-control logic inside a missile once it had been armed or its guidance system had been activated,"[145] thus rendering it ineffective. The most difficult type of altered chip to design and infiltrate into a system is one that can be activated by remote command, or "at will." There are unconfirmed rumors that French defense contractors have included chips containing kill switches in military equipment sold abroad so the equipment may be disabled if it falls into the hands of a force hostile to French interests.[146]

Similarly, following the Israeli airstrike on a suspected Syrian nuclear facility in September, 2007,

---

138 Altering the design of a microchip would not necessarily involve compromising the competitive position of a commercial chip manufacturer, either. Generic, programmable chips are used for many purposes around the world, including by defense contractors. Chip programmers may use up to two dozen software programs that they obtain from the internet to design the circuitry for such chips and "'[t]hat creates two dozen entry points for malicious code.'" Adee, *supra* note 135, at 4 (quoting Dean Collins, deputy director for the Defense Advanced Research Projects Agency's Microsystems Technology Office). Dean Collins is also the program manager for the Trust in Integrated Circuits program, which is developing a methodology for testing microchips for backdoors and kill switches, as well as developing plans to safeguard the supply of chips to be used in U.S. defense products. *See generally* Adee, *supra* note 135, at 2–6 (discussing the contractors and testing timelines for the chip-testing); CLARK &LEVIN, *supra* note 85, at 9–10 (discussing possible solutions to the need to safeguard the supply of domestically- and foreign-manufactured microchips).

139 *Id. See also* Adee, *supra* note 135, at 4–5.

140 CLARK & LEVIN, *supra* note 85, at 5.

141 Adee, *supra* note 135, at 2; *see also* CLARK & LEVIN, *supra* note 84, at 5 (stating that modern automated testing equipment "is designed to detect deviations from a narrow set of specifications; it cannot detect unknown unknowns.").

142 Adee, *supra* note 135, at 2.

143 *See, e.g.,* Adee, *supra* note 135, at 4–5 (discussing the possibility of embedding a kill switch or backdoor onto an encryption chip and using the example of shutting down the encryption technology in a military radio).

144 *See, e.g.*, Krishnakumar P., *Death from 30,000 Feet Above*, http://news.rediff.com/slide-show/2009/aug/14/slide-show-1-everything-you-wanted-to-know-about-drones.htm (interviewing Brigadier Gurmeet Kanwal (retired), Director, Center for Land Warfare Studies, on use of drones to kill fifteen high-value al Qaeda and Taliban targets and the use of cell phone signals to track an enemy's location).

145 CLARK & LEVIN, *supra* note 85, at 8.

146 Adee, *supra* note 135, at 1.

there was much speculation that the Syrian air defense system failed to warn of the incoming Israeli aircraft because the system had been temporarily disabled through the use of altered "commercial off-the-shelf microprocessors" in the Syrian system.[147] More recent reporting suggests other ways that the Israelis gained control over the Syrian air defense system. Richard A. Clarke and Robert K. Knake suggest three possibilities.[148] First, Clarke and Knake suggest that a stealth Israeli Unmanned Aerial Vehicle (UAV) was able to read the Syrian radar frequency and then use that frequency to send computer packets designed to spoof or control the system back down to the Syrian radar system.[149] This type of system is apparently based on similar capabilities developed by the United States government.[150] Second, they suggest that the Russian computer code used in the Syrian air defense control system was compromised in some way through the placement of a "trapdoor," or "Trojan Horse," that allowed someone access to the system, possibly with full administrator privileges.[151] This is the software version of the chip-level "kill switch" discussed above. Finally, Clarke and Knake suggest that the Israelis may have been able to gain control of the Syrian system by tapping into a fiber optic cable in Syria.[152] Regardless of method, the outcome would have been to ensure that the Syrians either could not see the incoming Israeli aircraft or could not achieve adequate targeting solutions in order to use their air defense missile systems.

