Michigan Law Review

Volume 106 | Issue 7

2008

Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare

Jeffrey T.G. Kelsey
University of Michigan Law School

NOTE

HACKING INTO INTERNATIONAL HUMANITARIAN LAW: THE PRINCIPLES OF DISTINCTION AND NEUTRALITY IN THE AGE OF CYBER WARFARE

*Jeffrey T.G. Kelsey**

Cyber warfare is an emerging form of warfare not explicitly addressed by existing international law. While most agree that legal restrictions should apply to cyber warfare, the international community has yet to reach consensus on how international humanitarian law ("IHL") applies to this new form of conflict. After providing an overview of the global Internet structure and outlining several cyber warfare scenarios, this Note argues that violations of the traditional principles of distinction and neutrality are more likely to occur in cyber warfare than in conventional warfare. States have strong incentives to engage in prohibited cyber attacks, despite the risk of war crimes accusations. This Note argues that belligerents will violate the principle of distinction more frequently in cyber warfare than in conventional warfare. Many cyber attacks will unavoidably violate neutrality law, making these violations more likely in cyber conflicts than in conventional wars. Rather than condemn all uses of cyber weapons, this Note argues that IHL should evolve to encourage the use of cyber warfare in some situations and provide states better guidance in the conduct of these attacks.

TABLE OF CONTENTS

---

* J.D. candidate, May 2008. I am grateful for all the help and feedback from my Note Editor, Leigh Wasserstrom, as well as from Andrew C. Adams, Brittany Parling, Benedict J. Schweigert, Kathryn Drenning, and Jim Driscoll-MacEachron. I thank Professor Steven R. Ratner for his insights and comments on the early drafts. I especially thank my fiancée, Katherine Meger, for her love and encouragement. I have been blessed with a loving and supportive family: Dad, this is for you.

INTRODUCTION

In May 2007, the Estonian government faced the reality of cyber warfare. An anonymous cyber attack targeted both civilian and government

systems.[1] Hitting the websites of banks, ministries, newspapers, and broadcasters, the assault left Estonia without the means to tell the world it was under attack.[2] The strike was both indiscriminate and surprisingly focused: " 'Particular "ports" of particular mission-critical computers in, for example, the telephone exchanges were targeted. Packet "bombs" of hundreds of megabytes in size would be sent first to one address, then another.' "[3] This attack was more than just an inconvenience to the Estonian population: the emergency number, used to call for ambulances and the fire service, was unavailable for more than an hour.[4] No state or terrorist group claimed responsibility after the attack, but analysts believed the complexity of the attack required the cooperation of a state and/or several large telecom firms.[5] Given the history of the Baltic State, some naturally suspected Russian involvement.[6]

The attack on Estonia illustrates the need to confront the seriousness of cyber warfare. As leaders begin to address the problem of defending against such attacks, they must not ignore the legal questions. For example, does a cyber attack constitute an "armed attack" under the United Nations Charter?[7] If analysts eventually link Russia to the attack, would the attack justify Estonia in invoking its right of self-defense under the Charter?[8] Or, should the international community view the attack as a mere criminal act for the criminal justice system to address? The recent news of individuals tied to the Chinese military hacking into the U.S. Defense Department's computer system raised very similar legal questions.[9] These issues will take time to address, and yet such *jus ad bellum*[10] issues barely scratch the surface of the legal conundrum.[11]

International and military lawyers must also consider how the *jus in bello*, or international humanitarian law ("IHL"),[12] applies to cyber warfare. For example, how would international humanitarian law apply to these attacks if a state of war existed between Estonia and Russia or the United

---

1. *Newly nasty*, ECONOMIST, May 26, 2007, at 63, 63.

2. *Id.*

3. *Id.* (quoting Linnar Viik, who is described as "Estonia's top internet guru").

4. *Id.*

5. *Id.*

6. *Id.*

7. *See* U.N. Charter art. 51; *The mouse that roared: Is cyberwarfare a serious threat?*, ECONOMIST.COM, Sept. 5, 2007, http://www.economist.com/daily/news/displaystory.cfm?story_id=9752625&fsrc=nwl [hereinafter *The mouse that roared*].

8. *See* U.N. Charter art. 51.

9. *The mouse that roared*, *supra* note 7.

10. Latin for "justice to war." It is the international legal framework that governs a state's decision to use force. *E.g.*, INTERNATIONAL COMMITTEE OF THE RED CROSS, INTERNATIONAL HUMANITARIAN LAW: ANSWERS TO YOUR QUESTIONS 15 (2002) [hereinafter ICRC, ANSWERS].

11. *See, e.g.*, Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L. 207 (2002).

12. This is the law governing the conduct of war. ICRC, ANSWERS, *supra* note 10, at 16.

States and China at the time of the attacks? Should the Geneva and Hague treaties apply to this form of warfare? While a general consensus exists that legal restrictions should apply to the use of cyber weapons in war, no apparent provision of international law explicitly bans or addresses their use.[13]

Military planners have been aware of the potential threat and opportunity of cyber warfare for at least a decade.[14] Unfortunately, the international community has yet to reach consensus on the application of IHL to this new form of conflict. Some have argued the existing framework of IHL is ill suited to cope with cyber warfare's new paradigm and have called for a new international convention to regulate its use.[15] At least one legal scholar has proposed an international convention.[16] Others, including the U.S. government, have opposed efforts to create a new treaty[17] and have argued that the current IHL framework can be applied to cyber warfare by analogy.[18] Some arguments against a new treaty are quite practical; George K. Walker argues:

> Given . . . technology's fluidity and exponential growth, the relative lack (thus far) of practice in [cyber warfare] situations, and the relatively small number (again thus far) of claims and counterclaims in the worldwide electronic arena, any international agreements on [cyber warfare] would likely be obsolete in terms of hardware and practice before their ink would be dry.[19]

Perhaps in acknowledgement of the legal uncertainty, President George W. Bush has issued National Security Directive 16, which ordered the devel-

---

13. Knut Dörmann, *Computer network attack and international humanitarian law*, INTERNATIONAL COMMITTEE OF THE RED CROSS, May 19, 2001, para. 29, http://www.icrc.org/web/eng/siteeng0.nsf/htmlall/5p2alj.

14. *See, e.g.*, Robert G. Hanseman, *The Realities and Legalities of Information Warfare*, 42 A.F.L. REV. 173, 187 (1997); Bruce Smith, *An Eye for an Eye, a Byte for a Byte*, FED. L., Oct. 1995, at 12.

15. *See, e.g.*, Jeffrey K. Walker, *The Demise of the Nation–State, The Dawn of New Paradigm Warfare, and a Future for the Profession of Arms*, 51 A.F. L. REV. 323, 337–38 (2001); Bradley Graham, *Military Grappling With Guidelines For Cyber Warfare; Questions Prevented Use on Yugoslavia*, WASH. POST, Nov. 8, 1999, at A1 ("Russia warned that information operations 'might lead to an escalation of the arms race.' It said 'contemporary international law has virtually no means of regulating the development and application of such a weapon.' ").

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

17. Graham, *supra* note 15.

18. *See, e.g.*, DEPT. OF DEFENSE OFFICE OF GEN. COUNSEL, AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS 11 (1999), http://www.maxwell.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf [hereinafter DOD, ASSESSMENT] ("There are novel features of information operations that will require expansion and interpretation of the established principles of the law of war. Nevertheless, the outcome of this process of extrapolation appears to be reasonably predictable."); Roger D. Scott, *Legal Aspects of Information Warfare: Military Disruption of Telecommunications*, 45 NAVAL L. REV. 57, 59 (1998) ("Anyone with an understanding of the fundamental principles of the law of war will not need specific, 'no-brainer' precedents to assess the legality of proposals for information attack.").

