The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict

Lesley Swanson
Loyola Law School Los Angeles, lesley.swanson@lls.edu

Follow this and additional works at: https://digitalcommons.lmu.edu/ilr

Part of the Law Commons

Recommended Citation
Available at: https://digitalcommons.lmu.edu/ilr/vol32/iss2/5

This Article is brought to you for free and open access by the Law Reviews at Digital Commons @ Loyola Marymount University and Loyola Law School. It has been accepted for inclusion in Loyola of Los Angeles International and Comparative Law Review by an authorized administrator of Digital Commons@Loyola Marymount University and Loyola Law School. For more information, please contact digitalcommons@lmu.edu.
THE ERA OF CYBER WARFARE: APPLYING INTERNATIONAL HUMANITARIAN LAW TO THE 2008 RUSSIAN-GEORGIAN CYBER CONFLICT

Lesley Swanson*

I. INTRODUCTION

In early August 2008, a full-scale war broke out between Russia and Georgia over the disputed territory of South Ossetia, a pro-Russian autonomous region of Georgia.¹ Bombs were dropped throughout the Georgian capital of Tbilisi, with Russian bombers targeting Georgia’s economic infrastructure, including the country’s largest Black Sea port, Poti, and the main road connecting the southern part of Georgia with the East.² In the two months leading up to this conflict, Georgia’s Internet infrastructure was also attacked and major Georgian website servers were brought down, hindering communication and causing confusion throughout the country.³ The kind of attacks used is known as distributed denial of service attacks.⁴ They are triggered

---

¹ Senior Production Editor, Loyola of Los Angeles International & Comparative Law Review (ILR), Volume 32; J.D., Loyola Law School, 2010; B.A., University of Southern California, 2007. I am grateful for the helpful comments and critiques of Professor Karl Manheim and the students of ILR. Most importantly, I want to thank my parents, my brother and sister, and Alex for their constant encouragement, support, and love.


³ Id.

when computers in a network are simultaneously ordered to bombard a website with millions of requests, which then overload the website server and cause it to shut down. These cyber attacks mainly hindered the Georgian government’s ability to communicate with its citizens, as well as other nations, both before and during the physical invasion by Russia. Official Georgian websites, including those for the President’s office, the Ministry of Foreign Affairs, and the Ministry of Defense were disabled, at least temporarily. Even after a cease-fire between the nations was ordered shortly after the physical invasion by Russia, major Georgian servers remained inoperable. The Russian-Georgian cyber conflict, which was perhaps the first time that cyber attacks were used alongside conventional military action, illustrates the havoc that can spread on the digital battlefield and re-energizes the debate over whether the laws of war apply to this new kind of warfare.

Whether the world is prepared or not, cyber weapons are becoming a staple of modern war. Combat no longer consists solely of physical attacks or invasions among nations with distinct military units. This new kind of warfare uses a target nation’s own technology against it, in order to bring down vital infrastructure. As Internet and computer technology continues to develop, so too will the methods and means of warfare. Moreover, given the low cost and wide availability of computers, as well as the ability to operate them anonymously, cyber attacks make for an attractive method of warfare. In recent years, there has been a dramatic increase in the number of cyber attacks, both by nations and by non-state actors.

5. Hart, supra note 3, at D1.
6. Id.
As modern society increasingly relies on global and domestic information structures, these structures tend to become targets during war and other hostilities. As described in a recent news article, a survey of the seventy largest Internet operators in North America, South America, Europe, and Asia found that malicious computer attacks were rising sharply and growing more sophisticated. Additionally, these attacks are being used not only in political conflict, but also in blackmail schemes and for the purpose of malicious mischief. While concerted online attacks have been a threat for years, the Russian-Georgian cyber conflict of 2008 illustrates how states are more forcefully engaging in cyber attacks as a way to weaken opponents’ critical infrastructures—systems and assets vital to national security, economic security, and public health and safety.

Currently, there is no provision in international humanitarian law (IHL) or customary international law (CIL) that explicitly outlaws cyber warfare or computer network attacks, either carried out independently or during times of war. This is understandable since the law of war dates back to the nineteenth century and has not yet been updated for applicability in the Information Age. Nonetheless, some legal restraints do apply.

This article argues that existing IHL principles should be used to analyze the legality of cyber attacks. Part II of this article discusses the increasing use of cyber warfare in international conflict. Part III of this article explains that IHL principles apply whenever cyber attacks, ascribed to a state, are more than simply sporadic in nature and are intended to cause, or will foreseeably cause, injury, death, damage, or destruction. On the other hand, IHL most likely does not apply in the absence of those

14. Id.
16. See infra Part III.A (discussing international humanitarian law, specifically the branch of international law that governs armed conflict).
17. Customary international law refers to aspects of international law that derive from custom and is reflected in state practice. See RESTATEMENT OF THE LAW (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES §102 (1986).
18. See HILAIRE MCCOUBREY, INTERNATIONAL HUMANITARIAN LAW: MODERN DEVELOPMENTS IN THE LIMITATION OF WARFARE 1 (2nd ed. 1998) (discussing how the principles of IHL have evolved to their present understanding).
consequences. Part IV applies IHL principles to the 2008 Russian-Georgian cyber conflict. Given the complexities and novelties involved in this new kind of warfare, however, Part V further proposes that the international community and powerful states should seek to supplement existing IHL principles with more explicit and transparent policies that best correspond to modern Internet technology and address the ways in which this technology can legally be used to carry out cyber attacks.

In sum, this article addresses the use of cyber or computer network attacks and considers how *jus in bello*, or the body of law concerned with what is permissible during hostilities, governs such conflict. This article ultimately seeks to answer the question: “Does a cyber attack constitute an act of war such that international humanitarian law principles apply and govern its use?”

II. RECENT CYBER ATTACKS ILLUSTRATE HOW STATES ARE MORE FORCEFULLY ENGAGING IN CYBER WARFARE AS A MEANS TO WEAKEN OPPONENTS’ CRITICAL INFRASTRUCTURES

The Internet has emerged as a powerful tool for government functions, information, and mobilization, as well as commerce and social networking. It has even become a way to disseminate ideological and political messages. With the increase in utilization of the Internet for more than just economic and social functions, the international community must be aware that it can also serve as a tool for conducting operations that lead to confusion, destruction, and even death. Examples of cyber attacks against nations in recent history underscore the potential implications in using the Internet as a weapon in war, as well as how there is now clear international recognition of cyberspace as a battlefield. This is evidenced by the fact that information warfare systems are currently being developed and used by at least 120 countries, including Peru, Iran, United Arab Emirates, Croatia, Vietnam, and Russia. In order to fully understand cyber attacks and their

---

19. See id. at 1-2 (describing the difference between *jus ad bellum* and *jus in bello*).
21. Id.
The Era of Cyber Warfare

implications, one must first define cyber warfare and its related concepts.

