From Nuclear War to Net War: Analogizing Cyber Attacks in International Law

Scott J. Shackelford*

* Scott Shackelford is a J.D. candidate at Stanford Law School and a Ph.D. candidate in international relations at the University of Cambridge. I wish to thank Stanford Professors Helen Stacy, Allen Weiner, Joseph Bankman, and Dean Larry Kramer for their guidance and support with this project. My thanks also to the editing staff at the *Berkeley Journal of International Law* especially Rosamond Xiang, and as always to Emily Craig, my partner in everything.

I.
INTRODUCTION

On April 27, 2007, Estonia was attacked. Only four weeks on the job, Estonian Defense Minister Jaak Aaviksoo was besieged by his aides. In a matter of hours, the online portals of Estonia's leading banks crashed. All of the principal newspaper websites stopped working and circulation suffered.[1] Government communications were largely blacked out. An enemy had invaded and was assaulting dozens of targets across the country.[2] This, however, was not the result of a traditional nuclear, chemical, or biological weapon of mass destruction ("WMD"), nor was it a classical terrorist attack or an invading army. A computer network was responsible for everything.[3]

Nevertheless, the effects of this assault were potentially just as disastrous as a conventional attack on this country, the most wired in Europe and popularly known as "eStonia."[4] By 2007, Estonia had instituted an e-government in which ninety percent of all bank services, and even parliamentary elections, were carried out via the Internet.[5] Estonians file their taxes online, and use their cell

1. *See generally* Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED MAGAZINE, Aug. 21, 2007, http://www.wired.com/politics/security/magazine/15-09/ff_estonia (detailing a rogue computer network's assault on Estonia).

2. *See id*.

3. *See id.*

4. *See id.*

5. *Estonia hit by 'Moscow cyber war'*, BBC NEWS, May 17, 2007,

phones to shop and pay for parking. The country is saturated in free Wi-Fi, while Skype, the free Internet phone company headquartered in Estonia, is rapidly taking over the international phone business.[6] Thus, in many ways this small Baltic nation is like a "window into the future."[7] Someday, "the rest of the world will be as wired as eStonia."[8] That is what made the cyber attack against Estonia all the more effective.

In a matter of days the cyber attacks brought down most critical websites, causing widespread social unrest and rioting, which left 150 people injured and one Russian national dead.[9] Never before had an entire country been targeted on almost every digital front all at once, and never before had a government itself fought back in such a prolonged and well-publicized campaign.[10] Indeed, the attacks were so widespread and the results so grave that Aaviksoo considered invoking Article 5 of the North Atlantic Treaty Organization ("NATO"), which states that an assault on one allied country obligates the alliance to attack the aggressor.[11] At the time, Russia was suspected of the attacks. Regardless of who was actually to blame, this was the first large-scale incident of a cyber assault on a state.[12] It was but a taste of what information warfare ("IW") can do to a modern information society.

To define the parameters of the threat posed, it is worth considering the worst-case scenario cyber attack. The 2007 summer blockbuster film *Die Hard 4.0* dramatized the prospect of a large-scale cyber assault on the Unites States. In that film, a frustrated former Pentagon insider working with a small team of hackers brought down U.S. air traffic control systems, the power and telecommunications grids, and wreaked havoc in the financial services sector.[13] If such a multifaceted cyber attack were coordinated professionally, it could destroy a

http://news.bbc.co.uk/2/hi/europe/6665145.stm.

6. *Estonia and Slovenia*, ECONOMIST, Oct. 13, 2005, http://www.economist.com/displayStory.cfm?Story_ID=E1_VDNVSPS (comparing the economic performance and information technology infrastructure of Estonia and Slovenia).

7. Davis, *supra* note 1.

8. *Id.*

9. *Putin Warns Against Belittling War Effort*, RADIO FREE EUROPE, May 9, 2007, http://www.rferl.org/featuresarticle/2007/05/704c2d80-9c47-4151-ab76-b140457a85d3.html.

10. Davis, *supra* note 1 (Aaviksoo explains that the attacks "were aimed at the essential electronic infrastructure of the Republic of Estonia…All major commercial banks, telecoms, media outlets, and name servers—the phone books of the Internet—felt the impact, and this affected the majority of the Estonian population"); *see also* BBC NEWS, *Estonia hit, supra* note 5.

11. Davis, *supra* note 1; North Atlantic Treaty art. 5, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243.

12. Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, GUARDIAN (LONDON), May 17, 2007, at 1.

13. There is also a biological analogy to be made along the lines of the movie *Outbreak*, in which a killer virus gets out of control and threatens an epidemic. To some extent, cyber attacks may similarly get out of the control of the cyber attacker. While the cyber attacks on Estonia were focused on specific areas, there is reason to be concerned that future attacks could trigger blanket internet outages that would in turn greatly disrupt internet usage around the world.

nation's economy and deprive much of its population of basic services, including electricity, water, sanitation, and even police and fire protection if the emergency bands similarly crashed.[14] This luckily did not happen in Estonia. Still, if such an attack did take place, it would constitute an "electronic Pearl Harbor" that would destroy most of a nation's information infrastructure, just as an electromagnetic pulse ("EMP") from a nuclear weapon causes destruction, dislocation and loss of life.[15] Ene Ergma, the Speaker of the Estonian Parliament who has a doctorate in nuclear physics, has made the comparison: "When I look at a nuclear explosion and the explosion that happened in our country in May, I see the same thing." As with nuclear radiation, cyberwar can destroy a modern state without drawing blood.[16]

Recognizing the scale of this threat, branches within the Russian government have publicly reserved the right to use nuclear weapons in response to IW. The Clinton and Bush Administrations have similarly likened the grave danger from IW to other conventional WMDs.[17] Yet, the international legal framework to deal with cyber attacks is severely underdeveloped. Whatever scholarly attention has been paid to the matter has mostly focused on cyber terrorism by private groups, rather than state-sponsored attacks.[18] Even though it is difficult to distinguish state-sponsored cyber terrorism from cyber attacks,[19] this article

14. *See, e.g.,* Alice Rivlin, *The Economy and the Internet: What Lies Ahead?*, BROOKINGS INSTITUTION (2008), http://www.brookings.edu/papers/2000/12technology_litan.aspx.

15. *Doomsday Fears of Terror Cyber-Attacks*, BBC NEWS, Oct. 11, 2001, http://news.bbc.co.uk/2/hi/science/nature/1593018.stm.

16. Kevin Poulsen, *'Cyberwar' and Estonia's Panic Attack*, WIRED, Aug. 22, 2007, http://blog.wired.com/27bstroke6/2007/08/cyber-war-and-e.html.

17. *See* To Develop Guidelines for Offensive Cyber-Warfare, NSPD-16 (July 2002), http://www.fas.org/irp/offdocs/nspd/index.html (classified); National Strategy to Combat Weapons of Mass Destruction, NSPD-17/HSPD (Sep. 14, 2002) http://www.whitehouse.gov/news/releases/2002/12/WMDStrategy.pdf; WHITE PAPER, THE CLINTON ADMINISTRATION'S POLICY ON CRITICAL INFRASTRUCTURE POLICY: PRESIDENTIAL DECISION DIRECTIVE 63 (May 22, 1998), http://www.fas.org/irp/offdocs/paper598.htm. The U.S., Britain, Germany, France and the Netherlands insist that a "first strike" nuclear option remains an "indispensable instrument" since there is "simply no realistic prospect of a nuclear-free world." Ian Traynor, *Pre-emptive Nuclear Strike a Key Option, Nato Told*, GUARDIAN (LONDON), Jan. 22, 2008, at 1.

18. *See e.g.,* Susan W. Brenner, *Toward a Criminal Law of Cyberspace: Distributed Security*, 10 B.U. J. SCI. & TECH. L. 1 (2004) (noting that the traditional model of law enforcement, with its reactive approach and hierarchical, military-style organization, cannot deal effectively with cybercrime). *See generally* Daniel M. Creekman, *A Helpless America? An Examination of the Legal Options Available to the United States in Response to Varying Types of Cyber-Attacks from China*, 17 AM. U. INT'L L. REV. 641 (2002) (noting the various ways in which the U.S. may respond to cyber terrorism emanating from China); Joginder S. Dhillon & Robert I. Smith, *Defensive Information Operations and Domestic Law: Limitations on Government Investigative Techniques*, 50 A.F. L. REV. 135 (2001) (discussing procedures in law enforcement of domestic information); Reuven Young, *Defining Terrorism: The Evolution of Terrorism as a Legal Concept in International Law and Its Influence on Definitions in Domestic Legislation*, 29 B.C. INT'L & COMP. L. REV. 23, 91, 100 (2006) (defining international terrorism by using cyber attacks as an example).

19. A good example of the difficulties in distinguishing terrorism sponsored by state from terrorism by private groups is the current flux in Iraq. There, the United States has accused Iran of

focuses on laying down a legal regime for the worst-case cyber attacks that rise to the level of an armed attack as these will likely have the most pronounced impact on both cyberspace and international security.

The difficulties in defining the boundaries of such a new legal regime test fundamental assumptions in international law regarding self-defense and the use of force. Only through an analysis of the available legal frameworks may a compromise position be synthesized that responds to the unique challenges posed by IW while preserving the integrity of Articles 2(4) and 51 in the U.N. Charter system that together provide the primary bulwark against the proliferation of violence in international relations.[20]

The technology-laden practice of modern IW, including responding to cyber attacks with armed force against information assets, raises a host of legal concerns. The first is whether cyber warfare represents a qualitative change in the meaning and nature of warfare. For example, attributing responsibility for a physical attack waged through conventional weapons is less difficult than establishing the origin of a cyber attack. As was the case in Estonia, digital invaders deliberately masked their origins by routing their attacks through remote locations. There are no flags or tanks in a cyber attack and the identity of the perpetrators is likely concealed.

Second, which laws of war are relevant to IW? And how do theoretical concerns surrounding sovereignty affect cyberspace? Can a cyber attack be a "use of force" as defined by Article 2(4) of the U.N. Charter?[21] If the answer to the final question is yes, would such an attack activate the Article 51 "right of self-defense"?[22] For example, even if Estonia could conclusively prove that Russia was behind the April 2007 attack, it is unsettled whether it could legally respond with force, cyber attacks, or other countermeasures pursuant to Article 2(4).

Third, how does international law generally, and international humanitarian law ("IHL") or international human rights law ("IHRL") specifically apply to limit cyber attacks, and what constitutes a "just" information war?[23] Responding on an *ad hoc* case-by-case basis is fraught with difficulties because existing treaties offer very little useful guidance. What level of civilian casualties is acceptable in a cyber attack, and should this be analyzed from an IHL or IHRL pa-

supplying Iraq insurgents, as foreign fighters continue to stream into the conflict zone. *See* Howard Cincotta, *Halt Flow of Arms and Foreign Fighters to Iraq, Rice Tells Iran*, BUREAU OF INT'L INFO. PROGRAMS, U.S. DEP'T OF STATE, Apr. 29, 2007,

http://www.globalsecurity.org/wmd/library/news/iraq/2007/04/iraq-070429-usia01.htm.

20. *See generally* Jeremy Carver, et al., *The Role of Article 50 of the UN Charter in the Search for International Peace and Security*, 49 INT'L & COMP. L. Q. 528 (2000).

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

22. U.N. Charter, art. 51.

23. Helen Stacy, Professor, Stanford Univ., International Humanitarian Law Issues, Remarks at the Meeting of the Committee on Policy Consequences and Legal/Ethical Implications of Offensive Information Warfare (Apr. 11, 2007).

radigm? How should the rubric for acts of IW change during times of conventional peace or armed conflict? Should responses to domestic versus foreign cyber attacks differ? What is the appropriate role of law enforcement in juxtaposition with the defense establishment? How are privacy concerns and other civil rights best balanced against national security interests? Together, these questions underscore the tension between classifying cyber attacks as merely criminal or as a matter of national security. This Article attempts to address each of these issues in kind.

The cyber attack on Estonia in April 2007 will be used as a case study throughout the Article.[24] It will illustrate that if IW is treated as a crime then the perpetrators would be subject to IHRL, while treating IW as a security threat would bring to bear IHL. There is a paucity of literature dealing with these issues as well as the ethical and human rights implications of IW on national security.[25] Treatments of IW outside the orthodox IHL framework are nearly nonexistent.[26] This is strange since both IHL and IHRL exist to protect the integrity of the human person, but take different approaches towards that end. IHL norms operate within the spatial and temporal constraints of an international armed conflict occurring between two or more states.[27] The body of law assumes that harm will occur, and seeks only to limit the extent of harm. In contrast, IHRL norms traditionally operate in peacetime during law enforcement investigations in which investigation is individual, and liability is criminal.[28] Reciprocity in the IHRL context, then, is far less important, whereas IHRL norms are continuous and the state is thus accountable through transparent processes. As a result of this confusion and overlap, it is currently unclear what legal rights a state has as a victim of a cyber attack.

IW's transnational reach suggests that while international legal norms found in the contemporary U.N. Charter law are helpful, the existing treaty framework is insufficient for solving this security dilemma since it takes for granted sovereign control and established state responsibility.[29] Two options

24. Notably, during the editing of this article, facts outlining the extent of the alleged Russian cyber attack on Georgia are coming to light, which would be a very useful comparative case study for follow-up research in this field.

25. As mentioned, existing studies focus on cyber terrorism. *See, e.g.,* Jonathan B. Wolf, *War Games Meets the Internet: Chasing 21st Century Cybercriminals With Old Laws and Little Money*, 28 AM. J. CRIM. L. 95 (2000); Debra Wong Yang et al., *Countering the Cyber-Crime Threat*, 43 AM. CRIM. L. REV. 201 (2006).

26. *See, e.g.,* Cpt. Robert G. Hanseman, *The Realities and Legalities of Inform The Realities and Legalities of Information Warfare*, 42 U.S.A.F. L. REV. 173 (1997).

27. Jefferson D. Reynolds, *Collateral Damage on the 21st Century Battlefield: Enemy Exploitation of the Law of Armed Conflict, and the Struggle for a Moral High Ground*, 56 A.F. L. REV. 1 (2005)

28. *See* Kenneth Watkin, *Controlling the Use of Force: A Role for Human Rights Norms in Contemporary Armed Conflict*, 98 AM. J. INT'L L. 1 (2004).

29. Christopher C. Joyner & Catherine Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework*, 12 EUR. J. INT'L L. 825, 865 (2001) (arguing that assessing

are available: create a new treaty system from whole cloth, or adapt current treaty regimes. This Article will advocate that the best way to ensure a comprehensive regime is a new international accord dealing exclusively with cyber security and its status in international law. The widespread, amorphous use and rapid evolution of the Internet challenges state sovereignty and makes international law slow to adapt. Part VI lays out a proposal for such an organization, which would include an international body with the power to regulate cyber security reminiscent of the United Nations Commission on the Limits of the Continental Shelf ("CLCS") under UNCLOS. In current practice, however, the United States and other advanced nations still oppose such a new treaty at this time.[30] Although the U.S. Senate recently ratified a European Convention on Cybercrime that now has 43 signatory nations, it exclusively deals with cybercrime, not state-sponsored cyber attacks.[31]

Thus, until such an accord focusing on state-sponsored cyber attacks becomes politically viable, it remains necessary to ascertain the extent to which existing treaty systems deal with cyber attacks. To that end this Article will draw on the most apt analogues in international law to form an appropriate legal regime to contain cyber attacks – whether it is humanitarian law (laws of war), human rights law (regulation of nation states behavior), or some novel combination of these bodies of law and other treaties.

As a corollary, this Article analyzes how existing international treaty systems apply to the investigation and prosecution of cyber attacks until a new regime is formed. In framing this regime, this Article argues that cyber attacks represent a threat to international peace and security that is potentially as daunting and horrific as nuclear war. Yet the nuclear non-proliferation model is not a useful analogy since the technology of IW—information networks—is already widespread in the international community. Therefore, this Article will consider other analogies including communications and cyber law, space law, and the law of the sea, among others, which could function together to both define inappropriate state conduct related to IW, and to provide the basis for a functioning regime. For instance, a cyber attack could potentially activate the following treaty and legal provisions: (1) Article 35 of the International Telecommunications Union that deals with government communications and safety services; (2) domestic cyber law, such as in the context of copyright infringement; (3) Articles 19 and 113 of UNCLOS if the defender nation was a coastal state; (4) applicable

self-defense responses to cyber attacks and the role of international institutions to attain these objectives need clear rules).

30. *See, e.g.*, Larry Downes, *Cybercrime Treaty: What it Means to You*, CIO INSIGHT, Mar. 6, 2007, http://www.cioinsight.com/c/a/Past-News/Cybercrime-Treaty-What-it-Means-to-You/. *See also* DEP'T OF DEFENSE, OFF. OF GEN. COUNS., AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS (2d ed., 1999) [hereinafter DOD, *Assessment*].

31. Council of Europe, Convention on Cybercrime, 41 I.L.M. 282 (2001), http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm [hereinafter Convention on Cybercrime].

Mutual Legal Assistance Treaties ("MLAT"s), extradition treaties, and Status of Forces Agreements ("SOFA"s); and (5) the potential for Chapter VII United Nations Security Council Resolutions.

But this regime remains imperfect. The main failing of existing international treaties that relate to cyber law is that most do not specify how armed conflict changes their applicability, or even suspends it entirely. Critically, many treaties also lack enforcement mechanisms such as mandatory reparations and sanctions in the event of breach. Regardless of whether or not cyber attacks fall below the threshold of an armed attack, these bodies of law do have a role to play in forming an appropriate regime. Meanwhile, the limitations of such a regime, created by analogy and the extension of principles developed to suit different challenges, demonstrates that the international community needs a new organization to cope with IW in the long term.

II.
DEFINING INFORMATION WARFARE AND THE THREAT OF CYBER ATTACKS

The recent cyber attack on Estonia has intensified international concern that hostile foreign governments could preemptively launch computer-based attacks on critical national or regional systems such as those supporting energy distribution, telecommunications, and financial services. As seen in Estonia, even small-scale exercises of IW have the potential to "severely damage or disrupt national defense or other vital social services and result in serious harm to the public welfare."[32] Modern Information Age societies rely so heavily upon networked systems and technology that substantial damage to a modern state's networked information infrastructure could paralyze its society or cause it to crash. The cataclysmic potential of cyber-based IW presents new international military implications and invites new analysis of how IW fits into the larger body of law on the use of force.[33]

Definitions and conceptions of IW are as numerous as they are complex, but generally entail preserving one's own information and information technology ("IT") while exploiting, disrupting, or denying the use of an adversary's. IW itself in general refers to a hostile attack by one hostile nation against the important IT systems and networks of another (as compared to a criminal or terrorist attack involving private parties). Second, IW refers to actions taken to defend IT systems and networks.[34] IW waged by terrorists,[35] or a hostile state,

32. Joyner & Lotrionte, *supra* note 29, at 858.

33. *Id.*

34. HERBERT LIN, NAT'L ACADS., POLICY CONSEQUENCES AND LEGAL/ETHICAL IMPLICATIONS OF OFFENSIVE INFORMATION OPERATIONS AND CYBER ATTACK (2007).

35. Similar to the difficulty involved in defining information warfare, terrorism too is a multifaceted concept. For this Article though, I refer to terrorism as non-state-sponsored attacks on civilians, perpetrated with the intent of spreading fear and intimidation. The goal of these attacks is to change perceptions on a high-impact basis in the vein of September 11, 2001. A more diffuse cam-

against any modern society replete with IT, such as the United States, is a matter of national concern. It is no secret that many critical sectors of contemporary economies as well as critical national infrastructure depend on IT systems and networks.[36]

IT today is ubiquitous and is essential to virtually the U.S.'s entire infrastructure including dams, nuclear power plants, air-traffic control, communications, and financial institutions.[37] Large and small companies alike rely on computers to manage payroll, track inventory and sales, and perform research and development. Every stage of the distribution of food and energy relies on IT. Western societies have spent years building this information infrastructure in ways that are interoperable, easy to access, and easy to use.[38] Yet this open philosophy is also the Achilles' heel of the system.

