Intended Consequences: Regulating Cyber Attacks

Wolfgang McGavran*

I. INTRODUCTION

> A gift consists not in what is done or given, but in the intention of the giver or doer.
>
> —Seneca the Younger
> (c. 4 B.C.-65 A.D.)

The 9/11 Commission report described the failure of the United States' security apparatus to foresee Al Qaeda's attacks in 2001 as, in part, a failure of imagination.[1] After the attacks, one step taken by the U.S. government to avoid being blindsided again was to set up a group of authors, Hollywood writers, and producers, whose works are often replete with imaginative human-imposed chaos, to brainstorm vulnera-

 J.D. candidate 2010, Tulane University School of Law; B.A. 2006, University of Texas at Austin.

1. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., 9/11 COMMISSION REPORT 339 (2004), *available at* http://9-11commission.gov/report/911Report.pdf.

bilities.[2] The minds behind *Die Hard* and *MacGyver* were among the participants.[3] In the most recent installment of the *Die Hard* film series, *Live Free or Die Hard*, the villains' weapon of choice is cyber warfare.[4] Previous plots included hijacked airliners[5] and bombed buildings.[6] In *Live Free or Die Hard*, a disgruntled computer hacker attempts to execute what he calls a "fire sale."[7] In the cyber warfare or terrorism context, that means transport infrastructure, utilities, nuclear facilities, banks, and exchanges are all crippled, more or less simultaneously.[8] Such a simultaneous attack would make coordinated response and damage mitigation difficult. In one scene, the villain reroutes gas pipelines to cause a pressure buildup and explosion.[9] Obviously the power to destroy such vital infrastructure would be useful to nations in conventional wars as well; after all, "why bomb your enemy's power-stations or stockmarkets if you can disable them with software?"[10] While modern network technologies have allowed society to reap enormous efficiencies, they have also left these systems vulnerable to just the type of attack imagined by the Hollywood writers and directors in *Live Free or Die Hard*.

The threat posed by cyber warfare and cyber terrorism is not just the stuff of fantasy. Indeed, the last decade has seen several high-profile examples, and there is no indication that the exploitation of networked systems' inherent vulnerabilities will abate in the future as even more of the systems that modern society relies on are connected to the Internet. Governments around the world are taking bold steps on their own in light of these threats. Some 120 nations are using the Internet to help fulfill their own "political, military, and economic espionage" goals.[11] Yet the laws that govern the relationship between nation-states are ill-prepared for the new world order of cyber warfare and terrorism. Until a new legal regime can be erected to deal with the threat of cyber warfare and cyber terrorism, actors in this emergent field will be forced to fit these

---

2. Steve Gorman, *U.S. Filmmakers Mull Terror Scenarios for Army*, REUTERS, Oct. 10, 2001.

3. *Id.*

4. LIVE FREE OR DIE HARD (20th Century Fox 2007).

5. DIE HARD 2 (20th Century Fox 1990).

6. DIE HARD WITH A VENGEANCE (20th Century Fox 1995).

7. LIVE FREE OR DIE HARD, *supra* note 4.

8. *See id.*

9. *Id.*

10. *Marching Off to Cyberwar*, ECONOMIST, Dec. 4, 2008, *available at* http://www.economist.com/sciencetechnology/tq/displaystory.cfm?story_id=12673385.

11. *Virtual Criminology Report—Cybercrime: The Next Wave*, MCAFEE, http://www.mcafee.com/us/research/criminology_report/default.html (last visited Aug. 22, 2009).

new forces by analogy into the currently unwieldy international law of war.

This Comment begins with a brief introduction to different types of cyber attacks. The term "cyber attack" is itself amorphous and runs the gamut from espionage to attacks ranging from the annoying to the apocalyptic. Next, the Comment examines several recent and high profile instances of cyber attacks, particularly those in the nations of Estonia and Georgia. Then the Comment examines some of the steps being taken by nation-states to confront the realities of cyber attacks. The Comment then applies current standards of international law to cyber attacks. In this analysis, the poor fit between currently existent laws and the threats posed by cyber attacks, which the drafters of currently enacted laws could hardly have imagined, will become evident.

Finally, this Comment joins a chorus of scholarly literature advocating modernization of international law to prepare actors that rely upon it for the inevitable growing role of cyber attacks by both nation-states and nonstate actors. This Comment argues that focusing on the primary intent of the cyber attacker is a workable way to deal with interpretive problems posed by cyber attacks. While an explicit acknowledgement of the problem through the United Nations would be an ideal solution, it is more likely that smaller bilateral and multilateral agreements between states will break the trail in rulemaking in the Internet realm.