A. What is Cyber Warfare?

The U.S. Army’s Cyber Operations and Cyber Terrorism Handbook defines cyber attack as: “The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or to further social, ideological, religious, political or similar objectives. Or to intimidate any person in furtherance of such objectives.” Such harm could be inflicted on the computer network, as well as to physical facilities and persons. Cyber attacks are distinct from cyber crimes, which are governed by national criminal statutes and include such acts as identity theft and Internet fraud. Cyber attacks, unlike cyber crimes, involve “an aggressive act on the part of one adversary—whether an individual, a competing organization or a rival government—against another in an ongoing struggle for hegemony in the marketplace or the political arena.”

In order to fully comprehend what is meant by cyber warfare, the concept of “cyberspace” should also be explored. Essentially, cyberspace is the sum of electronic networks including, but not limited to, the Internet, where various information operations occur.

Information warfare, on the other hand, is narrower than information operations and is defined as “information operations conducted during time of crisis or conflict to achieve or promote


24. Solce, supra note 22, at 300-01.


specific objectives over a specific adversary or adversaries."\textsuperscript{27} Information warfare has been conducted since at least the sixth century BC.\textsuperscript{28} Even before the rise of cyberspace, warring parties used electronic deception and disruption as essential ingredients of "real war." For instance, the U.S. Air Force has had information warfare squadrons since the 1980s, which were used successfully during the first Gulf War.\textsuperscript{29} Information operations is an evolving discipline within many nations' militaries.

Cyber warfare is simply the latest form of information warfare,\textsuperscript{30} and can include computer network attacks (CNA), which consist of "operations to disrupt, deny, degrade, or destroy information resident in computers or computer networks, or the computers and networks themselves."\textsuperscript{31} A CNA essentially involves the "hacking" of another nation's computer network, but uses data systems, as opposed to physical weapons, to execute the attack.\textsuperscript{32}

\textbf{B. Recent Cyber Attacks and the Resulting Damage}

Cyber attacks that have taken place in the past few years illustrate how states are utilizing modern technology and more forcefully engaging in information warfare to weaken opponents' critical infrastructures. There is significant international concern that hostile foreign governments could preemptively launch computer-based attacks on integral national or regional systems, such as those supporting energy distribution, telecommunications,

\begin{itemize}
\item \textsuperscript{29} See Mark Thompson & Douglas Waller, \textit{Onward Cyber Soldiers}, \textit{TIME}, Aug. 21, 1995, at 40, available at \url{http://www.time.com/time/magazine/article/0,9171,983318,00.html}.
\item \textsuperscript{30} See Sinks, supra note 26, at 5.
\item \textsuperscript{31} \textit{Wired Warfare}, supra note 27, at 367 (quoting JOINT CHIEFS OF STAFF, DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS, JOINT PUBLICATION 1-02 203 (2001)).
\item \textsuperscript{32} OFFICE OF GEN. COUNSEL, DEP'T OF DEFENSE, \textit{AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS} 5 (May 1999). See also \textit{Wired Warfare}, supra note 27, at 367 (describing the specificity of a computer network attack in contrast to other types of attacks).
\end{itemize}
and financial services. Since everything from transportation to commodity supply to health care to public safety to military operations now relies on computer information systems, cyber attacks have the potential to cause far greater damage than conventional weapons.

Recent publicly-known cyber attacks include attacks on Lithuanian commercial and government websites in June 2008, attacks on Estonian government websites in 2007, an e-mail breach in the Pentagon in June 2007, and hacks into Pakistan’s state-owned telephone company’s website in January 2003. Around August 2008, distributed denial of service (DDoS) attacks temporarily disabled official Georgian websites, including those for the President’s office, the Ministry of Foreign Affairs, and Ministry of Defense, and led to communication problems throughout the country. Even more recently, it has been discovered that Chinese hackers have breached the White House computer networks on numerous occasions, obtaining e-mail communication exchanged among government officials.

Additionally, the damage caused by many of these attacks included injury, death, and property damage. In perhaps the most extreme example, the 2007 attacks on Estonian websites caused more than just confusion for the nation’s population. At the time of these attacks, Estonia had essentially instituted an “e-government” where many aspects of the government were carried

34. Id.
36. See Etling, supra note 4.
out online. In addition to bringing down many of Estonia’s critical government and commercial websites, the cyber attacks also caused the emergency phone number used for calling ambulances and the fire service to be unavailable for more than one hour. As a result, widespread social unrest and rioting left 150 people injured and one Russian national dead. In contrast, the Lithuanian attacks involved the defacement of government and commercial websites with anti-Lithuanian rhetoric and communist symbols. The government, however, was able to prepare sufficient defenses to these attacks. These two examples demonstrate that the damage from a cyber attack can often be unpredictable.

C. The Methods Used in Carrying Out a Cyber Attack

Cyber weapons are not like traditional weapons of warfare. Individuals or nations that use cyber weapons may choose from a variety of options, including syntactic, semantic, and mixed weapons. Syntactic weapons, which target a computer’s operating system, include malicious code, such as viruses, worms, Trojan Horses, DDoS, and spyware. Through DDoS attacks, like those used against Georgia, the cyber attacker shuts down a website by bombarding it with large amounts of traffic. Conversely, semantic weapons target “the accuracy of information to which the computer user has access.” In other words, a semantic attack consists of altering information that enters the computer’s system

41. Prince, supra note 35.
42. Id.
44. Id. at 27; Solce, supra note 22, at 305.
46. Solce, supra note 22, at 305 (quoting Vida M. Antolin-Jenkins, Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?, 51 NAVAL L. REV. 132, 144 (2005)).
in order to produce errors without the user’s knowledge. Mixed or blended weapons combine syntactic and semantic weapons to attack both information and the computer’s operating system, resulting in a more sophisticated attack. An example of a mixed weapon is a “bot network,” which is a proliferation of “bots,” surreptitiously planted on innocent third-party computers. Bots are remote-controlled computer programs that infect other computers. A hacker who controls the bots can spy, copy, and transmit sensitive data, as well as organize the bots in a swarm attack against targeted computers.