19. George K. Walker, *Information Warfare and Neutrality*, 33 VAND. J. TRANSNAT'L L. 1079, 1200 (2000) (footnotes omitted). Walker notes that the first "internet" began in 1969 when the primary concern was maintaining communication in the face of nuclear attack. *Id.* at 1094.

opment of guidelines to regulate the use of cyber weapons in war.[20] The Directive also instituted strict rules of engagement requiring "top-level" approval for any attack.[21]

This Note takes the position that IHL applies to cyber warfare by analogy but contends that IHL must evolve to accommodate and, in some cases, even encourage cyber warfare over conventional methods. This Note argues that states have strong incentives to engage in cyber attacks that violate the traditional notions of distinction and neutrality.[22] As such, violations of these legal principles are likely to be more common in cyber warfare than in conventional warfare. Part I provides an overview of the world Internet structure and highlights the interconnected nature of civilian and military telecommunications systems. This Part also outlines several cyber warfare scenarios that IHL should address. Part II shows how the principle of distinction[23] applies to the use of cyber weapons and maintains that cyber warfare creates additional incentives for belligerents to violate this principle more frequently than they do when engaged in conventional warfare. Part III describes how similar incentives exist for belligerents to violate the principle of neutrality[24] more often in the context of cyber warfare. Part IV argues that IHL should evolve to encourage the use of cyber weapons in some situations and provide states with better guidance for conducting these attacks in compliance with IHL.

I. THE MODERN INTERNET AND THE OPPORTUNITIES FOR CYBER WARFARE

This Part provides a general background on the modern structure of the Internet while highlighting the substantial overlap between civilian and military cyber activities. Section I.A provides a general overview of the modern structure of the Internet. Section I.B outlines several cyber warfare scenarios that have tangible, physical effects.

---

20. Bradley Graham, *Bush Orders Guidelines for Cyber-Warfare: Rules for Attacking Enemy Computers Prepared as U.S. Weighs Iraq Options*, WASH. POST, Feb. 7, 2003, at A1.

21. *Id.*

22. This Note will focus only on these two principles of IHL. Other scholars have focused on the problems of defining combatants, the application of perfidy, and the principle of proportionality in cyber warfare. *See, e.g.*, Brown, *supra* note 16, at 198–203.

23. The principle of distinction requires belligerents to distinguish between civilian and military objects in attacks. For a detailed discussion of the principle, see *infra* Section II.A. "Distinction" is a technical term and is a central tenet of IHL. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, 257 (July 8); Heike Spieker, *Civilian Immunity*, *in* CRIMES OF WAR 84, 84 (Roy Gutman & David Rieff eds. 1999).

24. The principle of neutrality provides that the territory of a neutral state is inviolable and imposes rights and duties on belligerent and neutral states to maintain that neutrality. *See generally* Convention Respecting the Rights and Duties of Neutral Powers and Persons In Case of War on Land, Oct. 18, 1907, 36 Stat. 2310, T.S. 540 [hereinafter 1907 Hague Convention V]; Convention Concerning the Rights and Duties of Neutral Powers in Naval War, Oct. 18, 1907, 36 Stat. 2415, T.S. 545 [hereinafter 1907 Hague Convention XIII].

A. *The Modern Internet*

Computers control much of our civilian and military infrastructure, including communications, power systems, sewage regulation, and healthcare.[25] In the United States, the military uses over two million computers and has in excess of ten thousand local area networks.[26] Further, the Internet provides nearly universal interconnectivity of computer networks without distinction between civilian and military uses.[27] According to one count, "[a]pproximately '[ninety-five percent] of the telecommunications of the [Department of Defense] travel through the Public Switched Network,' and a significant amount of both the operation and maintenance of military-owned network segments is currently handled by civilians on a contracted-out basis."[28]

These statistics are unsurprising given that the Internet began as a military program to ensure redundant communication channels in case of attack.[29] The unitary term "Internet" implies a single network; in fact, the Internet's physical structure is made up of many different linked networks, which are known collectively as the "Internet backbone."[30] The Internet backbone has the capacity to carry data across the countries, continents, and oceans of the world.[31] Keeping with its military roots, the Internet has a significant level of redundancy in the backbone, such that if one network experiences a problem the Internet can reroute traffic in real time to avoid it.[32] However, as the Internet has become more commercialized, major network providers have begun to move to a "hub-and-spoke" system that funnels Internet traffic through nodes located in major cities.[33] Such a system, while easier to maintain, significantly increases the vulnerability of the Internet to attack by placing a large number of nodes in one location.[34]

---

25. *See* Jim Melnick, Op-Ed., *The cyberwar against the United States*, BOSTON GLOBE, Aug. 19, 2007, at E9 (noting that each year, more and more industries connect to the Internet to take advantage of the efficiencies offered).

26. Vida M. Antolin-Jenkins, *Defining the Parameters of Cyberwar Operations: Looking for Law in All The Wrong Places?*, 51 NAVAL L. REV. 132, 132 (2005).

27. *Id.* at 137–38.

28. Gregory F. Intoccia & Joe Wesley Moore, *Communications Technology, Warfare, and the Law: Is the Network A Weapon System?*, 28 HOUS. J. INT'L L. 467, 473 (2006) (quoting LAWRENCE T. GREENBERG ET AL., INFORMATION WARFARE AND INTERNATIONAL LAW 12 (1998), http://www.dodccrp.org/files/Greenberg_Law.pdf).

29. Walker, *supra* note 19, at 1094.

30. SecurityFocus Glossary of Terms, http://www.securityfocus.com/glossary/I (last visited Mar. 8, 2008) ("[The Internet backbone is t]he largest network making up the Internet, connecting the many smaller networks that make up the Internet.").

31. *See* Walker, *supra* note 19, at 1094 ("The Internet is an international network of interconnected computers.").

32. *See* Jeff Grabmeier, *Loss of Major Hub Cities Could Cripple Internet, Study Suggests; A More Decentralized Internet Is Best Solution*, OHIO ST. UNIV. RES. NEWS, Nov. 26, 2002, http://researchnews.osu.edu/archive/intsurv.htm.

33. *Id.*

34. *Id.*

All Internet communications traffic must pass through a node on its way to a destination. The communications protocol of the Internet divides every email, web search, and message sent over the Internet into discrete blocks of data called packets.[35] The Internet then routes the packets between nodes over data links shared with other Internet traffic.[36] A message sent from Country A to Country B may pass through nodes located in Country C and Country D before reaching Country B.[37] As noted above, the Internet re-routes data traffic if a node is shut down or rendered inoperable,[38] but the loss of a large number of nodes can result in the loss of Internet service for extended periods.[39]

The use of packets decreases the time required for data to move across the network and increases the robustness of communication.[40] The communications protocol may divide a longer message into several packets and then reassemble the message at the destination.[41] When the Internet divides a single message into multiple packets, each packet may follow a different route on its way to its destination.[42] A long message sent from Country A may be divided into Packets 1 and 2. While Packet 1 may pass through Countries C and D on its way to Country B, Packet 2 may pass through Countries E and F.[43] Under the current system, the user has little control over the route the packets take.[44] Due to the interconnected nature of the civilian and military computer networks,[45] the Internet may route military data through nodes located in less-than-friendly countries. More significantly, the Internet may route military communications of one or both sides through the nodes of a third party in the event of armed conflict. Indeed, the packet system, though originally designed as part of a military program, has grown and changed such that the Internet no longer makes any distinctions among potential allies, potential enemies, and potential neutrals.