II. TYPES OF CYBER ATTACKS

"Cyber attack" is an amorphous term that could describe multiple discrete actions or combinations thereof. A rudimentary understanding of these arrows in the cyber warrior's quiver is necessary to understand why current legal regimes are less than adequate in dealing with the threats and opportunities posed by different types of cyber attacks. In each type of cyber attack described below, the type of attack has little to do with the possible impacts of the attack. For example, a user could use a denial-of-service attack to shut down an air traffic control system (causing many casualties) using the same techniques as she would to temporarily shut down a social adversary's blog.[12] As that example illustrates, and this Comment will discuss, any type of rule making will need to distinguish the attack based upon *impact* of the cyber attack or *intent* of the cyber attacker, rather than the technical *means* employed.

12. Mindi McDonnell, U.S. Computer Emergency Ctr., Understanding Denial-of-Service Attacks (2004), http://www.us-cert.gov/cas/tips/ST04-015.html.

A. Espionage

Cyber espionage aims to obtain confidential information over the Internet. The targets of such information might range from personal information used to steal identities to access of state secrets. Unlike traditional spying, cyber espionage can be (and is) done from across the globe and without any need for physical exposure to risk by the perpetrator.[13] Traditionally, spies caught within the territorial bounds of a nation are subject to the domestic laws of that nation.[14] Lack of jurisdiction makes this approach untenable when dealing with cyber espionage where the information gatherer, if she can be tracked at all, is in a foreign nation.[15]

B. Denial-of-Service Attacks

Denial-of-service (DoS) attacks and their meaner cousins, distributed denial-of-service (DDoS) attacks, seek to render a computer resource such as a Web site unusable, either temporarily or permanently.[16] At their most rudimentary, DoS attacks seek to cripple a Web site by sending it an overwhelming amount of data requests, so that it is then unable to respond to legitimate data requests.[17] Other types of DoS attacks seek to take advantage of known hardware interface weaknesses and can permanently damage computer hardware.[18] A DDoS attack uses a multitude of computers that are preinfected with a virus that hijacks the computer to attack Web sites, making it exponentially more powerful than a standard DoS attack.[19]

Criminal syndicates rent these hijacked computers to the highest bidder.[20] The cost to rent an infected computer is low, perhaps four cents.[21] At this price, "[y]ou could fund an entire cyber warfare

---

13. *See, e.g.*, John Markoff, *Vast Spy System Loots Computers in 103 Countries*, N.Y. TIMES, Mar. 29, 2009, at A1 (reporting on the largest computer spying operation to be discovered).

14. Roger D. Scott, *Territorially Intensive Intelligence Collection and International Law*, 46 A.F.L. REV. 217, 220 (1999).

15. *See generally* Darrel C. Menthe, *Jurisdiction in Cyberspace: A Theory of International Spaces*, 4 MICH. TELECOMM. & TECH. L. REV. 69, 71-73 (1997-1998) (discussing various theories of jurisdiction in a cyber space context).

16. McDonnell, *supra* note 12.

17. *Id.*

18. *Id.*

19. *See id.*

20. Andy Greenberg, *Storm for Rent*, FORBES, (Jan. 1, 2008), http://www.forbes.com/2008/01/09/storm-worm-cybercrime-tech-security-cx_ag_0109storm.html.

21. John Markoff, *Cyber Attack Preceded Invasion*, CHI. TRIB., Aug. 13, 2008, *available at* http://archives.chicagotribune.com/2008/aug/13/business/chi-cyber-war_13aug13.

campaign for the cost of replacing a tank tread, so you would be foolish not to."[22]

C. Logic Bombs

A logic bomb is a type of cyber attack that sits dormant until certain conditions are met, at which point the program executes its malicious function.[23] By not manifesting its malicious function immediately, a logic bomb is able to spread more widely than it could if its negative impact was readily apparent, because this would rouse suspicions of the program that the logic bomb is embedded in. During the Cold War, the Central Intelligence Agency allegedly used this type of cyber attack to destroy a Soviet natural gas pipeline.[24]

D. Trojan Horses

A Trojan horse is a type of malicious software that fools a computer user into thinking that it will perform a wanted function but instead gives unauthorized access to the infected machine to a third party.[25] Once so compromised, the infected computer might become part of a botnet or be taken control over through remote access by the unauthorized user.[26]