Attacked computers or networks are systems that have been infected with malicious software through the use of these weapons, and that are then brought under the control of an attacker in a remote location. Infected devices continually listen for commands from the attacker and act upon them, with the intention of compromising the opponent’s security or critical infrastructure.

The Internet was originally a network of computers linked to the U.S. Department of Defense in the 1960s and 1970s. As the computer networks of universities and private research facilities merged through the development of hypertext, a global network with benefits to both military and civilian sectors was created. The new technology, however, has also created vulnerabilities for nations that rely heavily on the Internet, especially in their military and governmental infrastructures. This has created an opportunity for warring parties to exploit network vulnerabilities with various cyber weapons and attacks.

48. Id. at 39.
49. See Solce, supra note 22, at 305.
51. Id. at 10-11.
54. Terry, supra note 53, at 492.
III. INTERNATIONAL HUMANITARIAN LAW SHOULD GOVERN THE LEGALITY OF CYBER ATTACKS WHEN SUCH ATTACKS CONSTITUTE ARMED CONFLICT

Information gathering and disruption have always been major tools of war. Disrupting an enemy’s communications networks may even have greater strategic value than destroying its arsenals or supply lines. Indeed, some information warfare methods are considered so unsavory as to be prohibited by the laws of war. While a cyber attack is not truly kinetic or physical in nature like traditional forms of weaponry, a cyber attack may still lead to major physical destruction and even death. Therefore, because of these possible consequences, a cyber attack could constitute an armed conflict, such that IHL governs, if certain criteria are met. The threshold question is under what circumstances can a cyber attack be deemed an armed conflict, such that IHL applies. This is an important question because its answer provides guidance to nations on how they can respond to such attacks in a way that is consistent with international legal norms.

A. International Humanitarian Law Background

IHL is the branch of public international law that “seeks to moderate the conduct of armed conflict and to mitigate the suffering which it causes.” It is one of two principle divisions of the laws of war and is termed jus in bello, or the “law in war.” The other division is known as jus ad bellum, or the “law to war,” which governs the legality of resorting to armed force. The terms “law of war” and “law of armed conflict” are synonymous.

Jus in bello traditionally involves both Geneva and Hague law. Geneva law rests on the four 1949 Geneva Conventions and the two 1977 Additional Protocols. These treaties are particularly concerned with the protection of the victims of armed conflict, with Additional Protocol I focusing on the means and methods of warfare. Conversely, Hague law refers to the 1899 and 1907 Hague Conventions, and is mainly concerned with methods and means of warfare, tactics, and the general conduct of hostilities. In modern

55. See supra Part II.B.
56. MCCOUBREY, supra note 18, at 1.
57. Id.
58. Id.
59. Id. at 2.
usage, IHL is taken to comprise *jus in bello* in both its Geneva and Hague dimensions.60

**B. The Applicability of IHL to Cyber Attacks**

The law of armed conflict, as a part of international law, is binding on states, yet a violation may also involve the prosecution of individuals for war crimes.61 Some have argued that IHL cannot govern cyber attacks because there is nothing physical or kinetic about such operations.62 In other words, a CNA is not an armed conflict in the true sense of the phrase and, therefore, such an attack falls outside of the scope of IHL. Article 2, which is common to all four of the Geneva Conventions, provides that “[i]n addition to the provisions which shall be implemented in peacetime, the present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them.”63 Additional Protocol I also relies on this same “armed conflict” language. Article 1(3) of Additional Protocol I states that “[t]his Protocol, which supplements the Geneva Conventions of 12 August 1949 for the protection of war victims, shall apply in the situations referred to in Article 2 common to those Conventions.”64 Thus, in order for IHL to govern a cyber attack, such an attack must in fact constitute an armed conflict.

Nevertheless, commentaries to the Geneva Conventions and their subsequent Additional Protocols have posited that “armed conflict” can be viewed in a fairly expansive way.65 Armed conflict has been defined as “any difference arising between States and leading to the intervention of members of the armed forces.”66 A

---

60. *Id.*
62. See *Wired Warfare*, *supra* note 27, at 368-69 (describing the arguments against the applicability of IHL to computer network attacks).
65. See UK MINISTRY OF DEFENCE, *supra* note 61, at 29; *Wired Warfare*, *supra* note 27, at 372-73.
dispute resulting in the engagement of armed forces, however, cannot be the sole criterion. For example, the replacement of border police with soldiers or an accidental border incursion by members of the armed forces would not amount to an armed conflict.\(^{67}\) Thus, some degree of intensity and duration must be considered, as underlying principles of IHL make clear.\(^{68}\) IHL is founded upon the idea that victims of armed conflict, including personnel who have been rendered hors de combat,\(^{69}\) are entitled to protection.\(^{70}\) This protection is "usually framed in terms of injury, death, or in the case of property, damage or destruction."\(^{71}\) Therefore, fundamental principles of IHL provide that armed conflict occurs when a group takes measures that injure, kill, damage, or destroy,\(^{72}\) thereby narrowing the definition of armed conflict and limiting its applicability.

From the above discussion, it logically follows that a cyber attack may constitute armed conflict, even though the use of a computer as a weapon is not a traditional or physical method of warfare, as long as certain consequences arise. While cyber attacks employ modern technology not conceived of during the drafting of the Geneva Conventions, the language of Additional Protocol I, and in particular Article 36, indicate that the drafters anticipated the application of the rules to new developments in warfare methods.\(^{73}\) The law of armed conflict must change and develop to account for new humanitarian imperatives that may be generated

---

67. See id.
68. See Wired Warfare, supra note 27, at 372.
69. According to Additional Protocol I, art. 41(1) and (2), a person is hors de combat if "he is in the power of an adverse party; he clearly expresses an intention to surrender; or he has been rendered unconscious or is otherwise incapacitated by wounds or sickness, and therefore is incapable of defending himself . . . ." Additional Protocol I, supra note 64, 1125 U.N.T.S. at 22.
70. MCCOUBREY, supra note 18, at 1.
71. Wired Warfare, supra note 27, at 373.
72. Id.
73. KNUT DÖRRMANN, APPLICABILITY OF THE ADDITIONAL PROTOCOLS TO COMPUTER NETWORK ATTACKS 2 (2004), available at http://www.icrc.org/Web/eng/siteeng0.nsf/htmlall/68LG92/$File/ApplicabilityofIHLtoCNA.pdf [hereinafter APPLICABILITY OF THE ADDITIONAL PROTOCOLS TO COMPUTER NETWORK ATTACKS]. Article 36 provides: "In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party." Additional Protocol I, supra note 64, 1125 U.N.T.S. at 21.
by the evolution in the conduct of armed conflict itself.\textsuperscript{74} In fact, IHL anticipates technological change. For example, the “Martens Clause” found in the Preamble to the Hague Convention IV of 1907 “asserts that even in cases not explicitly covered by specific agreements, civilians and combatants remain under the protection and authority of principles of international law derived from established custom, principles of humanity, and from the dictates of public conscience.”\textsuperscript{75} In other words, attacks should essentially be judged largely by their effects, rather than by how they are employed.\textsuperscript{76}