Protecting an information infrastructure is an even more difficult proposition than securing all of a nation's ports or power plants against unwanted intruders. To spot a cyber attacker from all the normal cross-border data flows would be like picking out a single person with more luggage than usual from the thousands of passengers that pass through JFK Airport daily. Alternatively, instead of a single person with more luggage, it would be like surveilling for more Polish citizens than usual. Even if they appeared Polish, it would still be unclear exactly why they are there, if they are really Polish, and what their intentions are. As computer systems become more prevalent, sophisticated, and interconnected, society is becoming increasingly vulnerable to poor system design, accidents, and cyber attacks. The global reach and interconnection of computer networks multiplies these system vulnerabilities.[39]

Consequently, there is a myriad of practical problems associated with both launching and defending against cyber attacks, including the fundamental issue of attribution and in particular state responsibility for cyber attacks. Even if it is technically possible to attribute an attack to a particular geographic region, determining whether it was a state, a group, or an individual at work is a difficult proposition especially given that even discriminate attacks easily become indiscriminate because the Internet is interconnected. This interconnection masks

paign designed to illicit widespread disruptions and loss of public confidence in the ability of government to function effectively is also high impact. COMPUTER SCI. & TELECOMM. BD., NAT'L RES. COUNCIL, INFORMATION TECHNOLOGY FOR COUNTERTERRORISM: IMMEDIATE ACTIONS AND FUTURE POSSIBILITIES (John L. Hennessy et al. eds., 2003).

36. *See id.*; COMPUTER SCI. & TELECOMM. BD., NAT'L RES COUNCIL, CYBERSECURITY TODAY AND TOMORROW: PAY NOW OR PAY LATER (2002) [hereinafter *Cybersecurity Today*].

37. IT has four major elements: (1) the Internet; (2) the conventional telecommunications infrastructure; (3) embedded/real-time computing; and (4) dedicated computing devices. Damage to IT has three forms: (a) network unavailable; (b) network corrupted (does not provide accurate results or information when one would normally expect); (c) network compromised (person has gained privileged information for malign purposes). *See generally Cybersecurity Today, supra* note 36.

38. Joyner & Lotrionte, *supra* note 29, at 865.

39. SYS. SECURITY STUDY COMM., NAT'L RES. COUNCIL, COMPUTERS AT RISK: SAFE COMPUTING IN THE INFORMATION AGE (1991).

reality, making even the identification of IP addresses an unreliable way in which to track true identities. The goods and ills of the Internet are bound together through billions of optic fibers. Therefore, the international community cannot treat any cyber attack in isolation. An attack on any node of the system is an attack on the system as a whole, and must be dealt with accordingly. This is especially difficult though given the heavy involvement in the Internet of the private sector and non-governmental organizations. In essence then, there are two interconnected questions to ascertain. First, there is a factual determination about how to pierce the IT veil to determine the true identity of the attacker. Second, there is a legal determination about the scope of an appropriate response to such an attack.

A. The U.S. Response to the Global Threat of Cyber Attacks

The President's Commission on Critical Infrastructure Protection highlighted the scale and importance of IW both as an offensive weapon and defensive quagmire: in 2002, 19 million individuals had the knowledge necessary to launch cyber attacks.[40] Modern technology has made the tools of IW cheap and handy.[41] Little specialized equipment is needed. The basic attack tools consist of a laptop, modem, telephone, and software – the same instruments commonly used by hackers, and by many modern professionals for that matter.[42] Interpol has estimated that there are as many as 30,000 websites that provided automated hacking tools and software downloads. In 1999, a total of 22,144 attacks were detected on Defense Department networks, up from 5,844 in 1998.[43] As of 2008, the Defense Department estimates more than three million attacks occur annually.[44] Worldwide aggregate damage from these attacks is now measured

40. PRESIDENT'S COMM'N ON CRITICAL INFRASTRUCTURE PROTECTION, CRITICAL FOUNDATIONS: PROTECTING AMERICA'S INFRASTRUCTURE 9 (1997), http://www.ihs.gov/misc/links_gateway/download.cfm?doc_id=327&app_dir_id=4&doc_file=PCCIP_Report.pdf.

41. The following is a list of common IW weapons: *Sniffer*–a program executed from a remote site by an intruder, which allows the intruder to retrieve user IDs and passwords or other information; *Trojan Horse*–a program remotely installed into the controlling switching centers of the Public Switched Network; *Trap Door*–a program used to gain unauthorized access into secured systems; *Logic bomb*–lies dormant and can be hidden within a Trojan Horse until a trigger condition causes it to activate and destroy the host computer's files; *Video-morphing*–makes broadcasts indistinguishable from normal transborder data flows; *Denial of service attack*–prevents networks from exchanging data; *Computer worm or virus*–travels from computer to computer across a hospitals network, damaging files; *Infoblockade*–blocks all electronic information from entering or leaving a state's borders; *Spamming* – floods military and civil email communications systems with frivolous messages, overloading servers and preventing field communications; *IP spoofing*–fabricates messages whereby an enemy masquerades as an authorized command authority. Joyner & Lotrionte, *supra* note 29, 836-39.

42. Joyner & Lotrionte, *supra* note 29, at 831.

43. Jim Wolf, *Hacking of Pentagon Persists*, WASH. POST, Aug. 9, 2000 at A23.

44. Pamela Hess, *Pentagon Puts Hold on USAF Cyber Effort*, ASSOCIATED PRESS, Aug. 13, 2008,

in billions of U.S. dollars annually.[45] Private ownership of much of the modern IT infrastructure complicates the problems of protecting vital networks because most governments play a limited role in regulating the Internet.[46] Consequently IW has great potential to spread asymmetric warfare.[47]

Regardless, the great powers are also developing IW to supplement their offensive capabilities. 120 nations have either already or are currently in the process of establishing IW competence, including Russia and China.[48] As revealed by at least one press report, a Presidential National Security Directive, NSPD 16, issued in July of 2002, directed the U.S. to examine potential cyber attacks against enemy computer networks.[49] The Department of Defense ("DOD") has acknowledged this as a possible instrument of national security policy.[50] PDD-63 calls for a national effort to ensure the security of increasingly vulnerable and interconnected infrastructures in the U.S., and creates the National Infrastructure Protection Center ("NIPC") under the Federal Bureau of Investigation.[51] Funding for intelligence and law enforcement efforts against cyber attacks has increased from $1.14 billion in 1998 to $2.03 billion in 2001.[52] However, plans for a cyberspace command center through the U.S. Air

http://www.boston.com/news/nation/washington/articles/2008/08/13/pentagon_puts_hold_on_usaf_cyber_effort/ (reporting that during the Georgian conflict "[t]he Russians just shot down the government command nets so they could cover their incursion….This was really one of the first aspects of a coordinated military action that had cyber as a lead force, instead of sending in air planes.").

45. ABRAHAM D. SOFAER ET AL., STANFORD UNIV. A PROPOSAL FOR AN INTERNATIONAL CONVENTION ON CYBER CRIME AND TERRORISM (2000), http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

46. *See generally* Dawn C. Nunziato, *The Death of the Public Forum in Cyberspace*, 20 BERKELEY TECH. L.J. 1115 (2005) (indicating percentage of private ownership of the internet).

47. The widespread private ownership of critical IT infrastructure is more common in the U.S. than in Europe, potentially leaving the U.S. even more vulnerable to a cyber attack. *See generally* ROBERT MILLWARD, PRIVATE AND PUBLIC ENTERPRISE IN EUROPE: ENERGY, TELECOMMUNICATIONS AND TRANSPORT, 1830–1990 (2005) (examining the role that private and public enterprise have played in the construction and operation of the railways, electricity, gas and water supply, tramways, coal, oil and natural gas industries, telegraph, telephone, computer networks and other modern telecommunications in Europe in the nineteenth and twentieth centuries). For a general discussion of asymmetric warfare, *see* Clinton J. Ancker III & Michael J. Burke, *Doctrine for Asymmetric Warfare*, 83 MIL. REV. 18, 18 (2003) (arguing that "[w]hile asymmetric warfare encompasses a wide scope of theory, experience, conjecture, and definition, the implicit premise is that asymmetric warfare deals with unknowns, with surprise in terms of ends, ways, and means. The more dissimilar the opponent, the more difficult it is to anticipate his actions.").

48. Joyner & Lotrionte, *supra* note 29, at 831.

49. Bradley Graham, *Bush Orders Guidelines for Cyber-Warfare*, WASH. POST, Feb. 7, 2003 at A1.

50. *See generally* DOD, *Assessment, supra* note 30.

51. Joyner & Lotrionte, *supra* note 29. *See generally* Presidential Decision Directive, NSC-63 (May 22, 1998), http://www.american.edu/radiowave/CII%20SITE/pdd63.pdf (setting up a new organization for U.S. government cyber security and putting forward new guidelines for critical infrastructure protection).

52. Anthony H. Cordesman, *Defending America – Redefining the Conceptual Borders of Homeland Defense*, CSIS PUBLICATIONS, Feb. 14, 2001. However, more recently the DOD has consi-

Force continue to be in flux with funding in jeopardy.[53]

Among its numerous applications, IT has a major role to play in the prevention, detection, and mitigation of cyber attacks. The preeminence of IT infrastructure in the U.S. is both a target and a weapon. Counterterrorist IW thus seeks to reduce the probability and scope of attacks against valued IT targets.[54] A passive defense against IW will not work. Cyber attackers given enough free attempts will identify and exploit any system vulnerabilities since even a single vulnerability given enough "free" attempts will compromise the system.[55] Current passive defensive information technologies are inadequate for determining and countering an enemy's assets.[56] Therefore, an active defense in which the attacker is forced to pay a price for targeting a system is paramount.

Does such a philosophy of active defense, however, justify self-defense against cyber attacks – and if so, to what extent, and in which cases? Modern IW raises a huge variety of practical and legal concerns that are highlighted by analyzing the Estonian cyber attack.

III.
FROM RUSSIA WITH LOVE?: THE CYBER ATTACK ON ESTONIA

The Estonian public and private sectors were the subject of a prolonged IW campaign beginning on April 27, 2007 and running for a period of several weeks.[57] The primary weapon deployed against the state included "distributed

dered curtailing or cutting outright its cyberspace defense force due to budgetary constraints. *See* Hess, *supra* note 44.

53. *See, e.g.*, John Andrew Prime, *Cyber, Nuclear Missions Shift in Air Force*, SHREVEPORT TIMES, Oct. 9, 2008,

http://www.shreveporttimes.com/apps/pbcs.dll/article?AID=/20081009/NEWS01/810090332/1060 (noting that the Air Force has modified plans to stand up a separate Cyber Command, instead concentrating existing cyber units under a numbered air force).

54. An IT attack primarily takes three forms: (1) an attack can come in through the wires (virus or Trojan horse) or as a denial of service attack; (2) some IT element may be physically destroyed (critical data center blown up) or compromised (IT hardware modified); and (3) a trusted insider may be compromised. *See* Hess, *supra* note 44.

55. Lin, *supra* note 34.

56. *Id.*

56. Frank Vizard, *War.com: A Hacker Attack Against NATO Uncovers a Secret War in Cyberspace*, 255 POP. SCI. 80 (1999).

57. The attacks on Estonia proceeded as follows: On April 26-27, the day of the government's decision to relocate a disputed Soviet-era statue, a flood of junk messages hit the web sites of Parliament, the President and the Prime Minister and the sites crashed. On April 30, several daily newspaper websites were brought down and a high-level meeting took place with plans to protect vital services such as online banking. On May 2, Internet service providers from around the world succeeded in blocking most of the incoming malicious data. On May 5, the Estonian government announced that the attacks originated in Russia. On Victory Day in Russia, May 9, botnet attacks began and shut down Estonia's largest bank's online portal, leading to losses of more than one million dollars. In one case, the attackers sent a single huge burst of data to gauge the capacity of the network. Then, hours later, data from multiple sources flowed into the system, rapidly reaching the

denial of service" ("DDOS") attacks, which aim to crash a target site by bombarding it with bogus requests for information.[58] Data from Arbor Networks Active Threat Level Analysis System shows that there were at least 128 unique DDOS attacks targeting Internet protocols within Estonia during this period.[59] Internet traffic increased from 20,000 packets to more than 4 million packets per second.[60] The attacks lasted from anywhere between one to 10 hours, and originated from a diversity of countries such as Egypt, Peru, and Russia.

DDOS attacks are relatively commonplace – the cyber attack on Estonia is not the first time that such an attack has been used against a country. The "Apolo Ohno" controversy at the 2002 Salt Lake City Olympics resulted in attacks on several U.S.-based servers from machines that appeared to be based in South Korea.[61] Another episode involved the so-called "Titan Rain" series of cyber attacks on U.S. computer systems ongoing since 2003. According to the SANS Institute, a computer security training company, these attacks seemed to come from China and were the results of military hackers trying to garner information on U.S. defense systems.[62] In the 1998 "Solar Sunrise" attack, computers based in the United Arab Emirates managed to breach the DOD's security shield.[63] Yet it was not the UAE behind the attacks, but an Israeli teenager and two high school students from Cloverdale, California, who took advantage of the global integration of the Internet to hide their origin.[64] During the Kosovo Crisis, three

upper limit of the routers. May 18 saw the last major wave of attacks, though small-scale assaults continued for several weeks. Mark Landler & John Markoff, *Digital Fears Emerge after Data Siege in Estonia*, N. Y. TIMES, May 29, 2007, at A1.

58. *A Cyber Riot: Estonia and Russia*, ECONOMIST, May 12, 2007. DDOS attacks are also increasingly being used for extortion, in which a cyber attacker begins an attack and does not stop until the website owner pays "protection" money. *See* Susan Brenner, *At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare*, 97 J. CRIM. L. & CRIMINOLOGY 379, 384-86 (2007).

59. Sean Kerner, *Estonia Under Russian Cyber Attack?*, SECURITY, May 18, 2007.

60. A packet is the unit of data that is routed between an origin and a destination on the Internet. When any file is sent on the Internet, the Transmission Control Protocol (TCP) layer of TCP/IP (Internet Protocol) divides the file into "packets" of an efficient size for routing. Each of these packets is separately numbered and includes the Internet address of the destination. The individual packets for a given file may travel different routes through the Internet. When they have all arrived, they are reassembled into the original file. SearchNetworking.com, Definitions—"Packet,"

http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212736,00.html, (last visited Apr. 18, 2008).

61. In 2002 at the Salt Lake City Games, American Apolo Ohno won the gold medal in the 1,500-meter speed-skating race after South Korean Kim Dong-Sung was disqualified; soon after, several U.S.-based servers were hit with a DDOS. Robert Vamosi, *Cyberattack in Estonia – What It Really Means*, CNET NEWS, May 29, 2007, http://news.cnet.com/Cyberattack-in-Estonia--what-it-really-means/2008-7349_3-6186751.html?tag=mncol.

62. Bradley Graham, *Hackers Attack Via Chinese Web Sites,* WASH. POST, Aug. 25, 2005, at A1.

63. *See, e.g.*, Joyner & Lotrionte, *supra* note 29, at 839.

64. Solar Sunrise was a series of attacks on unclassified Department of Defense computer networks, which occurred between February 1 and February 26, 1998. The attack pattern, which exploited a well-known operating system vulnerability, suggested that the attacks were actually the

days after NATO bombings on March 30, 1999, hackers initiated a coordinated program to disrupt NATO's email communications system by overloading it. The conflict also saw numerous U.S. state-sponsored efforts to disrupt Milosevic's command and control.[65] Later the "Moonlight Maze" attacks of 2001 became the most extensive computer attack aimed at the U.S. government to that point. Allegedly, state-sponsored Russian hackers penetrated DOD computers for more than a year to secure technology from U.S. agencies such as the DOE and NASA, as well as from military contractors and universities.[66] But no country has ever before experienced a cyber attack on the scale of the 2007 assault on Estonia.

A. Timeline of the Cyber Attack on Estonia

Against the backdrop of the cyber attack on Estonia is a greater conflict between Estonia and Russia over the Soviet heritage in the former's capital, Tallinn.[67] Thousands of ethnic Russians in Estonia rioted over the removal of what they viewed as a cherished monument to wartime sacrifice.[68] The majority of Estonians, in contrast, viewed the statute as a symbol of a hated foreign occupation.[69] The removal of the monument infuriated even Russians outside Estonia. In Moscow, a Kremlin-youth movement surrounded and attacked the Estonian embassy prompting protests from the U.S., NATO, and the E.U.[70] The main group behind the protests in Russia is the government-funded pro-Kremlin "Nashi su" ("Youth Movement, Ours!"), which was created in 2005 as an anti-

precursor to an attack on the DII. The attackers followed the same attack profile: (a) probed to determine if the vulnerability exists, (b) exploited the vulnerability, (c) implanted a program (sniffer) to gather data, and (d) returned later to retrieve the collected data. At least eleven attacks followed the same profile on Air Force, Navy, and Marine Corps computers worldwide. Attacks were widespread and appeared to come from sites such as: Israel, the United Arab Emirates (UAE), France, Taiwan, and Germany. *See* JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 37-45 (2008); Porter Goss, *An Introduction to the Impact of Information Technology on National Security*, 9 DUKE J. COMP. & INT'L L. 391, 396 (1999); *see also* Solar Sunrise, GLOBALSECURITY.ORG, http://www.globalsecurity.org/military/ops/solar-sunrise.htm (last visited Nov. 4, 2008).

65. *See generally* ANTHONY H. CORDESMAN & JUSTIN G. CORDESMAN, CYBER-THREATS, INFORMATION WARFARE, AND CRITICAL INFRASTRUCTURE (2002).

66. Elinor Abreu, *Epic Cyberattack Reveals Cracks in U.S. Defense*, CNN, May 10, 2001, http://archives.cnn.com/2001/TECH/internet/05/10/3.year.cyberattack.idg/. *See also* Joyner & Lotrionte, *supra* note 29; *Cyber Attack!*, BBC NEWS, July 3, 2000,

http://news.bbc.co.uk/1/hi/programmes/panorama/archive/817114.stm.

67. The Soviets had built the monument in 1947 to commemorate their war dead after driving the Nazis out of the region at the end of World War II. *See* ECONOMIST, *Estonia and Slovenia, supra* note 6.

68. ECONOMIST, *Cyber Riot*, *supra* note 58.

69. *Id.*

70. U.S. House Passes Resolution Supporting Estonia, ESTONIAN AM. NAT'L COUNCIL, June 6, 2007, http://www.estosite.org/home/?p=19 (noting that Estonia was forced to close its embassy in Moscow briefly after pro-Kremlin youth groups staged raucous protests).

fascist student group that has since grown to more than 100,000 members.[71] Feeling the Western pressure and following a deal brokered by Germany, the blockade soon ended.[72] Even though the embassy battle was lost, the Internet war, which may have involved Nashi su, was just beginning.

The IW campaign against Estonia took on many forms. Some involved defacing Estonian websites, including replacing web pages and links with Russian propaganda. Most attacks, however, concentrated on shutting the sites down outright.[73] By May 9, 2007, when Russia and its allies commemorated the defeat of Nazi Germany in Red Square, at least six Estonian state websites were brought down. These included the foreign and justice ministries, as well as Estonian organizations, newspapers, and broadcasters.[74] The main news outlet was forced to sever its international Internet connections to stay online, effectively gagging the Estonian news services from telling the world about the attack on their country.[75] The attack also targeted "mission-critical computers," including those used in telephone exchanges.[76] Estonia was very near a complete digital collapse on May 10 that would have shut off many vital services and caused massive, widespread social disruptions.[77] Luckily, Estonia's Cyber Emergency Response Team ("ECERT") prevailed and Estonia avoided the worst-case scenario that many feared all too likely.[78] The Estonian Defense Minister, Jaak Aaviksoo, has argued that the cyber attacks amounted to a national security emergency likening the situation to a complete blockade, or an "infoblockade."[79] "This may well turn out to be a watershed in terms of widespread awareness of the vulnerability of modern society," said Linton Wells II after the attack, the principal Deputy Assistant Secretary of Defense for networks and information integration at the Pentagon.[80] But who was to blame,

71. It is commonly thought that the group was formed as a reaction to the student protests leading to Ukraine's Orange Revolution in 2004. Nashi Su, Official Website, http://nashi.su/ (last visited Apr. 18, 2008). *See also* Cathy Young, *Putin's Young 'Brownshirts'*, BOSTON GLOBE, Aug. 10, 2007,

http://www.boston.com/news/globe/editorial_opinion/oped/articles/2007/08/10/putins_young_brownshirts/?page=2; *Nashi: The Kremlin's Little Helpers*, NEARABROAD, Aug 1, 2007,

http://nearabroad.wordpress.com/2007/08/01/nashi-the-kremlins-little-helpers/.

