Rethinking Computer Network "Attack:" Implications for Law and U.S. Doctrine

Paul A. Walker
Rethinking Computer Network “Attack”

Implications for Law and U.S. Doctrine

Paul A. Walker
12/31/2009
RETHINKING COMPUTER NETWORK “ATTACK”: IMPLICATIONS FOR LAW AND U.S. DOCTRINE

I. INTRODUCTION
II. THE DEFINITION OF “ATTACK” IN INTERNATIONAL HUMANITARIAN LAW
   A. “ACTS OF VIOLENCE”
   B. DETERMINING WHETHER AN “ACT OF VIOLENCE” EXISTS
      1. ACTOR-BASED METHODOLOGY
      2. RESULTS-BASED METHODOLOGY
      3. CONSEQUENCES-BASED METHODOLOGY
III. CAPABILITIES USED IN INFORMATION-BASED ACTIONS
   A. DISTRIBUTED DENIAL OF SERVICE ACTIONS
   B. CHIP-LEVEL ACTIONS
IV. IMPLICATIONS FOR LAW AND U.S. DOCTRINE
   A. IMPLICATIONS FOR LAW
   B. IMPLICATIONS FOR U.S. DOCTRINE
V. CONCLUSION
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 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.

Article 49 of what is commonly known as Additional Protocol I to the 1949 Geneva Conventions defines "attack" in this 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

---

⁶ Id. at 655.
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 International Humanitarian Law for air and missile warfare, use 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) did not provide a definition of “attack,” but the ICRC study repeatedly uses the term in rules dealing with protection of the civilian

\(^8\) 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 that is examined in this paper, “act of violence,” is retained in the San Remo Manual formulation.

\(^{10}\) Manual on International Law Applicable to Air and Missile Warfare, Program on Humanitarian Policy and Conflict Research, Harvard University, pre-launch version (May 15, 2009), at 5 (stating that attack “means an act of violence, whether in offence or in defence.”) [hereinafter Air and Missile Warfare Manual].
population.\textsuperscript{11} Most of those rules are drawn either directly from Additional Protocol 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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{14} The key to understanding both articles, though, is the repeated use of "attack." It is "attack[s]" that cannot be directed against the civilian

\textsuperscript{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.


\textsuperscript{13} Id. (pointing to portions of Articles 51 and 52 as containing such principles).

\textsuperscript{14} Additional Protocol I, supra note 7, arts. 51, 52.
population or individual civilians. Likewise, it is an "attack" that shall not be directed at civilian objects. Article 51 also prohibits "indiscriminate attacks" against civilians, while Article 52 requires "attacks" to be "limited strictly to military objectives." But not every military operation or action is an "attack," as defined in Article 49 and used in these key provisions. 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. International humanitarian law ("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.

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

---

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").
attack." 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 methodology used to define an "attack" is then applied to known capabilities that may be (or, in some cases, have been) used in information-based operations or actions by a State. Such an examination is necessary not only because it is not well addressed by the

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 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).

22 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 traffic on the internet and at websites connected to the internet and effect 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 effected by a denial of service action, electrical company control systems generally operate separately from the internet, such that they cannot be effected by 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/pgarchive/Feb09/cyber.pdf (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).
legal literature, but also because "attack" is so comprehensively overused throughout our internet society. This is perhaps understandable in the media and the technical literature, where any adverse action against a computer or a computer network is termed an "attack." Unfortunately, this common parlance use of "attack" has bled over into legal analysis and also into military doctrine, specifically the United States doctrine of "Computer Network Attack." When the

23 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 Joint Publication 3-13, Information Operations, II-5, Feb. 13, 2006, available at http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf, 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.” The newly published Air and Missile Warfare Manual incorporated essentially all of this definition in its 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. Unfortunately, with the Commentary to the Manual not yet published, it is not possible to determine the basis for inclusion of such an expansive definition, especially one that, as demonstrated herein, is so clearly at odds with the customary international law definition of attack that the Manual itself also uses. See supra note 10. At the Manual’s rollout event at the American Society of International Law in February, 2010, the Manual was proclaimed to be declarative of lex lata, or law as it exists, rather than lex ferenda, or law as it should be. Simply including a definition of “computer network attack” at all renders this claim dubious, at best, as it is a term not used in any international treaty. To the extent that the forthcoming Commentary may claim that state practice is the basis for the use of this definition, such a claim is questionable, at best. Not only does the bulk of the “computer network attack” definition in the Manual come from the doctrine of one country, the United
meaning of "attack" is rigorously examined and applied to known action capabilities, 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, and perhaps most significantly, the doctrinal definition of "Computer Network Attack" used by the United States military is legally unsound and must be revised. These implications are particularly relevant at a time when the United States and Russia appear to be moving towards discussions of these issues. In light of the differing Russian approach to “computer network attack,” 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.

