July 14, 2008

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

Scott James Shackelford, *Stanford University*

FROM NUCLEAR WAR TO NET WAR: ANALOGIZING CYBER ATTACKS IN INTERNATIONAL LAW

by Scott J. Shackelford[1]

TABLE OF CONTENTS

ABSTRACT

On April 27, 2007, Estonia was attacked by a computer network causing widespread damage. It is currently unclear what legal rights a state has as a victim of a cyber attack. Even if Estonia could conclusively prove that it was Russia, for example, behind the March 2007 attack, could it respond with force or its own cyber attack? There

[1] Scott Shackelford is a J.D. candidate at Stanford Law School and a Ph.D candidate in international relations at the University of Cambridge.

is a paucity of literature dealing with these questions, as well as the ethical, humanitarian, and human rights implications of information warfare ("IW") on national and international security. Treatments of IW outside the orthodox international humanitarian law ("IHL") framework are nearly non-existent. This underscores the tension between classifying cyber attacks as merely criminal, or as a matter of state survival necessitating an exclusively national security approach.

This paper will advocate that the best way to ensure a comprehensive regime for cyber attacks is through a new international accord dealing exclusively with cyber security and its status in international law. But until such an accord becomes politically viable, the extent to which existing treaty systems deal with cyber attacks will be ascertained. Together, these treaties form a dual track approach to cyber attacks – one that is available for cyber attacks that do not rise to the level of an armed attack, and another that is activated once an armed attack occurs. To that end this paper will examine the most apt analogues in international law to form an appropriate legal regime for the various types of cyber attacks – whether it is humanitarian law (laws of war), human rights law (regulation of nation states behavior), or some novel combination of these and other treaty systems. In framing this regime, it will be argued that cyber attacks represent a threat to international peace and security as daunting and horrific as nuclear war. Yet the nuclear non-proliferation model is not a useful analogy since the technology necessary to conduct IW is already widespread in the international community. Instead, other analogies will be evoked including: communications and cyber law, space law, and the law of the sea, among others. The main failings of existing international treaties that touch on cyber law though are that most do not carry enforcement provisions. Nor do they specify how the frameworks are morphed or fall away entirely during an armed attack. Nevertheless, regardless of whether or not cyber attacks fall below the threshold of an armed attack these bodies of law have a role to play in forming an appropriate regime. The cyber attack on Estonia in March, 2007 will be used by way of a case study.

INTRODUCTION

On April 27, 2007, Estonia was attacked. Only four weeks into his position, Estonian Defense minister Jaak Aaviksoo was besieged by his aids. In a matter of hours, the online portals of Estonia's leading banks were brought down. All of the principal newspapers stopped functioning. Government communication was disrupted. An enemy had invaded and was assaulting dozens of targets across the country. This was not all accomplished though by a traditional nuclear, chemical, or biological weapon of mass destruction ("WMD"). Nor was it the result of a classical terrorist attack or an invading army. It was all done by a computer network.

Nevertheless, the effects of this assault were potentially just as disastrous as a conventional offensive on this, the most wired country in Europe, popularly known as "eStonia."[2] 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.[3] Estonians file their taxes online, and use their cell 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. Thus, in many ways this small Baltic nation is like a window into the future. Someday, "the rest of the world will be as wired as eStonia."[4] That is what made the cyber attack against Estonia all the more affective.

In a matter of days the cyber attacks brought down most critical websites, causing widespread social unrest and rioting leaving 150 people injured and one Russian national dead.[5] 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.[6] 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

---

[2] Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED MAGAZINE, Aug. 21, 2007 (detailing the assault on Estonia by a rouge computer network).
[3] *Estonia hit by 'Moscow cyber war'*, BBC NEWS, May 17, 2007.
[4] Davis, *supra* note 2.
[5] *Putin Warns Against Belittling War Effort*, RADIO FREE EUROPE, May 9, 2007. Available at: http://www.rferl.org/featuresarticle/2007/05/704c2d80-9c47-4151-ab76-b140457a85d3.html. Last visited: 4/20/2008.
[6] Davis, *supra* note 2 (Aaviksoo explains that the attacks "were aimed at the essential electronic infrastructure of the Republic of Estonia…All major commercial banks, telcoms, media outlets, and name servers — the phone books of the Internet — felt the impact, and this affected the majority of the Estonian population.").