72. ECONOMIST, *Cyber Riot*, *supra* note 58.

73. *Id.*

74. *Id.*

75. Davis, *supra* note 1.

76. *See* Jeffrey Kelsey, *Hacking into International Humanitarian Law: the Principles of Distinction and Neutrality in the Age of Cyber Warfare*, 106 MICH. L. REV. 1427, 1429 (2008).

77. Davis, *supra* note 1.

78. *Id.*

79. *Estonia Has No Evidence of Kremlin Involvement in Cyber Attacks*, RIA NOVOSTI (RUSSIAN NEWS & INFORMATION AGENCY), June 9, 2007,

http://en.rian.ru/world/20070906/76959190.html.

80. Landler & Markoff, *supra* note 57. *See also* Shaun Waterman, *Who Cyber Smacked Estonia*, UNITED PRESS INT'L, Jun. 11, 2007,

and what can or should be done about it?

B. Determining Responsibility for the Cyber Attack on Estonia

Determining the perpetrator for this cyber attack is the murkiest problem facing authorities in the aftermath of the Estonian assault. Estonian officials claim to have proof that some of the earliest salvoes originated from Russian government computing centers, or affiliated centers run by Nashi su and other similar organizations.[81] Yet it is exceedingly difficult to prove from where these attacks originated. Thousands of attacks came from untraceable private computers around the world.[82] Most of them were "script kiddies," who were goaded into attacking Estonian websites in Russian-language chat rooms, which posted detailed instructions on how to launch botnet attacks.[83] This is the equivalent of an army recruitment pitch complete with marching orders.[84] The ground troops were individuals using ping attacks; the air force was botnets; and the Special Forces were hackers using DDOS attacks.[85] An impromptu small number of savvy and well-connected Internet operators led by Hillar Aarelaid, the head of ECERT, fended off the worst of the attacks even as Vladimir Putin was proclaiming during a parade of 7,000 Russian troops in Red Square that: "Those who are trying today to ... desecrate memorials to war heroes are insulting their own people, sowing discord and new distrust between states and peoples."[86] The same chat room incitement has also played out in the recent conflict between Georgia and Russia.[87]

The Russian government has offered no cooperation to Estonia in tracking

http://www.spacedaily.com/reports/Who_Cyber_Smacked_Estonia_999.html.

81. Davis, *supra* note 1.

82. *Id.*

83. *See* Landler & Markoff, *supra* note 57; *see also* Evan Cooke, The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets, SRUTI 05 Technical Paper, Univ. of Mich. (2005), http://www.usenix.org/events/sruti05/tech/full_papers/cooke/cooke_html/ ("At the center of these threats is a large pool of compromised hosts sitting in homes, schools, businesses, and governments around the world. These systems are infected with a bot that communicates with a botcontroller and other bots to form... a zombie army or botnet.").

84. Davis, *supra* note 1.

85. *Id.*

86. This was not the first time that Russia had been accused of orchestrating IW. In fact, just prior to the Estonian attacks, a similar assault had been launched against an alliance of Russian opposition parties led by chess grandmaster Garry Kasparov. The attacks were designed to crash the opposition websites. With his site down, Kasparov had difficulty informing his followers, and was arrested for leading an illegal rally. *Id.*

87. *See* Brian Krebs, *Report: Russian Hacker Forums Fueled Georgia Cyber Attacks*, WASH. POST, Oct. 16, 2008,

http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html (discussing Russian officials' plausible connivance at the online assault on Georgia and the internet activities that led up to the assault).

down the true source of these botnets.[88] In many ways, the Internet is the perfect platform for plausible deniability. Estonia has opened criminal investigations into the attacks under felonies of computer sabotage, which led to the arrest of a teenager of Russian origin.[89] Since many alleged hackers were Russian, Estonia submitted a request for bilateral investigation under the Mutual Legal Assistance Treaty ("MLAT") between Estonia and Russia.[90] Despite earlier promises of assistance though, the Russian Supreme Procurature refused assistance to Estonia under the treaty.[91] Ultimately, the only conviction from the cyber attack was on January 24, 2008 when an ethnic Russian student living in Tallinn was found guilty of launching an assault on the Reform Party's website of Prime Minister Andrus Ansip and posting a fake letter of apology for removing the symbolic Soviet statue. He was fined $1,642.[92]

A month after the attacks, assessments conducted by the U.S. government and several private sector contractors determined that the cyber attacks were most likely carried out by politically motivated hacker gangs (such as Nashi su), not by Russian security agencies directly.[93] In the report, Mike Witt, Deputy Director of the U.S. Cyber Emergency Response Team ("USCERT"), an element within the Department of Homeland Security that "coordinates defense against and responses to cyber attacks across the nation,"[94] surmised that botnets utilizing slave computers known as "zombies" had been operated by unknowing individuals – many of these zombies had in fact originated in the U.S.[95] Witt concluded that the attacks against Estonia lacked the sophistication of the major powers. In this instance, USCERT worked with the Forum of Incident Response and Security Teams to coordinate the global response to the attacks.[96] In contrast, a Russian hacker SpORaw believes that the most efficient online attacks on Estonia could not have been carried out without the blessing of

88. BBC NEWS, *Estonia Hit, supra* note 5.

89. Konstantin Kornakov, *Estonia Arrests First Hacker over Cyberattacks*, VIRUSLIST, May 8, 2007, http://www.viruslist.com/en/news?id=208274078.

90. *Russia Refused Legal Assistance in Cyber Attacks Investigation*, 17 EST.REV. 3, 4 (2007), http://www.estonia.com.au/pics/er_27.pdf.

91. This episode demonstrates the weaknesses of MLATs given that such agreements lack mandatory enforcement mechanisms. A future international accord for cyber security would need to incorporate compulsory reparations for proven breaches of the agreement.

92. Jeremy Kirk, *Student Fined for Attack against Estonian Website*, IDG NEWS SERVICE, Jan. 24, 2008, http://www.infoworld.com/article/08/01/24/Student-fined-for-attack-against-Estonian-Web-site_1.html (reporting that a 20-year-old Estonian student has been fined 1,642 dollars for launching a cyber attack that crippled the websites of banks, schools, and government agencies). *See also* Kornakov, *supra* note 89; and Landler & Markoff, *supra* note 57.

93. Waterman, *supra* note 80.

94. United States Computer Emergency Readiness Team (US-CERT), About Us, http://www.us-cert.gov/aboutus.html (last visited Jan. 1, 2008).

95. Waterman, *supra* note 80.

96. *Id*.

the Russian authorities.[97] He and others have argued that the hackers apparently acted under "recommendations" from parties in higher positions, as demonstrated with the chat room postings[98] and by the fact that on at least one Estonian site attackers replaced the homepage with the phrase "Hacked from Russian hackers."[99]

It is not the goal of this article to determine whether the cyber attacks on Estonia were state sponsored. Rather, these attacks serve as a means to highlight the issues for considering how best to form a legal regime to deal with cyber attacks going forward, including the most recent alleged cyber attacks on Georgia as part of the Russian-Georgian international armed conflict.[100] These raise serious questions of state responsibility and attribution that will be addressed in Part V.

C. The Reaction of the U.S. and NATO to the Cyber Attack on Estonia

What was a near disastrous attack for Estonia has met ambivalence from U.S. officials. The former chief scientist of the Defense Advanced Research Project Agency ("DARPA") characterized the incident as "more of a cyber riot than a military attack."[101] The U.S. nonetheless is concerned about cyber attacks generally. Since it makes little sense for an opponent to challenge the U.S. military might head on, likelier avenues of challenge are asymmetric ones that exploit potential U.S. vulnerabilities, such as the civilian information infrastructure.[102] Defense assessments have laid out numerous challenges including interoperability, information systems security, and the culture of the intelligence community itself.[103] Information system protection lags behind usage.[104] To develop and deploy effective defenses in cyberspace would take more time than that which is necessary to develop and mount an attack due to the rate at which

97. Davis, *supra* note 1.

98. Landler & Markoff, *supra* note 57.

99. Davis, *supra* note 1. Of course, such statements could just as easily have been posted by unaffiliated hackers trying to conspicuously frame Russia for the cyber attack on Estonia. The ambiguity apparent in this situation underscores the problems of attribution and state responsibility inherent in IW.

100. John Leyden, *Russian Cybercrooks Turn on Georgia*, REGISTER, Aug. 11, 2008, http://www.theregister.co.uk/2008/08/11/georgia_ddos_attack_reloaded/.

101. This distinction based on the IW capabilities of governments underscores the danger of anticipatory self-defense and a reactive legal regime to deal with cyber attacks. *See* Waterman, *supra* note 80.

102. Steven Lambakis et al., NAT'L INST. FOR PUB. POL'Y, UNDERSTANDING 'ASYMMETRIC' THREATS TO THE UNITED STATES (2002),

http://www.missilethreat.com/repository/doclib/20021000-NIPP-asymmetricthreats.pdf (defining asymmetric threats as different and challenging threats mired in legal and political constraints and vulnerabilities that are designed to offset U.S. strengths).

103. DOD, *Assessment, supra* note 30.

104. Joyner & Lotrionte, *supra* note 29, at 832.

new hacking tools come online.[105] At the same time, law and national policy prohibits the DOD from retaliating against cyber attacks if the goal was not the deterrence of future attacks.[106] This gap is growing wider, especially now that the burgeoning U.S. Air Force Cyberspace Command is facing delays and potential cuts.[107] In other words, a cyber attack is far easier to orchestrate than cyber defense. The U.S., like Estonia and all countries and institutions in the Information Age, is right to be concerned about the continuing proliferation of these attacks. This is true across a broad range of actors from small NGOs to national defense departments, given the small, mobile actors at work that can crash a government website[108] almost as easily they can crash a nuclear power plant operating system.[109]

In deciding how Estonia and NATO ought to respond to these cyber attacks the search for analogies is paramount since cyber attacks are an unprecedented new way to make war. Some have contended that the cyber attacks, to the extent that they were incited by Russia, amount to a test for NATO on its defenses to IW.[110] If this is the case, then NATO failed. NATO members dispatched specialists to Tallinn, but did not or could not have done much else given that so much of the Internet is run by the private sector and international organizations.[111] Recently, more signs within NATO indicate that this mindset is now changing. On June 14, 2007, NATO defense ministers held a meeting issuing a joint communiqué that includes the placement of a newly planned NATO Cybernetic Defense Center in Estonia.[112] Other proposals include the development of redundant networks of backup servers.[113] Dealing with cyber attacks has never been in NATO's mandate, but the increasing number and scale of cyber attacks could convince NATO to integrate them into its mission. This is especially true as Rein Lang, Estonia's justice minister, has complained that "international law is of little help" in dealing with cyber attacks.[114]

105. James Adams, *Virtual Defense*, 80 FOREIGN AFF. 98, 104-06 (2001).

106. DOD, *Assessment, supra* note 30.

107. *See* Prime, *supra* note 53.

108. Editorial, *War, Redefined*, L.A. TIMES, Aug. 17, 2008, at A25.

109. *See* Greg Bruno, *The Evolution of Cyber Warfare*, COUNCIL ON FOREIGN REL., Feb. 27, 2008, http://www.cfr.org/publication/15577/evolution_of_cyber_warfare.html.

110. Davis, *supra* note 1.

111. *See generally* Gary Peach & Paul Ames, *Stung by Cyber Warfare, Estonia, NATO Allies to Sign Deal on Cyber Defense Center*, ASSOCIATED PRESS, Mar. 13, 2008, http://www.iht.com/articles/ap/2008/05/13/europe/EU-GEN-Estonia-NATO-Cyberterrorism.php.

112. ECONOMIST, *Cyber Riot, supra* note 58.

113. Peach & Ames, *supra* note 111.

114. *Id.*

IV.
SOVEREIGNTY OVER THE INFORMATION COMMONS

Before an international legal regime can be developed to deal with cyber attacks, the theoretical justifications for regulating cyberspace need to be considered.[115] Two options exist. First, the international community could agree that cyberspace is an arena over which nations can and should exercise sovereignty through the effects doctrine.[116] Second, the international community could treat cyberspace as an information commons over which no state may claim jurisdiction.[117] The former interpretation provides a firm legal grounding on which an international regime could be built. The latter understanding is inimical to the concept of the commons itself, but a compromise position may be found by examining the Common Heritage of Mankind ("CHM") principle.

A. Option 1: Regulating Cyberspace through the Effects Principle

The general principle of sovereignty—that territorial integrity be upheld and a state maintain its monopoly on coercive violence—is fundamental to international law and relations, but does not apply as directly to IT.[118] The principle would seem to hinder the regulation of cyberspace. As a practical matter, however, concerns over sovereignty should not forestall international action on cyber attacks. It is well established in international law that the effects principle permits the regulation of activities that impact upon a state's territory. The Third Restatement of Foreign Relations Law, for example, states that international law recognizes that a nation may provide for rules of law with respect to "conduct outside its territory that has or is intended to have substantial effect within its territory."[119]

115. Six pillars that have traditionally upheld the autonomous state system are: a cost/benefit ratio for the use of force, low physical externalities, low-levels of economic interdependence, low information flows, a predominance of authoritarian government limiting information flows, and a high degree of cultural, political, and economic heterogeneity. Mark W. Zacher, *The Decaying Pillars of the Westphalian Temple: Implications for International Order and Governance*, GOVERNANCE WITHOUT GOVERNMENT: ORDER AND CHANGE IN WORLD POLITICS 58-101 (James N. Rosenau & Ernst-Otto Czempiel eds., 1992).

116. *See* 22 U.S.C. § 6081(9) (2000). *Cf.* RESTATEMENT (THIRD) OF FOREIGN RELATIONS §402(1)(c) (1987).

117. *See e.g.*, James Boyle, *The Second Enclosure Movement and the Construction of the Public Domain*, 66 LAW & CONTEMP. PROBS. 33 (2003); Lawrence Lessig, *The Architecture of Innovation*, 51 DUKE L.J. 1783 (2002); Eben Moglen, *Freeing the Mind: Free Software and the Death of Proprietary Culture*, 56 ME. L. REV. 1 (2004).

118. For a discussion of the evolution of sovereignty, see S. A. Korff, *The Problem of Sovereignty*, 17 AM. POL. SCI. REV. 404, (1923); John Jackson, *Sovereignty-Modern: A New Approach to an Outdated Concept*, 97 AM. J. INT'L L 782, 785 (2003); W. Michael Reisman, *Sovereignty and Human Rights in Contemporary International Law*, 84 AM. J. INT'L L. 866 (1990).

119. 22 U.S.C. § 6081(9). *See also* RESTATEMENT (THIRD) OF FOREIGN RELATIONS § 402(1)(c) (1987).

On the other hand, cyberspace is not a customary arena over which states may exercise such control. Some have argued that cyberspace is an international commons akin to other commons territories. These traditional areas of the international commons include the deep seabed under the U.N. Convention on the Law of the Sea ("UNCLOS"), the Antarctic Treaty System ("ATS"), and outer space under the 1967 U.N. Outer Space Treaty.[120] Together, these regions constitute the sole exceptions to the system of Westphalian sovereignty that has long dominated international relations.[121] In the international commons, all of humanity is the sovereign under the CHM principle.[122] To the extent that cyberspace is a commons, it is one facing unique challenges and thus requiring exceptional regulatory solutions.[123]

B. Option 2: Regulating the Information Commons through the Common Heritage of Mankind

Scholars or policymakers have yet to agree on a comprehensive understanding of the CHM, but drawing from the available literature a working definition would likely comprise five main elements.[124] First, there can be no private or public appropriation; no one legally owns common heritage spaces.[125] As applied to cyberspace, this means that although computer networks owned by the private and public sectors provide the infrastructure for the information superhighway, they cannot actually own the data packets (the cars) on the Internet. Thus, the various government institutions and telecommunications firms that issue Internet protocol (IP) addresses within their countries do in a sense own Internet access, but not the Internet itself. Second, representatives from all nations must work together to manage resources since a commons belongs to all.[126] As

120. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, Jan. 27, 1967, 18 U.S.T. 2410, 610 UNTS 205 [hereinafter "Outer Space Treaty]."

121. Although criticized, Westphalian territorial sovereignty remains central to both international relations and law, and as such it has a role in finding international solutions to cyber attacks. The state's power is linked to the people and resources found within a set of boundaries, though not necessarily geographic ones. As U.S. Ambassador Richard Haass has said, "At the beginning of the twenty-first century, sovereignty remains an essential foundation for peace, democracy, and prosperity." Jackson, *supra* note 118, at 789. Rulers and political regimes of all kind have claimed to enjoy the benefit of sovereignty, the fundamental characteristic of authority on which the modern polity of state stands. *Id.* at 780.

122. *See* Jennifer Frakes, *Notes and Comments: The Common Heritage of Mankind Principle and the Deep Seabed, Outer Space, and Antarctica*, 21 WIS. INT'L L.J. 409, 426 (2003).

123. Anupam Chander & Madhavi Sunder, *The Romance of the Public Domain*, 92 CALIF. L. REV. 1331, 1331 (2004) (tracing the shift from land to information in property debates and explaining the underlying belief that "because a resource is open to all by force of law, it will indeed be equally exploited by all").

124. *See* Frakes, *supra* note 122, at 411-13.

125. *See id.* at 411.

126. *See id.* at 412.

collective management is unfeasible, a special agency must be set up to coordinate shared management to administer commons spaces.[127] The closest cyber analogue to such an organization is the Internet Corporation for Assigned Names and Numbers (ICANN), which is a non-profit international organization that sells domain names and keeps track of data routing for the system.[128]

Third, all nations must actively share in the benefits acquired from exploitation of the resources from the commons heritage region.[129] This aspect could arguably be fulfilled through the non-profit characteristic of the current system. Fourth, there can be no weaponry or military installations established in commons areas.[130] Cyber warfare, however, is already occurring to some degree in cyberspace -- all the more need for an international accord to limit such practices as much as possible. Finally, the commons should be preserved for the benefit of future generations,[131] and to avoid a "tragedy of the commons" scenario.[132] ICANN is taking steps to ensure the continued efficient functioning of cyberspace in the face of exponential expansion through the growth of services through Web 2.0 IP schemes.[133] Without continued new initiatives, excessive streams of data could lead to a tragedy of the commons scenario in which data would have to be prioritized and "junk data" would be deemed a form of environmental pollution.

Derived from the Greek *cyber* ("governor"), cyberspace "couples the idea of communication and control with *space*, a domain previously unknown and unoccupied, where 'territory' can be claimed, controlled, and exploited."[134] However, unlike the physical world, cyberspace is an abstract reality of ideas, information, and logic. A cyber attacker entering this domain can shed ties of citizenship and cross sovereign boundaries without a trace, anonymously masquerading as a real or fictitious entity.[135] Exactly which physical locations a

127. *See id* at 413.

128. *See* Internet Corporation for Assigned Names and Numbers (ICANN), Homepage, http://www.icann.org/tr/english.html (last visited Sep. 7, 2008).

129. *See* Frakes, *supra* note 122, at 412-13.

130. *Id.* at 413.

131. *Id.*

132. *See generally* Garrett Hardin, *The Tragedy of the Commons*, 162 SCIENCE 1243 (1968).

133. *See generally* Tim O'Reilly, *What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software*, 1 COMM. & STRATEGIES 17 (2007) ("Web 2.0 is the network as platform, spanning all connected devices; Web 2.0 applications are those that make the most of the intrinsic advantages of that platform: delivering software as a continually-updated service that gets better the more people use it, consuming and remixing data from multiple sources, including individual users, while providing their own data and services in a form that allows remixing by others, creating network effects through an architecture of participation, and going beyond the page metaphor of Web 1.0 to deliver rich user experiences.").

134. Stephen J. Lukasik, *Protecting the Global Information Commons*, 24 TELECOMM. POL'Y 519, 525 (2000) (arguing that if Internet-based information infrastructures are to continue to provide important services, and if they are not to be limited by their misuse, the protection of the information commons must become a central issue for its users).