Additional Protocol I to the Geneva Conventions provides important guidance in assessing the applicability of IHL to cyber attacks. Additional Protocol I codifies many existing principles of CIL and introduces important new treaty provisions relating to international armed conflict.\textsuperscript{77} Some provisions of Additional Protocol I are controversial such that they are said to only bind state parties to the treaty and, thus, they do not reflect customary law.\textsuperscript{78} Nevertheless, the significance of Additional Protocol I, as it relates to cyber warfare specifically and \textit{jus in bello} generally, is that it supplements the original Geneva Conventions as they apply to civilians in an armed conflict as well as to the prohibited methods of warfare in situations of conflict.\textsuperscript{79}

A key aspect of Additional Protocol I is the “doctrine of unnecessary suffering,” which is fundamental to \textit{jus in bello} in general.\textsuperscript{80} Article 35 states: “In any armed conflict, the right of the Parties to the conflict to choose methods or means of warfare is not unlimited. It is prohibited to employ weapons, projectiles and material and methods of warfare of a nature to cause superfluous injury and unnecessary suffering.”\textsuperscript{81} This principle serves to place some limits on the barbarity and the range of means and weapons

\textsuperscript{74} McCoubrey, \textit{supra} note 18, at 32.
\textsuperscript{76} Greenberg et al., \textit{supra} note 75, at 11.
\textsuperscript{77} UK Ministry of Defence, \textit{supra} note 61, at 15.
\textsuperscript{79} Id. at 1169.
\textsuperscript{80} McCoubrey, \textit{supra} note 18, at 212.
\textsuperscript{81} Additional Protocol I, \textit{supra} note 64, 1125 U.N.T.S. at 21.
that are available in today's modern society. Furthermore, Additional Protocol I was the first treaty to set out specifically the principle of proportionality, which requires that the losses resulting from military action should not be excessive in relation to the expected military advantage.\textsuperscript{82} Proportionality closely relates to the concept of indiscriminate attacks. Article 51(5)(b) describes an indiscriminate attack as one that “may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.”\textsuperscript{83} These principles are important to cyber warfare because they require that the attacker refrain from attacks that may be expected to cause excessive collateral damage.

Similar to nuclear weapons, cyber weapons are arguably \textit{sui generis} or, in other words, they are unique in their characteristics and therefore should be governed by a unique set of laws.\textsuperscript{85} Nevertheless, cyber weapons, just like nuclear weapons, are weapons that result in consequences similar to that of traditional weapons. Accordingly, IHL principles, such as the concept of unnecessary suffering and proportionality, still have relevance in the case of a cyber attack. Often, the question simply will be: To what extent do these principles apply? While some uncertainties remain, what is clear from this discussion is that an “armed conflict” occurs when an actor takes measures that injure, kill, damage, or destroy, regardless of the weapon used.\textsuperscript{86}

Scholars agree that an armed conflict exists and IHL governs once kinetic weapons are used in combination with CNAs.\textsuperscript{87} The question becomes more difficult when computer networks conduct the first or only hostile acts. The key in assessing such conduct, however, is the effects or consequences of the attacks. Based on this framework, IHL applies whenever cyber attacks, ascribed to a

\begin{itemize}
\item \textsuperscript{83} Additional Protocol I, supra note 64, 1125 U.N.T.S. at 26.
\item \textsuperscript{84} UK MINISTRY OF DEFENCE, supra note 61, at 26.
\item \textsuperscript{85} See MCCOUBREY, supra note 18, at 244.
\item \textsuperscript{86} See Wired Warfare, supra note 27, at 373.
\item \textsuperscript{87} See APPLICABILITY OF THE ADDITIONAL PROTOCOLS TO COMPUTER NETWORK ATTACKS, supra note 73, at 2.
\end{itemize}
state, are more than simply sporadic in nature and are intended to, and actually do, cause injury, death, damage, or destruction or such consequences are foreseeable. Other scholars agree that cyber attacks that lead to the subversion of political, economic, and non-military information bearing on a nation's capabilities may also implicate international law principles. This surely will be the case, even if cyber attacks are the only means of force used, as long as the particular consequences mentioned above result. On the other hand, IHL would probably not pertain where the actual, foreseeable, or intended consequences do not include injury, death, damage, or destruction.

The reason why a consequence-based approach is necessary in analyzing the application of IHL to cyber attacks is because once armed conflict has commenced, the means by which injury, death, damage, or destruction are produced has no bearing on the legality of that conduct. Thus, a lone cyber attack is subject to IHL if these particular consequences result.

Article 48 of Additional Protocol I mandates that parties to a conflict direct their operations against military objectives. Thus, targeting a military object, such as military air traffic control system, would be permissible. Since it is often the case that a CNA would target not purely military objectives, the next question is whether targeting civilian computer networks or systems are permissible. Based on the language of Article 48, however, the prohibition is not so much on targeting non-military objectives as it is on attacking them through acts of violence. Consequently, IHL would prohibit cyber attacks directed against non-military objectives that are intended to, or would foreseeably, cause injury, death, destruction, or damage. On the other hand, an attack targeting a non-military objective that is not likely to result in the aforementioned consequences would be permissible.