As with denial of service actions, none of the above examples have been confirmed by the States involved. In fact, the only known chip-level action conducted by a State was a covert operation conducted by the CIA against the Soviet Union in 1982. The operation was first revealed in a 1996 article by Dr. Gus Weiss, a Reagan-era National Security Council (NSC) staffer, in the CIA's *Studies in Intelligence*.[153] Weiss described how the CIA received the so-called "Farewell Dossier" from the French intelligence agency. It contained the Soviet "shopping list" for Western technology in computers and microelectronics (semiconductor chips). According to Weiss, he developed a plan to provide versions of the "wish list" material designed to fail or not work correctly to Soviet intelligence. Following approval by then-CIA Director William Casey, a joint CIA, Department of Defense ("DoD"), and Federal Bureau of Intelligence ("FBI") operation, with the assistance of

147 Adee, *supra* note 135, at 1; *see also* David A. Fulghum, Robert Wall & Amy Butler, *Cyber-Combat's First Shot*, Aviation Wk. & Space Tech. 26 Nov. 2007 (providing a timeline of the assault on the suspected reactor, including a kinetic strike on at least one Syrian air defense radar site, after which "the entire Syrian radar system went off the air for a period of time that included the raid" and, citing U.S. intelligence analysts, indirectly linked that action to "higher-level, nontactical penetrations . . . of the Syrian command-and-control capability done through network attack.").

148 *See* Richard A. Clarke & Robert K. Knake, Cyber War: The Next Threat to National Security and What to Do About It 4–9 (2010) (discussing the Israeli strike against suspected Syrian nuclear facility).

149 *Id.* at 6–7.

150 *Id.* at 7 (indicating that the technology is based on a U.S. system code-named Senior Suter). *See also* Richard B. Gasparre, *The Israeli "E-tack" on Syria – Part II*, airforce-technology.com (Mar. 11, 2008), *available at* http://www.airforce-technology.com/features/feature1669/ (last accessed May 14, 2010) (describing how the Senior Suter program "beam[s] electronic pulses into the antennas that effectively corrupt, if not hijack, the processing systems that present the enemy operators with their physical picture of the battlefield").

151 Clarke & Knake, *supra* note 148, at 7–8.

152 *Id.* at 8.

153 *See* Weiss, *supra* note 85. The facts in this paragraph are drawn from Weiss's article.

American industry, then proceeded to place "[c]ontrived computer chips . . . into Soviet military equipment, flawed turbines were installed on a gas pipeline, and defective plans disrupted the output of chemical plants and a tractor factory."[154]

Although Weiss did not provide further detail on the consequences of these actions in his 1996 article, Thomas C. Reed provided a wealth of additional detail in his 2004 book, *At the Abyss: An Insider's History of the Cold War*. Reed, a colleague of Weiss on the NSC staff, writes that "'Improved'-that is to say, erratic-computer chips were designed to pass quality acceptance tests before entry into Soviet service. Only later would they sporadically fail, frazzling the nerves of harried users."[155] The use of a random method would have been the only means available at the time given the limited scope of the internet and the isolated nature of the Soviet systems involved.

As far as the Siberian pipeline, Reed also provided substantially more detail. The CIA was able to ascertain that Soviet intelligence was looking to obtain specific software for the computers running the pipeline.[156] To do so, the Soviets were going to penetrate and steal the software from a Canadian company.[157] With that company's assistance, the CIA managed to provide Soviet intelligence with software that contained a Trojan Horse,[158] according to Reed. With the goal of severely disrupting the Soviet gas supply and economy, "the pipeline software that was to run the pumps, turbines, and valves was programmed to go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to the pipeline joints and welds."[159] The result was "the most monumental non-nuclear explosion and fire ever seen from space."[160] Though it was later determined that there were no injuries due to the remoteness of the explosion's location, physical damage to the pipeline itself did occur. [161]

Unlike denial of service actions, which are fairly uniform in their consequences, determining whether a chip-level action is an "attack" under IHL is more complicated. While denial of service actions are relatively uniform in their effects, especially with respect to a lack of physical damage

---

154 *Id.*

155 Reed, *supra* note 84, at 268.

156 *Id.*

157 *Id.*

158 This provides an example of one type of action that can be caused by malicious software, which is not separately addressed in this article.

159 *Id.* at 269. This is one of the earliest known examples of an action against a Supervisory Control and Data Acquisition ("SCADA") system.