III. EXAMPLES OF CYBER ATTACKS

A. Estonia

The Baltic nation of Estonia came under DoS attacks in 2007.[27] These attacks shut down several government Web sites.[28] Estonia has been a member of the North Atlantic Treaty Organization (NATO) since 2004.[29] The controversy that sparked these decidedly twenty-first century hostilities had at its genesis events in the middle of the twentieth. Estonian authorities relocated a Soviet-era bronze statue, the so-called "soldier of Tallinn," from the capitol in Tallinn to an international

---

22. *Id.*
23. What is a Logic Bomb?, http://tech-faq.com/logic-bomb.shtml (last visited Nov. 10, 2009).
24. David Hoffman, CIA Slipped Bug to Soviets (Feb. 26, 2004), http://www.msnbc.msn.com/id/4394002.
25. *See, e.g.*, U.S. Computer Emergency Ctr., Targeted Trojan Email Attacks (2005), http://www.us-cert.gov/cas/techalerts/TA05-189A.html.
26. *See* McDonnell, *supra* note 12.
27. *A Cyber-Riot*, ECONOMIST, May 12, 2007.
28. *Id.*
29. NATO, NATO Member Countries, http://www.nato.int/structur/countries.htm (last visited Aug. 22, 2009).

military cemetery.[30] Ethnic Russians make up a sizeable minority in Estonia, at around twenty-five percent of the population.[31] These ethnic Russians and the Russian government alike objected to this relocation, which they saw as a marginalization; the Kremlin labeled the relocation as blasphemous.[32] Estonia had to quell riots, but the assault upon its Internet infrastructure was what caught the world's attention—never before had a nation been subject to such coordinated Internet attack.[33]

Estonian infrastructure is, like that of any modern nation, reliant on Internet-dependent services. In fact, Estonia has been called "the most wired country in Europe."[34] Citizens can even vote over the Internet from home in national elections.[35] Over the course of the cyber attacks, numerous government Web sites were made unusable, including those of the foreign and justice ministries.[36] Other sites were hacked into and their content was replaced by propaganda.[37] In order to keep certain Web sites—from newspapers to banks—available for use by its own citizens, Estonia was forced to shut down its Internet connections to the rest of the world.[38] The attacks originated from the United States, Egypt, South America, and Russia.[39] Suddenly, as far as the Internet world was concerned, Estonia was *terra incognita*.[40] The flow of information from the nation was shut off. Trade and bank transactions became impossible.[41] The most wired country in Europe was thrust into isolation.[42]

---

30. *A Cyber-Riot*, *supra* note 27.

31. CIA, The World Factbook-Estonia, Mar. 19, 2009, https://www.cia.gov/library/publications/the-world-factbook/geos/en.html.

32. *A Cyber-Riot*, *supra* note 27.

33. NATO and the United States quickly dispatched envoys to Tallinn to observe the cyber attacks first hand. *Id.*

34. Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED MAG., Aug. 21, 2007, *available at* http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all. Estonia has been given the moniker E-stonia because of its high level of Internet integration. *See, e.g.*, Indranjit Basu, Estonia Becomes E-stonia (Apr. 9, 2008), http://www.govtech.com/dc/articles/284564.

35. Sutton Meagher, Comment, *When Personal Computers Are Transformed into Ballot Boxes: How Internet Elections in Estonia Comply with the United Nations International Covenant on Civil and Political Rights*, 23 AM. U. INT'L L. REV. 349, 351 (2008).

36. *A Cyber-Riot*, *supra* note 27.

37. *Id.*

38. *Id.*

39. Davis, *supra* note 34.

40. *Id.*

41. *Id.*

42. *See id.*

During and following the Internet attacks, Estonian officials publically accused Russia of having orchestrated the attacks.[43] Russia, for its part, has denied involvement.[44] Because proficient cyber warriors are capable of masking their locations, it is a nigh-impossible task to trace the perpetrators. The trail becomes cold after these attacks in hours or even minutes.[45] The cyber attacks on Estonia demonstrated several disturbing realities. First, they showed that cyber attacks are extremely difficult to trace, making them attractive tools for a nongovernmental terrorist group or a government who seeks to remain anonymous. Second, such attacks are relatively easy to carry out. Indeed, many of the computer users whose machines were used in the attack were not even aware of it. Third, the Estonian incident demonstrates that cyber attacks can cause real world harm and result in significant confusion and cost.