88. See id. at 3; Wired Warfare, supra note 27, at 374.
89. See Terry, supra note 53, at 491-92 (stating that the author of the reviewed book argues that these attacks may well constitute an unlawful use of force under international humanitarian law).
90. Wired Warfare, supra note 27, at 375.
92. Wired Warfare, supra note 27, at 376.
93. Id. at 378.
94. Id.
IV. THE RUSSIAN-GEORGIAN CYBER CONFLICT ILLUSTRATES THE COMPLEXITIES IN APPLYING IHL TO CYBER ATTACKS

Since IHL may apply to cyber warfare in certain situations depending on the results of an attack, it is not necessary to create a completely new set of laws or form a new treaty to apply solely to cyber attacks. Nevertheless, applying IHL to the 2008 cyber conflict involving Russia and Georgia illustrates the difficulties in being able to implement fully IHL in these instances and to articulate concretely the reactions to such attacks. The most notable difficulties involve attributing responsibility for the attacks and determining the difference between military objectives and non-military objectives in the context of targeted websites and computer systems.

A. Was Russia Responsible for the Attacks on Georgian Websites?

Both Russia and Georgia are state parties to Additional Protocol I, which pertains to the protection of victims of international armed conflict. Thus, as parties to the treaty, its provisions bind them, including the duty before carrying out an attack to “do everything feasible to verify that the objectives to be attacked are ... military objectives.” Even for states not a party to the Protocol, customary law would still require their forces to attack only military objectives, meaning that these targets must be distinguished from civilian objectives. The Institute of International Law even points out that existing international law prohibits the use of all weapons that, by their nature, affect indiscriminately both military and non-military objectives.

Additional Protocol I further requires that in the time of armed conflict, states must ensure that legal advisers are available, when necessary, to counsel military commanders regarding the application of the Geneva Conventions and Additional Protocol

95. The list of state parties to Additional Protocol I is also located at http://www.icrc.org/ihl.nsf/WebSign?ReadForm&id=470&ps=P.
I. Therefore, both Russia and Georgia had an obligation to ensure that they were following IHL in their physical altercation in August 2008. Nevertheless, given the relatively small amount of equipment required to launch a cyber attack and the pervasiveness of the Internet, ascertaining whether Russia, as opposed to non-state actors, was responsible for the attacks on Georgian websites, such that legal implications are created, is extremely difficult. Conversely, actually engaging in cyber war or bombarding a website is relatively simple. As demonstrated by one reporter, all one needs to do is save a copy of a certain Georgian website to one’s hard drive and then open it on the computer’s browser. Once accessed, the page will load thumb-nailed versions of a dozen key Georgian websites in a single window. All the cyber “soldier” must do is set the page to update automatically every three to five seconds and from then on the browser will continue to send thousands of queries to the most important Georgian websites, helping to overload them and bring them down. This is the simple way of bringing down a website, but there are more sophisticated and creative options, including obtaining certain kinds of software to carry out DDoS attacks.

The evidence is currently not clear whether Russia was involved in the shutdown of Georgian websites or whether the attacks can be attributed to non-state actors. Jose Nazario, an Internet security specialist, believes that non-state actors likely caused the attacks on Georgian websites, because there is a history of the kind of botnet attacks involved previously attacking commercial or non-political targets. Cyber attacks are often difficult to trace and it can take several months to reach definitive answers. For example, in 1998 an investigation by U.S. intelligence

---

101. Id.
103. PBS News Hour, supra note 102.
officials initially linked Iraq to a series of breaches of the Department of Defense computers. The real suspects ended up being two teenagers in Northern California.  

Project Grey Goose, an open-source initiative launched on August 22, 2008, has examined the Russian-Georgian cyber war and has drawn conclusions regarding the Russian government's involvement in the attacks. The group based its conclusion on data collected from two Russian hacker forums, www.xakep.ru and www.stopgeorgian.ru, along with network log files detailing 29,000 status events indicating the up/down status of 149 Georgian websites. In its Phase I Report issued on October 17, 2008, Project Grey Goose concluded that "the Russian government will likely continue its practice of distancing itself from the Russian nationalistic hacker community thus gaining deniability while passively supporting and enjoying the strategic benefits of their actions." The group was unable to find any direct link to Russian state organizations guiding the attacks, but maintained that there is significant historical evidence that Russian officials endorse cyber warfare initiated by their country's hacker community. For example, General Vladislav Sherstyuk, the current Russian Federation Security Council Deputy Secretary and former Deputy Director of the Federal Agency for Government Communications and Information, stated in 2002 that "strike-capable military computer viruses" would be used in the cyber battlefield. Furthermore, a letter from a Russian Duma member stated in March 2006: "In the very near future many conflicts will not take place on the open field of battle, but rather in spaces on the Internet, fought with the aid of information soldiers, that is hackers."  

As Project Grey Goose noted, it is unreasonable to conclude that there is no connection between Russian hackers and the

106. Id. at 2.  
107. Id. at 6.  
108. Id.  
109. Id.  
110. Id. at 7.
Russian government. There has been consistent support from members of the Russian government and essentially an implied consent in its refusal to intervene or stop the hackers' attacks. If indeed the Russian government or persons acting on behalf of the Russian government were responsible for the attacks on Georgian sites, then the only question as to the applicability of IHL would be whether such attacks resulted in death, damage, destruction, or injury.

Besides the possibility of ordinary Russian citizens being responsible for the attacks, analysts have also accused the Russian Business Network (RBN), a network of criminal hackers with close links to the Russian mafia and government, of the Georgian attacks. Visits to Georgian government websites seemingly were re-routed through servers in Russia and Turkey where the traffic was blocked. According to experts, these servers are widely known to be under the control of the RBN and influenced by the Russian government. If the RBN were acting on behalf of the Russian government, then this would constitute conduct by a state.

If the actors were civilians, the problem in applying IHL becomes more complex. Even civilians or non-state actors who attempt to neutralize an enemy network, via a CNA that results in the aforementioned consequences, could be considered as direct participants in hostilities for purposes of Geneva law. This would mean that these civilians are illegal combatants and, therefore, not immune from retaliatory attack. Civilians could also be subject

111. Id. at 8. See also THE EVOLVING STATE OF CYBER WARFARE, PROJECT GREY GOOSE PHASE II REPORT Chap. 3 (Mar. 20, 2009), available at http://www.scribd.com/doc/13442963/Project-Grey-Goose-Phase-II-Report (stating that there is new evidence pointing to how the Russian government pays leaders of Russian youth organizations to engage in information operations to silence or suppress opposition groups).