---

35. *See* Microsoft Technet Glossary of Terms, http://www.microsoft.com/technet/prodtechnol/Visio/visio2002/plan/glossary.mspx#E2TAE (defining "Packet Switching") (last visited Mar. 8, 2008).

36. *Id.*; *see also* Walker, *supra* note 19, at 1095–96.

37. *See* Walker, *supra* note 19, at 1095–96.

38. *Id.*

39. *Loss Of Major Hub Cities Could Cripple Internet, Study Suggests*, SCIENCEDAILY, Nov. 26, 2002, http://www.sciencedaily.com/releases/2002/11/021126072153.htm.

40. RAND Corporation, Paul Baran and the Origins of the Internet, *available at* http://rand.org/about/history/baran.html (last visited Mar. 17, 2008).

41. *Id.*

42. *See* Microsoft Technet, *supra* note 35.

43. *See* Walker, *supra* note 19, at 1096.

44. The United States Defense Advanced Research Projects Agency ("DARPA") is developing a next-generation Internet that may allow the user more control and perhaps allow the user to avoid routes that are undesirable. Linktionary.com, Active Networks, http://www.linktionary.com/a/active_network.html (last visited Mar. 8, 2008) (noting that under the DARPA proposal "users can 'program' the network by supplying their own programs to perform these computations").

45. *See* Antolin-Jenkins, *supra* note 26, at 137–38 (noting that military communications use public interfaces).

B. *Cyber Warfare Scenarios*

This Section outlines several scenarios relevant to the application of IHL to cyber warfare. Most people experience the Internet through email, web browsing, and chat rooms, but the Internet's uses—and vulnerabilities—extend far beyond these functions.[46] Cyber warfare is more than just an issue for websites and some forms of communication; indeed, some cyber attacks may cause serious physical, tangible effects, as evidenced by the attack on Estonia.[47] Had the attack been more global in nature, millions of people could have been without communications for some time—a situation both life threatening and damaging to the global economy. Similarly, cyber attacks on purely military targets may be capable of effectively neutralizing a hostile threat without risking lives or equipment.

1. *Using a Cyber Attack to Shut Down an Air Defense Station*

Some military thinkers have proposed using a cyber attack to disable an air defense site for a specific period of time in order to accomplish one part of a larger mission.[48] The cyber attack may take the form of a computer virus or other "malicious code" that can disable the air defenses without the physical destruction of the station.[49] An attacker could deliver the weapon via the host country's Internet or possibly "beam" the weapon to the target directly from an aircraft. If properly executed, the result of the cyber strike would be the same as a conventional bombing raid but without the risk of civilian or military casualities.[50] In this way, such a cyber strike could be the "ultimate in precision weapons."[51]

2. *Infiltration of the Enemy's Centralized Defense Network*

During NATO's Kosovo campaign in the 1990s, NATO air war planners devised a cyber attack to insert false messages and targets into the Serbian military's centralized air-defense command network.[52] As in the attack discussed in Scenario 1, NATO could have delivered the weapon via the host country's Internet or possibly could have "beamed" the weapon to the target directly from a NATO warplane. This attack would have limited Serbia's ability to accurately target NATO warplanes during the bombing campaign,

---

46. *See* Melnick, *supra* note 25.

47. The situation easily could have been life threatening. *Newly nasty*, *supra* note 1, at 63.

48. *See* Brian T. O'Donnell & James C. Kraska, *Humanitarian Law: Developing International Rules for the Digital Battlefield*, 8 J. CONFLICT & SECURITY L. 133, 149 (2003).

49. *See id.*

50. *See id.*

51. Bradley Graham, *Cyberwar: A New Weapon Awaits a Set of Rules; Military, Spy Agencies Struggle to Define Computers' Place in U.S. Arsenal*, WASH. POST, July 8, 1998, at A1.

52. William M. Arkin, *The Cyber Bomb in Yugoslavia*, WASHINGTONPOST.COM, Oct. 25, 1999, http://www.washingtonpost.com/wp-srv/national/dotmil/arkin.htm (last visited Mar. 8, 2008). "A Top Secret U.S.-only operation . . . was approved soon after the bombing began . . . ." *Id.*

but, if improperly planned, such a cyber attack could have put civilian targets at risk, with the air-defense network possibly confusing relief planes or commercial aircraft for military targets. Further, fuel-depleted missiles launched at false targets could have fallen on civilian structures, such as homes, hospitals, and schools. NATO did not ultimately launch this cyber attack, but in the future NATO commanders might be tempted to risk additional harm to the civilian population to reduce risk to the lives of NATO pilots.[53]

3. *Cyber Attack on Power Plants*

Militaries may also develop cyber weapons to disable civilian infrastructure serving both military and civilian functions. Many recent U.S. aerial bombing campaigns have included the outright destruction of such targets, which include power plants, telecommunications, and transport infrastructure.[54] Unlike conventional strikes, which may leave civilians without power for months or even years,[55] a cyber strike could disable the power grid for the duration of hostilities yet allow electrical service to resume immediately once the fighting was over.[56] This result would not completely eliminate the public health and safety concerns, but cyber warfare at least offers the possibility of lessening the damage relative to a conventional attack.

4. *Cyber Attack on a Media Station*

Belligerents could use cyber weapons to attack media outlets broadcasting enemy-regime propaganda.[57] For example, a denial-of-service attack could disrupt the station's ability to communicate with the outside world.[58] Another option would be for a belligerent to actually hijack the station's

---

53. Such a balancing act may violate IHL, since the risk to civilian lives is to be balanced against the expected military advantage to be gained, not the reduction in risk to military forces. *See infra* Section II.A.

54. These are called "dual-use" targets and strikes on them remain controversial under IHL due to the possible impact on civilian public health and safety. *See* DOD, ASSESSMENT, *supra* note 18, at 8–9.

55. As James Fallows reported:

> Despite the precision of the [American] bombing campaign, by mid-April [2003] wartime damage and immediate postwar looting had reduced Baghdad's power supply to one fifth its pre-war level, according to an internal Pentagon study. In mid-July the grid would be back to only half its pre-war level, working on a three-hours-on, three-hours-off schedule.

James Fallows, *Blind Into Baghdad*, THE ATLANTIC, Jan.–Feb. 2004, at 52, 70.

56. DOD, ASSESSMENT, *supra* note 18, at 8–9 (discussing the war crime allegations surrounding the coalition bombing of the electrical power system in Baghdad).

57. On April 23, 1999, NATO bombed the headquarters and studios of the Serbian state radio and television station (RTS). Eric David, *Respect for the Principle of Distinction in the Kosovo War*, 3 Y.B. INT'L HUMANITARIAN LAW 81, 86 (H. Fischer & Avril McDonald eds., 2000). Although cyber warfare offers several possible nonlethal alternatives for future military campaigns, this Note will discuss the legal implications of this strike. *See infra* Part II.