135. *Id.* at 525.

virtual entity traversed defy later detection. There are no physical wires or devices that can be easily identified as the "circuit" carrying a particular cyber transaction (though submarine cables may provide a useful analogue), and in fact current information systems are designed to have as many alternates and redundancies as possible to enhance reliably.[136] Though hardware is physically rooted in sovereign jurisdictions, the information contained in these systems and the software that controls them is not. An attacker is not physically present at the attack, except in the form of anonymous, invisible radio waves or electrons.[137] As cyberspace is increasingly being used to harm sovereign interests through offensive cyber weapons, the effects principle dictates that cyber security should "become an element of national strategy and a matter for political negotiation between sovereign entities."[138]

Yet even if sovereignty can be established over portions of the information commons through international negotiations,[139] it is very difficult to attribute a particular computer network attack ("CNA") to a foreign state although the effects principle permits a state to do so for the reasons outlined above. Article 2(4) of the U.N. Charter limits its definition of uses of force to a specific territory. A breach of territorial integrity then signifies some threat to a pristine condition.[140] Cyberspace does not easily fit within this classical interpretation. Use of a nation's communications networks as a conduit for an electronic attack is not as obvious a violation of its sovereignty as would be a flight through its airspace.[141] In other words, cyberspace has eroded the connection between territory and sovereignty. In a networked world, "no island is an island"–threats to social order are no longer easily identifiable as either internal (crime/terrorism) or external (war).[142] It is also unclear whether reparations are also due to the

136. *Id.*

137. DOD, *Assessment, supra* note 30, at 5. In theory, it is possible to locate the IP addresses of cyber attackers and use that information to locate them. *See, e.g.,* Jamie Smyth, *Hacking Away at Cyber Underworld*, IRISH TIMES, Apr. 27, 2001, 60. However, since sophisticated hackers are able to re-route or otherwise confuse programs designed to locate them, this is a far from foolproof approach to combating cyber war.

138. Lukasik, *supra* note 134, at 525.

139. The purpose of international political theory is to understand, explain, and predict international outcomes resulting from interactions among sovereign entities. Classical theorists such as Boden and Hobbes have shaped sovereignty to advocate an urgent need for international order, influencing centuries of international relations to follow. This dialogue endures. While free information flows and increasing economic interdependence have eroded and even overwhelmed the Westphalia structure, the institution remains nonetheless. The intersection of the two, as stated by Rosalyn Higgins, is the domain of law. *See* ROSALYN HIGGINS & MAURICE FLORY, TERRORISM AND INTERNATIONAL LAW 265 (1997).

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

141. Nor are cyber attacks analogous to a classic situation such as the ICJ faced in the *Corfu Channel* case in which British warships intruded on Albanian territorial waters. *Corfu Channel* (U.K. v. Alb.) 1949 I.C.J. Reports 4 (Apr. 9).

142. Brenner, *Attribution, supra* note 58, at 382.

victim of cyber attacks.[143] To answer these issues of attribution and to pin down those responsible for attacks, it is necessary to institute a standard of state responsibility that recognizes the difficulties inherent in cyber law. This Article will explore this dilemma further in Part V.

Consequently, sovereignty should not preclude the regulation of the information commons.[144] Nations have every right to protect their sovereign interests through the effects principle. Yet, given that many regard cyberspace as a commons territory, it would be prudent to regulate the commons as in other CHM areas through an international organization, similar to the United Nations Commission on the Limits of the Continental Shelf ("CLCS") under UNCLOS. This body could regulate cyber security similar to the ATS and outer space, but through greater private sector partnerships. Such a theoretical system is reminiscent of John Herz's notion of "neoterritorality," whereby sovereign states recognize their common interests, that is, cyber security, through extensive cooperation, while also mutually respecting one another's independence and the increasingly important role of non-state actors.[145] This system of mutual autonomy in the context of international collaboration to deter, defend, and punish cyber attackers may fit well with a theoretical basis for regulating against cyber attacks in international law. Sovereignty then should be conceived not as an application of state *control* but of state *authority*.[146] In the context of cyberspace, this authority should take the form of national and international efforts to regulate the largely privatized information commons, the details of which will be addressed in Part V. As cyberspace is testing traditional conceptions of

143. Depending on the context, reparations are often due a nation whose rights under international law were violated by another nation. *See* Factory at Chorzow (Germ. v. Pol.), 1927 P.C.I.J. (ser. A), No. 17, at 28 (Sep. 13).

144. Instead of calling for its decline and death in legal or political terms, it seems more useful to discuss the transformation of sovereignty into what John Jackson termed "sovereignty-modern." Jackson, *supra* note 118, at 790. This re-invention posits that as the world trends towards interdependence, substitutes for portions of nation-state sovereignty will fall to international institutions that embrace a series of legitimizing good-governance characteristics.

145. *See generally* FRED DALLMAYR, ALTERNATIVE VISIONS: PATHS IN THE GLOBAL VILLAGE 64 (1998) (arguing that Frankfurt School philosopher Jürgen Habermas upholds the idealist tradition of Kant, Hegel, and Marx, arguing for a critical theory of modern society that fuses critical philosophy and emancipatory politics.) Postmodernists, influenced by Nietzsche and Heidegger, alternatively view the humanist project of reason and progress as fundamentally flawed. *See id.* Bunn-Livingstone's intersubjectivity is one way in which to make constructive progress with diverse groups expressing everything from radical relativism to xenophobia. *See id.* There is, according to this view, much more that unites than divides us, a sentiment in keeping with the transition from absolute to popular sovereignty. *See id.* A more moderate viewpoint is Michael Mann's assertion that nation-states continue to wield some economic, ideological, military and political powers in the world order, albeit at a reduced level. In this, the dominant view, sovereignty is now universal, having migrated from Europe and become a mainstay of global politics and a central philosophy of the world's sole remaining superpower. Hugh Willis, *The Doctrine of Sovereignty Under the United States Constitution*, 15 No. 5 VA L. REV. 437 (1929).

146. Janice Thomson, *State Sovereignty in International Relations: Bridging the Gap between Theory and Empirical Research*, 39 INT'L STUDIES Q. 213, 225 (1995).

sovereignty, so too is IW forcing a reinterpretation of the terms "use of force" and "armed attack" under the U.N. Charter itself.[147]

V.
ANALOGIZING PEACETIME RESPONSES TO CYBER ATTACKS IN INTERNATIONAL LAW

It is little disputed whether the use of chemical and biological weapons should be viewed as a force within the classic meaning of armed attacks in international law. Much more contentious to date has been the characterization of IW, since it also threatens widespread destruction but through unconventional tactics—the same end with modern means. Cyber attacks that directly and intentionally result in non-combatant deaths and destruction of property breach modern prohibitions on the use of force.[148] However, the literature to date has been silent on the appropriate legal analogy to use as a baseline for regulatory responses to IW. This Article will argue that the broad-based and extraordinary nature of the worst possible cyber attack is most analogous in its scope and results to nuclear warfare. Already, nations such as Russia and the U.S. have compared the threat posed by IW to a nuclear exchange. Yet non-proliferation is not a useful option to curtail the spread of IW capabilities since nearly 120 nations and millions of people already have the necessary equipment and software.[149] Thus, to develop an international response to this dire threat, other international law regimes deserve consideration in the absence of a comprehensive international treaty on cyber security.

Both Russia and the United States have noted the similarity between IW and nuclear war, as well as the necessary military response. The Russians have stated: "An attack against the telecommunications and electronic power industries of the U.S. would, by virtue of its catastrophic consequences, completely overlap with the use of weapons of mass destruction."[150] In fact, according to a DOD report, a Russian academic recently published a statement "to the effect that Russia reserves the right to respond to an information warfare attack *with nuclear weapons.*"[151] On the other hand, former CIA Director John Deutch ranks information warfare "a close third behind threats from weapons of mass destruction and the proliferation and terrorist use of a nuclear, biological, or chemical (NBC) weapon."[152] Although the U.S. has not as brazenly argued that IW is tantamount to a nuclear exchange, Deutch's meaning is clear. These haw-

147. Joyner & Lotrionte, *supra* note 29, at 844-45.

148. *Id.* at 850.

149. However, there is some question about the scale of IW necessary to bring about effects analogous to a nuclear war.

150. Joyner & Lotrionte, *supra* note 29, at 831 (emphasis added).

151. DOD, *Assessment, supra* note 30, at 20.

152. Paul Mann, *Cyber-threat Expands with Unchecked Speed*, 145 AVIATION WEEK & SPACE TECH. 63, 64 (1996).

kish statements point to the extreme danger that great powers see in IW, as well as the extraordinary harm that could result in not laying out an appropriate legal framework from the outset to deal with cyber attacks.[153]

Given the problems of non-proliferation, what is the most appropriate analogy in international law for IW? Is there a possibility that IW could be outlawed as nuclear weapons nearly were by the International Court of Justice ("ICJ") in the *Nuclear Weapons Advisory Opinion*?[154] The answer to these queries will do much to guide the discussion of cyber warfare's place in IHL and IHRL. Simply put, there is no stand-alone analogy for IW. Each regime of international law examined here, including communications law, space law, the law of the sea, and other applicable accords, is inadequate in some way for the task. Yet by fitting together elements of these various regimes it is possible to graft together one framework applicable in peacetime and another after an armed attack occurs. The two frameworks are necessary to ensure that legal principles are coherently applied to avoid gaps in humanitarian protection,[155] as well as to guard against the continued propagation of cyber attacks. As has been stated, a new comprehensive international regime that builds on these treaties and customary international law would be preferable to the current system.

A. Banning Cyber Weapons through International Law

Unlike arms control treaties that seek to ban chemical, biological, or nuclear weapons, it is not a straightforward matter to prohibit the use of cyber warfare under international law. This difficulty stems from the fact that the computer codes that comprise IW are often indistinguishable from innocent information requests. In fact, in many cases the attacks merely constitute an abnormally high number of such requests.[156] Thus, developing a regime to ban IW on the generative Internet is challenging-- it is exceedingly difficult to ban one line of code the same way that it is to limit nuclear, biological, or chemical weapons. In an effort to determine the extent to which such a ban is possible, this Article will consider other treaty systems that have sought to limit the use of weapons, including nuclear weapons, space law and the Antarctic Treaty System, which will be analyzed in turn.

153. The dangers and opportunities afford by IW is of course not limited to the U.S. and Russia. In fact, a wide pool of nations, including China, has been aggressively developing IW capabilities. *See* Peter Brookes, *Countering the Art of Information Warfare*, HERITAGE FOUNDATION, Oct. 15, 2007, http://www.heritage.org/Press/Commentary/ed101607a.cfm.

154. *See generally* Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226 (July 8).

155. *See* Kenneth Watkin, *Controlling the Use of Force: A Role for Human Rights Norms in Contemporary Armed Conflict*, 98 AM. J. INT'L. L. 1 (2004).

156. Davis, *supra* note 1.

1. The Analogy of Nuclear War

The conventions and applicable case law on nuclear warfare are relevant to controlling the scope and tools of IW. In 1994, the United Nations General Assembly ("UNGA") voted to submit a request for an advisory opinion to the ICJ on the question of whether the threat or use of nuclear weapons could ever be lawful.[157] The U.S. argued in the case that nuclear weapons cannot be banned in the abstract, but rather each case must be examined individually.[158] Ultimately, the Court stated that the threat or use of nuclear weapons "would generally be contrary to the rules of international law applicable in armed conflict, and in particular the principles and rules of humanitarian law."[159] However, the Court did not define whether "the threat or use of nuclear weapons would be lawful or unlawful in an extreme circumstance of self-defense, in which the very survival of a state would be at stake."[160] The ICJ elaborated:

> [T]he principles and rules of law applicable in armed conflict—at the heart of which is the overriding consideration of humanity—make the conduct of armed hostilities subject to a number of strict requirements. Thus, methods and means of warfare, which would preclude any distinction between civilian and military targets, or which would result in unnecessary suffering to combatants, are prohibited. In view of the unique characteristics of nuclear weapons, to which the Court has referred above, the use of such weapons in fact seems scarcely reconcilable with respect for such requirements.[161]

Although the U.S. has not embraced a *per se* rule banning the use of nuclear weapons, it acknowledges that the law of armed conflict, including the rules of proportionality, necessity, moderation, discrimination, civilian immunity, neutrality, and humanity, governs such use.[162] As noted, some of the effects of nuclear weapons can be similar to a worst-case cyber attack on a state. An all-out attack could disable or destroy *all* critical infrastructures, leave the victim nation completely helpless and terrorize its population.[163]

Cyber attacks on the scale of those against Estonia, like nuclear warfare, do not discriminate between combatants and non-combatants, nor do they pass the test of proportionality. If the use of nuclear weapons is subject to the rules of IHL listed above, as the U.S. maintains, so too should cyber attacks. Even though the ICJ did not declare all nuclear weapons illegal, the logic of its hold-

157. FOREIGN & INT'L LAW COMM. OF THE NEW YORK COUNTY LAWYERS' ASS'N (NYCLA), ON THE UNLAWFULNESS OF THE USE AND THREAT OF NUCLEAR WEAPONS (2000) [hereinafter NYCLA, UNLAWFULNESS OF NUCLEAR WEAPONS],
http://www.nuclearweaponslaw.com/JournalsReport/NYCLA_Report.pdf.

158. *Id.*

159. Legality of Nuclear Weapons, 1996 I.C.J. at 266.

160. *Id.*

161. *Id.* at 262.

162. *See* NYCLA, UNLAWFULNESS OF NUCLEAR WEAPONS, *supra* note 157.

163. Dickon Ross, *Electronic Pearl Harbor*, GUARDIAN (LONDON), Feb. 20, 2003 (laying out the scenarios for potential cyber attacks).

ing that "methods and means of warfare … which would result in unnecessary suffering to combatants, are prohibited"[164] is just as applicable to cyber war as it is to nuclear war. Cyber attackers could have a larger role in non-combatant casualties than would a nuclear aggressor state launching a mass assault, since cyber attacks by their nature may be targeted to specific systems whereas nuclear weapons cannot be similarly focused due to collateral damage from even the smallest devices. Even the lowest yield weapons result in substantial collateral damage.[165] Yet the ICJ has refused to rule such low-yield nuclear weapons illegal, or even explicitly consider IW.[166] As this decision indicates, as of yet there is little to no customary international law on the use of cyber attacks beyond the basic principle in the *Nicaragua Case* that "every sovereign [s]tate [has a right] to conduct its affairs without outside interference . . . [this] is part and parcel of customary international law."[167] As a result, it is yet impossible as a matter of customary international law to argue that IW is illegal, especially given that state practice routinely shows otherwise.

Custom according to the *North Sea Continental Shelf Case* requires "widespread and representative participation provided it include[s] that of [the] [s]tates whose interests were specially affected."[168] State practice in the aftermath of cyber attacks suggests widespread condemnation but no consensus on how to respond, or even at what level a cyber attack becomes an armed attack. In the absence of custom, several treaty regimes may provide bases for the regulation or outright prohibition of cyber attacks in international law. These regimes together form a useful, if imperfect, system that may give recourse until a comprehensive treaty on cyber security is implemented.

2. The Analogy of Space Law and the Antarctic Treaty System

Outer space is inherently similar to cyberspace; both are incredibly vast areas of the international commons. International law does not permit outer

164. Legality of Nuclear Weapons, 1996 I.C.J. at 262.

165. Robert W. Nelson, FED. OF AM. SCIENTISTS, FAS PUBLIC INTEREST REPORT - LOW-YIELD EARTH-PENETRATING NUCLEAR WEAPONS (2008),

http://www.fas.org/programs/ssp/nukes/new_nuclear_weapons/loyieldearthpenwpnrpt.html.

166. Legality of Nuclear Weapons, 1996 I.C.J. at 262.

167. Military and Paramilitary Activities (Nicar. V. U.S.), 1986 I.C.J. 14, 106 (June 27) [hereinafter *Nicaragua*].

168. N. Sea Cont'l Shelf (F.R.G. v. Den.; F.R.G. v. Neth.), 1969 I.C.J. 41, 42 (Feb. 20). A rule of customary international law requires two elements: (1) general state practice; and (2) "state adherence to the rule based on a belief that such adherence is legally required (*opinio juris*)." Andrew T. Guzman, *Why LDCs Sign Treaties That Hurt Them: Explaining the Popularity of Bilateral Investment Treaties*, 38 VA. J. INT'L L. 639, 646 n. 20 (1996). *See also* Statute of the International Court of Justice art. 38, June 26, 1945, 59 Stat. 1055, 3 Brevans 1179 ("The Court…shall apply…international custom, as evidence of a general practice accepted as law."); Cont'l Shelf (Libya v. Malta) 1985 I.C.J. 13, 29 (June 3) ("It is of course axiomatic that the material of customary international law is to be looked for primarily in the actual practice and *opinion juris* of states… .").

space or cyberspace to be nationalized.[169] Space and telecommunications systems are also intertwined, including in such functions as communications relay, imagery collection, missile warning, navigation, weather forecasting, and signals intelligence.[170] However, space law's failure to address whether the legal regime applies during armed conflict[171] foretells the limitations inherent in applying space law as an analogy for IW.[172] There is also no legal prohibition against developing and using space weapons except for placing nuclear weapons into orbit.[173]

The military use of space was not completely forbidden by the 1967 U.N. Outer Space Treaty, as evidenced by the existence of earth-orbit military reconnaissance satellites, remote-sensing satellites, military global-positioning systems, and space-based aspects of an antiballistic missile system. Yet this treaty prohibited any objects carrying nuclear weapons or any other kinds of weapons of mass destruction in outer space, whether in orbit around the Earth or on celestial bodies.[174] Still, even this limitation applies only to the Moon and other celestial bodies and not the empty space in between.[175] Thus, no legal regime currently prohibits weapons being placed in the void between bodies. *Vision for 2020*, a 1998 government report, explains that the role of the U.S. Space Command ("USSC") will be to dominate "the space dimension of military operations

169. The Outer Space Treaty, dubbed as the Magna Carta for space, states that "Outer space, including the Moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means." Outer Space Treaty, *supra* note 120. Interview with Steve Doyle, Executive Vice President, Clean Energy Systems, in Sacramento, Cal. (Oct. 2, 2007).

170. *See* DOD, *Assessment, supra* note 30.

171. Since 1958, space law has created a whole new field of legal terminology that has challenged national governments to redefine the scope of space operations. Space law recognizes all humans as the holders of fundamental, non-transferable rights. This puts it at odds with traditional notions of Westphalian sovereignty by limiting the positive rights of states. *See* Scott Shackelford, *The Tragedy of the Common Heritage of Mankind*, 28 STAN. ENVTL. L.J. (forthcoming Feb. 2009).

172. An example of this phenomenon is the context of space law occurred when both the U.S. and U.S.S.R. began launching spy satellites that crossed over one another's territory. Since both countries were already engaging in this practice, it soon became part of customary international law, which entered into the 1967 Outer Space Treaty and as a result laid the foundation for the governance regime of outer space. In contrast, air law was developed at a time when many nations were fielding air forces together and as such had a mutual stake in creating a highly restricted regime based on severe conceptions of sovereignty and territorial integrity. An applicable Civil Aviation accord includes the 1944 Convention on International Civil Aviation (Chicago Convention). This treaty codifies safe passage and service (Article 28), and compliance with international standards (Article 37). Most of the provisions of the Chicago Convention are "inconsistent with a state of armed conflict." Convention on International Civil Aviation, art. 89, Dec. 7 1944, 61 Stat. 1180, 15 U.N.T.S. 295. Yet, given the already pervasive use of cyber attacks the international community could quickly find itself in a situation more analogous to space law than air law.

173. In 1989, a U.S. Congressional study, "Military Space Forces: The Next 50 Years," envisioned the day when aerospace corporations would "mine the sky" for profit. The study cited U.S. plans to establish military bases on the Moon and control the shipping lanes from the Earth. *See generally* JOHN COLLINS, MILITARY SPACE FORCES: THE NEXT 50 YEARS (1989).

174. Outer Space Treaty, *supra* note 120.

175. BIN CHENG, STUDIES IN INTERNATIONAL SPACE LAW 517, 529 (1997).

to protect U.S. interests and investment…." General Joseph Ashy, Commander-in-Chief of the USSC, noted, "Some people don't want to hear this…but we're going to fight in space… . That's why the U.S. has development programs in directed energy and hit-to-kill mechanisms."[176] This statement underscores the Bush Administration's desire to maintain the U.S. as the world's foremost space power at the expense of multilateral cooperation. The Bush Administration has maintained a very similar stance in relation to eschewing international cooperation in dealing with cyber warfare. The Obama Administration is more open to negotiating treaties to further international security and could very well change U.S. policy in this regard. Although lacking specific policy proposals, his campaign has stated that: "We must urgently seek to reduce the risks from three potentially catastrophic threats: nuclear weapons, biological attacks, and cyber warfare."[177] The fact that his campaign's online portals have already been the victims of a cyber attack may persuade the Obama Administration to confront this threat early.[178]

International efforts to form a legal regime regarding cyber attacks have been just as happenstance as those aimed at limiting the spread of space weapons. Russia and China have advocated for such a treaty, but the U.S. has demurred.[179] The usual rationale given by the U.S. is that it wants to maintain its space dominance. Similar efforts to cement a treaty for cyber attacks have also failed thus far for the same reasons. As for space weapons, Russia has drafted a resolution calling on nations to ban the development and production of information weapons. The U.S. has taken the position that it is premature at this point to discuss negotiating an international agreement on IW, but NATO leaders have agreed to adopt a common stance to help a member nation repel a cyber attack when requested while leaving undefined specific instances in which NATO Article V should be activated.[180] Yet, unlike the sophisticated infrastructure and advanced technology needed to develop and deploy space weapons, nearly all nations participate in the Information Age to some degree, while only thirty are in space.[181] Barring a major conflict, most states do not expect or have the re-

176. Karl Grossman & Judith Long, *Waging War in Space*, NATION, Dec. 9, 1999, http://www.thenation.com/doc/19991227/grossman.