160 *Id.*

161 *Id. See also* William Safire, Op-Ed, *The Farewell Dossier*, N.Y. Times, Feb. 2, 2004, at A21, *available at* http://www.nytimes.com/2004/02/02/opinion/the-farewell-dossier.html. CIA responsibility for the explosion was denied by a retired KGB officer, Vasily Pchelintsev, who headed the KGB's Tyumen region office in 1982. Anatoly Medetsky, *KGB Veteran Denies CIA Caused '82 Blast*, Moscow Times, Mar. 18, 2004. According to Pchelintsev, only one such explosion occurred that year on a natural gas pipeline in the Siberian wilderness and it resulted from faulty construction, rather than from faulty software. *Id.* (stating that a government commission found that that workers failed to put a bend in the pipe to protect it during sharp changes in temperature and they failed to put sufficient weights on it to keep it down in the marshland). Pchelintsev also stated that the explosion occurred in April, rather than in Summer, as Reed claimed, and he confirmed that there were no injuries as a result of the explosion. *Id.* According to Pchelintsev, the resulting physical damage only required one day to repair. *Id.*

to computers or networks, the effects of chip-level actions vary. Chip-level effects range from a permanent backdoor in a computer or network that can be accessed and exploited for intelligence purposes to the ability to affirmatively cause physical destruction.[162] In between these two extremes, chip-level actions may be used to render a system ineffective, as with the rumored action against the Syrian air defense system, or non-functional, as with the suspected "kill switches" placed into export-versions of French missiles and the known instance of "contrived" microchips directed at Russian military systems.

Applying the consequence-based methodology to chip-level actions yields easy answers at the extremes. Chip-level backdoors may be subject to IHL governing espionage, but they are not attacks under IHL. Conversely, using a chip-level action to cause intentional destruction, such as a pipeline explosion, clearly is an attack to which all the rules and protections of IHL apply. The harder case is that of the potential use of "kill switches."

In the case of the Syrian air defense system, chip-level action was possibly used to render the system ineffective without the need to bomb the command-and-control facility or a substantial amount of the air defense emplacements. First, it is worth applying the consequence-based methodology to what was not alleged to have occurred, as that type of action may arise in the future. The action did not, by itself, induce the firing of an errant missile or some other action that resulted in a violent consequence. In that event, the chip-level action would have been taken with the intent that the chip's programming would, on its own initiative, launch a missile (a kinetic act). Such a chip-level action should be considered an attack under IHL. It also does not appear that the chip-level action was used to cause false information to be fed into the system in order to induce the system operator to fire an errant missile or take some other kinetic action in response to the false information. If false information was fed into the system and it was reasonably foreseeable that it could induce kinetic acts or other actions by the system operators that would result in violent consequences, then the use of the chip to provide such information would also constitute an attack under IHL.

As for what is rumored to have occurred to the Syrian air defense system, the question becomes, for purposes of applying IHL, is the chip-level action separable from the subsequent air strike on the suspected reactor? If it is separable, then should the subsequent air strike be considered a foreseeable consequence (an obviously violent one) that triggers application of IHL to the chip-level action?

The default interpretation of Additional Protocol I appears to be that elements of an attack are

162 Although it is not clear whether the Siberian natural gas pipeline explosion was, in fact, caused by chip-level action, given the advances in technology in the past three decades, the possibility cannot be ruled out. Although focused on the threat from malicious software (which could easily be introduced via a chip-level backdoor), pipelines are definitely on the short-list of critical infrastructure concerning U.S. policy makers. *See SCADA Systems and the Terrorist Threat: Protecting the Nation's Critical Control Systems: Joint Hearing Before the Subcomm. on Econ. Sect'y, Infrastructure Protection, and Cybersecurity with the Subcomm. on Emergency Preparedness, Science and Tech. of the H. Comm. Homeland Sec.,* 109th Cong. 2 (2005) (statement of Rep. Daniel Lungren, Chairman, Subcomm. on Econ. Sec., Infrastructure Protection, and Cybersecurity); *id.* at 10 (statement of Donald Purdy, Acting Director, Nat'l Cyber Sec. Division, U.S. Dep't of Homeland Sec.); *id.* at 17, 20 (statement of Sam Varnando, Director, Information Operations Center, Sandia Nat'l Laboratory). *See also* Byres, *supra* note 23, at 58–59 (describing the effects of malicious software, the Slammer worm, on control systems and highlighting the fact that the worm used at least five different pathways to get into the victimized control systems).

separable, at least for purposes of determining "military advantage."[163] Under this interpretation, if viewed on its own, the chip-level action against the air defense system is not an attack for IHL purposes. Although it appears to be a potential "but for" cause of the airstrike, it is not. The argument is that the airstrike would have occurred anyway and, if chip-level action were not available, then kinetic bombs would have been used to achieve the same effect, but with very different consequences in terms of the level of violence used. Here, again,[164] it is plain to see that, even though such action would not be subjected to the IHL distinction and proportionality analysis (because not an "attack"), the objectives of IHL are still achieved by using the chip-level capability in this restrained, but effective, manner. Of course, if viewed within the whole of the larger attack, the chip-level action is actually a small portion of that attack, and the IHL analysis would properly focus on the kinetic portion of the airstrike.