B. Georgia

The cyber attacks against Georgia present a second and even more timely example of a nation as a target of cyber warriors. Unlike in the Estonian example, the assault on Georgian Internet infrastructure anticipated and coincided with an assault on Georgian sovereign territory from land, sea, and air. Although enjoying a generally good relationship with the West, Georgia is not a member of NATO.[46]

Georgia launched a ground and air attack against the restive provinces of South Ossetia and Abkhazia, claiming to be responding to Russian troop movements.[47]

The cyber attacks took the form of DoS attacks, Web site hijacking, and the defacing of Georgian news and government Web sites to include propaganda.[48] For example, the Web site of the Georgian President, Mikheil Saakashvili, was hacked, and anyone who visited the site would see his photos juxtaposed with those of Adolf Hitler.[49] The effects of the cyber attacks were not as pronounced as in the previous attack on Estonia

---

43. *A Cyber-Riot*, *supra* note 27.

44. *See id.*

45. *See* Frontline: *Cyberwar!* (PBS television broadcast Apr. 24, 2003), *available at* http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/.

46. NATO, NATO's Relations With Georgia, http://www.nato.int/issues/nato-georgia/index.html (last visited Aug. 22, 2009).

47. The contention that the Georgians were merely responding to Russian troop movement has been largely criticized, including by NATO and the United States. Ralf Beste et al., *The West Begins To Doubt Georgian Leader*, DER SPIEGEL, Sept. 15, 2008, *available at* http://www.spiegel.de/international/world/0,1518,578273-2,00.html (Christopher Sultan trans.).

48. Jeremy Kirk, Estonia, Poland Help Georgia Fight Cyber Attacks (Aug. 12, 2008), http://www.cio.com/article/443314/Estonia_Poland_Help_Georgia_Fight_Cyber_Attacks.

49. *Id.*

because Georgian infrastructure is not as firmly enmeshed in the Internet. Therefore, fewer targets could be reached through DDoS attacks. This cyber vandalism is suspected to be the handiwork of Russian nationalists, but, as in Estonia, there is no direct evidence of Russian government involvement.[50] Another reason that Georgia was not as severely affected as might otherwise have been the case is that what has been dubbed a "cyber alliance" formed to help them mitigate the damage of the cyber attacks.[51] Poland and Estonia, also ex-Soviet bloc nations, lent resources in the form of experts and (presumably more secure) server space for targeted Georgian Web sites.[52]

The cyber attacks preceded and followed the Russian military offensive. In the month before the Georgian War began, several Georgian Web sites were the targets of cyber attacks.[53] It has been theorized that these attacks were a dress rehearsal for the much larger attacks that occurred during the war itself.[54] Then, even after Russian tanks crossed back into Russia, attacks against Georgian government and news sites continued unabated.[55]

IV. NONDIPLOMATIC SOLUTIONS: DIGITAL DETERRENCE?

With little in the way of treaties or laws specifically dealing with cyber attacks, the notion of deterrence as an alternative way for the United States to rein in the problem of cyber attacks has gained prominence. One commentator likened the idea that a nation could defend itself from cyber attack without a strong retaliatory ability to relying on gated castles in the days of bombers and artillery.[56] The better strategy, the argument suggests, is to destroy or deter the cyber attacker rather than to erect static defenses.[57] The United States could build a network that could launch crippling DDoS attacks against computers that launch attacks at the United States—"carpet bombing in cyberspace."[58]

---

50. *Id.*
51. Kirk, *supra* note 48.
52. *Id.*
53. Markoff, *supra* note 21.
54. *Id.*
55. Vasanth Sridharan, Russia Calls Off Attack on Georgia—Cyber Attack Continues (Aug. 12, 2008), http://www.businessinsider.com/2008/8/russia-calls-off-attack-on-georgia-cyber-attack-continues.
56. Charles W. Williamson III, *Carpet Bombing in Cyberspace*, ARMED FORCES J. (2008), *available at* http://www.armedforcesjournal.com/2008/05/3375884.
57. *Id.*
58. *Id.*

Much has already been done in the United States to prepare for this new domain of warfare.[59] The United States Air Force has emerged as a cyberspace leader, although a myriad of other agencies and departments, such as the FBI and Secret Service, have their own cyber operations.[60] The notion of a separate military branch—a "Cyber Force" on equal footing with the Army, Navy, and Air Force—has even been proposed.[61] Amongst the factors arguing for such a separate military branch are the stability and funding typical of military institutions, the importance of networked activity to all other military branches, and the need to maintain competiveness with other nations pouring resources into this field.[62]