58. DOD, ASSESSMENT, *supra* note 18, at 9.

signal and replace an enemy's programming with broadcasts of its own.[59] This programming could present false information regarding troop movements or armistice negotiations under the guise of a legitimate broadcast. Though such an action may actually violate IHL, it could still prove to be effective as part of a larger military or political struggle.[60]

II. WHILE THE LEGALITY OF POTENTIAL CYBER ATTACKS WILL OFTEN BE CLEAR, THE NONLETHAL POTENTIAL OF CYBER WARFARE MAY LEAD TO MORE FREQUENT VIOLATIONS OF THE PRINCIPLE OF DISTINCTION THAN IN CONVENTIONAL WARFARE

This Part argues that states may violate the principle of distinction more frequently in cyber warfare than in conventional warfare because states may increasingly use cyber weapons to attack traditionally protected objects and individuals. Section II.A discusses the principle of distinction under current IHL treaties and customary law. Section II.B shows that the legality of a potential cyber attack under the principle of distinction will be clear for many operations. Section II.C contends that the nonlethal potential of cyber warfare may lead to more frequent violations of the principle of distinction as compared to conventional warfare.

A. *The Meaning of Distinction in International Humanitarian Law*

The 1977 Additional Protocol I to the Geneva Convention ("Additional Protocol I") illustrates the principle of distinction: "[A] technical term in the laws of armed conflict intended to protect civilian persons and objects. Under this principle, parties to an armed conflict must always distinguish between civilians and civilian objects on the one hand, and combatants and military targets on the other."[61] Under Additional Protocol I, civilians and civilian objects cannot be the targets of attack.[62] The treaty bars belligerents from rendering useless those objects that are indispensable to the survival of the civilian population, such as foodstuffs, agricultural crops, livestock, drinking water installations and supplies, and irrigation works.[63] States "must consequently never use weapons that are incapable of distinguishing between civilian and military targets."[64]

---

59. This is a form of so-called psychological operations.

60. The U.S. DOD has stated that such an action would violate the ban on perfidy and constitute a war crime. DOD, ASSESSMENT, *supra* note 18, at 10.

61. Spieker, *supra* note 23, at 84. While not every state has adopted the provisions of Additional Protocol I, the principle of distinction is accepted as customary law. *Id.*

62. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) arts. 51(2), 51(1), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I].

63. *Id.* art. 54(2).

64. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, 257 (July 8).

In the conduct of military operations, belligerents have a duty to exercise constant care to minimize the loss of civilian lives and damage to civilian objects.[65] Military commanders must limit attacks to strictly military targets, which the treaty defines as those objects that "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*."[66] Belligerents also have a duty to exercise care in attacks to protect the natural environment[67] and protect works and installations containing dangerous forces, such as dams and nuclear power plants.[68] Belligerents have a further duty not to undertake attacks that have the primary purpose of spreading terror among the civilian population.[69]

Some objects serve both civilian and military purposes.[70] These so-called dual-use targets complicate the application of the principle of distinction.[71] This category of targets includes power-generating stations, telecommunications, bridges, and other civilian infrastructure used by the military in times of war.[72] If the object makes an effective contribution to military action, this "secondary military use" may turn a civilian object into a legitimate military objective.[73] Even so, such attacks remain controversial.[74]

B. *The Legality of Potential Cyber Attacks Under the Principle of Distinction Will Be Clear for Many Operations*

The analysis of a cyber attack's compliance with the principle of distinction will be very similar to the analysis for a conventional attack, and in many operations the cyber attacks will clearly comply with the principle. As militaries develop plans for using cyber weapons, the military and legal communities will need to reinterpret the principle to effectively apply it to cyber warfare. This process seems relatively straightforward for most uses of cyber weapons.[75] Some military operators believe that anything qualifying as a legitimate military target for a conventional attack is a legitimate military target for a cyber attack.[76] Likewise, the relevant prohibitions in IHL do

---

65. Additional Protocol I, *supra* note 62, art. 57.

66. *Id.* art. 52(2) (emphasis added).

67. *Id.* art. 55.

68. *Id.* art. 56.

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

70. MARCO SASSÒLI, LEGITIMATE TARGETS OF ATTACKS UNDER INTERNATIONAL HUMANITARIAN LAW 7 (2003).

71. O'Donnell & Kraska, *supra* note 48, at 157.

72. SASSÒLI, *supra* note 70, at 7.

73. *Id.*

74. DOD, ASSESSMENT, *supra* note 18, at 8–9 (discussing the controversy surrounding the bombing of Baghdad power plants in Gulf War I).

75. *Id.* at 8.

76. *See* Graham, *supra* note 15.

not depend on the type of weapons or warfare used and should unquestionably apply to cyber warfare.[77] As such, some uses of cyber weapons are clearly acceptable under the principle of distinction, while the principle clearly prohibits other uses.

At one end of the spectrum of possible attacks, the principle will likely permit a state to use a cyber weapon to attack a purely military target. It seems obvious that such a use would not violate the principle of distinction. For example, an attack that neutralizes an air defense station as part of a general campaign would offer the belligerent a definite military advantage.[78] The use of a cyber weapon may in fact result in fewer civilian deaths than the use of a conventional aerial bombing campaign.[79] The legality of such an attack seems like a "no-brainer."[80]

In operations carrying higher risks of civilian casualties, like the attack on an air-defense network,[81] the principle of distinction will likely play a large role in defining the military operation. At a minimum, IHL requires military commanders to "know not just where to strike but be able to anticipate all the repercussions of an attack."[82] If the false messages and targets sent to an air-defense network could endanger relief planes or commercial aircraft, the principle of distinction would force the commander to evaluate whether such a plan was the best way to achieve the expected military advantage while minimizing the loss of civilian lives. Again, the principle would likely dictate a change to the scope of the operation to avoid the threat to civilians.

At the other end of the spectrum, IHL will likely ban a cyber attack that would be the "direct and intentional cause of [civilian] death and destruction."[83] Examples of this type of attack might include the "disruption of an air traffic control system that caused a civilian airliner to crash, or corruption of a medical database, causing civilians or wounded soldiers to receive transfusions of the incorrect blood type."[84] The high civilian death toll, the likelihood of superfluous injury, and the lack of a clear military advantage from such attacks should lead a military commander to forgo such attacks.

---

77. As Dörman notes:

> For example, certain attacks against objects indispensable to the survival of the civilian population, such as drinking water installations and irrigation works, or attacks against installations containing dangerous forces, namely dams, dykes and nuclear electrical generating stations are prohibited. These prohibitions are independent of the type of weapons or methods of warfare used.

Dörmann, *supra* note 13, at para. 16; *see also* Additional Protocol I, *supra* note 62, arts. 55–56.

78. *See supra* Section I.B.

79. *See* O'Donnell & Kraska, *supra* note 48, at 149–50.

80. Scott, *supra* note 18, at 59.

81. *See supra* Section I.B.

82. Graham, *supra* note 15. "[C]omplicating large-scale computer attacks is the need for an extraordinary amount of detailed intelligence about a target's hardware and software systems." *Id.*

83. *See* GREENBERG ET AL., *supra* note 28, at 11.

84. *Id.* at 11–12.

Similarly, IHL will ban any cyber attack that would seriously damage the environment or cause the release of natural forces in violation of Articles 54, 55, and 56 of Additional Protocol I.[85] Again, for these attacks, the use of a cyber weapon would not change the analysis.[86]

C. *The Nonlethal Potential of Cyber Warfare May Lead to More Attacks on Traditionally Protected Objects and Individuals than Occurs in Conventional Warfare*

The potentially nonlethal nature of cyber weapons may cloud the assessment of an attack's legality, leading to more frequent violations of the principle of distinction in this new form of warfare than in conventional warfare.[87] On each end of the spectrum, as discussed above, the legality of a potential cyber attack is clear. For those situations that fall in the middle, the principle of distinction may be an ineffective guide for military commanders. This is due, in part, to the highly interconnected nature of the military and civilian networks, which renders much of the Internet a dual-use target.[88]

The advantages offered by cyber weapons, particularly their potentially nonlethal nature, only exacerbate the difficulty in applying the principle of distinction in modern warfare. A legal gray area already exists in the principle of distinction, created by the modern concept of war, which "does not exclude targets whose destruction or neutralization do not directly advance the overall objective of the war, but do nonetheless degrade the enemy's ability and will to fight."[89] In providing belligerents a gain in military advantage without an additional threat to civilian lives, cyber warfare is more likely than conventional warfare to lead belligerents to ignore the principle of distinction to attack directly what IHL has traditionally sought to protect.