Even more intriguing than the use of chip-level actions against an air defense system is the potential use of chip-level action against individual weapons, such as air-to-air missiles. As has been shown,[165] this is a very real possibility, with a very distinct probability that it has already occurred. In an interesting twist, in such episodes the chip-level action is actually used to *prevent* a violent act, i.e., the proper functioning of the weapon. In other words, the capability of the weapon is degraded or disrupted because of the chip-level action against the weapon's information system (its internal computer). So, depending on the design of the chip-level action, the missile may not fire, or, even if it does, it may not arm, thus rendering it ineffective. A chip-level action used in this manner—to prevent the occurrence of an "act of violence" by the adversary—is not itself an act that has violent consequences and therefore is not an attack under IHL.

Moving out of the realm of using "kill switches" against weapons, it is necessary to examine the use of such actions, whether chip-level or not, against more benign systems, such as telephone or cell phone systems.[166] For instance, during an armed conflict against an enemy using improvised explosive devices, a cell phone system could be targeted by an information-based action in order to

---

163 A minority of the 169 states that have ratified Additional Protocol I, many of them allies of the United States, included an understanding that emphasizes the use of "the attack considered as a whole" for purposes of determining the military advantage anticipated from an attack. The Declaration of New Zealand provides the best example of such a declaration:

> In relation to paragraph 5(b) of Article 51 and to paragraph 2(a)(iii) of Article 57, the Government of New Zealand understands that the military advantage anticipated from an 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 that attack and that the term "military advantage" involves a variety of considerations, including the security of attacking forces.

Additional Protocol I, *supra* note 7, Reservation by New Zealand, Aug. 2, 1988.

164 See *supra* note 122 and accompanying text (discussing this issue with respect to the NATO attack on the Serbian television station during the Kosovo campaign).

165 *See supra* note 132 and accompanying text (describing the placement of defective chips in Soviet military systems).

166 Jensen, *supra* note 61, at 1166–67 (arguing that military commanders must weigh the military necessity of the CNA in deciding whether to target a telephone system).

disrupt or deny the ability to explode the devices.[167] Such an action is normally temporary in nature, designed to last for the length of the military operation or perhaps the passage of a convoy. As with the example of the chip-level action directed at an enemy's missiles, this information-based action is designed to prevent an act of violence. In fact, if done correctly, there are no violent consequences at all.[168] Such an action is not an attack under IHL and, although an evaluation of military necessity might occur as a matter of policy, it is not legally required.[169]

IV. Implications for Law and U.S. Doctrine

The preceding sections conclude that not all information-based actions against information systems or computer networks meet the international humanitarian law definition of "attack." In fact, many do not. This conclusion has substantial implications for much of the ongoing academic legal discussions regarding the state of international law in this area, including claims that new treaties are necessary. There are also significant implications for U.S. doctrine in this area. Those implications are addressed in the following sections.

A. Implications for Law

Much of the academic debate in this area has centered on applying the IHL principle of distinction to information-based actions and capabilities..[170] While often admitting the lack of available knowledge given the classified nature of the subject matter, many commentators find that information-based actions are problematic because of the belief that such capabilities, for instance, denial of service actions, cannot discriminate between military and civilian objects..[171] Some commentators have also focused on the indiscriminate nature of such "weapons," comparing them to biological and chemical weapons,[172] at least in their reach if not always in their physical consequences. Finally, some commentators, confronted with the distinction problems posed by "computer network attack" have concluded that existing international law is insufficient and have called for the creation of new

167 *Cf.* Technology, Policy, Law, *supra* note 44, at 1 (defining "cyberattack" similarly to "computer network attack" and stating that "[d]omestic law enforcement agencies also engage in cyberattack when they jam cell phone networks in order to prevent the detonation of improvised explosive devices.").

168 It is not a violent consequence of the information-based action if the IED later explodes while the adversary is examining it to see why it did not explode earlier.

169 *But cf.* Jensen, *supra* note 61, at 1166 (stating that IHL applies "just as [it] would to any other target" to "temporarily debilitating the communication networks for the opposing force's telephone systems.").

170 *See, e.g.*, Kelsey, *supra* note 123.

171 *See Id.* at 1436–39; Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 Lewis & Clark L. Rev. 1023, 1042–44 (2007); Brown, *supra* note 57, at 193–97; Mark R. Shulman, Note, *Discrimination in the Laws of Information Warfare*, 37 Colum. J. Transnat'l L. 939, 953-57 (1999).