Opposed to this view are those who argue that "[t]here is not always a meat-space analog to issues in cyber space," and there is little reason to believe that cyber attacks could be deterred in the same way as a conventional military strike.[63] Under this view, deterrence and nonproliferation models are doomed to fail to stop cyber attacks because the differences between an innocent software company and a malicious one are hard to discern and easily obfuscated.[64] Furthermore, there is fear that overzealous government involvement might mark "every computer science graduate as a potential e-A.Q. Kahn."[65]

Nation-states are, however, not the only players with a stake in the game of locating rogue perpetrators of cyber attacks. After all, the gross domestic product of some third-world nations pales in comparison to some corporations' income statements. So too does their vulnerability to cyber attack. Such vulnerability has spurred Microsoft to recently offer $250,000 for information leading to the capture of the author of a malicious software program known as "Conficker."[66] The Conficker program has infected millions of computers, which together form a

---

59. The U.S. National Security Agency Director, Air Force General Michael Hayden, announced that "[i]nformation is now a place. It is a place where we must ensure American security as surely as . . . sea, air, and space." Thomas C. Greene, *NSA Stakes Out Virtual Battlefield*, REGISTER, Oct. 17, 2000, http://www.theregister.co.uk/2000/10/17/nsa_stakes_out_virtual_battlefield/.

60. Natasha Solce, Comment, *The Battlefield of Cyberspace: The Inevitable New Military Branch*, 18 ALB. L.J. SCI. & TECH. 293, 311, 317 (2008).

61. *See id.*

62. *See id.* at 313-16.

63. Posting of Michael Tanji to Danger Room, http://blog.wired.com/defense/2009/02/deterring-a-cyb.html (Feb. 19, 2009, 14:31).

64. *Id.*

65. *Id.*

66. John Markoff, *Computer Experts Unite To Hunt Worm*, N.Y. TIMES, Mar. 18, 2009, *available at* http://www.nytimes.com/2009/03/19/technology/19worm.html?_r=1&ref=science.

botnet that is suspected to have become active on April 1, 2009.[67] Computers on U.K. warships and belonging to the Houston Municipal Court are among those that have been infected.[68] The purpose of the program is yet unclear but could have, in a worst-case scenario, disrupted nations or the Internet itself.[69]

V. FITTING CYBER WAR INTO CURRENT LAW

It is evident that cyber attacks have become prevalent, and that various groups—from governments to terrorist groups—recognize the important role that such attacks will play in the future. But how should such attacks be treated? Should perpetrators be prosecuted as criminals for defacing Georgian Web sites as they would be if they had painted graffiti on the steps of the Georgian Capitol? What if, using the same techniques, the perpetrators cause a nuclear power plant to go critical? If the proposed Cyber Force launches an attack, would this be an act of war? These are vexing questions. These are not, however, entirely new questions to legal theorists and policy makers. The terrorist attacks of 2001 necessitated a reevaluation of how to approach terrorism from a legal perspective. The different approaches and the lessons learned in categorizing acts of terrorism should be seen as instructive for purposes of creating a legal order for cyber attacks.[70] The lessons learned from the terrorism context, combined with the novel and idiosyncratic problems posed by cyber attacks, offer strong support to the growing chorus of

---

67. *Id.*

68. John Leyden, *Houston Justice System Laid Low by Conficker Worm*, REGISTER, Feb, 9, 2009, http://www.theregister.co.uk/2009/02/09/houston_malware_infection/ ("The infection forced municipal courts in the Texan city to shut down on Friday, and police had to temporarily stop making arrests for minor offences, such as those for outstanding traffic warrants or minor drug possession."); Lewis Page, *MoD Networks Still Malware-Plagued After Two Weeks*, REGISTER, Jan. 20, 2009, http://www.theregister.co.uk/2009/01/20/mod_malware_still_going_strong/.

69. Page, *supra* note 68.

70. Duncan Hollis summarizes these approaches into four categories. The first approach is where the law on terrorism was pre-September 11—treating terrorism as a crime. The second was to abandon the criminal approach to terrorism in favor of treating it as a war and, as such, governed by the law of war. A third, hybrid approach sought to combine the criminal and war approaches to combat terrorism. Finally, some advocated the abandonment of the criminal and war dichotomy in favor of new laws specifically tailored to combat terrorism. Hollis contends that "devising a new legal framework . . . may offer the most effective response to the challenges of regulating cyberspace conflicts." Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1026-28 (2007).

commentators that advocates a new legal regime specifically designed to address cyber attacks.[71]

A. The Current Legal Regime

Currently, the law of war applies to cyber attacks by analogy only.[72] There is little indication that nations, including the United States, are acting to modernize the rule of war by explicitly addressing information warfare.[73] The Geneva Convention, in article 36 of Additional Protocol I, obligates member nations to determine whether a "new weapon, means or method of warfare" would be prohibited by that protocol or other international law.[74] Cyber attacks could clearly be considered a new weapon if they were used to cause physical destruction in the way bombs do today. In that example, the applicability of the rule of war by analogy is straightforward since both create the same effect as a traditional kinetic attack. Other possible uses of cyber attacks are less easily dealt with by the rules of war.