NATO's bombing of the Serbian media station RTS during the Kosovo campaign illustrates one aspect of this difficulty, particularly if it is re-

---

85. *See* Additional Protocol I, *supra* note 62, arts. 54–56.

86. *See* Dörmann, *supra* note 13.

87. *Cf.* Hays Parks, *The Protection of Civilians from Air Warfare*, 27 Isr. Y.B. on Hum. Rts. 65, 87–90 (1997) (discussing how the development of smart bombs has resulted in a similar effect on the utility of the principle of distinction).

88. GREENBERG ET AL., *supra* note 28, at 12. One military leader has noted, "'[t]here is no logical distinction . . . between military or civil systems or technologies. [Therefore] there is also no technical distinction between exploitation, attack or defense of the information warfare target set.'" *Id.* (quoting Vice Admiral Arthur Cebrowski) (alteration in original); *see also* O'Donnell & Kraska, *supra* note 48, at 148 ("[N]et-war . . . tends to defy and cut across standard boundaries, jurisdictions, and distinctions between state and society, public and private, war and peace, war and crime, civilian and military . . . legal and illegal.").

89. Brown, *supra* note 16, at 193; *see also* MICHAEL IGNATIEFF, THE WARRIOR'S HONOR 126 (1998) (stating that the purpose of war now seems to include "terrorizing, deporting, and even exterminating the other side's civilian populations"); O'Donnell & Kraska, *supra* note 48, at 155 ("In the fog of modern war, in which a state's entire society becomes vested in warfare, it is especially difficult to distinguish between lawful and unlawful targets . . . .").

imagined as a cyber strike.[90] At the time, NATO justified the attack on RTS by emphasizing that the media station was an instrument of Serbian propaganda as well as a military communications relay site.[91] Given the broad nature of NATO's strategic objectives, it was unsurprising that NATO considered RTS a military target.[92] Some have argued that the small military advantage gained from the attack did not justify the loss of sixteen civilian lives.[93] The use of a cyber weapon in this situation could have strengthened NATO's argument for attacking a predominantly civilian target. With a cyber weapon, NATO might have avoided the loss of any civilian lives. While questions about the military significance of RTS would have remained, the sought-after objective—elimination of RTS as a communications platform for the Milosevic regime—would have been achieved. Further, in such a situation, the legal community might decry the violation of the principle of distinction given the target's questionable military value and obvious civilian nature; however, those complaints are unlikely to generate great public sympathy when unaccompanied by any civilian deaths.[94]

Applying this logic, a belligerent is more likely to engage in attacks that violate the principle of distinction using cyber warfare than when using conventional methods since it can do so without incurring the political cost associated with civilian casualties. For example, a belligerent might use cyber weapons in place of conventional methods to attack targets traditionally protected as "civilian objects."[95] IHL has protected these objects because a conventional attack would cause substantial civilian casualties and greatly affect civilian lives and property, while serving only an indirect military purpose.[96] Unlike a conventional attack, a cyber attack could neutralize these targets without causing physical injury to the civilians or physical damage to the site, while the attacker could argue that the strike has at least some impact on the targeted belligerent's capacity to continue its military

---

90. *See supra* Section I.B. The United States has maintained that the legality of an attack on a civilian radio station used by a belligerent for purely psychological operations "is an issue that has yet to be addressed authoritatively by the international community." DOD, ASSESSMENT, *supra* note 18, at 9; *see also* Michael N. Schmitt, *Wired warfare: Computer network attack and* jus in bello, 84 INT'L REV. RED CROSS, 365, 381 (2002) ("[I]f the operation were designed to cause, for example, mere inconvenience, it would not rise to the level of an attack and would thus be permissible regardless of the target's nexus, or lack thereof, to military operations.").

91. *See* David, *supra* note 57, at 88–89. It should be noted that NATO made no allegations that RTS had incited the population to commit war crimes. *Id.*

92. W.J. Fenrick, *The Law Applicable to Targeting and Proportionality after Operation Allied Force: A View from the Outside*, 3 Y.B. INT'L HUMANITARIAN L. 53, 72 (2000) ("NATO's strategic objectives included 'Damaging Serbia's capacity to wage war against Kosovo in the future or spread the war to neighbours [sic] by diminishing or degrading its ability to wage military operations . . . .' " (omission in original)).

93. *See, e.g.*, David, *supra* note 57, at 107.

94. *See* Schmitt, *supra* note 90, at 381–82.

95. *See* Additional Protocol I, *supra* note 62, art. 52. Banks and stock exchanges are two examples of civilian objects.

96. Brown, *supra* note 16, at 194.

campaign.[97] As such, cyber warfare may be more likely to lead a belligerent to violate the principle of distinction. Further, as one commentator has stated, "[i]t is less obvious that attacks with less tangible results, such as the disruption of a financial or social security system, or the disclosure of confidential personal information, constitute the sort of injury against which humanitarian law is supposed to protect civilians."[98] Given these considerations, direct attacks on civilian objects are more likely with cyber weapons than with conventional weapons, regardless of the risk of war-crime accusations.[99]

III. THE PRINCIPLE OF NEUTRALITY REGULATES CYBER WARFARE, BUT MANY INTERNET-BASED ATTACKS WILL UNAVOIDABLY VIOLATE NEUTRALITY DUE TO THE STRUCTURE OF THE INTERNET

The principle of neutrality similarly applies to cyber warfare in a unique way, complicated by the structure of the Internet. Cyber warfare implicates the principle of neutrality because a belligerent may launch attacks against another belligerent using the international structure of the Internet. The core issue is the routing of these cyber attacks through neutral countries, which is likely given the current structure of the Internet.[100] For example, when Belligerent A launches a cyber attack against Belligerent B, the attack may be routed through the Internet nodes of Neutrals C and D, even if the belligerents share a common border.[101] As the attacks pass through the Internet nodes, there may be no discernable effect on Neutrals C and D, but IHL may compel the targeted neutral to take action to halt the attack.

Section III.A briefly outlines some elements of neutrality law that influence the conduct of cyber warfare, particularly the telecommunications exception defined in the 1907 Hague Convention.[102] Section III.B argues that sending a cyber weapon across the Internet nodes of a neutral state likely violates the law of neutrality. Section III.C argues that belligerents will nevertheless choose to engage in such attacks to capture the advantages offered by cyber warfare.

---

97. *See* Antolin-Jenkins, *supra* note 26, at 145 ("A direct attack on financial markets, particularly a mixed attack, which would both change economic data and target financial programs created to respond to that data, has huge long term destructive potential."). *But see* Brown, *supra* note 16, at 194 (stating that attacks on banks or telephone networks would likely be condemned as violating IHL since attacks on these targets seem to serve no legitimate military purpose).

98. GREENBERG ET AL., *supra* note 28, at 12.

99. *See* O'Donnell & Kraska, *supra* note 48, at 156 ("As we enter the computer warfare age, nations will attempt to further exploit [the] seam between the protected status of the civilian and the belligerent actions of the state.").

100. *See supra* Section I.A.