alliance to attack the aggressor.[7] At the time, Russia was commonly thought to be behind the attacks. Regardless of who was actually to blame though, what is critical about this episode is that it was the first large-scale incident of a cyber assault on a state.[8] And it is 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. A dramatization of a large-scale cyber assault on the U.S. was popularized by the Hollywood blockbuster *Die Hard 4.0* during the summer of 2007. 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 wrought havoc in the financial services sector. If such a multifaceted cyber attack were coordinated professionally, it could destroy a nation's economy and leave much of its population without basic services, including electricity, water, sanitation, and even police and fire protection if the emergency bands similarly crashed. This luckily did not happen in Estonia. But if such an attack were to take place it would constitute an "electronic Pearl Harbor" that would destroy most of a nation's information infrastructure reminiscent of an electromagnetic pulse ("EMP") from a nuclear weapon causing massive amounts of destruction, dislocation and loss of life.[9] Ene Ergma, the Speaker of the Estonian Parliament who has a doctorate in nuclear physics, has made the comparison that "When I look at a nuclear explosion and the explosion that happened in our country

---

[7] North Atlantic Treaty art. 5, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243.
[8] Ian Traynor, *Russia accused of unleashing cyberwar to disable Estonia*, THE GUARDIAN, May 17, 2007.
[9] *Doomsday fears of terror cyber-attacks*, BBC NEWS, Oct. 11, 2001. Available at: http://news.bbc.co.uk/2/hi/science/nature/1593018.stm. Last visited: 4/18/2008.

in May, I see the same thing…Like nuclear radiation, cyberwar doesn't make you bleed, but it can destroy everything."[10]

Recognizing the scale of this threat, elements 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 as analogous to other conventional WMDs. Yet the international legal framework to deal with cyber attacks is severely under-developed. What scholarly attention that has been paid to the matter has mostly focused on cyber terrorism by private groups, rather than state-sponsored attacks. 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 keeping intact 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.

The technology-laden practice of modern IW, including responding to cyber attacks with armed force against information assets, raises a host of legal concerns. Among these fundamental issues are: (1) does cyber warfare represent a qualitative change in the meaning and nature of warfare?; (2) 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?; [11] and perhaps most importantly to the functioning of a useful legal regime (3) can a cyber

---

[10] Davis, *supra* note 2.

[11] Remarks by Prof. Helen Stacy. *Meeting of the Committee on Policy Consequences and Legal/Ethical Implications of Offensive Information Warfare*, Apr. 10-11, 2007. Stanford Univ., Lou Henry Hoover Building.

attack be a "use of force" as defined by Article 2(4) of the UN Charter?[12] If the answer to the final question is yes, would such an attack activate the Article 51 right of self-defense?[13] Critically, what are the standards of proof required to establish the origin of a cyber attack? The identity of the perpetrators is likely to be hidden as was the case in Estonia; there are no flags or tanks in a cyber attack. Is a pre-emptive cyber attack the same as a pre-emptive physical invasion? This will depend on the scale of the attack. But responding on an ad hoc case-by-case basis is fraught with difficulties. What level of civilian casualties is acceptable in a cyber attack, and should this be analyzed from an IHL or IHRL paradigm? How does this rubric change in wartime and peacetime? Should responses to domestic versus foreign cyber attacks differ? What is the appropriate role of law enforcement in juxtaposition with the defense establishment? How do theoretical concerns surrounding sovereignty interact with cyberspace? Thoughts on each of these questions will be provided throughout the paper.