In analyzing the legal implications of cyber attacks, a threshold issue is whether or not such cyber attacks constitute a use of "force" under the U.N. Charter.[75] Section 2(4) of the U.N. Charter states, "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any manner inconsistent with the Purposes of the United Nations."[76]

Three approaches have developed to fitting cyber attacks into this regime, but "[e]ach approach proves inadequate in the modern context."[77] One approach, known as the "instrumentality" approach, would place cyber attacks outside of the definition of the use of force because cyber

---

71. *See id.* at 1029 (advocating the adoption of an international law for information operation, or ILIO, to remedy the uncertainty, complexity, and insufficiency of using the rules of war to regulate Internet operations).

72. *See id.* at 1037.

73. *See id.* at 1037-38.

74. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol 1), art. 1.2, adopted June 8, 1977, 1125 U.N.T.S. 3, *available at* http://www.icrc.org/IHL.nsf/WebART/470-750045?Open Document ("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.").

75. But this threshold question is far from the only troublesome area. The ban of perfidy, the requirement for civilian distinction, and the laws of neutrality also present vexing questions. *See* Hollis, *supra* note 70, at 1040 n.66.

76. U.N. Charter art. 2, para. 4.

77. Hollis, *supra* note 70, at 1040-41.

attacks are materially different in form from the traditional, i.e., kinetic, forms of military action.[78] A second approach, known as the "target-based" approach, holds that a cyber attack would be the equivalent in terms of U.N. law of an armed attack whenever it penetrates the critical infrastructure of a nation.[79] A third approach, known as the "consequentiality" approach, would equate a cyber attack with an armed attack whenever the consequences of the cyber attack reproduce the type of damage that would be caused by a traditional military attack.[80]

These definitions, studied individually, suffer from either under- or overinclusiveness. An underinclusive definition could leave a targeted nation remediless under international law. For example, under the instrumentality approach, if a cyber attack caused two commuter trains to collide, the attack would still not be considered a use of force—despite the fact that railways are vital parts of national infrastructure and such an attack is almost sure to cause casualties. Conversely, some definitions carry the risk of being both under- and overinclusive. For example, under the target-based approach, a cyber attack on a railway system that makes the system's Web site display incorrect fares might count as a use of force, but a cyber attack that disrupts a roller coaster's control system and causes a fatal accident would not—all because the former constitutes critical infrastructure and the latter does not. Furthermore, the target-based approach requires a complicated threshold decision of what qualifies as "critical infrastructure."[81]

Just as an underinclusive definition might leave a targeted nation remediless, an overinclusive definition carries the risk of rapid and dangerous escalation. Such a danger is especially acute in cases of preexisting alliances and in situations where a nation might be seeking justification in order to escalate tensions to armed conflict. For example, the NATO treaty mandates:

> The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defense recognized by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including

78. *Id.* at 1041. The text of the U.N. Charter offers support for this view; Article 41 lists "measures not involving the use of armed force" to include "complete or partial interruption of . . . telegraphic, radio, and other means of communication." U.N. Charter art. 41.

79. Hollis, *supra* note 70, at 1041.

80. *Id.*

81. *Id.*

> the use of armed force, to restore and maintain the security of the North Atlantic area.[82]

Armed attack is, in turn, defined as an armed attack on the territories or forces of a member state.[83] Under such treaties, similar interpretive problems arise as under the "use of force" provision of the U.N. Charter. In cases involving mutual-defense treaties, the interpretation of a cyber attack as an armed attack could initiate mandatory assistance, up to and including traditional armed response.[84] As long as nations disagree over the definition of a cyber attack, they will be able to pigeonhole cyber attacks as either uses of force or not to suit their immediate political needs.

B. Towards a Workable Definition—The Importance of Intent

Fitting cyber attacks into the currently existing international legal framework requires specific definitions that take into account the idiosyncrasies of this new international arena. The primary purpose of such definitions should be to help provide a modicum of certainty by which to judge the consequences of various actions. For some issues, continuing reliance on domestic criminal codes does not endanger international stability.[85] It is critical, however, that workable definitions be adopted to fit cyber attacks into the "use of force" and "armed attack" context.