177. Confronting 21st Century Threats, July 16, 2008, BARACKOBAMA.COM, http://www.barackobama.com/2008/07/16/fact_sheet_obamas_new_plan_to.php.

178. Demetri Sevastopulo, *Cyber attacks on McCain and Obama Teams 'came from China,'* FINANCIAL TIMES, Nov. 7, 2008, *available at*: http://www.ft.com/cms/s/0/3b4001e2-ac6f-11dd-bf71-000077b07658.html.

179. John Borland, *Russia, China Propose Space Arms Treaty*, WIRED, Feb. 12, 2008, http://blog.wired.com/wiredscience/2008/02/russia-china-pr.html (arguing that Russia and China have been pushing for talks on this issue since the beginning of the decade, against the wishes of the U.S. to maintain its dominance in space).

180. Ben Bain, *Cybersecurity's New World Order*, FED. COMPUTER WKLY., Apr. 28, 2008, http://www.fcw.com/print/22_11/features/152349-1.html?page=3.

181. *See* Internet Usage Statistics, INTERNET WORLD STATS, June 30, 2008, http://www.internetworldstats.com/stats.htm; Scott Horowitz, *Nations in Space,* AMERICA.GOV, July

sources to be either an attacker or a defender in space in the near future.[182] In contrast, with information systems, nearly all states can reasonably expect to be both the attacker and defender in future conflicts putting added pressure on the need for an international accord on cyber security. This is true not only in Estonia but across the world, as cyber attacks continue to proliferate most recently against Georgia.

Space law illustrates that it is possible to regulate an area of the international commons to bar the most egregious military weapons systems. Space law though does not quite fit cyber attacks because of the accumulation of seemingly innocent intrusions that together may amount to a WMD attack. There is no cyber equivalent of a nuclear weapon--no piece of code currently known that can, by itself, bring a country to its knees. Rather, it is the coordination of many attacks that can paralyze a nation's infrastructure.

Rather than banning only the most egregious cyber use, it may be more thorough to regulate all hacking that could become a cyber attack. The Antarctic Treaty System ("ATS") provides a fruitful analogue of a commons area that has gone the extra step of banning *all* military activities.[183] In effect, the ATS sets aside Antarctica as a scientific preserve, establishes freedom of scientific investigation, and bans military activity on the continent.[184] The main objective of the ATS[185] is to ensure "in the interests of all mankind that Antarctica shall continue forever to be used exclusively for peaceful purposes and shall not become the scene or object of international discord."[186] Just like Antarctica, the Internet has rich resources as a repository of knowledge and channel for communication, and its potential is growing daily. Imposing such a freeze on developing new software capable of malicious attacks, even if possible, stifles innovation just as shutting down the generative nature of the Internet world. Nor would a traditional international accord be capable of keeping up with the rapidly changing nature of IT, save for a standing committee that would amend the treaty as demanded by new challenges. Subsequent ratification by national legislatures would thereafter pose a significant problem, unless the mandate of the committee explicitly included that power. On the surface then, it appears

29, 2008, *available at*

http://www.america.gov/st/space-english/2008/July/20080817210902SrenoD0.1624262.html.

182. Horowitz, *supra* note 181.

183. Antarctic Treaty pmbl., Dec. 1, 1959, 12 U.S.T. 794, 402 U.N.T.S. 71.

184. These signatory countries were Argentina, Australia, Belgium, Chile, France, Japan, New Zealand, Norway, South Africa, the U.S.S.R., the U.K., and the U.S. It is important to note the restrictions on property rights and ban on military maneuvers that denote Antarctica as a quasi-CHM area. ATS was also the first arms control treaty of the Cold War. *See id.*

185. Like the deep seabed and the Arctic, the continent of Antarctica is an expanse of undeveloped land that contains substantial mineral deposits. Unlike them, however, nations have made and continue to assert overlapping territorial claims to Antarctica. The 1959 Antarctic Treaty attempts to clarify these conflicting demands. The ATS defines Antarctica as all land and ice shelves south of the southern 60th parallel. Antarctic Treaty, *supra* note 183, at art. VI.

186. Antarctic Treaty, *supra* note 183.

than neither barring certain malignant code nor all possible variations of known cyber attacks under international law is an effective, efficient response to the problem of cyber attacks.[187]

B. Determining Liability for Cyber Attacks through Domestic Legal Mechanisms

As international accords do not define a comprehensive legal system to deal with cyber attacks, domestic mechanisms should be considered. These include both enforcement procedures required under international law, as well as domestic cyber law statutes. The U.S. serves as a case study in this regard, with special attention given to the existing system of vicarious liability. A new international accord regulating IW could build upon this system.

1. The Analogy of Communications and U.S. Cyber Law

In many ways, the development of international communications law was the direct precursor to cyber law, beginning with agreements dating from the 1800s designed to protect submarine cables.[188] Modern communications law is crafted by the International Telecommunications Union ("ITU"), a specialized U.N. Agency for information communication technologies.[189] The ITU Constitution militates against "harmful interference," defined in the Annex 3 of the document as that which "endangers . . . *safety services* or seriously degrades, obstructs or repeatedly interrupts a radio communication service operating in accordance with the Radio Regulations."[190] This passage could serve to hold those states that use cyber attacks to "endanger…safety services" responsible under international law.[191] "Safety services" conceivably includes public services such as health, police, and public transport, all of which are vulnerable to cyber attacks. However, lack of mandatory enforcement mechanisms limits the efficacy of this regime.

In addition, some provisions of the ITU Charter give governments wide discretion in regulating private activity that may appear dangerous to the security of the state.[192] This includes "cut[ting] off any private telecommunications which may appear dangerous…or contrary to [s]tate laws, to public order, or to decency."[193] Unlike space law or the ATS, Article 48 does have an exception

187. *See generally* David A. Koplow, *When Is an Amendment Not an Amendment?: Modification of Arms Control Agreements Without the Senate*, 59 U. CHI. L. REV. 981, 1023 (1992) (considering the process of treaty modification in international law).

188. DOD, *Assessment*, *supra* note 30, at 36.

189. *See* Int'l Telecomm. Union [ITU], About ITU, http://www.itu.int/net/about/index.aspx (last visited Feb. 24, 2008).

190. CONST. OF THE INT'L TELECOMM. UNION, art. 6, 34 (2006) [hereinafter ITU Constitution] (emphasis added).

191. *See id.* at art. 34.

192. DOD, *Assessment*, *supra* note 30, at 33-34.

193. *See* ITU Constitution, *supra* note 191, at art. 34.

for military activities,[194] but does not specify how the treaty applies during "armed conflict." Since the British cut the five submarine cables serving Germany in the days following the outbreak of WWI, communications facilities have been regarded as priority military targets.[195] State practice still suggests that these treaties may not apply during international armed conflicts.[196] Critically, international communications law currently contains no direct and specific prohibition against the conduct of information operations by military forces, even in peacetime.[197] As a result, while Articles 34 and 48 of the ITU can help to develop felony statutes to deal with state-sponsored IW perpetrators, they offer limited guidance in crafting a comprehensive legal framework to deal with state-sponsored cyber attacks that have risen to the level of an armed attack.

2. U.S. Cyber Law Applied to Information Warfare

Cyber law is relatively new. It has to be considering the fact that twenty years ago in 1988, there were only sixty thousand computers, all at research institutions, connected to the Internet.[198] Initial efforts at cyber security in the U.S. occurred after the first Internet worm on November 2, 1988, when a Cornell graduate student infected MIT's burgeoning network from Ithaca.[199] The attack exposed difficulties in U.S. law that would make the prosecution of cyber attackers exceedingly difficult.[200] As a direct result, USCERT was founded. Its largely successful track record, however, is less a proof of its efficacy than a reflection of the relative scarcity of major malicious viruses and worms since 1988.[201]

As the threats posed by cyber attacks grow, it is prudent to look to and analogize from applicable domestic as well as from international law. U.S. law does possess certain principles that are applicable to cyber attacks. The fact that most of the critical infrastructure in the U.S. is privatized signifies that principles of tort law and other related common law doctrines could prove decisive in developing a U.S. legal regime to address cyber attacks. For example, consider vicarious liability,[202] a form of strict secondary liability that arises under the common law doctrine of agency, *respondeat superior*. Under this theory, the principal is responsible for the acts of the subordinate, or as applied to cyberspace, the network administrator for network integrity. In a broader sense, a

194. *Id.* at art. 48.

195. DOD, *Assessment*, *supra* note 30, at 33.

196. *Id.*

197. *Id.* at 36.

198. *See* Zittrain, *supra* note 64, at 36.

199. *Id.*

200. U.S. GOV. ACCOUNTABILITY OFFICE, GAO/IMTEC-89-57, VIRUS HIGHLIGHTS NEED FOR IMPROVED INTERNET MANAGEMENT 5, 30-34 (1989).

201. Zittrain, *supra* note 64, at 44.

202. RESTATEMENT (SECOND) OF TORTS § 520 (1965).

third party that has the right, ability, or duty to control the activities of a violator but refuses or neglects to do so may be liable for the violator's actions in some cases.[203] Applied to cyber attacks, this principle may hold companies liable for knowingly or negligently failing to provide sufficient cyber security for the persons or resources, including infrastructure, under their care during a CNA.

Several recent precedents help lay the foundation for this regime of vicarious liability applied to IW. For example, the U.S. Supreme Court recently held in *Metro-Goldwyn-Mayer Studios, Inc., v. Grokster, Ltd.* that software distributors could be held liable for contributory infringement of copyright based on the distributor's knowledge of extensive infringement.[204] As this case illustrates, if a technology company is aware of a nefarious act and the firm refuses to develop filtering tools to diminish the infringing activity, then the company may be held liable for any resultant criminal or terrorist consequences. For example, in *Fonovisa v. Cherry Auction, Inc.*, the court found vicarious liability because the defendants had control over direct infringers, and had an explicit financial interest in the infringing activity.[205] Together, these cases place the onus of surveillance on the private sector, which largely controls the Internet, by policing its managed infrastructure so as to lessen the potential for damaging cyber attacks. In doing so, however, companies (notably Internet service providers) cannot be overzealous and block innocent websites, otherwise they would violate the First Amendment and trigger intermediate scrutiny.[206] Nor do companies have secondary liability for providing Internet services if they have no knowledge of the violation or infringement.[207]

In addition to case law, several U.S. criminal statutes could also serve as a rubric for cyber attacks. For example, U.S. felony statutes criminalize violations of international accords dealing with international radio or wire communications,[208] and malicious interference with satellites, similar to wire fraud.[209] These statutes could extend to external and internal cyber attacks that do not reach the level of an armed attack. In this way, the U.S. terrorism statutes, which define terrorism as "committing acts constituting crimes under the law of any country to intimidate or coerce a civilian population; to influence government policy by intimidation or coercion; or to affect the conduct of government by mass destruction, assassination, or kidnapping," could be used to further cri-

203. Meyer v. Holley, 537 U.S. 280, 284 (2003).

204. Metro-Goldwyn-Mayer Studios, Inc., v. Grokster, Ltd., 545 U.S. 913 (2005). *Cf.* CoStar Group v. LoopNet, Inc., 373 F.3d 544, 556 (4th Cir. 2004) (holding that a web provider was not liable as the manager of a system used by others who were violating U.S. law).

205. Fonovisa v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996).

206. Ctr. for Democracy & Tech. v. Pappert, 337 F. Supp. 2d 606 (E.D. Pa. 2004).

207. Hendrickson v. eBay, Inc., 165 F. Supp. 2d 1082 (C.D. Cal. 2001).

208. *See* 47 U.S.C. §502 (2000) (imposing an additional $500 per day fine on anyone who "willfully and knowingly violates any rule . . . made or imposed by any international radio or wire communications treaty or convention").

209. 18 U.S.C. §§ 1343, 1367 (2000).

minalize the various forms of cyber attacks.[210] Similar statutes could be enacted to deal with IW collaborators.

Today, the fact that 439 million computers are now connected to a ubiquitous Internet has destroyed any online ethical code that once existed.[211] As an evidence of this trend, business plans for "bad code" have proliferated through the use of botnets now emerging at the rate of 1 million per month and are used for blackmail and other criminal acts.[212] These botnets also now routinely affect national security. In May 2006, a virus infected the U.S. State Department's Eastern Asia bureau, forcing a system crash during North Korea's missile tests.[213] The right advanced worm released today making use of botnets and zombie networks could infect and crash every computer connected to the Internet simultaneously.[214] How it is possible to avoid such an eventuality?

Cyber attacks expose the weaknesses of a generative network, that is, networked computers that retrieve and install code from sources anywhere on the network.[215] The current system is analogous to nibbling food from hundreds of different people, some established vendors, some street peddlers.[216] This strategy exponentially increases system flexibility, but at the cost of security. The alternative is to transform the personal computers into information appliances, like a game console, in which one central administrator approves content for all of the machines. Such a resolution of the cyber security conundrum would stifle innovation, be a hard sell to the international community, and sacrifice the central characteristic of the generative Internet. As a result, other treaty regimes should also be considered so as to avoid this drastic scenario.

C. The Role of the Private Sector in Regulating the Commons

The private sector was marginalized when it came time to create legal regimes governing the international commons, including outer space and the deep seabed. Over time, competitive pressures and resource shortages have changed the role of the private sector in these areas. Now the private sector is increasingly being given an ever more central role to play in the management of commons resources. This will be demonstrated as applied to the law of the sea below. The same lesson must be applied to cyberspace given the already dominant role that private sector actors play in maintaining the generative Internet.

---

210. 18 U.S.C.§ 2331 (2000). For more definitions, *see, e.g.*, Mohammad Iqbal, *Defining Cyberterrorism*, 22 J. MARSHALL J. COMPUTER & INFO. L. 397, 397 (2004).

211. Zittrain, *supra* note 64, at 45 (postulating that there was once an online ethical code among the original scientists and other internet users that has since dissolved as the internet has expanded).

212. *Id.*

213. *Id.* at 47.

214. *Id.* at 52.

215. *Id.* at 38.

216. *Id.* at 55.

1. The Analogy of the Law of the Sea

The law of the sea, like outer space, has many parallels with cyberspace. The process that ultimately resulted in the first United Nations Convention on the Law of the Sea ("UNCLOS") treaty began in 1945 with the codification of four Geneva Conventions, beginning with UNCLOS I in 1958.[217] However, UNCLOS I did not sufficiently address concerns about the legal status of the deep seabed, among much else. This served as an impetus for UNCLOS III, which was tasked with regulating the use, exploration, and exploitation of all living and non-living resources of the international sea.[218] Still, the role of the private sector remained truncated. As the deep seabed mining provisions of UNCLOS proved ultimately unsatisfactory to the industrialized world, in 1993, preparations were laid for the 1994 New York Agreement. This amendment changed the nature of the deep seabed regime into one that comports with private economic development. The story of the evolution of UNCLOS is the imperative that the private sector must be given a place if real progress in regulating the commons is to be made.

As applied to cyber attacks, UNCLOS Article 19 states the customary international law obligation for a nation's territorial sea not to engage in activities "prejudicial to the peace, good order, or security of the coastal [s]tate."[219] This includes the collection of information, or propaganda, or any way interfering with any systems of communications. Article 113 requires domestic criminal legislation to punish willful damage to submarine cables.[220] As a result, UNCLOS is important for its prohibition on staging any attacks that interfere with the security or good order of a coastal state. An argument could be made that this Article 19 prohibition should also apply to Article 113 claims involving submarine cables. This would mean that cyber attackers who send code through submarine cables to a coastal state would be in breach of international law obligations. Still, this accord also does not specify its status in wartime.[221] Nor does it include enforcement mechanisms.

Nonetheless, UNCLOS has also illustrated a regime, which was unsuccessful until it recognized the needs of the private sector, as well as doing away with

217. In 1956, the United Nations held its first Conference on the Law of the Sea ("UNCLOS I"). UNCLOS I resulted in four treaties: Convention on the Territorial Sea and Contiguous Zone, Convention on the Continental Shelf, Convention on the High Seas, and Convention on Fishing and Conservation of Living Resources of the High Seas. *See* United Nations, Oceans and Law of the Sea, http://www.un.org/Depts/los/index.htm.

218. Alvaro de Soto, *Reflections on UNCLOS III: Critical Junctures*, 46 LAW & CONTEMP. PROBS. 65 (1983) (detailing some of the critical negotiating junctures in negotiating UNCLOS III).

219. UNCLOS art. 19, Dec. 10, 1982, 1833 UNTS 3; 21 ILM 1261 (1982).

220. *Id.* at art. 113.

221. Nor does espionage law provide a fruitful analogue for cyber attacks. During an armed conflict, espionage law covering the covert collection of intelligence about other nations only applies to a person relying on protected civilian status or while wearing an enemy uniform. This is much less well developed in peace-time.

mandatory technology transfers. If an international legal regime is to be created, it must ensure sufficient protections for private enterprise to promote innovation while not mandating technology transfers on developed nations. This militates against drastically changing the nature of the generative Internet, and underscores the central primacy that non-state actors have in curtailing cyber attacks and the consequent need for multilateral cooperation in keeping with neoterritoriality theory.

D. Analogizing Other Applicable Accords to Information Warfare

Numerous bilateral and multilateral treaties dealing with everything from legal assistance, extradition, diplomatic relations, friendship, to status of forces agreements include elements that affect the prosecution of cyber attackers. Beginning with Switzerland in 1977, the U.S. is a party to dozens of Mutual Legal Assistance Treaties ("MLATs"),[222] which could be used to seek criminal prosecution of those found responsible for cyber attacks, especially those treaties termed broadly enough to cover *all* law enforcement investigations.[223] The problem with this approach, however, would be to treat a cyber attack as analogous to terrorism. As a result, the IHL framework would drop away unless state-sponsored terrorism is included within the regime.[224] There are often no enforceable obligations under these treaties. The U.S. is also a party to more than 100 bilateral extradition treaties.[225] Without such accords national governments will often have neither an international obligation nor the domestic authority to deliver custody of an individual for prosecution.[226] These treaties could be evoked to more effectively bring the perpetrators of cyber attacks to justice. As such, international criminal law has a distinct role to play in cyber attacks, a subject that will be reprised in Part V.

The 1961 Vienna Convention on Diplomatic Relations enshrines the right of inviolability of the premises of a diplomatic mission,[227] its archives,[228]

222. For a collection of current agreements in force, see Mutual Legal Assistance (MLAT) and Other Agreements, U.S. Dep. of State,

http://travel.state.gov/law/info/judicial/judicial_690.html (last visited Oct. 19, 2008).

223. *See, e.g.*, Mutual Legal Assistance Treaty, U.S.-Can., Jan 24, 1990, MLAT: Treaty Doc. 100-14; 100th Cong., 2nd Sess. Exec. Rept. 100-28; 100th Cong, 2nd Sess. Exec. Rept 101-10; 101st Cong., 1st Sess. XXIV ILM No. 4, 7/85, 1092-1099.

224. JOHN MURPHY, STATE SUPPORT OF INTERNATIONAL TERRORISM: LEGAL, POLITICAL, AND ECONOMIC DIMENSIONS 59-60 (1989).

225. *See generally* U.S. Treaties of Extradition, Cornell Univ. Law School, http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00003181----000-notes.html (last visited: Oct 19, 2008).

226. DOD, *Assessment*, *supra* note 30, at 35.

227. 1961 Vienna Convention on Diplomatic Relations art. 2, April 18, 1961, 23 U.S.T. 3227; 500 U.N.T.S. 95.