There is a paucity of literature dealing with these issues as well as the ethical and human rights implications of IW on national security. Treatments of IW outside the orthodox IHL framework are nearly non-existent. This is strange since both IHL and IHRL are aimed at protecting the integrity of the human person, but take different approaches towards that end. IHL norms operate within the spatial and temporal constraint of an international armed conflict occurring between two or more states. The body of law assumes that harm will occur, and seeks only to limit the extent of harm.[14] In contrast, IHRL norms traditionally operate in peacetime during law enforcement investigations in which investigation is individual, and liability is criminal. Reciprocity

[12] UN Charter, Art. 2, para 4.
[13] UN Charter, Art. 51.
[14] The Hague and Geneva Conventions rely on this system of immediate reciprocity between states.

in the IHRL context, then, is far less important, whereas IHRL norms are continuous, meaning that the state is 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. Even if Estonia could conclusively prove that it was Russia behind the March 2007 attack, could it respond with force, or its own cyber attack? These questions underscore the tension between classifying cyber attacks as merely criminal, or a matter of national security.

The transnational nature of IW suggests that while international legal norms found in the contemporary U.N. Charter law are helpful, the existing treaty framework is insufficient for reaching acceptable solutions to this security dilemma.[15] As a result, two options exist – create a new treaty system from whole cloth, or adapt current treaty regimes. This paper will advocate that the best way to ensure a comprehensive regime is through a new international accord dealing exclusively with cyber security and its status in international law. A proposal for such an organization is laid out in part VI, but in brief it 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. However, the U.S. and other advanced nations are on record as opposing such a new treaty at this time. Thus until such an accord becomes politically viable, the extent to which existing treaty systems deal with cyber attacks will be ascertained. To that end this paper will examine the most apt analogue in international law to form an appropriate legal regime for cyber attacks – whether it is humanitarian law

[15] Christopher C. Joyner & Catherine Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework*, 12 Nov. 5 EJIL 835, 865 (2001) (arguing that clearer rules are needed for what self defense responses are permissible to cyber attacks and how international institutions might facilitate the attainment of these objectives.).

(laws of war), human rights law (regulation of nation states behavior), or some novel combination of these and other treaties. In framing this regime, it will be argued that cyber attacks represent a threat to international peace and security as daunting and horrific as nuclear war. Yet the nuclear non-proliferation model is not a useful analogy since the technology necessary to conduct IW is already widespread in the international community.

Consequently, this paper will analyze existing international treaty systems to determine the extent to which such regimes are applicable to investigating and prosecuting cyber attacks until such time as a new treaty system comes online. These other analogies including communications and cyber law, space law, and the law of the sea among others 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 were a coastal state; (4) applicable MALT, extradition treaties, and SOFAs; and (5) the potential for Chapter VII United Nations Security Council resolutions. But this regime is imperfect. The main failing of these existing international treaties that relate to cyber law are that most do not specify how the frameworks are morphed or fall away entirely during an armed attack. Many critically also do not include enforcement mechanisms such as mandatory reparations in the event of breach. Nevertheless, regardless of whether or not cyber attacks fall below the threshold of an armed attack these bodies of

law have a role to play in forming an appropriate regime. The cyber attack on Estonia in March, 2007 will be used by way of a case study throughout.

I. DEFINING INFORMATION WARFARE AND THE THREAT OF CYBER ATTACKS

The recent cyber attack on Estonia has fed the already significant 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."[16] When and if a modern state's networked information infrastructure crashes, an Information Age society could be paralyzed or even crash. The pervasively destructive potential of cyber-based IW presents new international military implications and invites new analytical considerations of where IW fits into the larger body of contemporary international legal rules pertaining to the use of force.[17]

Definitions and conceptions of IW are as numerous as they are complex, but generally entail preserving one's own information and information system while exploiting, disrupting, or denying the use of an adversary's.[18] IW itself is a generic term that refers to a hostile attack by one nation or hostile party against the important information technology ("IT") systems and networks of another (as compared to a criminal or terrorist attack). Secondarily, IW refers to actions taken to defend IT systems

[16] Joyner, *supra* note 15 at 858.
[17] *Id.*
[18] Such a conception suggests the possibility that IHL could indeed be stretched to cover cyber law.

and networks.[19] IW conducted against any modern society replete with information technology such as the U.S., either by terrorists[20] or a hostile nation, is a matter of national concern. This is due to the well-known dependence of many critical sectors of contemporary economies as well as critical national infrastructure on information systems and networks.[21]

IT today is ubiquitous and is essential to virtually the United State's entire infrastructure including dams, nuclear power plants, air-traffic control, communications, and financial institutions.[22] 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.[23] 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 simultaneously against unwanted

---

[19] Herbert Lin, *Policy Consequences and Legal/Ethical Implications of Offensive Information Operations and Cyberattack*, COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD, NATIONAL ACADEMIES, Apr. 4, 2007.