172 Brown, *supra* note 57, at 195–97 (arguing that computer viruses and other malicious code "that make [] no distinction between lawful and unlawful targets should be prohibited.").

international law to govern this area.[173] A treaty text has even been proposed.[174]

A new treaty is not needed, however. Instead, more precision is needed in identifying exactly what is an attack under IHL, and what is not. The conclusion of the foregoing analysis is that only those information-based actions that have violent consequences are attacks under IHL. Specifically, DDoS actions are simply not attacks under IHL. They may be annoyances and they may be harassment, but they do not cause physical damage or other violent consequences that equate to an "act of violence."

With denial of service actions out of the equation, one can see that the distinction problem is much less dramatic than has been portrayed. In fact, the examples discussed in the earlier analysis demonstrate that, to be effective, an information-based attack must be tightly focused with respect to how the attack capability is delivered to the target and the anticipated outcome. The implication of that observation is that real-world, information-based attack capabilities must be target-specific in their design and heavily dependent on accurate intelligence for proper design, delivery, and expected consequences.

Calls for a new treaty to govern this new area of warfare are premature for two reasons. First, to the extent that such calls were based on a perceived distinction problem because of the effort to fit every type of information-based action under the umbrella of IHL, this article demonstrates that concern is overblown, especially where that concern is based on denial of service actions.[175] Second, there is insufficient state practice in this area to ascertain what additional controls might be needed or what current rules need to be clarified. No state has publicly acknowledged carrying out an information-based action that has risen to the level of an attack under IHL.[176] Even if Russia were to acknowledge a formal role in the denial of service actions against Georgia, those actions would not implicate IHL.

B. Implications for U.S. Doctrine

The primary reason for the terminological imprecision that this article has attempted to address is the flawed definition of "computer network attack" in United States Information Operations doctrine. The "computer network attack" definition is legally unsound because it is overbroad and

---

173 *See* Hollis, *supra* note 171, at 1023; Brown, *supra* note 57, at 180–81; *see also* William J. Bayles, *The Ethics of Computer Network Attack*, PARAMETERS 44, 56–57 (2001) (discussing the main issues that a US computer network attack policy should address).

174 Brown, *supra* note 57, app. at 215–20.

175 *See* Brown, *supra* note 57, at 188 (stating that "[a] denial-of-service attack is another example of an information attack under the results-oriented approach."); Hollis, *supra* note 170, at 1033 (pointing to denial-of-service actions against Estonia as "open[ing] up the possibility that [Information Operations] will create new battlefields for state-to-state conflicts").

176 The details surrounding the CIA covert "feed" operation that led to the pipeline explosion were released in two informal publications, though one was published by the CIA's Center for the Study of Intelligence. *See generally* Weiss, *supra* note 85. These details have not been publicly confirmed by the United States.

inclusive of many actions that actually are *not* attacks under IHL.[177] The risk is that this overinclusive definition will come to be seen as state practice.[178] To infer from Ian Brownlie, it is an attack because states call it an attack.[179] If the overinclusive definition does become accepted as state practice,[180] such that the limiting effect of "violence" is read out of Article 49, the real risk becomes migration of this concept to other areas of warfare. Such a result would accelerate an already evident trend toward treating any military action that impacts civilians, however slight the impact, as prohibited, despite the lack of legal support for such a trend in IHL. This trend should be resisted.

United States doctrine defines a "computer network attack" as "actions 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."[181] The problem with the definition, as has been repeatedly shown in the examples and analysis in this article is that disrupting and degrading information in computers rarely, if ever, leads to the kinds of consequences that are an attack under IHL. Those concepts should be removed from the definition of "computer network attack," and placed in a separate category under "computer network operations."[182] In other words, because "computer network attack" uses the word "attack," it needs to comport with the definition of "attack" under customary international law. To do that, "computer network attack" should only cover those actions that cause violent consequences (death, physical injury, or damage or destruction

177 It might be argued that the U.S. definition is purposefully overinclusive in order to ensure, as a matter of policy, that more actions are subject to the constraints on attacks under IHL and are subjected to the principles of proportionality and necessity. However, there is no statement to this effect in the U.S. manual. *See* JOINT PUBLICATION 3-13, *supra* note 26, at II-5. The Department of Defense legal assessment for this area was published prior to the adoption of a specific definition of "computer network attack." *See generally* DEPARTMENT OF DEFENSE, OFFICE OF GENERAL COUNSEL, AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS (2d ed. Nov. 1999), *reprinted in Computer Network Attack and International Law*, 76 J. INT'L L. STUDIES 1, app. at 467 (Michael N. Schmitt & Brian T. O'Donnell, eds. 2002) (stating that "[o]ne of the principal forms of information attack is likely to be computer network attack, or in today's vernacular, the 'hacking' of another nation's computer systems.").