26 “Capability” is used, along with “action” throughout this article in an effort to be terminologically precise and, especially, to not call something 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. The use to which the capability is put becomes key.


28 See infra note 136.
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 chip-level actions. 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. Part V is the requisite conclusion.

II. THE DEFINITION OF “ATTACK” IN INTERNATIONAL HUMANITARIAN LAW

29 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 notes 116-121, infra.
The four Geneva Conventions concluded in 1949 use the word “attack” fourteen times without ever defining what constitutes an “attack.” Similarly, the body of treaties and international law that preceded the four seminal Geneva conventions sporadically referred to “attacks” or “attacking force” without need for further definition. 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. 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

---


31 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, supra note 22, art. 23.
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,”33 and provides the best starting point to understand 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”

33 Additional Protocol I, supra note 7, art. 49(1).
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,\(^{34}\) 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.\(^{35}\) 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. In the context of information weapons, the analogous activity usually involves a computer, keyboard and usually some type of software program, though the analysis below will also examine a hardware-based

\(^{34}\) 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.

action against information systems.\textsuperscript{36} 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 at high velocity and causes injury or death if it hits a person, or physical damage if it hits an object.\textsuperscript{37}

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, effect action of one sort or another against an information system or computer network. Those actions have

\textsuperscript{36} See infra notes 93-107.

consequences, consequences that may or may not be the desired result of the button pusher.\textsuperscript{38}

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 tremendous amount of doctrinal development by the world’s armed forces in this area.\textsuperscript{39} 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.\textsuperscript{40}

\textsuperscript{38} 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 State is legally unsound and risks expansion of customary international law in a direction not favorable to U.S. interests, see infra part IV.B.


\textsuperscript{40} Compare \textit{Information Operations, supra} note 40, 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
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.” The Commentary makes it clear that the intent of the drafters was to provide a broad definition of “attack.” But, this “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. The Commentary then goes on to characterize this offensive and defensive back and forth as “combat action,” 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.” As the Commentary makes clear, although the definition of “attack” was to be applied to all uses of the word in Protocol I, the definition was specifically excluded from Article 2 and placed in the section on

Information Operations as possible stand-alone capabilities) with INFORMATION OPERATIONS, supra note 40, 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).

41 Int’l Committee of the Red Cross [ICRC], COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949 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”)).

42 Id.

43 Id.

44 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”).
protects for civilians to give it “special significance” with respect to defining attacks against civilians for the purposes of distinction and proportionality.\(^\text{45}\)

**B. Determining Whether an “Act of Violence” Exists**

Given the fact that the Commentary is focused on 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 very out of context,\(^\text{46}\) the statement in the Commentary that “the term ‘attack’ means ‘combat

---

\(^{45}\) ICRC Commentary, *supra* note 31, at 603.

\(^{46}\) See text accompanying notes 32-33.
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 State’s will agree to accept. Regardless of whether they are parties to Protocol I, current state practice is to apply international humanitarian law 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.”

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

---

47 Schmitt, supra note 18, at 378.
computers systems and networks.  When these actions are used to gather information for analysis and production as intelligence, permissible espionage is occurring. Most, if not all, states have a decided interest in keeping the permissive international legal regime on espionage in place. Thus, any methodology that places that regime in jeopardy 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 determining whether international humanitarian law applies “to any given situation.” Simply put, according to Brown’s formulation, international humanitarian law applies “if an information attack achieves the same result that could have been achieved with bombs or bullets.” 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.

48 TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 190-192 (William A. Owens, Kenneth W. Dam, & Herbert S. Lin, eds., 2009) [hereinafter TECHNOLOGY, POLICY, LAW].
50 Id.
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.\(^{51}\)

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.\(^{52}\) 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 increase the humanitarian impact on battlefields precisely because information-based actions can accomplish the same or similar results without the destruction resulting from a kinetic strike.\(^{53}\) To equate the two as Brown’s results-

\(^{51}\) Id.

\(^{52}\) Id.

based approach does, would be to constrain these humanitarian ends by limiting the ability to use information-based actions under international humanitarian law.

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.” Brownlie goes on to find such “devices” to constitute a “use of force” not only because the military agencies called them “weapons,” but primarily because “these weapons are employed for the destruction of life and property.” 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.”