In general, the consequentiality approach is the best starting point for such a definition. Recall that under this approach, a cyber attack would count as the use of force if its *effects* are the same as those that would have resulted from conventional military attacks. Such destructive measures—that likely produce property damage and deaths—should not be considered not to be a "use of force" or "armed attack" merely because they are perpetrated using a logic bomb rather than a bombing run.

At the same time, there are many forms of cyber attacks that should reasonably be considered uses of force even though they do not create damage comparable to bombs or bullets.[86] In such situations, the consequentiality approach is insufficient. The type of target (e.g., critical infrastructure or otherwise) should not be determinative in such

---

82. North Atlantic Treaty art. 5, Apr. 4, 1949, 63 Stat. 2241, 2244, 34 U.N.T.S. 243.

83. *Id.* art. 6.

84. *See id.* art. 5.

85. For example, twenty states treating music piracy twenty different ways is unlikely to lead to war.

86. *See* Hollis, *supra* note 70, at 1042.

situations. Rather, the *intent* of the attack should be given an important role.

One possibility is to differentiate cyber attacks based upon their primary purpose and intent. For example, cyber attacks that disable or deface a Web site, spread propaganda, or otherwise cause annoyance could be distinguished from cyber attacks that primarily seek to cause disruption. However, distinguishing between annoyance attacks and disruptive attacks causes interpretive problems of its own. For example, the defacement of a Web site obviously disrupts the Web site's operation. But, by focusing on the primary intent, which could be deduced under a totality of circumstances test, annoyance attacks can be distinguished from attacks that intend to cause disruption.

Examples of disruptive attacks could include attacks that disable real world systems, such as emergency services, electrical grids, and finance. The hallmarks of an annoyance attack could include temporary or limited duration, zero to low probability of resultant loss of life or property damage (excluding, perhaps, opportunity costs), and informational, vandalistic, or hooliganistic motives. In contrast, disruptive attacks are distinguished by lasting or lingering impact and the interruption or confusion of services or goods to individuals and organizations.

In conjunction with a consequentiality approach, the primary intent approach, distinguishing between annoyance attacks and disruptive attacks, could provide a solid basis on which states could model new international agreements to regulate cyber attacks into existing "use of force" terms. Some, but by no means all, problems of under- and overinclusiveness are remedied by such a definition, and states would be able to act with more certainty as to how their actions, and actions taken against them, will be judged on the international stage.

VI. CONCLUSION

Are the urgent calls for a new legal regime, or even a new military branch, devoted to cyber attacks making a mountain out of a molehill? Would such actions constitute a waste of resources and political energies? Many argue that this is indeed the case, and that cyber attacks could better be described as "weapons of mass annoyance" than weapons of destruction, mass or otherwise.[87] Cyber attacks are, as the argument

87. *See, e.g.*, Interview by *Frontline* with James Lewis, Senior Fellow at Ctr. for Strategic and Int'l Studies (Feb. 18, 2003), *available at* http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/lewis.html; *see also* Gabriel Weimann, *Cyberterrorism: How Real Is the Threat?*, U.S. INST. FOR PEACE, Dec. 2004, *available at* http://www.usip.org/resources/cyberterrorism-how-real-threat.

goes, both much more difficult to carry out than oft reported and less effective.[88] Furthermore, cyber attacks are not ideally suited to either nation-states or terror groups.[89] Nation-states are themselves too dependent on global networks of communication and finances to risk their disruption.[90] Cyber attacks are also a poor fit for terror groups, because cyber attacks have not yet been shown to cause spectacular damage, mass casualties, or public hysteria.[91] Yet the mere fact that a cyber attack of sufficient scale, a "digital Pearl Harbor," to shake away all doubts as to feasibility, has not yet occurred is insufficient ground to delay creating a legal regime to handle these problems. A cyber attack could, theoretically at least, be much more than a weapon of mass nuisance. Further, even a nuisance can in aggregate cause massive economic harm that warrant nation-states' actions. For example, cyber attacks following September 11, 2001, caused $3 billion in damage.[92] Therefore, states should strive to establish an international legal regime to address the current reality and future possibilities of cyber attacks.

A full-scale invasion into sovereign territory, the ultimate example of "use of force" under the U.N.'s rules, requires the resources of a nation-state. Conversely, a cyber attack might be launched by a terrorist group via a satellite uplink from a desolate mountain base, by a hacker via an Internet café, or a well-paid corporate consultant from the top story of a skyscraper. Naturally, nation-states can play too.