178 It is entirely possible that this over-inclusive definition is already being viewed as state practice based on its inclusion in the AIR AND MISSILE WARFARE MANUAL. *See* AIR AND MISSILE WARFARE MANUAL, *supra* note 10.

179 *See* BROWNLIE, *supra* note 63, at 362 ("It would seem that use of these weapons could be assimilated to the use of force . . . . [because] the agencies concerned are commonly referred to as 'weapons' and as forms of 'warfare.'") (citation omitted).

180 The number of academic commentators citing the definition of "computer network attack" already indicates widespread acceptance of the definition. *See, e.g.,* Hollis, *supra* note 171, at 1030–31 (defining and using the term throughout); O'Donnell & Kraska, *supra* note 61, at 138 (same); Jensen, *supra* note 61, at 1146–48 (same); Schmitt, *supra* note 20, at 367 (same)*; but cf*. Brown, *supra* note 57, at 186 (accepting the definition, but rejecting the term as too "unwieldy" and using "information attack," instead).

181 JOINT PUBLICATION 3-13, *supra* note 32 at II-5.

182 At least one Russian information warfare theorist has done so. V.I. Tsymbal lists eight categories of systems, two of which are "[t]he debilitation of communications and scrambling of enemy data," and [t]he destruction of enemy computer nets and software programs." INFORMATION OPERATIONS, *supra* note 46, at 1946 (citing V.I. Tsymbal, Kontseptsiya "Informatsionnoy voyny" (Concept of Information Warfare), Speech at the Russian-US conference on Evolving Post-Cold war National Security Issues (Sept. 12-14, 1995)). This division of between "debilitation" (disrupting and degrading in the U.S. definition) and destruction is appropriate and in keeping with the IHL analysis developed in this article.

of property) when such consequences are reasonably foreseeable. In application, of course, this may become an event-by-event determination, because capabilities can be used to achieve a variety of outcomes, some violent and some not.

Of course, there are also those capabilities, such as denial of service that may always be on one side of the line or the other. In the cases where a capability is not an "attack," ensuring that it is properly designated as such will ensure that its use is not subject to unwarranted constraints. What becomes abundantly clear from applying a consequences-based definition of "attack" to such capabilities is the number of opportunities to substitute these non-attack options for kinetic action, with the exemplar being the bombing of the Serbian television station by NATO compared with the "Russian" denial of service actions against Georgian media and communication centers. The use of such attack substitutes should be encouraged.

C. Critique of the Air and Missile Warfare Manual

The Manual on International Law Applicable to Air and Missile Warfare (Air and Missile Warfare Manual) was released to the public in February 2010,[183] with the Commentary to the Manual released the following month.[184] Although not a treaty or a document that has state imprimatur, the Air and Missile Warfare Manual is an attempted restatement of IHL applicable to airborne operations.[185] Similar to the San Remo Manual on International Law Applicable to Armed Conflicts at Sea,[186] the Air and Missile Warfare Manual was created by an international Group of Experts under the sponsorship of the Program on Humanitarian Policy and Conflict Research at Harvard University.[187] The "Black-letter Rules" portion of the Manual was developed over a six-year period and adopted at a final meeting of the experts in May 2009.[188] The Air and Missile Warfare Manual "restates current applicable law,"[189] "based on the general practice of States accepted as law (opinio juris) and treaties in force."[190] According to the Commentary, "the sole aim has been to systematically capture in the text the lex lata as it is."[191] Such an assertion is problematic at best, if not wrong altogether, given the Air and Missile Warfare Manual's treatment of "computer network attack."

As an initial matter, it is hard to understand how a definition of "computer network attack" can be part of already extant IHL applicable to warfare, much less the specific regime of air and missile warfare, when there have been very few, if any, instances of such actions acknowledged by states. In other words, acknowledged state practice in this area is non-existent. Russia has not acknowledged

183 Claude Bruderlein, *Foreword* to AIR AND MISSILE WARFARE MANUAL, *supra* note 10, at iii-iv.

184 AMW COMMENTARY, *supra* note 30, at ii.

185 Bruderlein, AIR AND MISSILE WARFARE MANUAL, *supra* note 10, at iii ("This Manual provides the most up-to-date restatement of existing international law applicable to air and missile warfare, as elaborated by an international Group of Experts.").