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 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 dogma or policy.


55 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.

56 Brownlie, *supra* note 44, at 362.

57 *Id.* at 362-63.
result of an “information attack,”\(^{58}\) where the resulting physical damage “could not otherwise be accomplished without conventional munitions.”\(^{59}\) 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 (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, that 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

\(^{58}\) Brown, supra note 40, 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.”).

\(^{59}\) Id.
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,\(^{60}\) 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\(^{61}\) 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 conflict" under Common Article 2.\(^{62}\) In both cases, he was building a case for why international

---

\(^{60}\) 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.

\(^{61}\) Professor Schmitt actually uses the term "Computer Network Attack," or "CNA" in his writings, but for consistencies 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.

\(^{62}\) 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.”).
humanitarian law 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."

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. 63 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 force boundary." 64 Importantly, according to Schmitt's formulation, the consequences of the information-based action must be reasonably foreseeable. 65

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

63 Schmitt, supra note 21, at 913.
64 Id. at 915. The factors are: severity, immediacy, directness, invasiveness, measurability, and presumptive legitimacy. Id. at 914.
65 Id. at 916
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."66

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. 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."67 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

---

67 *Id.* at 376 (emphasis in the original).
violent consequences is an "attack." Those violent consequences are exactly the kind that are contemplated in other provisions of Additional Protocol I: "shielding protected individuals from injury or death and protected objects from damage or destruction." He adds, "that inconvenience, harassment or mere diminishment in quality of life does not suffice; human suffering is the requisite criterion." 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" was secondary to his larger point regarding armed conflict, but it was the correct one to apply. In fact, of the three levels of Schmitt’s analysis discussed in this section, the consequence-based methodology was 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 attack. It also has the advantage of not being over-inclusive. Unlike Brown's results-based methodology, every action that yields a result that previously could only have occurred by kinetic means does not equate to

---

68 See id. at 377.
69 Id.
70 Id.
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 be incentivized to use information-based actions to accomplish the same results as kinetic means, but without the violent consequences.

III. CAPABILITIES USED IN INFORMATION-BASED ACTIONS

This section of the article 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 then 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\(^\text{71}\) actions.

\(^71\) This specific term comes from a recent *Foreign Affairs* article that identifies microchips as the “soft spot” in hardware-based information systems. Wesley J. 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 (1996),
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. 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. 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. When the subject is a computer or a network, the denial of service acts to prevent that computer or network from 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

72 Houle & Weaver, supra note 20.
73 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.
mitigate the effect of the action.\textsuperscript{75} 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.\textsuperscript{76} 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.\textsuperscript{77} Significantly, a DDoS action does not cause any physical damage to the targeted system or network.\textsuperscript{78} 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.\textsuperscript{79}

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

\textsuperscript{75} 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).

\textsuperscript{76} Larry Rogers, What is a Distributed Denial of Service (DDoS) Attack and What Can I Do About It?, \url{http://www.cert.org/homeusers/ddos.html} (last visited Nov. 29, 2009).

\textsuperscript{77} See, Householder, supra note 62, 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, see John Bumgarner & Scott Borg, \textit{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]; \url{http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf}, which discusses the impacts of a well-coordinated DDoS on the email and phone systems of Georgia.

\textsuperscript{78} Instead, the “primary goal” of a denial of service action “is to deny the victim(s) access to a particular resource,” Householder, supra note 62, at 1, and is often indistinguishable from heavy, legitimate loads on a network. \textit{Id.} at 2.

\textsuperscript{79} 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 65, at 6.
gives a DDoS action its increased effectiveness. Control over the required number of computers is accomplished in a variety of ways. Multiple individuals can cooperate, either formally or informally, to share "attack" scripts for DDoS actions, often for political or activist reasons. 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 the DDoS action. 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 visiting tainted websites, which loads the DDoS malware on the unsuspecting visitor; and by social engineering techniques that are designed to trick the computer's unsuspecting owner to load the DDoS software on his own system, often by opening an email or clicking on an email attachment. 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 via Internet Relay Chat protocols and communications links. This dispersion of effort is the primary reason that it is difficult to attribute DDoS

80 See Puri, supra note 61, at 1-2.
82 Id.
83 Id.
84 Id.
85 Id.
actions to the perpetrators. 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.