101. *See id.*

102. *See* 1907 Hague Convention V, *supra* note 24, art. 8.

A. *General Overview of Relevant Neutrality Law*

Neutrality law regulates the coexistence of war and peace, giving states not participating in a conflict the ability to maintain relations with all of the belligerents.[103] The Hague Conventions, which are the primary source of the rules governing neutrality, outline the rights and duties of belligerent and neutral states to maintain their neutrality during the course of the conflict.[104] Importantly, the Conventions dictate that the territory of a neutral state is inviolable.[105] Belligerents may not move troops, weapons, or other materials of war across the territory of a neutral state,[106] nor may belligerent military aircraft penetrate the jurisdiction of a neutral state.[107] The Conventions require neutral states to prevent belligerents from engaging in these violations.[108] With respect to naval activity, the vessels of a belligerent may move through the waters of a neutral state,[109] but belligerents may not engage in any act of hostility while in those waters.[110]

Neutrality law also defines a limited telecommunications exception.[111] Under Article 8 of the 1907 Hague Convention V, "[a] neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals,"[112] so long as the neutral state impartially permits the use of those structures by all belligerents.[113] The United States has said this article applies to the tools of modern communications: satellites as well as ground-based facilities.[114] However, nothing in 1907 Hague Convention V suggests that this exception applies beyond communications infrastructure to digital systems that actually generate information, such as satellite imagery, weather, and navigation systems.[115] Any neutral state supplying such information to one belligerent could allow the opposing

---

103. STEPHEN C. NEFF, THE RIGHTS AND DUTIES OF NEUTRALS 1 (2000).

104. *See generally* 1907 Hague Convention XIII, *supra* note 24.

105. 1907 Hague Convention V, *supra* note 24, art. 1.

106. *Id.* art. 2.

107. Jurists Commission, *General Report on Rules for the Control of Radio in War and Aerial Warfare*, 17 AM. J. INT'L L. (SUPP.) 242, 258 (1923). Article 40 of the Rules of Aerial Warfare was written at the 1923 Hague Conventions, and while never signed into law, many legal commentators believe these rules may restate custom. *See* Walker, *supra* note 19, at 1135 n.222.

108. *See* 1907 Hague Convention V, *supra* note 24, art. 5.

109. 1907 Hague Convention XIII, *supra* note 24, art. I.

110. *Id.* art. II.

111. DOD, ASSESSMENT, *supra* note 18, at 10.

112. 1907 Hague Convention V, *supra* note 24, art. 8.

113. *Id.* art. 9.

114. DOD, ASSESSMENT, *supra* note 18, at 10 ("The plain language of this agreement would appear to apply to communication satellites as well as to ground-based facilities.").

115. *Id.* at 10. 1907 Hague Convention V explicitly mentions only cables and communications apparatus, not devices that generate information. 1907 Hague Convention V, *supra* note 24, art. 8.

belligerent to take action against the neutral to prevent the transfer of information.[116]

B. *Cyber Warfare Operations Conducted via the Internet Violate Neutrality Law*

The use of the Internet to conduct cross-border cyber attacks violates the principle of neutrality. Contrary to views of some legal scholars, a belligerent violates neutrality law when it launches a cyber attack that crosses the Internet nodes of a neutral state.[117] An additional violation may occur because the current structure of the Internet makes halting these incursions extremely difficult.

Cyber attacks routed across the Internet nodes of neutral states violate neutrality law, despite the lack of physical intrusion.[118] Both the text of the 1907 Hague Convention V and the ultimate effect of such attacks support the view that cyber attacks crossing the Internet nodes of neutral states violate IHL. Under Article 8 of the Hague Convention V, belligerents may use "telegraph or telephone cables," or a "wireless telegraphy apparatus" belonging to the neutral state or to companies or private individuals, to transmit signals containing intelligence, orders, or other dispatches.[119] Although this language might indicate that the passage of cyber weapons does not violate neutrality law,[120] the Hague Convention V also explicitly states that belligerents "are forbidden to move troops, *or convoys of either munitions of war or supplies* across the territory of a neutral Power."[121]

Rather than transmitting a mere communication signal, a cyber attack moves a weapon across the territory of the neutral state.[122] The United States Air Force has defined "weapons" as "[d]evices designed to kill, injure, or disable people, or to damage or destroy property."[123] Cyber weapons fit into this definition: cyber attacks "can destroy both military and civilian targets . . . [although] they affect humans indirectly rather than directly. Cyber

---

116. *See* DOD, ASSESSMENT, *supra* note 18, at 10 ("For example, if a belligerent nation demanded that the U.S. government deny GPS navigation services to its enemy, and if the U.S. were unable or unwilling to comply, the belligerent may have the right to take necessary and proportional acts in self-defense, such as jamming the GPS signal in the combat area.").

117. *Id.* at 10; GREENBERG ET AL., *supra* note 28, at 10.

118. *But see* GREENBERG ET AL., *supra* note 28, at 10 ("The encroachments beyond a nation's borders that may violate its neutrality have, in the past, been physical intrusions by troops, ships, or planes.").

119. 1907 Hague Convention V, *supra* note 24, art. 8.

120. *See* DOD, ASSESSMENT, *supra* note 18, at 10.

121. 1907 Hague Convention V, *supra* note 24, art. 2 (emphasis added).

122. Brown, *supra* note 16, at 184 ("In the information age, armed forces need not always deploy bombers and artillery to accomplish these objectives. In other words, the use of computer technology to wage war necessitates a reevaluation of the definition of the term 'weapon.'").

123. DEPT. OF THE AIR FORCE, POLICY DIRECTIVE 51-4, COMPLIANCE WITH THE LAW OF ARMED CONFLICT para. 6.5 (1993).

weapons thus share some similarities with weapons of yesterday."[124] As one legal scholar has noted, "[w]hen an information packet containing malicious code travels through computer systems under the jurisdiction of a neutral state, a strict construction of the law of neutrality would result in that state's neutrality being violated."[125] Indeed, the Hague Convention forbids the movement of weapons, even those the size of an electron, across the territory of a neutral state.[126]

Furthermore, a cyber attack, like any other attack conducted across the neutral state's territory, may have the effect of drawing the neutral state into the conflict. For example, the use of the neutral state's Internet nodes might allow the belligerent to engage in a broader attack along multiple lines of approach, increasing the potential scope and effect of the attack. If the neutral state cannot or does not take action to halt the attack, the opposing belligerent may choose to physically attack the neutral state's communications infrastructure to limit or halt the cyber attack.[127] Thus, even without the physical violation of the neutral state's territory, a cyber attack may force a neutral state to become involved unwillingly in the conflict. This loss of nonbelligerent status is precisely the result the law of neutrality seeks to avoid.[128]

The current structure of the Internet poses several practical problems to a neutral state in complying with the principle of neutrality. IHL requires the neutral state to take action to prevent the cyber attack in order to comply with the duty of neutrality, although the scope of this duty may vary.[129] Under Hague Convention V Article 5, however, the neutral state has an absolute duty to prevent all violations of its territory.[130] Yet neutral states do not have a practical method of detecting such attacks.[131] Further, even if the neutral state could detect the violation, under the existing structure of the Internet, "a state may not be able to prevent [cyber] attacks from leaving its jurisdiction unless it severs all connections with computer systems in other states."[132] Requiring this would clearly be unreasonable and would lead to the disruption of legitimate Internet communications.[133]

---

124. William J. Bayles, *The Ethics of Computer Network Attack*, PARAMETERS, Spring 2001, at 44, 45.

125. Brown, *supra* note 16, at 210.

126. *See* 1907 Hague Convention V, *supra* note 24, art. 2.