186 SAN REMO MANUAL, *supra* note 8.

187 AIR AND MISSILE WARFARE MANUAL, *supra* note 10, at iii–iv.

188 *Id.* at iii.

189 *Id.*

190 AMW COMMENTARY, *supra* note 30, at 2.

191 *Id.*

state action behind the DDoS actions against Estonia or Georgia[192] and Israel has refused to acknowledge whether, and to what extent, information-based actions played a role in the attack on the suspected Syrian nuclear facility.[193] Likewise, much of the United States' efforts in this area remain highly-classified, including important annexes to the Joint Doctrine[194] and the Senior Suter project, which allegedly provided the technological capability that enabled the Israeli airstrike to go undetected.[195]

The *AMW Commentary* is inexplicably silent as well. There is no source provided for the definition of "computer network attack" used in the *Air and Missile Warfare Manual*. As there is no treaty that provides such a definition, the drafters of the *Manual* must intend that their definition of "computer network attack" is part of customary international law. Yet, there is no discussion of state practice or *opinio juris* to support such a determination.[196] As discussed previously, the bulk of the definition consists of the U.S. warfighting doctrinal definition (plus two problematic additions),[197] yet nowhere is that doctrinal definition cited or acknowledged. In fact, the only citation in the Commentary's discussion of the "computer network attack" definition is to the U.S. doctrinal definition of "information operations" contained in the Department of Defense Dictionary of Military Terms,[198] hardly a statement of binding legal opinion. There is simply no support provided for the notion that any definition of "computer network attack," much less this particular one, should be considered part of customary international law. Such a significant, unsupported addition severely undercuts any notion that the *Air and Missile Warfare Manual* constitutes *lex lata*. Instead, it appears that the incorporation of the term "computer network attack" and its definition into the *Air and Missile Warfare Manual* is an instance of precisely the type of innovation of the law that is disclaimed by the *Manual*'s drafters.[199]

Quite apart from the question of why such a definition was included at all, the chosen definition has at least two significant substantive problems. First, the definition of "computer network attack" is incompatible with the *Air and Missile Warfare Manual*'s own definition of "attack." This problem is, at least, recognized and acknowledged by the Commentary when it states that

The term "attack" in "computer network attack" is not meant to necessarily imply that all such operations constitute an attack as that term is used elsewhere in this Manual (see definition of "attack" as set forth in Rule 1 (e)). Some CNA operations may rise to the level of an attack as defined

192 *See supra* notes 101–102 and accompanying text.

193 Richard B. Gasparre, *The Israeli "E-tack" on Syria – Part I*, airforce-technology.com (Mar. 10, 2008) http:/www.airforce-technology.com/features/feature1625/airforce-technology.com (last visited Aug. 25, 2010) (stating that the Israeli Air Force has not provided any details on the raid and quoting the Israeli Defense Minister, Pinchas Buchris as stating "[h]ow the Israeli system works, [you] can't share with anybody . . . . Offensive and defence network warfare is very interesting, [but] it's very sensitive – any such capabilities are top secret.").

194 JOINT PUBLICATION 3-13, *supra* note 26, app. A, at 1 (stating that the operational supplement is classified and separately published).

195 *See* Fulghum, *supra* note 148 and accompanying text.

196 *See* AMW COMMENTARY, *supra* note 30, at 34.

197 *See supra* note 29.

198 *See* AMW COMMENTARY, *supra* note 30, at 34.

199 *Id.* at 2 ("No attempt has been made to be innovative or to come up with a *lex ferenda*").

in Rule 1(e), whereas others will not . . . .[200]

However, in this case, recognizing a difference in terms is simply not sufficient to overcome the negative effects of such legal imprecision. As previously demonstrated in this Article, there is already rampant confusion in popular and legal commentary such that "computer network attack" is often incorrectly used in place of "attack,"[201] which leads to the inclusion of actions that merely cause inconvenience, such as denial of service actions, as attacks.[202] The use of "attack" in "computer network attack" as used in the *Air and Missile Warfare Manual* will only lead to increased confusion.