112. Swaine, supra note 102.


114. APPLICABILITY OF THE ADDITIONAL PROTOCOLS TO COMPUTER NETWORK ATTACKS, supra note 73, at 3.


to criminal prosecution under domestic law for the mere fact of taking part in hostilities.\textsuperscript{117}

If the actors who carried out the cyber attacks against Georgia were members of Russia’s armed forces, such personnel would have all the rights and liabilities of combatants. They could be attacked in retaliation like any other military personnel and could be able to achieve prisoner of war status. Again, the situation becomes more problematic when the technicians that act for the nation or military are not incorporated into the armed forces, but rather are simply computer-savvy civilians.\textsuperscript{118}

\textbf{B. Defining Military Objectives}

As mentioned above, in the context of military operations, only military objectives may be directly attacked. The definition of military objectives as provided in Additional Protocol I may be considered a part of CIL. Under Article 52(2) of the Protocol, “military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.”\textsuperscript{119} Military equipment and their facilities, other than medical and religious structures, are clearly military objectives and, therefore, subject to direct cyber attacks.\textsuperscript{120}

The problem arises, however, when dual-use objects, objects that serve both military and civilian purposes such as airports and bridges, are targeted. The source of the dilemma in clearly defining military objectivés versus non-military objectives is in interpreting the terms found in Article 52 of Additional Protocol I.\textsuperscript{121} Commentaries to the Protocol seem to define military objectives more narrowly, stating that they are objects “directly used by the armed forces,” locations “of special importance for military operations,” and objects intended for use or being used

\textsuperscript{117} INTERNATIONAL HUMANITARIAN LAW, supra note 115, at 9.


\textsuperscript{119} Additional Protocol I, supra note 64, 1125 U.N.T.S. at 27.

\textsuperscript{120} Wired Warfare, supra note 27, at 380; APPLICABILITY OF THE ADDITIONAL PROTOCOLS TO COMPUTER NETWORK ATTACKS, supra note 73, at 5-6.

\textsuperscript{121} See Wired Warfare, supra note 27, at 380, 384-85.
for military purposes. In contrast, nations like the United States take a more expansive approach by including economic targets as military objectives.

Essentially, once the determination is made whether a cyber attack caused injury, death, damage or destruction, opinions will likely differ on whether the intended target was a civilian or military object. Chances are that if the attack results in none of the aforementioned consequences, the fact that a civilian object was targeted will probably be of little concern. This again underscores why the results of a cyber attack are central to the legal analysis.

C. The Attacks on Georgian Websites Likely Do Not Amount to an Instance of Armed Conflict, Such That IHL Governs

Assuming that Russia was responsible for the cyber attacks on Georgia, the next question must be whether IHL governs this conflict. While the cyber attacks on Georgia appeared to eventually be part of a classic conflict in which the Russian military later invaded Georgia, the cyber conflict itself did not result in the kinds of consequences necessary to rise to the level of an armed conflict. As previously mentioned, during the cyber conflict, major Georgian servers were brought down, resulting in confusion throughout the country and hindering communication. An argument could be made, perhaps, that damage or destruction was done to Georgian property, even if death or injury did not occur. Nevertheless, because it appears that the main results of the Georgian attacks were confusion and inconvenience, the attacks were thus permissible, regardless of whether the targets were deemed military or non-military objectives.

Even so, cyber attacks that result in confusion, miscommunication, or the temporary shutdown of networks are serious problems, and can be harmful to countries that rely heavily on the Internet. Furthermore, it is entirely possible for the shutdown of a nation’s major websites to lead to far greater consequences.

Because investigators in one country do not ordinarily have the authority to cross international borders, the investigation into

122. Id. at 380.
123. Id. at 380-81.
124. See Hart, supra note 3, at D1.
125. See Wired Warfare, supra note 27, at 380-81.
the source of a cyber attack is often difficult. Law enforcement or national security personnel cannot unilaterally pursue investigations into networks located in other countries. Just as it is difficult to determine who conducted a cyber attack, it is equally difficult to determine what a permissible retaliatory response to this kind of attack is, especially when the attack inflicts minimal damage. In the absence of death or widespread destruction, whether the international community would consider a conventional military attack a proportionate response is questionable. For example, although the United States recognizes that initial patterns of attack or infiltration can rise to the level of an armed attack, it takes the position that reprisals involving armed conflict or the use of force are illegal. The United States thus justifies a responsive use of force in the exercise of the right of self-defense. Some also argue that cyber attacks require an expansion of the definition of the use of force, such that there would be greater permissible responses through self-defense. But expanding the definition in order to create greater conflict is not necessary and does not serve any legitimate purpose, particularly when the initial attack does not result in widespread destruction or loss of life. Moreover, legal developments in this area should move in the direction of narrowing the permissible causes for armed conflict, not enlarging them.

The 2008 Russian-Georgian cyber conflict provides a good example of how the many uncertainties and novelties of cyber warfare make the application of IHL difficult in certain instances. It is especially hard when determining responsibility for attacks or clearly defining the distinction between military and non-military objectives. An analysis of the Georgian attacks is meant to highlight the types of issues that arise when applying IHL to such conduct. This does not mean that IHL is not the proper regime to


128. ELLIS, supra note 126, at 12.

129. See Sinks, supra note 26, at 20.
deal with cyber attacks in the future. Rather, it underscores the continued work that must be done by the international community in the upcoming years to more clearly define certain terms and to set forth more transparent policies. What is clear, however, is that cyber attacks should only be undertaken in a way that respects international law principles.

V. INTERNATIONAL ORGANIZATIONS AND POWERFUL STATES MUST SET FORTH MORE EXPLICIT AND TRANSPARENT POLICIES REGARDING CYBER WARFARE ISSUES IN ORDER TO SUPPLEMENT EXISTING IHL PRINCIPLES

Existing principles governing the law of war need not be abandoned in the era of modern warfare. Rather, existing rules and mechanisms simply need to be applied in novel ways and old tenets of warfare must be rethought. The challenges, as well as the opportunities, of cyber warfare need to be better understood, and its laws and procedures need to be updated to accommodate the changes in global technology. Over the past few years, some states and international organizations have devoted considerable effort to devise and implement preventative measures aimed at ensuring better compliance with IHL in the event of a cyber attack. Expert seminars have been assembled to discuss various ideas and proposals, particularly through the International Committee of the Red Cross (ICRC). Many participants have acknowledged a positive obligation on states not involved in an armed conflict to take action against states that are violating IHL, particularly by using their influences to stop the violations.

Some argue that a new international accord or treaty must be created in order to deal specifically with cyber warfare. The rationale is that the Internet takes advantage of legal loopholes where state and non-state actors can ignore traditional Western notions of war as described by IHL and, therefore, more international laws are needed to apply directly to cyberspace.