127. *See* Brown, *supra* note 16, at 210. Whether the belligerent will actually choose to launch such an attack will depend on the scale and nature of the cyber attack.

128. *See* NEFF, *supra* note 103, at 1.

129. *Compare* 1907 Hague Convention V, *supra* note 24, art. 5, *with* Walker, *supra* note 19, at 1199 ("A neutral's duty to repel [belligerent] incursions varies with the modality of incursion.").

130. *See* 1907 Hague Convention V, *supra* note 24, art. 5.

131. *See Newly nasty*, *supra* note 1.

132. Brown, *supra* note 16, at 210.

133. *Id.*

Alternatively, IHL might view the duty of the neutral state through the prism of the law of naval warfare.[134] In naval warfare, IHL uses a "means at a neutral's disposal" test to evaluate the conduct of neutral parties.[135] The international community could adopt such a test to govern cyber warfare: the neutral state could satisfy its duty under IHL as long as it had applied the means at its disposal to detect and repel a belligerent's incursions.[136] However, as discussed above, the current structure of the Internet offers the neutral state little opportunity to detect and prevent the belligerent's incursions.

Regardless of the test adopted, IHL permits the targeted belligerent to take proportional action to counter these Internet incursions if the neutral state is unable to stop them.[137] Should the targeted belligerent choose to exercise this option, the neutral state may resort to self-defense measures against the aggrieved belligerent to repel what it sees as a violation of its territory.[138] This chain of events could repeat itself, drawing in more and more states and widening the conflict.

C. *Belligerents Have Incentives to Engage in Attacks That Violate Neutrality Law and Will Choose to Engage in Prohibited Conduct*

Belligerents have many incentives to engage in cyber warfare across the Internet nodes of neutral states and will choose to launch attacks that violate neutrality laws. Conducting attacks over the Internet allows belligerents to inflict damage on each other without the costs associated with conventional warfare. Indeed, war via the Internet is potentially cheaper than waging a conventional campaign.[139] Belligerent A could avoid violating neutrality law when launching a cyber attack by inserting operatives directly into Belligerent B or using aircraft outside the airspace of neutral states.[140] Most belligerents are unlikely to use these delivery methods, however. Many states lack the technical and logistical capabilities necessary, and the states possessing such capabilities may not want to accept the risk to lives and equipment inherent in such an approach. Further, in many conflicts, a targeted belligerent is unlikely to risk widening the conflict by retaliating against a neutral state unwilling or unable to prevent attacks across its territory. Instead, the targeted belligerent will likely launch its own Internet-based attacks and exploit the neutral state's vulnerabilities in a similar fashion.

---

134. Walker, *supra* note 19, at 1199.

135. *Id.*

136. *Id.*

137. *Id.* at 1183.

138. *Id.*

139. *Id.* at 1108.

140. Unless, of course, Belligerent A moved its forces through neutral territory.

Additionally, the lack of accountability offers an incentive for states to engage in prohibited cyber attacks.[141] The structure of the Internet makes detection and attribution unlikely.[142] As investigators are discovering, "[c]overing one's fingerprints and footprints online is relatively simple, compared with getting rid of physical evidence. IP addresses can be spoofed, and an attack that appears to come from one place may actually originate somewhere else."[143] As discussed above, a cyber weapon may pass through a neutral state without even alerting the neutral government. Additionally, the target of the attack may find it impossible to trace the route of the attack, leaving it unable to demand that the neutral state take prevention measures. As such, belligerents will likely utilize, intentionally or unintentionally, the Internet nodes of a neutral state and possibly violate IHL without fear of detection or punishment.[144]

IV. IHL SHOULD EVOLVE THROUGH CUSTOM AND STATE PRACTICE TO ENCOURAGE THE USE OF CYBER WEAPONS IN SOME SITUATIONS AND TO PROVIDE STATES BETTER GUIDANCE IN THE CONDUCT OF THESE ATTACKS

Given the difficulty of applying the principles of distinction and neutrality in the context of cyber warfare and the incentives belligerents have to violate these IHL principles in that context, IHL needs to evolve to provide better guidance to states. Section IV.A argues that IHL should evolve to address these situations and actually encourage the use of cyber weapons over conventional methods of warfare in certain situations. However, Section IV.B contends a new treaty is not the best approach for evolving these norms and advocates development through customary international law.

A. *The Current Definitions of Distinction and Neutrality Are Too Narrow and Should Evolve to Accommodate Cyber Weapons and, in Some Cases, Encourage Their Use over Conventional Methods of Warfare*

Cyber warfare poses a challenge to international humanitarian law because the current definitions of the principles of distinction and neutrality are too narrow. Cyber warfare's compliance with the existing principles is

---

141. *Cf.* DOD, ASSESSMENT, *supra* note 18, at 8 ("The long-distance and anonymous nature of computer network attacks may make detection and prosecution unlikely, but it is the firmly established policy of the United States that U.S. forces will fight in full compliance with the law of war.").

142. Cyrus Farivar, *Cyberwar I: What the Attacks on Estonia Have Taught Us About Online Combat*, SLATE, May 22, 2007, http://www.slate.com/id/2166749/.

143. *Id.*

144. The DARPA-proposed active network likely would affect this analysis, since the belligerent would be able to reconfigure the Internet nodes and possibly circumvent neutral parties entirely. *See supra* note 44.

not impossible.[145] Yet some prohibited uses of cyber weapons offer states the possibility of dealing blows to an enemy with a low cost in human life and possibly little physical damage to civilian objects. These advantages make cyber warfare a tempting policy option for decision makers concerned with lowering the number of civilian and soldier deaths while at the same time rapidly achieving victory.[146] Rather than prevent the development of these weapons, the concepts of distinction and neutrality should evolve to encourage states to use cyber weapons in some circumstances while also properly restraining their use in others.

1. *Expanding the Principle of Distinction*

The principle of distinction should expand the definition of military target beyond its customary confines when evaluating the legality of cyber attacks. The changing scope and objectives of modern military conflict have eroded the distinction between civilian and military objects, but the potentially nonlethal nature of cyber warfare justifies expanding the list of objects that qualify as military targets. The new definition should include some infrastructure and services that have traditionally been identified as civilian objects.

The modern concept of war has challenged the definition of military target in part because the nature of warfare has dramatically changed.[147] The traditional rule of distinction was "based on the principle that, while the aim of a conflict is to prevail politically, acts of violence for that purpose may only aim at overcoming the military forces of the enemy."[148] Yet the belief that overcoming the military forces of the enemy should be the sole strategic objective of warfare seems out of date on the battlefield of the twenty-first century, where today's civilian can become tomorrow's insurgent, where the military's capabilities are largely dependent on the private sector, and where a well-placed psychological blow can topple an opposing regime. States have long criticized Additional Protocol I as "being focused too narrowly on definite military advantage and paying too little heed to war sustaining capability, including economic targets such as export industries."[149] At the same time, a return to the indiscriminate attacks of World War II would be abhorrent, despite the potential for effective long-term damage to a belligerent's economic or administrative infrastructure.

---

145. *See supra* Section II.B.

146. *See* R.B. Brandt, *Utilitarianism and the Rules of War*, 1 PHIL. & PUB. AFF. 145, 154 (1972) ("[N]either side will consent to or follow rules of war which seriously impair the possibility of bringing the war to a victorious conclusion.").

147. *See* O'Donnell & Kraska, *supra* note 48, at 155.

148. SASSÒLI, *supra* note 70, at 3.

149. Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia, para. 40, June 8, 2000, 39 I.L.M. 1257.