The second problem with the definition is the addition of the terms "manipulate" and "gain control over the computer or computer network" to the framework of the U.S. doctrinal definition. These additions unnecessarily extend the definition to actions that could encompass acts of espionage rather than any kind of action in support of an attack or hostilities. In fact, the Commentary includes "penetrating a system to observe data resident therein" as an example of a "CNA operation" covered by the definition.[203] The additions are probably intended to ensure civilians that may operate systems, such as Senior Suter, in support of attacks are targetable under the direct participation in hostilities standard of the *Air and Missile Warfare Manual*. The problem, however, is that the definition extends the *Manual*'s direct participation in hostilities standard to spies, in essence making espionage part of "hostilities." Such a result is without precedent in international humanitarian law, which treats espionage and spies under separate provisions from those participating in hostilities, either as a combatant or unprivileged belligerent. The "gain control" language is also problematic because, as the Commentary makes clear, control can be used for a wide variety of purposes. But it should be those purposes that determine the legal significance of gaining control, not the fact of gaining control itself. For instance, prior to the 2003 Iraq War, Clarke and Knake relate that the United States had sufficient access and control over the Iraqi Defense Ministry e-mail system to send Iraqi military officers e-mails telling them how to surrender their equipment and urging them

200 AMW Commentary, *supra* note 30, at 34.

201 *See supra* notes 23, 25, 61 and accompanying text.

202 *See supra* notes 126–129, and accompanying text. As pointed out in *supra* note 129, even the AMW Commentary recognizes that temporary denials of internet access are merely "inconvenience" and that some experts do not consider it an attack. AMW Commentary, *supra* note 30, at 28 (commenting on the definition of "attack").

203 AMW Commentary, *supra* note 30, at 34.

to abandon their posts and return to their homes.[204] Although a valid and viable psychological operation, such an action should not be considered an "attack" under IHL, nor should it be improperly characterized as part of a "computer network attack." Even without the addition of those two terms, as discussed above in Section IV.B, even the remaining definition of "computer network attack" is problematic and should be revised in order to not encompass actions that do not meet the definition of "attack" under IHL.

V. Conclusion

When undertaking a fundamental rethinking of a concept as entrenched as "computer network attack," the likely result is a challenge to the existing paradigm. Being heard is sometimes the easy part; gaining acceptance is much harder. But such shifts have previously occurred in the area of information operations doctrine. At one time the term "Information Warfare" was just as entrenched in U.S. doctrine as "computer network attack" is today.[205] The reason it is no longer en vogue with the U.S. military is very similar to the argument made here for revising the current definition of "computer network attack": "The term 'information warfare,' as the U.S. military uses it, is too broad because in addition to offensive uses, it covers non-offensive uses such as operational security, deception, electronic counter-measures, psychological operations, and computer network defense."[206] As a result, "information warfare" was eliminated from U.S. doctrine when the most recent Joint Chiefs of Staff publication on Information Operations was published in 2006.[207]

This article is not advocating similar elimination for "computer network attack," but simply a revision of the term's definition to fully account for the nuances of IHL that this Article highlights. As was the case with "information warfare," the definition of "computer network attack" is overbroad. There are disruptive and degrading computer actions that do not lead to the kinds of consequences that constitute an attack under IHL. The definition should be revised to eliminate those actions and only encompass computer actions foreseeably resulting in violent consequences. More importantly, the disruptive and degrading actions that do not cause violent consequences should not be characterized as "attacks" in any new term devised to only cover those non-violent actions. As this Article makes clear, properly applying the definition of "attack" under IHL will increase the

204 Clarke & Knake, *supra* note 148, at 9–10. Although the text of the e-mail has not been released, Clarke & Knake use their sources to approximate the e-mail's text as follows:

> This is a message from United States Central Command. As you know, we may be instructed to invade Iraq in the near future. If we do so, we will overwhelm forces that oppose us, as we did several years ago. We do not want to harm you or your troops. Our goal would be to displace Saddam and his two sons. If you wish to remain unharmed, place your tanks and other armored vehicles in formation and abandon them. Walk away. You and your troops should go home. You and other Iraqi forces will be reconstituted after the regime is changed in Baghdad.

Id. at 10.

205 *Id.* at 21–24 (comparing Information Warfare and Information Operations).

206 Brown, *supra* note 57, at 186.

207 Joint Publication 3-13, *supra* note 26, at iii (Feb. 13, 2006) (stating in the summary of changes that "information warfare" as a term has been removed from Joint IO doctrine).

flexibility of military commanders to apply humane, non-violent means to accomplish military goals instead of using bombs and other destructive devices.