130. Contra Shackelford, supra note 35, at 7 ("[T]he best way to ensure a comprehensive regime is through a new international accord dealing exclusively with cyber security and its status in international law.").
131. See INTERNATIONAL HUMANITARIAN LAW, supra note 115, at 20.
132. Id. at 21.
133. Id. at 22.
135. See id. at 75-77.
International treaties, however, would not offer any real alternative to developing and continuing the dialogue among nations, and would likely complicate the issues at stake. While technological improvements and transparent policies can help nations deal with the attribution problem, there still must be greater discourse regarding cyber warfare issues in order to clear up existing ambiguities. Cyber warfare, if properly limited, may allow militaries to act on an expanded list of targets while also avoiding the loss of civilian lives. In other words, cyber warfare could play an important niche role, by supplementing or amplifying more traditional forms of warfare.

International organizations and states should continue their open dialogue regarding cyber warfare issues and should strive for transparency in their policies, such that there are clear international guidelines for how states can permissibly use computers to carry out attacks either independently or part and parcel of a traditional armed conflict. The international legal community must extend the existing IHL framework to apply to cyber warfare, and states must evolve new norms in the form of custom or codification based on experience.

A. The Role of International Organizations

The International Telecommunications Union (ITU) is a specialized intergovernmental organization with state members and private organizational members. Founded in 1865, it is now a constituent part of the UN. While the ITU’s main purpose is adopting international regulations governing the electromagnetic frequency spectrum, the organization’s agenda also includes developing a global information infrastructure. In developing standards for online security and digital certificates, the ITU could also attempt to establish standards dealing with cyber attacks and information warfare. Regulations promulgated under the ITU

136. See Kelsey, supra note 39, at 1449-50 (noting that the creation and enforcement of a new treaty for cyber warfare would prove to be difficult).
137. See id. at 1449. See generally Shackelford, supra note 35, at 49-54 (discussing attribution and state responsibility for cyber attacks).
139. Id. at 1449.
have some applicability to cyber attacks if they involve use of the electromagnetic spectrum or international telecommunications networks. However, the ITU would likely have little effect, even in peacetime, because a violation of ITU rules has few repercussions. Even if there were stiffer repercussions, a country might still decide that these consequences would not outweigh its need to conduct operations against a particular adversary. Because of the importance of satellites for international telecommunications, as well as for military command, control, and intelligence, some forms of cyber warfare may involve orbital assets and, thus, implicate the ITU and other telecommunication regulators. Despite these concerns, the work of the ITU could still prove to be valuable in increasing international dialogue regarding cyber warfare issues, particularly through the ITU’s Global Cybersecurity Agenda, which works on coordinating responses to cyber attacks.

The European Network and Information Security Agency (ENISA) was created in 2004 as a response to concerns about cyber security throughout the European Union. Most of the efforts by the European Commission have resulted in creating technical standards specifically with regard to Internet governance, as opposed to supplementing international law norms. ENISA has, however, recognized the complexity of the technological environment and the threat posed by cyber attacks against electronic communications networks on the availability and integrity of the information accessed through these networks, creating a high-risk situation. Similarly, an Asian regional forum, the Telecommunications and Information Working Group of the Asian-Pacific Economic Cooperation, has also promoted regional cooperation in fighting cyber attacks and terrorist misuse of cyber

---

142. ELLIS, supra note 126, at 3-4.
143. Id. at 4.
144. GREENBERG ET AL., supra note 75, at 8; see also FERRERA ET AL., supra note 141, at 337-38.
Other Asian countries are also looking to bolster cyber defenses. The Malaysian government supported the establishment of the International Multilateral Partnership Against Cyber-Terrorism, or IMPACT, in May 2008. IMPACT is focused mostly on the "upper end of cyber threats" or attacks that would damage a nation's critical infrastructure, such as air traffic control. It is clear that individual nations or governments cannot address cyber warfare issues alone; international cooperation is required. The aforementioned organizations recognize the difficulties in applying IHL principles to cyber attacks, but are working to establish clearer policies on which nations can rely.

As mentioned earlier, a major concern is the ability to attribute a cyber attack to a particular government entity because, although an IP address can be tracked, it does not necessarily mean that a military or government official is behind the keyboard. In the near future, however, Internet anonymity may be lessened, thus making it easier to trace the source of cyber attacks. The UN National Security Agency has been participating in the "IP Traceback" drafting group since the fall of 2008. But this proposal has raised concerns among a number of international organizations. While the upshot of this may be that governments will be able to more effectively track cyber attacks to the source, it is also likely that this type of capability could be misused. Some people believe that traceback mechanisms will no longer serve much of a purpose because there are too many sources in a DDoS attack to be useful, and the source computer was, in many cases, hacked in the first place.

While the UN has no power to impose Internet standards on the world, it has been lobbying for more influence over the way

150. Id. (quoting the chairman of IMPACT's management board).
151. Id.
153. Id.
154. Id.
155. Id. Internet addressing is under the control of the Internet Corporation for Assigned Names and Numbers (ICANN), a private not-for-profit California corporation.
the Internet is managed, most prominently through the World Summit on the Information Society. Still, it is unlikely that any sort of mandatory IP Traceback or authentication regime will or could be imposed by national governments or international bodies. While international organizations should continue to advocate transparent policies on cyber warfare in order to assist states, resorting to over-management of the Internet is not the right solution.

B. States Should Develop Clearly Defined Cyber Strategies and Comprehensive Government-Network Defenses

The conduct and practices of states are itself a major source of CIL and would assist in supplementing conventional norms regarding the law of war and its application to cyber warfare. Particularly, China and the United States serve as examples of states working to establish strong national policies on cyber attacks.

The Chinese military and nationally supported groups have prepared detailed plans regarding cyber attacks as a way to achieve electronic dominance. China's ambitions extend to crippling an enemy's financial, military, and communications capabilities early in conflict, and there is evidence to indicate that China regards offensive computer operations as essential to taking control in the first stages of war. Furthermore, China has developed viruses to attack enemy computers and has even recently hacked into the White House computer network. While these plans may raise numerous concerns for other nations, China's push to make cyber warfare an integral part of their national army is prudent. The sooner states embrace the concept of cyber warfare, the sooner IHL ambiguities can be resolved.