228. *Id.* at art. 24.

private residences and property of its agents,[229] and its *communications*.[230] Applied to cyber law, this regime, then, could protect all communications made to and from government embassies and missions against cyber attack or espionage. In addition, the vast majority of treaties of friendship, commerce, and navigation are archetypical examples of agreements that will likely be suspended during an armed conflict between state parties.[231] Tourism is antithetical to a war zone. Though, most NATO Status of Forces Agreements ("SOFA") would remain in place during an armed conflict. These agreements include the necessity of respecting the host nation's laws. Typically, the stationed forces must notify the host nation of any change in operations, including information warfare. This would help decrease the possibility of actual foreign soldiers perpetuating cyber attacks on foreign nations without the host government's tacit consent.

Taken together, these diverse treaty provisions provide the basis for a framework to deal with cyber attackers during peacetime. If a host nation's domestic laws criminalize cyber attacks, then applicable MLATs and extradition treaties would apply to make perpetrators accountable in various jurisdictions.[232] If the attack is directed against a foreign mission or embassy, then the Vienna Convention on Diplomatic Immunity would provide remedies and potentially reparations to the victim nation in international law. Moreover, provisions under UNCLOS III regulating submarine cables, the ability to prosecute private parties in breach of the ITU treaty in telecommunications law, or interference with satellite transmissions in space law, all place significant restrictions on cyber attacks. However, few if any of these treaties, with the exception of SOFAs, would remain in force during an armed conflict. The extent to which these treaties are applicable during an international conflict then depends on whether or not cyber attacks rise to the level of armed attacks activating IHL.

VI.
ARMED ATTACKS IN INFORMATION WARFARE

Under what circumstances can a CNA constitute an act of war? International law requires that for self-defense to be permissible there must be an attack

229. *Id.* at art. 30.

230. *Id.* at art. 27. Although "communications" in the context of Article 27 refers to mail, telephone, and other communication methods most commonly used in the early 1960s when the Vienna Convention was negotiated and ratified, this definition is not limited to such devices. Thus, the reference may be analogized to modern communication devices, including email and the internet. But, it should be noted that Article 27(1) notes that a "mission may install and use a wireless transmitter only with the consent of the receiving state." Modern telecommunications is not necessarily wireless, such as LANs, but nevertheless this passage must be given full effect in all cases involving diplomatic missions.

231. DOD, *Assessment*, *supra* note 30, at 4.

232. It should be noted, however, that the Estonian-Russian MLAT proved entirely ineffective, since Russia refused to honor the treaty in this instance.

so egregious that the victim would be justified in responding in kind.[233] This conception rules out preemptive or aggressive self-defense in most instances. U.N. General Assembly Resolution 2625 ("UNGA 2625") declares a war of aggression "a crime against the peace" and exhorts states to refrain from "acts of reprisal involving the use of force…[and] from organizing, instigating, assisting, participating in acts of civil strife or terrorist attacks in another [s]tate."[234] Yet it is not UNGA 2625, but the U.N. Charter itself, that governs the use of force. The question then is whether and to what extent CNAs constitute a use of armed force.[235]

The U.N. Charter anticipates such situations as the presence of troops and the use of traditional military weapons on another nation's territory, not simultaneous multimodal network attacks on a state. In the case of IW, fundamental questions arise over what types and degrees of network attacks may fall within the legal scope of Article 2(4). U.N. Charter law prohibits international intervention through the use of armed force, but is silent on other, subtler forms of subversive coercion that do not involve a perceived threat of armed force.[236] State practice has shown that such coercion or other forms of "aggression" do not activate Article 2(4) protections. Therefore, a state could have a right to self-defense in response to a CNA only when that attack rose to the level of an armed attack. As shown in the Estonia case study, the main legal hurdles in pursuing a self-defense rationale are: (1) proving that the cyber attack rose to the level of a traditional armed attack by military forces; and (2) that this attack can be attributed to a state. The former is generally a far easier question to answer than the latter.

First, it is possible for a cyber attack to rise to the level of an armed attack as traditionally recognized under IHL.[237] IW is an expansive category of military activities. It includes physical attacks on information systems by traditional military means, psychological operations, military deception, and electronic welfare operations such as jamming.[238] IW is not the first arena of high technology to fall under the IHL framework. Even futuristic electro-magnetic pulse weapons, directed-energy lasers, microwave devices, and high-energy radio fre-

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

234. G.A. Res. 2625 (XXV), U.N. Doc. A/8028 (Oct. 24, 1970).

235. In 1974, the General Assembly defined "aggression" as "the use of armed force by a [s]tate against the sovereignty, territorial integrity or political independence of another [s]tate, or in any manner inconsistent with the Charter of the United Nations." Definition of Aggression, G.A. Res. 3314 (XXIX), art. 1, U.N. GAOR, 29th Sess., Supp. No. 31, at 142, U.N. Doc. A/9631 (1975), 13 I.L.M. 710 (Dec. 14, 1974).

236. Joyner & Lotrionte, *supra* note 29.

237. The debate about what constitutes an armed attack can be framed in reference to the September 11 attacks. Some authors maintain that these attacks on the U.S. were armed attacks under the meaning of the U.N. Charter and thus are open to self-defense. Others look to the UNSC for guidance, while still others view the attacks as a horrific international crime for which the perpetrators should be punished as criminals. *See* Watkin, *supra* note 155.

238. DOD, *Assessment*, *supra* note 30.

quency guns operate similarly enough to traditional weapons that they will trigger IHL protections. The difficult issue arises in the guise of a pure information (computer network) attack. Using electronic means to gain access or to change information in a targeted system does not damage any physical components in the traditional sense. Such undertakings are now easier than ever before since global communications have essentially made distance and geographic boundaries irrelevant to the conduct of computer network attacks.[239]

Estonians have already witnessed the potential for cyber attacks to disrupt and destroy a society. In a worst-case scenario, CNAs could indeed cripple a society, shut down vital public services, and lead to the breakdown of public order. Property damage and loss of life would be on the order of a traditional military attack. Therefore, the question thus turns on a definition of "force,"[240] which could be interpreted strictly in accordance with the text, or with the broad object and purpose of the U.N. Charter.[241] Although it is a contentious issue, it may be stated with some confidence that the boundaries of "force" do not correspond to those of armed force only.[242] What matters then are the ends sought, not the means. Thus, it is theoretically possible for a CNA to rise to the level of an armed attack. For example, a CNA aimed at causing harm to property and humans can be "reasonably characterized as a use of armed force" to fall under the prohibition of Article 2(4).[243] The CNA itself is only an instrument to carry out that attack in the same way that any other weapon would be. The international community would be well advised to reinterpret traditional understandings of armed attacks in consideration of Twenty-first Century threats.

Second, the 1986 Libya attack precedent held that states who unwittingly, or permissively, allow their territory to be used to carry about attacks are committing an act of aggression.[244] The problem then becomes one of attribution, that is, the all too familiar scenario of computer systems being used maliciously without the knowledge of the network administrator. For example, many of the 'zombie' computers used to carry out botnet attacks against Estonia turned out to be in the U.S.. [245] Should Estonia then have a right of self-defense against the U.S.? Upping the ante, how would it be possible to prove a causal chain in the

239. *Id.*

240. Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 900 (1999).

241. Vienna Convention on the Law of Treaties art. 31, para. 1, May 23, 1969, 1155 U.N.T.S. 331. Analysis based on both U.N. Charter travaux and text leads to an interpretation excluding economic, and for that matter political, coercion from Article 2, paragraph 4's prescriptive sphere. *See* United Nations Conference on International Organization, Doc. 784, I/1/27, 6 U.N.C.I.O. Docs. 331, 334, 609 (April 25, 1945).

242. Schmitt*, supra* note 240, at 908.

243. *Id* at 913. The severity of a CNA attack may be considered along a sliding scale, which includes such factors as: severity, immediacy, directness, invasiveness, measurability, and presumptive legitimacy. *Id.*

244. G.A. Res. 41/38, U.N. Doc. A/RES/41/38 (Nov. 20, 1986).

245. Landler & Markoff, *supra* note 57.

heat of a cyber attack with a society's infrastructure falling down by the second? For such a legal regime to work, the doctrine of state responsibility for cyber attacks would have to be restructured and sufficiently defined.

A. State Responsibility for Cyber Attacks

At a time when the sovereign authority of states is breaking down in many areas,[246] state responsibility remains a bastion of international security. The speed and anonymity of cyber attacks makes it difficult to distinguish among "the actions of terrorists, criminals, and nation states."[247] Simultaneously, the instances of state-sponsored terrorist acts have increased since the end of the Cold War.[248] Proving state responsibility for such acts though is exceedingly difficult. As seen in the Estonian cyber attack, a sponsoring state may not cooperate in the investigation, apprehension, and extradition of those who committed criminal or terrorist acts on its behalf.[249] A nation-state might even be able to suborn "'civilian' cybercriminals and cyberterrorists to conduct their operations from within its borders" to hide the "purpose and origins of the state-sponsored attacks" behind a civilian front.[250] Consequently, should the cyber attack on Estonia be characterized as: (1) cybercrimes, with Russian Nashi hackers orchestrating a coup; (2) cyberterrorism by a group pursuing idiosyncratic ideological goals; or (3) cyberwarfare, a virtual sortie by Russian intelligence operatives?[251] Determining this distinction will also shape the appropriate response, including the extent of involvement by civilian law enforcement or the military.

Cyberterrorism consists of using computer technology to engage in terrorist activity, distinguishable from cybercrime since "crime is personal, while terror-

246. DAVID HELD, MODELS OF DEMOCRACY 293-97 (2006) (noting that globalization makes it harder for states to chart their own independent economic policies); *see generally* Robert B. REICH, THE WORK OF NATIONS: PREPARING OURSELVES FOR 21ST-CENTURY CAPITALISM (1991) (explaining that territorial boundaries have become increasingly irrelevant in the age of globalized production)

247. WHITE HOUSE, NATIONAL STRATEGY TO SECURE CYBERSPACE 19, 64 (2003), http://www.whitehouse.gov/pcipb/ ("Cyber attacks cross borders at light speed...."); Brenner, *supra* note 58.

248. *See, e.g.*, Christopher C. Joyner & Wayne P. Rothbaum, *Libya and the Aerial Incident at Lockerbie: What Lessons for International Extradition Law?*, 14 MICH. J. INT'L L. 222, 229 (1993) ("State-sponsored terrorism has emerged since the 1970s as a dangerous strain of international violence."). *But see* Susan W. Brenner & Anthony C. Crescenzi, *State-Sponsored Crime: The Futility of the Economic Espionage Act*, 28 HOUS. J. INT'L L. 389 (2006) (economic espionage as state-sponsored crime); Douglas R. Burgess, Jr., Hostis Humani Generi: *Piracy, Terrorism and a New International Law*, 13 U. MIAMI INT'L & COMP. L. Rev. 293, 302-03 (2006) (writing that sixteenth-century British government regarded piracy "in much the same way as state-sponsored terrorism is viewed today"). "State-sponsored crime" denotes state involvement in the commission of conventional crimes, such as the theft of intellectual property. Brenner, *supra* note 58, at 424.

249. *See, e.g.,* Russian-Estonian MLAT*; see also* Davis, *supra* note 1.

250. Brenner, *supra* note 58, at 424.

251. *See id.*

ism is political."[252] Classic conceptions of terrorism are discernible from warfare, which is not supposed to target civilians.[253] Yet, history is replete with examples from WWII to the genocide at Srebrenica of those bright lines blurring and ambiguity between terrorism and warfare increasing.[254] In IW, nation states use cyberspace for the same ends that they pursue through the use of conventional military force – "achieving advantages over a competing nation-state or preventing a competing nation-state from achieving advantages over them."[255] Boundaries are breaking down in the twenty-first century – "certain states generate crime, terrorism, and war, while individuals wage war in addition to committing crimes and carrying out acts of terrorism."[256] Yet it is too simple to pigeonhole an attack into the "cybercrime/cyberterrorism" framework if the attack did not come from a state actor.[257] Given the clandestine nature of cyberspace, states may easily incite civilian groups within their own borders to commit cyber attacks and then hide behind a (however sheer) veil of plausible deniability and thus escape accountability.

Yet, states remain the focus of containing IW as the Estonia incident and the Russian-Georgian armed conflict reveal more and more of a cyber dimension to international conflicts. Just before the recent Russian armed attack on Georgia, in particular, a cyber attack reportedly crippled the IT systems of the Georgian military and the Presidency, both of which were forced to resort to U.S. government and Google accounts while Estonian advisors helped to deflect the ongoing onslaught.[258] The Russian incursion into Georgia is a classic international armed conflict in which the state participants are bound by their respective international legal obligations. Thus, despite the breakdown of sovereignty in some areas, state responsibility and attribution remain at the core of a working international security system.

B. The Crucial Issue of Attribution

Attribution of a cyber attack to a state is a, if not *the*, key element in building a functioning regime. The laws of war require states attacking another state

252. *See id*.

253. *See* Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 75 U.N.T.S. 287, http://www.unhchr.ch/html/menu3/b/92.htm.

254. *See generally* BARD E. O'NEILL, INSURGENCY & TERRORISM: INSIDE MODERN REVOLUTIONARY WARFARE (2001) (arguing that insurgency may be the most prevalent type of armed conflict since the creation of organized political communities, and that modern insurgencies are increasingly blurring the line between guerilla and classic warfare).

255. Brenner, *supra* note 58.

256. *Id.*

257. *Id.*

258. *See, e.g.*, Stephanie Hoffman, *Russian Cyber Attacks Shut Down Russian Websites*, CHANNELWEB, Aug. 12, 2008, http://www.crn.com/security/210003057. *See also* Noah Shachtman, *Estonia, Google Help 'Cyberlocked' Georgia (Updated)*, WIRED, Aug. 11, 2008, http://blog.wired.com/defense/2008/08/civilge-the-geo.html.

to identify themselves, although this convention is apparently honored more in the breach than in compliance.[259] The International Law Commission ("ILC") Draft Articles elaborate on this basic law: "The conduct of any [s]tate organ shall be considered an act of that state under international law."[260] According to the ILC, an organ includes "any person or entity which has that status in accordance with the internal law of the [s]tate."[261] Such an official body cannot avoid responsibility by claiming that the actors exceeded their authority.[262] While this expands the pie of illegal state-sponsorship of terrorist activities, there is a need for a broader interpretation of the use of force to meet contemporary security challenges. Transnational cyberspace activities that affect the internal affairs of a state might breach general legal principles upholding respect for sovereignty and non-intervention.[263] A government-sponsored CNA involving transnational networks and telecommunications should trigger legal implications arising from the prohibitions in Article 2(4) if an attack rose to the level of an armed attack.[264] But as has been stated, cyber attacks of the type that we have seen and will likely persist are typically not at the public behest of an official state organ. As such, the international law doctrine of attribution is in fact an essential ground for regulating cyber attacks.

The relevant ILC section attributes the conduct of a person or group to a state under international law if "the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that [s]tate in carrying out the conduct."[265] Two standards, the doctrine of effective control and the doctrine of operational control, offer guidance on interpreting this provision. The effective control doctrine, originating in the ICJ *Nicaragua* case, recognizes a country's control over paramilitaries or other non-state actors only if the actors in question act in "complete dependence" on the state.[266] In contrast, the operational control doctrine, illustrated in the International Criminal Tribunal for the Former Yugoslavia *Tadic* case, held that where a state has a role in organizing and coordinating, in addition to providing support for a group, it has sufficient overall control so that the group's acts are attributable to the state.[267]

259. *See* Hague Convention No. III Relative to the Opening of Hostilities art. I, Oct. 18, 1907, 36 Stat. 2259, 2271, T.S. 598 (1907), *entered into force* 26 Jan. 1910, art. 1; Brenner, *supra* note 58.

260. Report of the International Law Commission to the General Assembly, (2001) II pt. 2 Y.B. Int'l L. Comm'n 40, U.N. Doc. A/CN.4/SER.A/2001/Add.1 (Part 2).

261. *Id.* at art. 4(2).

262. *Id.* at art. 7.

263. Examples of such accords include the 1970 Declaration on Principles in International Law and the 1965 Declaration on the Inadmissibility of Intervention in the Domestic Affairs of State.

264. Joyner & Lotrionte, *supra* note 29.

265. Report of the International Law Commission to the General Assembly, *supra* note 260, at art. 8.

266. Military and Paramilitary Activities (Nicar. v. U.S.) 1986 I.C.J. Rep. 14, 62 ¶ 110 (June 27).

267. Prosecutor v. Tadic, Case No. IT-94-1-I ICTY (Oct. 2, 1995).

The *Nicaragua* and *Tadic* standards differ over whether or not the state must be in direct control of operational planning. One argument is that the *Nicaragua* standard relates to the specific case of the trigger point for self-defense and attribution in relation to the use of force.[268] The ICJ has consistently used the more restrictive *Nicaragua* standard in its jurisprudence. For example, in the *Bosnian Genocide* decision,[269] the Court adopted *Nicaragua* in exculpating Serbia from the genocide at Srebrenica.[270] Yet given the secretiveness of CNAs, the *Tadic* standard of attribution should apply in cyber attacks. It is far too easy for governments to hide their IW operations under the *Nicaragua* standard. It should be enough to prove operational control of government in a CNA, rather than complete governmental control of a CNA. If the *Tadic* standard were used instead, it is possible that the Russian incitement behind the cyber attack on Estonia, if proven, would be sufficient for state attribution. A comprehensive legal regime in the future would grant Estonia adequate reparations for the attacks. If *Nicaragua* remains the dominant paradigm for determining state responsibility for cyber attacks, even a victim state of a worst-case scenario cyber attack may not achieve justice.

1. Proposal: Incitement to Genocide through Cyber Attack

Once attribution is satisfied, victims of the most horrific cyber attacks may be able to bring those responsible to justice under the rubric of incitement to genocide in the International Criminal Court or another appropriate forum. Some have already recognized that cyber attacks should be considered under the IHL framework, and that the perpetrators of a cyber attack should be guilty of war crimes.[271] It is only one logical step further that cyber attackers should be guilty of genocide in the most horrific cases, which concern the destruction of national groups. The Genocide Convention defines 'genocide' as the inchoate commission of any acts "to destroy, in whole or in part, a national, ethnical, racial or religious group."[272] The Convention does not specify the proportion of a popu-

268. Telephone Interview with Marc Weller, Director, European Centre for Minority Issues, in Kosovo (Mar. 14, 2008).

269. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Mont.), 2007 I.C.J. 1, 140 ¶ 391 (Feb. 26) [hereinafter "*Bosnian Genocide*"].

270. The Srebrenica Massacre was the July 1995 killing during the Bosnian War of an estimated 8,000 Bosnian males, ranging in age from young teens to the elderly, in the region of Srebrenica in Bosnia and Herzegovina by units of the Army of Republika Srpska under the command of General Ratko Mladić.

271. *See e.g.*, Reynolds, *supra* note 27, at 107.

272. Under Article II, genocide includes the following acts: (a) Killing members of the group; (b) Causing serious bodily or mental harm to members of the group; (c) Deliberately inflicting on the group conditions of life calculated to bring about its physical destruction in whole or in part; (d) Imposing measures intended to prevent births within the group; and (e) Forcibly transferring children of the group to another group. Convention on the Prevention and Punishment of the Crime of Geno-

lation that must be harmed for it to legally constitute genocide.[273] Nor does Article IX expressly impose an obligation on states to prevent or be held accountable for genocide.[274] However, the ICJ has recently established such an obligation in the *Bosnian Genocide* decision. For the first time in legal history, and after three other genocide cases, the ICJ unequivocally held in *Bosnian Genocide* that states can be found responsible for genocide, rather than simply obliged to punish the individual perpetrators.[275] A state using a weapon of mass destruction against a national group, such as what would occur in worst-case scenario cyber attack, thus could be liable for genocide if it had the requisite specific intent to destroy the group to which the victims belonged.[276] Trial Chamber I of the International Criminal Tribunal for Rwanda recently found three Rwandan media leaders guilty of incitement to genocide for publishing words and pictures that promoted ethnic atrocities.[277] Notably, it was private individuals, rather than an official state organ, that were found guilty of incitement to genocide. However, the ICJ affirmed that states, as a matter of law, can indeed be found guilty of genocide. Thus, the door is open for future litigation against states.

States that sponsor or launch cyber attacks designed to produce atrocities similar to Srebrenica or Rwanda should also be found liable for genocide. The Russian incitement to the cyber attack on Estonia is well documented, but since the attack did not result in widespread death and destruction, it does not constitute this most horrific of international crimes. Moreover, proving specific intent would not be a simple matter.[278] It should also be noted that determining liabili-

cide, Dec. 9, 1948, 78 U.N.T.S. 277, *entered into force* Jan. 12, 1951 [hereinafter Genocide Convention].