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 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. 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: private individuals acting in such way as to carry out objectives of direct benefit to a State's political and military policy, and

---

86 Id.
87 Id.
89 See infra notes 72-84 and accompanying text.
90 In 50 U.S.C. §413b(e), “covert action” is defined 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.”
done in such a way that State involvement can be denied. 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."91 US-CCU also concluded, however, that the organizers of the DDoS actions "had advance notice of Russian military intentions" and "were tipped off about the timing of the Russian military operations while these operations were being carried out."92 Reports at the time indicated that the DDoS action preceded the Russian military advance by as much as 24 hours.93 Such "close cooperation"94 apparently occurred well before the actual military action was initiated because the actions were not preceded by the usual level of reconnaissance and mapping required to shut down the Georgian sites as quickly and effectively as this DDoS action did.95 In addition, US-CCU also concluded that "the signal to go ahead

---

92 Id. at 3.
94 US-CCU Overview, supra note 65, at 3.
95 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 74. 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 65, at 5.
[with the DDoS action] had to have been sent before the news media and general public were aware of what was happening militarily."96

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.97 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.98 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.99 These second wave actions occurred after Russian troops took

96 Id. at 3.
97 Id. at 6 ("The targets for attack were nearly all ones that would produce benefits for the Russian military.").
98 Id. at 4.
99 Id. at 4. See also Evgeny Morozov, An Army of Ones and Zeros: How I Became a Soldier in the Georgia-Russia Cyberwar, SLATE, Aug. 14, 2008 (describing his effort to “enlist” in the
positions inside Georgia,\textsuperscript{100} again indicating 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."\textsuperscript{101} These actions sowed considerable confusion, preventing the organization of an effective response by the government and disrupting patterns of civilian communications and normal business operations.\textsuperscript{102}

Significantly, the DDoS actions did not cause physical damage\textsuperscript{103} and they ended soon after the completion of Russian military activity.\textsuperscript{104} 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 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), http://www.slate.com/id/2197514/.

\textsuperscript{100} US-CCU Overview, \textit{supra} note 65, at 5.
\textsuperscript{101} \textit{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.
\textsuperscript{102} \textit{Id.}
\textsuperscript{103} 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." \textit{Id.} But these types of attacks did not occur, despite the fact that the sophisticated manner in which the narrowly focused DDoS and website defacements were carried out indicated "considerable technical expertise" on the part of the initiators. 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." \textit{Id.}
\textsuperscript{104} \textit{Id.} at 6.
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 sever (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.105

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.106 In fact, if the hand of Russia was, indeed, behind the denial of service actions against Georgia, such action stands as a silent, 

105 Id.
106 BBC News, Bombed Serb TV Back on Air, BBC Online, April 23, 1999, http://news.bbc.co.uk/2/hi/europe/326339.stm. US-CCU assumes that the effectiveness of the DDoS action meant there was no need to bomb those facilities. US-CCU Overview, supra note 65 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 supra note 43 and accompanying text.
unacknowledged rebuttal to NATO’s attack, which resulted in sixteen deaths and only kept the television station off-air for six hours.\textsuperscript{107}

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,\textsuperscript{108} specifically Google.\textsuperscript{109} 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, it is easy to see that a denial of service action is not an attack under international humanitarian law. 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

\textsuperscript{107} BBC News, \textit{supra} note 85. 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. \textit{See} Jeffrey T.G. Kelsey, Note, \textit{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.” \textit{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).

\textsuperscript{108} US-CCU Overview, \textit{supra} note 65, at 7.

\textsuperscript{109} CLARK \& LEVIN, \textit{supra} note 59, at 3.
such consequences. The economic disruptions that resulted were temporary in nature and did not result in the kind of 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 that are more tenuously connected to Russia than the actions against Georgia.\textsuperscript{110}

The conclusion that IHL does not apply to even very sophisticated, targeted denial of service actions is not surprising. After all, denial of service actions are probably the most commonly occurring adverse action on the internet, occurring on a daily basis without violent consequences resulting.\textsuperscript{111} Such actions, while disruptive to targeted businesses and websites, are generally viewed as temporary annoyances, rather than serious threats to cause violent consequences.\textsuperscript{112} 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

\textsuperscript{110} See Bright, supra note 70.
\textsuperscript{112} 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”).
actions taken by businesses, organizations (national or international), and
governments.\textsuperscript{113} Denial of service actions are properly viewed as harassment, and
not attacks, under international humanitarian law.