Cyber weapons offer a third path, one that IHL should encourage states to follow. Cyber warfare, if properly limited, may allow belligerents to act on an expanded list of targets while also avoiding the loss of civilian lives and damage to civilian objects. Because of the nonlethal potential of these weapons, IHL should offer states greater flexibility in deploying cyber weapons rather than regulating cyber warfare with the same restrictive rules that apply to conventional weapons. For example, IHL could allow for the targeting of any object that provides effective war-sustaining capability or indirectly contributes to military action, regardless of whether its neutralization offers a definite military advantage. Such an expanded definition would incentivize states to develop their cyber warfare capability to take advantage of an expanded target set.

At the same time, the principle of proportionality could play an expanded role to properly limit the effects of the attack.[150] This principle states that the "[l]oss of life and damage to property incidental to attack must not be excessive in relation to the concrete and direct military advantage expected to be gained."[151] So long as the loss of civilian lives remained low and some discernable military advantage existed, states would be able to attack certain traditionally protected targets.[152] If either condition were lost, the principle of proportionality would function to prevent the cyber attack.[153] This would ensure that civilian lives were properly protected. Thus, the principle of distinction could expand to include additional targets without an additional increase in truly indiscriminate attacks and accompanying loss of civilian lives.

2. *Evolving Neutrality to Focus on Intent*

The definition of neutrality must also evolve. Belligerent and neutral states face significant difficulties in complying with IHL under the current structure of the Internet.[154] In recognition of these difficulties, the scope of the duties imposed under IHL on neutral and belligerent states should change. IHL should preserve respect for the principle of neutrality and offer neutral states a way to effectively maintain that neutrality while avoiding unrealistic limitations on the use of cyber weapons.[155]

One approach would be to adopt an intent-based view of neutrality.[156] Under this view, a belligerent would not violate IHL unless it intentionally directed cyber weapons through the Internet nodes of a neutral state.[157] Simi-

150. *See* O'Donnell & Kraska, *supra* note 48, at 156.

151. *Id.*

152. *See* Schmitt, *supra* note 90, at 396–98.

153. *See id.*

154. *See supra* Part III.

155. Brown, *supra* note 16, at 210.

156. *Id.* at 210–11.

157. *See id.*

larly, this view would not require the neutral state to take action to prevent the unintentional passage of the cyber weapons through its borders, and a belligerent could not take action against a neutral state that was unable to prevent the passage of cyber weapons through its networks.[158] If the neutral state took some act to support the attack of one belligerent or the other, then the targeted belligerent would be able to take action against the neutral state.[159] Under this view of neutrality, as long as the neutral state takes no action to favor one belligerent or the other, it maintains its neutrality, and the risk of an ever-widening conflict may be averted.[160] Such an approach would acknowledge the reality of cyber weapons while also preserving a measure of respect for the principle of neutrality.

B. *The Evolution of New Norms—Treaties Are Not the Answer*

New norms should develop to govern the conduct of cyber warfare, but a new treaty is neither possible nor necessary. The international legal community can extend at least some of the existing framework to apply to cyber warfare. Further analysis will likely expand the other principles of IHL in a similar way.[161] Rather than coming from an international agreement, these norms should evolve through custom, codes of conduct, or rules of engagement, perhaps with an eventual goal of codification based on experience.

Any action toward a new treaty would be premature. Indeed, states will seek to "avoid prematurely limiting a weapon that could potentially offer some measure of non-lethality to conflict."[162] While developing clear norms is in the self-interest of states,[163] states are unlikely to limit the use of a new weapon when so little is known about its full capabilities.[164] Unlike the conventional weapons treaties of the 1980s involving land mines or blinding lasers,[165] wealthy states have little incentive to create a new treaty for this method of war because cyber weapons offer these states the opportunity to conduct war with minimal expense in lives and resources. Similarly, poor states may have an opportunity to achieve a measure of parity with wealthy states through the development of cyber weapons.[166] Rather than prema-

---

158. *See id.*

159. *Id.* at 211.

160. *See supra* Section III.B.

161. Indeed, some scholars have already attempted these extensions. *See, e.g.*, Brown, *supra* note 16, at 201–02.

162. BRYAN W. ELLIS, THE INTERNATIONAL LEGAL IMPLICATIONS AND LIMITATIONS OF INFORMATION WARFARE: WHAT ARE OUR OPTIONS? 14 (2001).

163. *Id.*

164. *Id.*

165. *See* Conventions on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects Protocol II, Oct. 10, 1980, 1342 U.N.T.S. 168, 19 I.L.M. 1529.

166. Wealthy states may be far more vulnerable to cyber weapons given the increased level of technological sophistication of their infrastructure. *See* ELLIS, *supra* note 162, at 14 ("An outright

turely limit the use of these weapons, the majority of states will only seek a new treaty once they have deployed cyber weapons in combat or simulation and so better understand their possible effects.

Further, enforcing any new treaty would prove difficult. Any potential enforcer would face serious difficulties in linking belligerents to cyber attacks. Understanding cyber warfare also requires expert knowledge. Even determining whether or not a violation has occurred at all may be difficult. Traditional mechanisms for enforcement in other areas of international law, such as the International Court of Justice or other tribunals that are composed primarily of lawyers, may be ill suited to handle these cases.[167] Additionally, states may resist the creation of a new treaty when non-state actors, such as terrorists and criminal organizations, are likely to ignore its prohibitions.[168]

Rather than focus efforts on creating a new treaty, states can evolve new norms for cyber warfare through other methods. This would leave open the possibility of eventual codification into a treaty based on a better understanding of the nature of cyber warfare. As one commentator put it:

> Haphazard as the prospect may be, rules for [cyber warfare] should be left to developing customary norms and general principles, derived by analogy from other well-developed bodies of war like the [Law of the Sea], the law of naval warfare, and the law of aerial warfare, perhaps with help from commentators, before serious consideration of a treaty begins.[169]

One way these norms may evolve is through the development of processes that force commanders to consider the possible legal ramifications of an attack.[170] These processes, which could require commanders to examine the various effects of the attack on physical infrastructure at different levels of predictability, would apply the principles of IHL to cyber warfare and could be used to develop new rules of engagement to govern cyber warfare.[171] By forcing military commanders to justify their actions according to legal principles, states should be able to study how the principles of IHL change with the deployment of cyber weapons in combat, and a common state practice may begin to emerge.

CONCLUSION

This Note has shown that international humanitarian law does regulate the conduct of cyber warfare, and that violations of the traditional notions of

---

ban on IW or placing strict controls on the weapons of IW appears sensible from the U.S. perspective, particularly if we find our vulnerabilities outweigh our technological advantages.").

167. One proposed convention extends the authority of the ICJ as its enforcement mechanism. *See* Brown, *supra* note 16, at 213–14.

168. ELLIS, *supra* note 162, at 14. Other approaches to creating new norms similarly may fail to obtain the compliance of non-state actors.

169. Walker, *supra* note 19, at 1200–01 (citation omitted).

170. *See* O'Donnell & Kraska, *supra* note 48, at 159.

171. *See id.*

distinction and neutrality are more likely to occur in cyber warfare than in conventional warfare. States are unlikely to refrain from engaging in some forms of prohibited conduct. Because of the potentially nonlethal nature of cyber weapons, the meaning of these principles should evolve to accommodate and, in some cases, encourage the use of this new and changing method of warfare. Such an evolution will allow the rule of law to guide the development of cyber warfare to ensure that civilian lives are protected in the age of cyber warfare.