If they are wise, nation-states will use their privileged position vis-à-vis lawmaking to ensure that they "monopolize" the legitimate use of cyber force to the greatest extent possible.[93] Max Weber, the influential political economist, wrote that an entity is a state to the extent that its administration "[successfully] claims the *monopoly of legitimate force* for itself."[94] The geographical extent to which a nation could exercise this monopoly defined its borders.[95] The threat of cyber attacks impacting a state's territory jeopardizes this legitimacy. Nation-states seeking to maintain their monopoly of force within their borders will be motivated to come to agreement with similarly motivated nation-states. To the

88. Interview by *Frontline* with James Lewis, *supra* note 87.
89. *See id.*
90. *See id.*
91. *See id.*
92. Arguments that such damage figures are highly speculative and based in large part on lost opportunity cost are strong. *See, e.g.*, Weimann, *supra* note 87.
93. *See* MAX WEBER, POLITICS AS A VOCATION (1919), *reprinted in* MAX WEBER'S COMPLETE WRITINGS ON ACADEMIC AND POLITICAL VOCATIONS 156 (John Dreijmanis ed., Gordon C. Wells trans., 2008).
94. *Id.*
95. *Id.*

extent that cyber attacks can be traced, agreement-privy states could mutually agree to prevent cyber attacks from being launched and to prosecute those that launch them. State authorities and "the vetted" within such states can act to disconnect computers launching cyber attacks.[96] International organizations could be erected that could coordinate responses by authorities within states.

It is likely that preexisting organizations, especially those with mutual defense in mind, will be among the first to address the threats of cyber attack in a comprehensive manner. Preexisting treaty organizations such as NATO already have the rule making machinery and motivation to coordinate against cyber attacks. Indeed, in the case of Estonia, some coordination has already occurred between actors in NATO member states, although not through NATO channels. Considering that cyber attacks often coincide with spats with the Russians, NATO might be especially interested in addressing the issue.

Indeed, in 2008 NATO began the process of establishing the Cooperative Cyber Defence Centre of Excellence in (where else?) Estonia.[97] In parallel to these programs, NATO militaries have agreed on a Cyber Defence Concept "which adds practical action programmes to fit within the overarching policy."[98]

Individual nations, such as the United States, should next establish bilateral mutual commitments with nations outside of those with which they already share mutual-defense obligations. Reliance on preexisting agreements, while a good place to start, will prove inadequate and necessitate the drafting of agreements specifically tailored for problems that arise in cyberspace. For example, after the attacks in Estonia, the Estonian government attempted to compel the Russian authorities cooperation under a bilateral mutual legal assistance treaty.[99] The lack of "fit" between the troubles faced by Estonia and the treaty became readily apparent as Estonians were unable to obtain the cooperation in their investigation that they argued was promised under the treaty's

---

96. "The Vetted" is the term given to a group of individuals that have significant control over Internet infrastructure so as to be able to disconnect computers sending cyber attacks. *See, e.g.*, Davis, *supra* note 34.

97. NATO Opens New Centre of Excellence on Cyber Defence (May 14, 2008), http://www.nato.int/docu/update/2008/05-may/e0514a.html. Understandably, Estonia was one of the earliest proponents of a common cyber defense, calling for it even while it was under cyber attack. Adrian Blomfield, *Estonia Calls for Nato Cyber-Terrorism Strategy*, TELEGRAPH, May 18, 2008, http://www.telegraph.co.uk/news/worldnews/1551963/Estonia-calls-for-Nato-cyber-terrorism-strategy.html.

98. Defending Against Cyber Attacks, http://www.nato.int/issues/cyber_defence/index.html (last visited Oct. 13, 2009).

99. Hollis, *supra* note 70, at 1026 n.19.

provisions.[100] The Russians argued that Estonia had not met the procedural requirements of the treaty.[101] The finger pointing in the aftermath of the Estonian cyber attacks demonstrates that without specific treaties dealing with cyber attacks, nations will likely find themselves floundering in any criminal and forensic investigations that they undertake. The anonymous and cross-border nature of cyber attacks greatly compounds the problem—clearly investigators need all the help that they can get.[102]

In the negotiation of these treaties, one issue that will face contracting parties will be how to define various types of cyber attacks. One option that states should consider is to use an intent-based definition of cyber attack to differentiate between cyber attacks that are intended as annoyances and those that are intended to disrupt. Disruptive cyber attacks threaten a state's monopoly on the legitimate use of force and deserve to be treated as uses of force under international law.

100. *Id.*
101. *Id.*
102. *See id.*