\textbf{B. Chip-Level Actions}

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 \textit{Foreign
Affairs}, however, has highlighted the dangers of compromised microprocessor
chips.\textsuperscript{114} Clark and Levin point out that, as early as 1982,\textsuperscript{115} 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."\textsuperscript{116}

Chip-level actions against the hardware component of an information system
or computer network have certain advantages over software- or externally-based

\textsuperscript{113} \textit{See generally} Dorothy E. Denning, \textit{Activism, Hacktivism, and Cyberterrorism: The Internet
as a Tool for Influencing Foreign Policy}, 16 COMPUTER SEc. J. 15 (2000), \textit{available at
http://faculty.nps.edu/dedennin/publications/Activism-Hacktivism-Cyberterrorism.pdf.}
\textsuperscript{114} \textit{Id. at} 4.
\textsuperscript{115} 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. \textit{See United States v.
Morris}, 928 F.2d 504 (2d Cir. 1991).
\textsuperscript{116} \textit{Clark &Levin, supra} note 59, 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. \textit{See infra}, notes 107-115 and accompanying text.
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. Assuming accurate and actionable intelligence support, then, chip-level actions have the capacity to be very effective against information systems or networks.

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. 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. A chip can also be altered by adding extra logic on to the chip itself. This addition could occur either by adding extra transistors to the chip during the 400-step manufacturing process or by incorporating extra transistors into the design-stage of the chip manufacturing process.

---

117 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).

118 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. 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. Id.

119 Id.

120 CLARK & LEVIN, supra note 59, at 5.
The second type of chip-level action, creating a backdoor in the chip logic to allow someone from outside the targeted system to enable (or disable) specific functions, occurs by placing extra logic on the chip using one of these methods.

The chip alterations, whether physically or by design, are extremely difficult to detect. Because it is possible for a chip to hold up to a billion transistors, most chip testing programs only test for specific functionality. 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." If the chip contained a backdoor, it might then be possible to override any encryption used on

---

121 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 97, 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 97, at 2-6 (discussing the contractors and testing timelines for the chip-testing); CLARK & LEVIN, supra note 59, at 9-10 (discussing possible solutions to the need to safeguard the supply of domestically- and foreign-manufactured microchips).

122 Id. See also Adee, supra note 97, at 4-5.

123 CLARK & LEVIN, supra note 59, at 5.

124 Adee, supra note 97, at 2; see also CLARK & LEVIN, supra note 59, at 5 (stating that modern automated testing equipment "is designed to detect deviations from a narrow set of specifications; it cannot detect unknown unknowns.").

125 Adee, supra note 97, at 2.
the phone and obtain access to the conversation "in the clear." 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. 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," 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. Similarly, following the Israeli airstrike on a suspected

126 See, e.g., Adee, supra note 97, 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).
127 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 enemies location).
128 CLARK & LEVIN, supra note 59, at 8.
129 Adee, supra note 97, at 1.
Syrian nuclear facility in September, 2007, 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. 130

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. 131 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")

---

130 Adee, supra note 97, 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.").

131 See Weiss, supra note 59. The facts in this paragraph are drawn from Weiss’s article.
operation, with the assistance of 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."\footnote{132}

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, \textit{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."\footnote{133} 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.\footnote{134} To do so, the Soviets
were going to penetrate and steal the software from a Canadian company.\footnote{135} With
that company’s assistance, the CIA managed to provide Soviet intelligence with

\footnotesize
\textsuperscript{132} \textit{Id.}
\textsuperscript{133} Reed, \textit{supra} note 59, at 268.
\textsuperscript{134} \textit{Id.}
\textsuperscript{135} \textit{Id.}
software that contained a "Trojan Horse," 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." The result was "the most monumental non-nuclear explosion and fire ever seen from space."

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. 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 to computers or

---

136 This provides an example of one type of action that can be caused by malicious software, which is not separately addressed in this article.
137 Id. at 269. This is one of the earliest known examples of an action against a Supervisory Control and Data Acquisition ("SCADA") system.
138 Id.
139 Id. See also William Safire, 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.
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. 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

---

140 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. on Homeland Sect’y, 109th Cong. 2 (2005) (statement of Rep. Daniel Lungren, Chairman, Subcomm. on Econ. Sect’y, 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 22, 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).
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 separable, at least for purposes of determining “military advantage.” 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, 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, when viewed within the whole of the

141 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.