273. Article I of the Convention necessarily implies a prohibition against states themselves committing genocide, and that, if an organ of the state, or a person or group whose acts are attributable to the State, commits an act of genocide or a related act enumerated in Article III of the Convention, the state incurs international responsibility. *Bosnian Genocide, supra* note 269, at 166; Scott Shackelford, *Holding States Accountable for the Ultimate Human Rights Abuse: An Analysis of the ICJ Bosnian Genocide Decision*, 14 NO. 3 HUM. RTS. BRIEF 30 (2007).

274. Article 9 of the Genocide Convention states: "Disputes between the Contracting Parties relating to the interpretation, application or fulfillment of the present Convention, including those relating to the responsibility of a [s]tate for genocide or for any of the other acts enumerated in article III, shall be submitted to the International Court of Justice at the request of any of the parties to the dispute." Genocide Convention, *supra* note 272, art. 9.

275. *Bosnian Genocide*, *supra* note 269. *See also* Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Croatia v. Yugo.) 2002 I.C.J. Order 118 (Nov. 19); Legality of the Use of Force Case (Yugo. v. U.K.) 1999 I.C.J. 124, 132 (Order of 2 June 1999); Trial of Pakistani Prisoners of War (Pak. v. India), 1973 I.C.J. Rep. 328 (Dec. 15).

276. Statement to the Press by H.E. Judge Rosalyn Higgins, President of the International Court of Justice, Feb. 26, 2007.

277. Prosecutor v. Nahimana, Barayagwiza, & Ngeze, Case No. ICTR-99-52-T, Judgment and Sentence (Dec. 3, 2003); Catharine MacKinnon, *International Decision: Prosecutor v. Nahimana, Barayagwiza, & NGEZE*, 98 AM. J. Int'l L. 325, 328 (2004).

278. The ICJ imposed a specific intent standard requiring that the government in question specifically intended and took action to destroy a group of people. Given the nature of CNAs, such de-

ty of incitement to genocide remains muddied by divergent state practice and confused jurisprudence.[279] Yet given the costs of IW defense, a viable prevention regime is critical and must look beyond the genocide conventions. Nevertheless, using the Genocide Convention can be a vehicle to hold accountable perpetrator nations that experience genocide as a result of a massive and deadly state-sponsored IW campaign.

C. Cyber Attacks and Self-Defense

If the attack is real or the threat imminent, the victim state of a cyber attack, without any alternative means, may invoke self-defense to justify reasonable, necessary, and proportional measures to safeguard its security under Article 2(4) of the U.N. Charter if that attack reaches the level of an armed attack.[280] Coercion not involving armed force does not violate Article 2(4) or result in action under Article 39. It does not follow in these circumstances that "states may react unilaterally" pursuant to Article 51."[281] This section of the U.N. Charter seeks to ensure international peace and security.[282] Uses of force that destabilize the peace fall within Article 2(4)'s scope,[283] while threats of force, or economic coercion, do not fall under the gambit of Article 2(4) protection. Since a cyber attack is unlike a classic armed attack, the only way that a CNA could activate Article 2(4) is if such an attack rose to the level of an armed attack, that is, to the same effect as an attack by traditional military forces.

A valid exercise of self-defense would require irrefutable proof of aggression to satisfy state responsibility and to justify any sort of retaliation.[284] International law forbids forcible retaliation. Rather, the notion of preemptive or anticipatory self-defense permits a state to defend itself against imminent danger or an actual threat of armed attack. The legal caveat is that the threat must be real and credible and create an imminent need to act in accordance with the *Caroline* doctrine.[285] No strict prohibition precludes preemptive government use

finitive proof would be exceedingly difficult to locate. For a more general discussion of specific intent, *see* Shackelford, *supra* note 273.

279. William Schabas, *The Genocide Convention at Fifty*, SPECIAL REP. 41, UNITED STATES INST. OF PEACE, Jan. 7, 1999, http://www.usip.org/pubs/specialreports/sr990107.html.

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

281. Schmitt, *supra* note 240, at 929.

282. *Id*. at 900.

283. This is true given the "other manner" language in Article 2(4), which extends coverage to virtually all cases of uses of force not explicitly covered in the Charter. *See id.* at 900-01.

284. Joyner & Lotriante, *supra* note 29, at 83.

285. Letter from Daniel Webster to Lord Ashburton (Aug. 6, 1842), *reprinted in* 2 JOHN MOORE DIG. OF INT'L LAW 411-12 (1906). The Caroline incident involved a Canadian insurrection in 1837. After suffering defeated, the insurgents retreated into the U.S. where they recruited and planned further operations. In doing so, they used the *Caroline*. British troops crossed the border and destroyed the vessel. Britain justified the action on the grounds that the U.S. was not enforcing its laws along the frontier and that the action was a legitimate exercise of self-defense. *Id.* at 409-11.

of cyber-force as long as the perceived threat is demonstrated to be real and immediate, and the state adheres to the criteria of proportionality and necessity in applying computer-generated coercion.[286] Whether the international community would accept such a use of force depends entirely on context.[287] If a state were faced with a CNA that does not occur in conjunction with, or as a prelude to, conventional military force, the state would be allowed to respond with force in self-defense only if the CNA was intended to directly cause physical destruction or injury.[288]

In addition to Article 51 protections, the Security Council can also legally determine whether an attack would constitute a Chapter VII threat to international peace and security.[289] It has the power to call upon member states to apply "measures not involving the use of armed forces" including the "complete or partial interruption of . . . telegraphic, radio, or other means of communications."[290] Similarly, the DOD has stated that, "a computer network attack that caused widespread damage, economic disruption, and loss of life could well precipitate action by the Security Council."[291] The U.N. itself, however, was conspicuously silent regarding the attacks on Estonia.[292] The inaction regarding Estonia belies the continuing legal uncertainty of cyber attacks in the international system.

The DOD has argued that attacks that cannot be shown to be state-sponsored generally do not justify acts of self-defense in another nation's territory. Rather, a nation harmed by the private conduct of an individual acting within the territory of another nation should request the latter's government to stop such conduct.[293] However, the appropriate response when a state, and not a private individual, stands behind such an act remains unclear. In practice, these two scenarios may be hard to tell apart. As previously stated, it is not as if the cyber attacker is unlikely to be wearing the military uniform of the hostile government sponsor.[294]

One option to resolve the problem of self-defense in cyber attacks is through a graduated scheme that would shift the emphasis during a cyber attack away from customary law enforcement and counter-intelligence to "national de-

286. Joyner & Lotrionte, *supra* note 29, at 858-59.

287. Schmitt, *supra* note 240, at 903.

288. *Id*. at 929.

289. U.N. Charter art. 1, para. 2.

290. U.N. Charter art. 41 (According to the article, "these may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations.").

291. DOD, *Assessment, supra* note 30, at 15.

292. Tomas Ilves, President, Address to the 62d Session of the United Nations General Assembly, Sep. 25, 2007, http://www.un.org/webcast/ga/62/2007/pdfs/estonia-eng.pdf.

293. DOD, *Assessment, supra* note 30, at 22.

294. *See infra* sub-part c.

fense mode," as termed by the DOD.[295] Such a national defense strategy would need to be tempered by procedural and institutional safeguards to be legal, including: (a) a statement of general criteria establishing the options of national security responses; (b) identification of officials or agencies taking part in the decision to use force; and (c) procedures to be followed, including most importantly a graduated scheme systematizing different levels of cyber attacks with varied armed responses.[296] These criteria go beyond the stated DOD objectives. These procedures would help institute a test of reasonableness for self-defense, both subjective and objective given the greater stakes of a national security response making use of armed forces. Still, it is far from clear to what extent the world community will regard computer network attacks as "armed attacks" or "uses of force," which in turn clouds how doctrines of self-defense and countermeasures apply to such situations. Interpretations are ultimately likely to turn more on the consequences of such an attack. In the case of the Estonia cyber attack indicator, the international community would not have condoned an Estonian armed response then, however infeasible, against Russia. What is unclear is how that collective perspective would have changed if the cyber attack succeeded in bringing the entire country to a halt, capsizing the economy, and unleashing widespread unrest, riots, and possibly deaths. Should such an event rise to the level of an armed attack by classic military forces, it could open the door to an Article 2(4) right of self-defense that would go beyond a cyber counterattack.

D. The Intersections of International Humanitarian and Human Rights Law

In order to determine what combination of international humanitarian law and international human rights law should deal with cyber attacks that rise to the level of an armed attack, it is necessary to investigate the intersections between them. IHRL and IHL differ in formulation, structure, application, and enforcement.[297] While the distinctions between the two regimes are far from merely

295. *Id.* Michael Schmitt offers a useful conceptual chart of this normative framework: "(1) Is the technique employed in the CNA a use of armed force? It is if the attack is intended to directly cause physical damage to tangible objects or injury to human beings; (2) If it is not armed force, is the CNA nevertheless a use of force as contemplated in the U.N. Charter? It is if the nature of its consequences track those consequence commonalities which characterize armed force; (3) If the CNA is a use of force (armed or otherwise), is that force applied consistent with Chapter VII, the principle of self-defense, or operational code norms permitting its use in the attendant circumstances?; (a) If so, the operation is likely to be judged legitimate; (b) If not and the operation constitutes a use of armed force, the CNA will violate Article 2(4), as well as the customary international law prohibition on the use of force; (c) If not and the operation constitutes a use of force, but not armed force, the CNA will violate Article 2(4); (4) If the CNA does not rise to the level of the use of force, is there another prohibition in international law that would preclude its use? The most likely candidate, albeit not the only one, would be the prohibition on intervening in the affairs of other States." Schmitt, *supra* note 240, at 934-35.

296. DOD, *Assessment, supra* note 30, at 24.

297. *See, e.g.*, RENE PROVOST, AID AND INTERVENTION: INTERNATIONAL HUMAN RIGHTS AND

"semantic and contextual,"[298] there are areas of overlap. Since WWII, a growing international consensus has led to the establishment of numerous norms and standards in both human rights and humanitarian law aimed at better protecting human integrity.[299] Faced with the threat of a CNA, can these norms and standards meet distinctive societal needs during peace and war?

Criminal law enforcement and laws of war overlap when the conflict involves non-state actors and nations disagree on how to characterize the conflict. In turn, it is ambiguous whether human rights law, often associated with law enforcement, or humanitarian law, applicable during armed conflict, would apply.[300] Human rights conventions generally impose obligations on states, not individuals. However, if there is an applicable treaty or *erga omnes* customary law obligation, then states must protect these rights *at all times* or break their international legal obligations.[301]

In contrast, IHL was created to protect members of specific groups during limited types of armed conflicts including inter-state conflicts, national liberation armed conflicts, non-international armed conflicts, and internal armed conflicts.[302] The provisions of the 1907 Hague Convention, the 1949 Geneva Conventions, and the 1977 Additional Protocols protect the rights of identified subgroups such as combatants, POWs, and unarmed civilians.[303] Although IHRL and IHL were originally designed to apply in different circumstances, the two bodies of law may cross-fertilize as they relate to cyber attacks. It is wise, after all, to look to the "totality of opinions as to the legal character of a situation."[304] Both IHRL and IHL are rooted in respect for human values and the dignity of the human person--first principles that are applicable at all times and from which no derogation is permitted.[305] The point of departure for IHL is the need to balance humanity with military necessity during armed conflict.

HUMANITARIAN LAW 345 (2002); INT'L COMM. FOR THE RED CROSS, INTERNATIONAL HUMANITARIAN LAW AND INTERNATIONAL HUMAN RIGHTS LAW: SIMILARITIES AND DIFFERENCES (2003) [*hereinafter* Red Cross Report], http://www.icrc.org/Web/Eng/siteeng0.nsf/html/57JR8L.

298. PROVOST, *supra* note 297, at 343.

299. JACK DONNELLY, INTERNATIONAL HUMAN RIGHTS 4 (1998).

300. Watkin, *supra* note 155.

301. Treaties can have an important impact on the development of general custom. However, the treaty in question must be law making. According to the ICJ, that means that the rule in question must be of potentially general application, it must be sufficiently specific and must not be capable of attracting reservations. This principle was altered by the *Nicaragua* decision in which the key question was whether customary rules apply when both states are also subject to a treaty covering the same grounds. The Court decided that: "…there [are] no grounds for holding that when customary international law is comprised of rules identical to those of treaty law, the latter 'supervenes' the former." *Nicaragua*, *supra* note 167, at 95 ¶ 177.

302. Red Cross Report, *supra* note 297.

303. *Nicaragua*, *supra* note 167; *see also* BRENT G. FILBERT & ALAN G. KAUFMAN, NAVAL LAW 208 (1998).

304. PROVOST, *supra* note 297, at 341.

305. Watkin, *supra* note 155.

The nature and scale of violence in inter-state conflicts have a distinct impact on the control of force in IHL. A human-rights paradigm normally would address the internal use of force.[306] IHL, on the other hand, applies to both international and certain domestic armed conflicts. The relationship between the two is much more complex than a division of responsibilities.[307] For example, IHRL still applies during armed conflicts, as the ICJ decided in the *Nuclear Weapons Advisory Opinion*, whereas the IHL, as *lex specialis*, determines any arbitrary deprivation of the right to life.[308] Now an elaborate system of treaties on the law of war governs many aspects of the conduct of modern warfare, from permissible weapons to the treatment of POWs and non-combatants.[309] A gap remains in the literature with regards to how these treaties apply to IW.

1. Applying IHL to Cyber Attacks

For IHL to regulate contemporary armed conflict effectively, IHL rules on the use of deadly force should reflect the levels of violence and the nature of the threat posed to society. The special case of IW calls attention to several IHL norms: (1) the paramount distinction between combatants and non-combatants; (2) the distinction between civilian and military infrastructure; and (3) the prohibition against disproportionate attacks.

First, according to the distinction between combatants and non-combatants, cyber attackers forfeit the combatant privilege because they do not identify themselves as combatants. According to the combatant privilege under the Hague Conventions, only members of a nation's regular armed forces are entitled to use force against the enemy.[310] Combatants must follow laws of war, but failing to do so does not remove "combatant" status.[311] Under Protocol I, Article 44, "soldiers" who did not identify themselves as combatants by wearing a uniform or by carrying arms openly during or in preparation for the engagement most likely would be stripped of their combatant privilege by a tribunal.[312] Given the lack of markers indicating traditional combatant such as insignia in IW, would the Hague Conventions apply to captured cyber attackers? On the other hand, cyber attackers captured in the IHL context would be prosecuted as

306. *Id.*

307. *Id*.

308. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, 240 (Jul. 8).

309. The U.S., for example, is party to eighteen law-of-war treaties. For a survey, see U.S. Dep't of State, *Treaties in Force 2007*, http://www.state.gov/s/l/treaty/treaties/2007/index.htm.

310. Protocol Additional to the Geneva Conventions of Aug. 12, 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol I) art. 43, June 8, 1977, 1125 U.N.T.S. 609 [hereinafter Protocol I].

311. *Id.* at art. 44.

312. *Id.*

prisoners of war.[313] Specifically, cyber attackers disguise their attacks on state and civilian networks as innocent requests for information, in the same manner as a soldier who feigns civilian status would be prosecuted under Article 37(c).[314] Given the anonymity of cyber warfare, it may be possible to prosecute those accused under Protocol I, Article 37 provisions against perfidy.

Second, the scope of cyber attacks exceeds the IHL limitation on permissible objectives. The laws of war distinguish between military and civilian personnel, objects and installations, and limiting attacks to military objectives.[315] Article 52.2 of Protocol I states that, "military objectives are limited to objects that are effective contributions to military action and whose destruction offers a military advantage."[316] In other words, infrastructure that makes no direct contribution to the war effort remains immune from deliberate attack. In the Estonian case, everything from banks to broadcasters to government services and air-traffic control suffered attacks because the Internet was essential to the functioning of Estonian society.[317] This cyber attack failed to discriminate between military and civilian targets and thus would have run afoul of Protocol I, Article 51(4). The attacking state could argue, as NATO did during the Kosovo conflict when it attacked the Serbian TV towers that broadcasted propaganda to further genocide, that these facilities were used for command and control and thus were in fact military objectives.[318] Although this is a fine line, an indiscriminate, wholesale cyber attack is inconsistent with this ICTY precedent. Recognizing this facet of cyber attacks, the DOD has stated that targeting analysis must be conducted for CNAs just as it would be for attacks using traditional weapons.[319] In some cases it is not merely the result, but also the initial scope of an attack, that makes it indiscriminate. Taking the prohibition on non-combatant deaths one step further, IHL also forbids the disproportionate use of force as such attacks increase the risk of collateral damage and non-combatant casualties.[320]

Third, the law of war places much of the responsibility for collateral damage resulting from disproportionate attacks on defending forces that have failed

313. Soldiers captured during an international armed conflict are to be treated as prisoners of war under the third Geneva Convention. Geneva Convention Relative to the Treatment of Prisoners of War art. 5, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135.

314. "It is prohibited to kill, injure or capture an adversary by resort to perfidy. Acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence, shall constitute perfidy." Protocol I, *supra* note 310, art. 37.

315. *Id.* at art. 48.

316. *Id.* at art 52.2.

317. Davis, *supra* note 1.

318. Comm. Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia, Final Report to the Prosecutor, ¶¶ 71-79, 39 I.L.M. 1257, 1277 (June 13, 2000), http://www.un.org/icty/pressreal/nato061300.htm.

319. DOD, *Assessment*, *supra* note 30, at 8.

320. *See, e.g.,* W. J. Fenrick, *Targeting and Proportionality during the NATO Bombing Campaign against Yugoslavia* 12 EUR. J. INT'L L. 489 (2001).

to properly isolate military targets from noncombatants and civilian property.[321] Protocol I, Article 51 codifies the law of proportionality: "An attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects … which would be excessive in relation to the concrete and direct military advantage anticipated [is to be considered indiscriminate]."[322] This principle entails the balancing act between military advantage and the harm to civilians. Invoking the case study, the fact that Estonia did not attack any other armed force signifies that any aggressive act against the state would be inherently disproportionate. However, if an actual armed conflict had been waged, the entirely indiscriminate nature of the cyber attack against Estonia would have made it disproportionate and hence illegal under IHL and in violation of Protocol I.

Together, the IHL provisions discussed above point to a basis in existing IHL treaties for the use of limited, targeted, and proportionate cyber attacks in wartime.[323] In fact, according to the DOD, "the law of war is probably the single area of international law in which current legal obligations can be applied with the greatest confidence to information operations."[324] This fact is especially important given how many treaties lose effect during armed conflicts.[325] Collectively, these principles form the basis of non-degradable norms that should be applied with the greatest confidence to IW.

2. Information Warfare, International Criminal Law, and Human Rights Law

Efforts to control the power of the state and its impact on individual citizens spawned human rights norms "concerned with the organization of state power vis-à-vis the individual."[326] Increasingly, especially in the aftermath of the September 11, 2001 attacks, the use of force during armed conflict is being assessed through the perspective of human rights law.[327] This is relevant even though some authors have argued law enforcement as the modus operandi for

321. *Id*.

322. Protocol I, *supra* note 310, at art. 54.

323. For example, Articles 8 and 9 of the Hague Convention Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land 1907 state, "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 telegraph apparatus belonging to it or to companies or private individuals." Hague Convention V Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land arts. 8-9, Oct. 18, 1907, 36 Stat. 2310, T.S. 540, 1 Bevans 654.

324. DOD, *Assessment*, *supra* note 30, at 11, 14.

325. Consider the norm of reciprocity. This is correctly integral to IHL, but is far less important in human rights norms. States may not ignore human rights obligations simply because another state has done so. Provost, *supra* note 297, at 289.