Engineering standards are set by the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C), both of which are voluntary industry organizations. These private agencies have no regulatory power per se, but set standards that de facto control the Internet. WORKING GROUP ON INTERNET GOVERNANCE, BACKGROUND REPORT OF THE WORKING GROUP ON INTERNET GOVERNANCE (2005), available at http://www.wgig.org/docs/BackgroundReport.pdf.

156. McCullagh, supra note 152.
158. Id.
159. Beam, supra note 104.
Because cyber attacks are not going to disappear, it is better that states establish clear national policies, such that the rest of the international community can follow suit.

The United States has become increasingly concerned about the threats of cyber attacks. In recent years, there have been a series of cyber attacks on military and homeland security computer networks in the United States, many of which have been traced back to China. Presumably as a way to deal with these dangers, the United States has developed cyber warfare contingency plans under the National Security Presidential Directive (NSPD) 16, which was implemented in 2002. The directive, however, has remained classified and, therefore, does little to deter potential enemies. Nevertheless, this directive apparently ordered the development of guidelines to regulate the use of cyber weapons in war. Additionally, NSPD 16 instituted strict rules of engagement requiring “top-level” approval for any such attack. Some people in the United States believe that the nation needs to do more to develop an offensive cyber war capability, similar to that of China. In all reality, nations will probably not be able to develop a complete military offensive until there is further clarity in determining the attribution of attacks. Furthermore, the lines separating crime, terrorism, and warfare are often hard to draw. Nevertheless, the United States is taking action by attempting to develop and sustain a cyber-force with personnel trained in conducting cyber warfare. More nations should seek to develop transparent standards regarding cyber attacks so that the law can continue to develop and nations can better understand how to respond to such attacks.


162. Id.


164. Id.

C. The Future of Cyber Warfare: The Cyber Defense Era

The near future of cyber warfare will likely resemble that of nuclear defense, in which the growing trend will be for nations to set up cyber defense systems as a way to deter cyber attacks by other nations. Recently, seven NATO countries backed the establishment of a new cyber warfare defense center in Estonia.166 The Cooperative Cyber Defence Centre of Excellence (CCDCOE) began operations in the Fall of 2008, and conducts research and training in cyber warfare.167 A large portion of the CCDCOE’s staff are specialists from the sponsoring countries, Estonia, Germany, Italy, Latvia, Lithuania, Slovakia, and Spain, and the United States has agreed to send an observer.168 In June 2009, the CCDCOE held a Conference on Cyber Warfare to discuss definitions of cyber warfare and the enhancement of cyber defense capabilities.169

In the near future, there will likely be greater adoption of counter-strategies by states in order to deflect radicalization that is used for inciting violence or attacking enemy infrastructures over the Internet. These strategies might include open-source intelligence gathering and infiltration efforts.170 In addition, nations may also seek to take advantage of opportunities to use offensive information operations to achieve specific outcomes, including operations to undermine group cohesion and to interfere with decision-making, or to constrain terrorist activities in order to preempt attacks.171 The reason for this is that reactive defense is not very effective against increasingly powerful cyber attacks.172 Thus, more effective defense measures should incorporate predictive, active, and preemptive elements.173

The United States, through the Department of Defense (DOD), has also created a program known as Computer Network

168. Leyden, supra note 166.
170. Taipale, supra note 20, at 6-7.
171. Id. at 8.
172. Wilson, supra note 11, at 11.
173. Id.
Defense (CND), which describes activities that are designed to protect U.S. forces against information operational attacks from adversaries.\footnote{Id. at 2.} CND is defined as “defensive measures to protect information, computers, and networks from disruption or destruction.”\footnote{Id. at 4.} While acknowledging that a legal review of cyber warfare issues is necessary, the DOD has also pushed for the recruitment of cyber warriors as part of the armed forces.\footnote{Id. at 12.} This is a pragmatic approach because it would help solve the attribution problem that often creates difficulties in applying IHL to cyber attacks. Additionally, more nations will likely follow the United States' lead by creating these kinds of defense mechanisms in the near future.

VI. CONCLUSION

Cyberspace has been in existence for a number of years, but government entities are increasingly taking advantage of this domain as a way to carry out various kinds of war-like attacks with the help of computers. This raises many concerns, given that major aspects of a nation's critical or physical infrastructure are connected to cyberspace.\footnote{Solce, supra note 22, at 302.}

This article has shown that international laws that are currently in place do address the ever-changing nature of warfare. The Geneva Conventions, as well as the IHL principles of proportionality and unnecessary suffering, all provide a framework for addressing cyber warfare issues. The international legal community, however, must continue to work to address certain ambiguities that exist in applying IHL so that nations have a clear understanding as to how to go about carrying out or defending against a cyber attack. The key for states and international organizations in the upcoming years is to find better, more efficient ways to determine who is responsible for particular cyber attacks and to establish more transparent national policies regarding evolving cyber warfare issues. Although cyber attacks are usually not immediately directed at human beings, they do have the potential to indirectly cause severe injuries or even
The effects of a cyber attack will determine whether it is classified as an armed conflict for purposes of IHL. Additionally, the outcome of the attack will drive the victim-nation’s response.

Science fiction literature and film are replete with future wars in which enemy nations or worlds disrupt civilian and military communications networks as a way to gain military and economic control. Except that this is no longer science fiction. As early as 2001, it was recognized by the international community that cyber warfare would be a major threat in the future.

As expected, there are competing theories for how to best handle these changes in war tactics. Some advocate that a nation’s military should actually create a “Cyber Force” that focuses entirely on cyber attacks. Others argue that cyber attacks only produce a limited breadth of damage and, therefore, are not a major threat such that there should be international legal concerns. Nevertheless, the unpredictable consequences and unexpected adversarial advantages that stem from a cyber attack can be just as destructive and damaging as a physical attack. Accordingly, states and international organizations must take proactive stances toward establishing national cyber security strategies and adhering to international legal norms, with the recognition that cyber warfare is here to stay.


179. See, e.g., Fletcher Knebel & Charles W. Bailey II, Seven Days in May (Upperscroft 1977) (1962) (depicting a diversion of the country’s communications media and infrastructure); Star Trek: Deep Space Nine (CBS television broadcast Jan. 3, 1993 – June 2, 1999) (showing a disruption of Earth’s power grid by alien sabotage); The Day The Earth Stood Still (Twentieth Century Fox 1951) (illustrating the shutdown of electric power across Earth by alien forces).


181. See Solce, supra note 22, at 296 (arguing that Congress should elevate cyberspace operations to more than a command within the Air Force by creating a new cyber-focused group within the military).