142 See supra note 107 and accompanying text for discussion of this issue with respect to the NATO attack on the Serbian television station during the Kosovo campaign.
larger attack, the chip-level action is actually a small portion of that attack, where
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, 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. For instance,
during an armed conflict against an enemy using improvised explosive devices, a

---

143 See infra note __, and accompanying text (describing the placement of defective chips in
Soviet military systems).
144 Jensen, supra note 43, at 1166 (using the example of targeting a telephone system).
cell phone system could be targeted by an information-based action in order to disrupt or deny the ability to explode the devices.\textsuperscript{145} 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.\textsuperscript{146} 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.\textsuperscript{147}

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

---

\textsuperscript{145} See TECHNOLOGY, POLICY, LAW, supra note 48, at 1 (defining “cyberattack” similarly to “computer network attack” and stating that “[d]omestic law enforcement agencies engage in cyberattack when they jam cell phone networks in order to prevent the detonation of improvised explosive devices.”).

\textsuperscript{146} 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.

\textsuperscript{147} Cf. Jensen, supra note 43, at 1166 (stating that IHL applies “just as [it] would to any other target” to “temporarily debilitating the communications networks for the opposing force’s telephone systems”).

47
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 international humanitarian law principle of distinction to information-based actions and capabilities. 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. Some commentators have also focused on the indiscriminate nature of such “weapons,” comparing them to nuclear and chemical weapons, 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

---

148 See, e.g., Kelsey, Note, infra note 107.
150 Brown, supra note 40, at 187.
insufficient and have called for the creation of new international law to govern this area.\textsuperscript{151} A treaty text has even been proposed.\textsuperscript{152}

A new treaty is not needed, however. Instead, more precision is needed in identifying exactly what is an attack under international humanitarian law, and what is not. The conclusion of the foregoing analysis is that only those information-based actions that have violent consequences are attacks under international humanitarian law. Specifically, distributed denial of service actions are simply not attacks under international humanitarian law. They may be annoyances, 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 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.

\textsuperscript{151} See Hollis, supra note 122, at 1023; Brown, supra note 40, at 180-81; see also William J. Bayles, The Ethics of Computer Network Attack, PARAMETERS 44, 57 (2001).
\textsuperscript{152} Brown, supra note 40, at 215-20.
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 international humanitarian law, this article demonstrates that concern is overblown, especially where that concern is based on denial of service actions. 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 international humanitarian law. Even if Russia were to acknowledge a formal role in the denial of service actions against Georgia, those actions would not implicate international humanitarian law.

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 inclusive of many actions.

153 See Brown, supra note 40, at 188 (stating that “[a] denial-of-service attack is another example of an information attack under the results-oriented approach”); Hollis, supra note 122, at1033 (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”).

154 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 Weiss, supra note 59, and have not been publicly confirmed by the United States.
that actually are not attacks under international humanitarian law. The risk is that this over-inclusive definition will come to be seen as State practice. To paraphrase Ian Brownlie, “it is an attack because states call it an attack.” If the over-inclusive definition does become accepted as State practice 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 international humanitarian law. 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.” The problem with the definition, as has been repeatedly shown in the examples and analysis in this article is that disrupting and degrading

155 As discussed at length in note 25, supra, 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.

156 See BROWNLIE, supra note 45, 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.’”).

157 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 122, at 1030 (defining and using the term throughout); O’Donnell & Kraska, supra note 43, at 138 (same); Jensen, supra note 43, at 1147 (same); Schmitt, supra note 18, at 367 (same); but cf. Brown, supra note 40, at 186 (accepting the definition, but rejecting the term as too “unwieldy” and using “information attack,” instead).

information in computers rarely, if ever, leads to the kinds of consequences that are
an attack under international humanitarian law. Those concepts should be
removed from the definition of “computer network attack,” and placed in a
separate category under “computer network operations.”159 In other words,
because “CNA” 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 of property) and 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,

159 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 32, at 194. This division of “debilitation” (disrupt and
degradation in the U.S. definition) and destroy is appropriate and in keeping with the international
humanitarian law analysis developed in this article.
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.

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.\textsuperscript{160} 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.”\textsuperscript{161} As a result, “information warfare” was eliminated from U.S.

\textsuperscript{160} Id. at 21-24 (comparing Information Warfare and Information Operations).
\textsuperscript{161} Brown, supra note 40, at 186.
doctrine when the most recent Joint Chiefs of Staff publication on Information Operations was published in 2006.¹⁶²

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 international humanitarian law that this article highlights. As this article makes clear, properly applying the definition of “attack” under international humanitarian law will increase the flexibility of military commanders to apply humane, non-violent means to accomplish military goals instead of using bombs and other destructive devices.

¹⁶² Joint Pub. 3-13, at iii (Feb. 13, 2006) (stating in the summary of changes that “information warfare” as a term has been removed from Joint IO doctrine).