326. Watkin, *supra* note 155, at 13.

327. *Id.* at 1.

dealing with most problems posed by criminals and hackers.[328] In addition, the argument also places ninety percent of the burden of preventing cyber attacks on the private sector.[329] To put such theory into practice may raise cost and upset coordination for businesses, international organizations, and governments. This is especially troubling given the checkered history of international efforts to criminalize cyber terrorism.[330]

The first efforts to coordinate efforts to prevent cyber crime and terrorism stretch back nearly three decades. At the urging of then Assistant U.S. Attorney General Telly Kossack, Interpol began harmonizing disparate national legislations on cyber crime for Interpol in 1981.[331] Progress had been slow until after the end of the Cold War. By 1997, the G8 established the Subgroup of High-Tech Crime, and adopted the "Ten Principles" in the combat against computer crime. The goal was to ensure that no criminal receives a "safe haven" anywhere in the world.[332] In a Justice and Home Affairs Communiqué on May 11, 2004, the G8 argued that all countries should improve laws that criminalize misuses of computer networks and that allow for quicker, more efficient cooperation on Internet-related investigations.[333]

Various other regional bodies and the U.N. have since enacted initiatives to deal with cyber attacks through harmonizing divergent national laws. The Council of Europe's Convention on Cybercrime, in force since July 1, 2004, provided another vehicle to harmonize divergent state cyber crime laws.[334] Meanwhile, the Asian-Pacific Economic Cooperation ("APEC") leaders have also agreed to strengthen their respective economies' ability to combat cyber crime by enacting domestic legislation consistent with the provisions of international legal instruments, including the Convention on Cyber Crime of 2001.[335] Similarly, the Organization of American States ("OAS") approved a resolution in April 2004 stating that member states should "evaluate the advisability of implementing the principles of the Council of Europe Convention on Cybercrime (2001); and consider the possibility of acceding to that convention."[336]

328. Cordesman & Cordesman, *supra* note 65, at 9.

329. *Id.*

330. *See generally* Susan W. Brenner & Marc D. Goodman, *In Defense of Cyberterrorism: An Argument for Anticipating Cyber-Attacks*, 2002 U. ILL. J.L.TECH. & POL'Y 1, 12-24, 27 (2002).

331. Stein Schjolberg, Chief Judge, Moss Ingrett Ct., Nor., Presentation at the 11th UN Criminal Cong.: Law Comes to Cyberspace, Workshop 6: Measures to Combat Computer-Related Crime (Apr. 18-25, 2007).

332. It should be noted that since then only one G8 member, Russia, has been accused of harboring cyber attackers (those from the Estonian attacks).

333. *G8 Justice and Home Affairs Communiqué*, ¶ 10, Washington DC (May 11, 2004), http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-1377540.

334. *See* Convention on Cybercrime, *supra* note 31.

335. *Id*.

336. Organization of American States [OAS], AG/RES. 2040 (XXXIV-O/04), § IV(8) (June 8, 2004), http://www.oas.org/juridico/english/cyber.htm.

Another subsequent UN General Assembly Resolution, adopted in 2000, concerned combating the criminal misuse of information technologies. This non-binding resolution provides that states should eliminate safe havens for criminals who misuse information technologies so as to "protect the confidentiality, integrity, and availability of data and computer systems."[337] Together, these regional initiatives and accords have made important progress in the fight to unify diverse national cyber criminal laws into the beginnings of a global regime regulating cyber criminals.

International efforts are also underway to integrate cyber attacks into leading international criminal treaties. The Rome Statute of the ICC, specifically Article 5, limits the jurisdiction to the most serious crimes of concern to the international community as a whole. These include the crimes of genocide, crimes against humanity, and war crimes. The Rome Conference recommended that a review conference pursuant to Article 123 of the Statute of the ICC consider such crimes with the view of their inclusion in the list within the jurisdiction of the Court.[338] States parties to the ICC should include cyber attacks and serious cybercrimes by amendment in 2009 in accordance with Articles 121 and 123 of the Rome Treaty, which created the ICC.[339] If this were to occur, the international community would no longer have to scramble from attack to attack, but instead rely on a multilateral response to cyber attacks already based on a preexisting international legal system. Nevertheless, even if this multilateral response were feasible, unique issues of balancing human rights, such as privacy concerns, would still need resolution at the level of nation-states.

One issue in human rights raised by IW defense is privacy. A patchwork of privacy protections could include the right to expect and enjoy physical privacy, privacy of personal information, privacy of communications and space, and freedom from surveillance. Insofar as IHRL focuses more on individual criminal conduct at all times, privacy and continuing innovation will only bring more challenges. Precisely because states and individual hackers can hide behind the privacy the Internet affords, regulating cyberspace also hazards on intruding on the privacy of innocents. Moreover, just as states can hide behind the anonymity of the Internet after launching a cyber attack, they also have an excuse to intrude on their citizens' privacy in the name of protecting them from cyber attacks.[340] Balancing national security interests with civil rights in this regard

337. G.A. Res. 55/63, U.N. Doc. A/RES/55/63 (Jan. 22, 2001), http://documents-dds-ny.un.org/doc/UNDOC/GEN/N00/563/17/pdf/N0056317.pdf?OpenElement.

338. United Nations Diplomatic Conference of Plenipotentiaries on the Establishment of an International Criminal Court, June 15-17, 1998, *Rome Statute of the International Criminal Court*, art. 123, U.N. Doc. A/CONF.183/9 (July 17, 1998), http://documents-dds-ny.un.org/doc/UNDOC/GEN/N98/281/44/img/N9828144.pdf?OpenElement.

339. *See* Convention on Cybercrime, *supra* note 31.

340. *See Cyber Attacks: The National Protection Plan and Its Privacy Implications: Hearing on S.R. 106-889 Before the Subcomm. on Tech., Terrorism and Gov. Info. of the S. Comm. on the Judiciary,* 106th Cong. 11 (2000), http://loc.gov/law/find/hearings/pdf/00076638986.pdf.

will be a challenge, and will likely get different legal treatments around the world.

In summary, state-sponsored cyber attacks can straddle the worlds of IHRL and IHL. Non-state actors that engage in international violence at the behest of states, regardless of whether it rises to the level of an armed conflict, do not fit within either paradigm. A threat of weapons of mass destruction by a transnational terrorist group may not be amenable to a human rights review approach, for example. Classifying IW may be difficult, but like most terrorist attacks, IW also has a tangible harm. Moreover, aggressive acts in cyberspace are not assessed by their consequences, but also by their intentions, such as inchoate crimes.[341] The difficulty lies in proving those intentions.

Similar to the debate surrounding IW, shifting counter-terrorism from a crime control to a conflict model raises concerns about displacing human rights norms as a primary legal constraint. Such a situation requires a compromise between individual civil and political rights, on the one hand, and economic and national security interests on the other.

VII.
SUMMARY OF THE PRESENT LEGAL REGIME AND A PROPOSAL FOR GOING FORWARD

Neither IHL, nor IHRL, or any of the other treaty systems or legal principles discussed in this Article serve as a panacea for state-sponsored IW. Yet the international community already faces situations in which cyber attacks are being sponsored by states more or less. In the case of the Estonian assault, for example, some available evidence hints at Russian involvement in inciting and abetting the cyber attack on Estonia. Even though that attack did not rise to the level of an armed attack required to activate IHL, sponsoring states should not be able to hide behind cyberspace to avoid liability. The fog of identity in cyberspace necessitates the creation of a legal regime that takes into account a level of uncertainty. Specifically, this requires a two-tiered system in international law for response to cyber attacks, a default state for peacetime and another triggered by an international armed conflict.

The capacity for existing treaty frameworks to form a useful legal regime to deal with cyber attacks that fall short of an armed attack may be illustrated by using the Estonian case study. The attack disrupted the basic functioning of the Estonian government, and thus endangered the "safety services" referred to in Article 35 of the ITU. If Russia were attributed blame for the cyber attack then,

341. The fact that IHRL is designed to function in peacetime, contains no rules governing the methods and means of warfare, and applies only to one party to a conflict led at least one human rights nongovernmental organization to look to IHL to provide a "methodological basis for dealing with the problematic issue of civilian casualties and to judge objectively the conduct of military operations by the responsive parties." Weller, *supra* note 268.

it would be in breach of the ITU Charter and Estonia could bring international pressure to bear for reparations under international law, although there is no mandatory enforcement mechanism available under this treaty. The Estonian government could also hold liable those companies most affected by cyber attacks if these companies were aware of the nefarious activity and did not adequately prepare for or respond to the threat, as the courts in the U.S. have done in the context of copyright infringement.[342] Similarly, Estonia, as a coastal state could invoke UNCLOS, which prohibits the staging of any attacks that interfere with the security or good order of a coastal state. Arguably, this Article 19 prohibition should also apply to Article 113 claims involving submarine cables.[343] This would mean that states could prosecute cyber attackers who sent subversive code through fiber-optic submarine cables to a coastal state, although UNCLOS does not apply directly to individuals. Doubtless code from several of the hundreds of DDOS attacks on Estonia traveled by way of submarine cable at some point in their global journey. This would also open up another route to reparations and possible sanctions from the Security Council under its Chapter VII authority to regulate breaches of international peace and security.[344] Finally, Estonia could use MLATs, extradition treaties, and potentially the ICC to bring those responsible to justice in the victim nation if the host nation is unwilling or unable to prosecute those responsible (as was the case with Russia after the Estonian cyber attack).[345] Together, these widely-adopted treaty provisions form the basis of a legal regime that both defines inappropriate conduct related to IW, and provides for reparations or other compensation to affected nations.

After a cyber attack rises to the level of an armed attack, an international security system is activated combining elements of IHL and IHRL.[346] Both regimes have much to offer in forming a final regulatory system. For example, it may be possible to graft IHL's proportionality principle onto IHRL. A framework that considers human rights alone is insufficient since it would not address the relative importance of critical infrastructure and people, or the proportionate assessment regarding the number of non-combatant casualties. Moreover, command responsibility is well established under IHL and commanders should apply the same IHL principles to computer attacks that they do to the use of

342. *See infra* sub-part V(B)(2).

343. UNCLOS, *supra* note 219, at arts. 19 & 113.

344. U.N. Charter, chap. VII, art. 52.

345. *See* Davis, *supra* note 1.

346. Given the degree of interaction between IHRL and IHL and their sharing of many functional principles, it may become more and more difficult to suggest that human rights bodies should not apply alongside principles of IHL during armed attacks. States, after all, do exercise internal governance during armed conflict. *See* Watkin, *supra* note 155, at 24. There is an ongoing tension between efforts to incorporate humanitarian standards into non-international armed conflicts and the view of states that such conflicts involve the legitimate suppression of criminal activity. *Id.* at 5. The challenge lies in separating incidents that are simply criminal in nature from those that form part of the armed conflict.

bombs and missiles.[347] Also, in controlling the use of force, IHRL seeks review of every use of lethal force by agents of the state, while IHL presumes that force will be used and humans intentionally killed. In practical terms, a human rights supervisory framework works to limit the development and use of a shoot-to-kill policy, whereas IHL is directed toward deploying how such a policy is implemented.[348]

To enable IHL to regulate contemporary armed conflict effectively, it must set forth realistic rules governing the use of deadly force that reflect the levels of violence and the nature of the threat posed to society. Armed conflict does not occur in isolation. Society will still have to be governed according to human rights norms. Incorporation of IHRL principles of accountability can enhance the regulation of the use of force during armed conflict.[349] "The Appeals Chamber's decision in *Tadic*, the Statute of the ICTR, and the Rome Statute of the ICC have recognized the need to extend the accountability process" under IHL to conflicts of all types,[350] as had the Inter-American Court of Human Rights in applying IHL to several cases. In *Abella*, for example, the IACHR relied on the "concerted nature of the hostile acts undertaken by the attackers, the direct involvement of governmental armed forces, and the nature and level of violence" in deciding to apply IHL.[351] The ECHR has reached a similar conclusion in *Ergi v. Turkey*.[352]

The dual track legal framework described above is applicable to CNAs whether they rise to the level of an armed attack or not. Yet the regime is by no means preferable to the adoption of a comprehensive treaty dealing exclusively with cyber security. A more comprehensive treaty should: (1) define when a CNA rises to the level of an armed conflict; (2) clarify which provisions apply during armed conflicts; and (3) provide for enforcement mechanisms. Several U.S. government agencies maintain that the most effective instruments in creating international law are bilateral and multilateral accords.[353] One example is

347. *See* Reynolds, *supra* note 27.

348. *See id.*

349. Watkin, *supra* note 155, at 34.

350. *Id.* at 23.

351. Abella v. Argentina, Case 11.137, Inter-Am. C.H.R., Report No. 55/97, OEA/SER.L/V/II. 98, doc. 6 rev. ¶ 155 (1997). *See also* ANTONIO A. CANÇADO TRINDADE, 1 TRATADO DE DIREITO INTERNACIONAL DOS DIREITOS HUMANOS 269-80 (Sergio Antonio Fabris ed., 1997) (examining the normative, interpretive and operative relationship between human rights, humanitarian, refugee law). The American Declaration had its genesis in the recognition that the atrocities of World War II had demonstrated the linkage between respect for human rights and peace, the threat to fundamental rights in times of war, and the need to develop protections independent of the reciprocal undertakings of states.

352. *See* Ergi v. Turkey, 1998-IV Eur. Ct. H.R. 1751, ¶ 79 (1998) (holding that the state is responsible not only when "there is significant evidence that misdirected fire from agents of the [s]tate has killed a civilian" but also where they fail to take "all feasible precautions [against] . . . incidental loss of civilian life" in running a security operation"").

353. *See* DOD, *Assessment, supra* note 30.

the Cyber Crime Pact Council of Europe of December 2000.[354] Another is the 2000 Proposal for an International Convention on Cyber Crime and Terrorism drafted at Stanford University ("Stanford Proposal").[355] The findings of the Stanford Proposal include several arguments for greater international cooperation in combating cyber attacks:

> Cyber criminals exploit weaknesses in the laws and enforcement practices of [s]tates, exposing all other [s]tates to dangers that are beyond their capacity unilaterally or bilaterally to respond. The speed and technical complexity of cyber activities requires prearranged, agreed procedures for cooperation in investigating and responding to threats and attacks.[356]

Article 12 of the Stanford Proposal argues for the creation of an international Agency for Information Infrastructure Protection ("AIIP"). The AIIP is intended to serve as a formal structure in which interested groups will cooperate between experts in countries around the world in developing standards and practices concerning cyber security. The structure of AIIP representation is inspired by treaties establishing the International Civil Aviation Organization and the International Telecommunication Union.[357] This would address the key concern of rapidly evolving CNAs. The new NATO Cybernetic Defense Center should serve as a model organization for such a body, potentially a World Cyber Emergency Response Center ("WCERC"), and would be similar to other commons management schemes such as the CLCS under UNCLOS. However, the Stanford Proposal excludes state conduct, addressing only conduct by individuals or groups.[358] This underscores the fact that most international cooperation dealing with international information operations law has emphasized the need to cooperate on international criminal efforts to catch cyber terrorists. Little to no effort has been made to determine an appropriate legal framework for state-sponsored cyber attacks. Such a framework would have to be well defined

354. *See* Convention on Cybercrime, *supra* note 31.

355. *See* Stanford Treaty Proposal, *supra* note 45.

356. *Id.*

357. The Stanford Proposal states that all state parties are represented in the AIIP Assembly, which would adopt objectives and policies consistent with the Convention, approve standards and practices for cooperation, and approve technical assistance programs, among other responsibilities. The AIIP Council, elected by the Assembly, would, among other duties, appoint committees to study particular problems and recommend measures to the Assembly. The Draft also provides for a Secretariat to perform administrative tasks. The AIIP would build upon and supplement, not attempt to modify or substitute for, private-sector activities. *See* Stanford Treaty Proposal, *supra* note 45.

358. Article 3 describes the conduct it covers, including: "interfering with the function of a cyber system, cyber trespass, tampering with authentication systems, interfering with data, trafficking in illegal cyber tools, using cyber systems to further offenses specified in certain other treaties and targeting critical infrastructures. State parties would agree to punish all the forms of conduct specified. Article 3 was drafted with the goal of securing speedy agreement among nations to adopt uniform definitions of offenses and commitments, despite having different network capabilities and political interests. Offenses related to more controversial issues, including protection of intellectual property and regulation of political, ethical or religious content, are therefore omitted. Implementation of treaty offenses will be effected in domestic law of signatories in accordance with Article 2." Stanford Treaty Proposal, *supra* note 45.

in an accord, as would an effective and mandatory enforcement mechanism such as binding international arbitration.

An international treaty on state-sponsored cyber attacks should use the effects principle to bypass concerns over regulating cyberspace, and provide for an international committee to preserve the commons and promote international cooperation and innovation. Each area of the international commons has lessons on how and how not to regulate cyberspace to best deter attacks. Cyberspace is not a classic CHM area, like the deep seabed, but given that so many characteristics are shared, the CHM analogy is useful. All commons regulated by the CHM share the need for international management of the commons territory, and the prohibition of weapons or military installations on that territory. The goal of this regulation is to preserve the commons, that is, in this case the generative Internet, for future generations. Yet cyber weapons cannot be outlawed, as they face the same concerns that the ICJ grappled with in the *Nuclear Weapons Advisory* Opinion. Outlawing the computer code used to launch cyber attacks outright would mean changing the fundamental generative nature of the Internet, turning PCs into information appliances. This would constitute an extreme negative impact on the private sector of the type that, as the UNCLOS saga has taught, should be avoided for the commons to prosper. Nor would such an option be feasible, unlike in the ATS or outer space, given the rapidly evolving nature of IT. What is needed instead is a standing international body, such as WCERC, which would have the power to investigate and partner with affected nations to respond to cyber attacks as they occur.[359]

After all, international law changes with events: "The life of the law has not been logic; it has been experience."[360] In this way, the cyber attack on Estonia and similar events have pushed the international community to recognize the necessity of acting swiftly to combat the proliferation of IW. There is evidence that at least some subset of countries, namely NATO, have begun international efforts aimed at increasing collaboration to prevent, investigate, and respond to attacks as they occur. Other nations, notably Russia and China, have already come forward with proposals to prohibit the use of IW in Twenty-first Century warfare. However, if information operations techniques are seen as just another new technology and not a grave threat to national security interests, it is unlikely that dramatic legal developments will occur.[361] Just as much of an impetus is the U.S.'s refusal to negotiate to prohibit these weapons in order to keep its technological edge in IT. It is essential for policymakers to consider cyber attacks as the revolutionary threat that they are to the security and welfare of citizens around the world for real and lasting progress to be made.

359. International support exists for curtailing IW. The U.S. should call Russia and China's potential bluff and begin work on an international treaty on IW.

360. DOD, *Assessment*, *supra* note 30, at 1-2.

361. *Id*.

VIII.
CONCLUSION

The ultimate form and function of an international regime for dealing with cyber attacks will depend largely on the international reaction to the particular circumstances at play. More likely than not, the international community will be more focused on the consequences of a computer network attack than on its mechanism. This does not put aside state responsibility, but places the primary focus of international attention on the scale and targeting of IW to decide whether or not the attack has reached the level of an armed attack actionable under international law. Then, the *Tadic* standard, as opposed to the *Nicaragua* standard, should decide attribution and state responsibility.

The international legal system is unlikely to form a coherent body of "information operations" law soon. The criteria used to distinguish normal cross-border data flows from cyber attacks needs to be clearer and more precise.[362] In some areas, such as the law of war, existing legal principles are adequate for a cyber attack that reaches the level of an armed attack. As far as active defense as self-defense, it is unclear how the international community will react. The main failings of relevant international treaties are that most do not specify how the frameworks are morphed or fall out entirely during an armed attack, and many treaties do not include any enforcement provisions. To the extent that cyber attacks are below the threshold of an armed attack, provisions of space law, nuclear non-proliferation, UNCLOS, and communications law, all have a role to play in crafting a functioning legal regime. Although the combination is an imperfect regime, the international community should use all the tools available to tackle the issue of cyber attacks. Nations are making use more and more of the weapons potential of cyberspace, increasing the likelihood of attack. The mission statement adopted by the U.S. Air Force in 2005 to "fight in air, space, and cyberspace" is a reminder of this reality.[363]

The best, most comprehensive approach to containing IW is a new international accord dealing with state-sponsored cyber attacks in international law, including the creation of a standing emergency response body along the lines of WCERT proposed above. The U.S. should welcome such a treaty regime. Without such an organization, the international community will lurch from case to case with the worry that the attack on Estonia was merely a step towards Net War Version 2.0. When IW reaches the scale of nuclear war, a new and distinct regime incorporating elements of existing international law is in order: otherwise nations risk systemic infrastructure crashes that not only will cripple societies, but also could shake the Information Age to its foundations.

362. Joyner & Lotrionte, *supra* note 29, at 50.

363. Mitch Gettle, *Air Force Releases New Mission Statement*, AIR FORCE PRINT NEWS, Dec. 8, 2005, http://www.af.mil/news/story.asp?storyID=123013440 (last visited Apr. 20, 2008).