[20] Similar to the difficulty involved in defining information warfare, terrorism too is a multi-faceted concept. For purposes of this paper though, terrorism will be defined in terms of 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 campaign designed to illicit widespread disruptions and loss of public confidence in the ability of government to effectively function is also high impact. *Information Technology for Counterterrorism*, NATIONAL RESEARCH COUNCIL OF THE NATIONAL ACADEMIES, Apr. 9, 2007.

[21] *See Information Technology for Counterterrorism*, CSTB/NATIONAL RESEARCH COUNCIL (2003); *Cybersecurity Today and Tomorrow: Pay Now or Pay Later*, CTSB/NATIONAL RESEARCH COUNCIL (2002).

[22] IT has four major elements: (1) the Internet; (2) the conventional telecommunications infrastructure; (3) embedded/real-time computing; and (4) dedicate computing devices. The ways in which IT can be damaged falls into three categories: (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). *Id.*

[23] Joyner, *supra* note 15 at 865.

intruders. An analogy to locating a cyber attacker amidst all the normal transborder 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. Or instead of a single person, being alert to more Polish citizens than normal, though it is unclear exactly why they are there, if they are even 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.[24]

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

The scale and importance of IW both as an offensive weapon and defensive quagmire is highlighted by the President's Commission on Critical Infrastructure Protection. The report noted that in 2002, 19 million individuals had the knowledge with which to launch cyber-attacks.[25] Modern technology has made the tools of IW cheap, readily available, and easily obtainable.[26] 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

---

[24] *Computers at Risk: Safe Computing in the Information Age*, NATIONAL RESEARCH COUNCIL, 1991.
[25] *President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructure* A-48, 49 (Oct. 1997).
[26] The following is a list of common IW weapons: *Sniffer* – executed from a remote site by an intruder that would allow the intruder to retrieve user IDs and passwords or other information; *Trojan Horse* – 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 until a trigger condition causes it to activate and destroy the host computer's files. It can be hidden within a Trojan horse; *Video-morphing* – makes broadcasts indistinguishable from normal transborder data flows (a potential violation of the perfidy doctrine); *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 email communications systems preventing field communications; *IP spoofing* – fabricates messages whereby an enemy masquerades as an authorized command authority. Joyner, *supra* note 15.

matter.[27] Interpol has estimated that there are as many as 30,000 websites that provided automated hacking tools and software downloads. In 2000, a total of 22,144 attacks were detected on Defense Department networks, up from 5,844 in 1998.[28] Worldwide aggregate damage from these attacks is now measured in billions of U.S. dollars annually.[29] Problems of protecting the information technology infrastructure in many Western states are compounded by the fact that much of it is owned by the private sector such that the government can generally play a limited role. Consequently IW has great potential for the proliferation of asymmetric warfare.[30]

That is not to say that the great powers are not also developing IW to supplement their offensive capabilities. One-hundred-twenty nations have either already or are currently in the process of establishing IW competence, including Russia and China.[31] At least one press report has indicated a Presidential National Security Directive, NSPD 16, issued in July 2002 directed the U.S. to examine potential cyber attacks against enemy computer networks.[32] The Department of Defense ("DOD") has acknowledged this as a possible instrument of national security policy.[33] PDD-63 calls for a national effort to ensure the security of increasingly vulnerable and interconnected infrastructures in the United States, and creates the National Infrastructure Protection Center ("NIPC") under

---

[27] Joyner, *supra* note 15.
[28] *Hacking of Pentagon Persists*, WASHINGTON POST, Aug. 9, 2000.
[29] A Proposal for an International Convention on Cyber Crime and Terrorism, Stanford University, Aug. 2000.
[30] 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 (1992) (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.).
[31] Joyner, *supra* note 15.
[32] Bradley Graham, *Bush Orders Guidelines for Cyber-Warfare*, WASHINGTON POST, Feb. 7, 2003 at A1.
[33] *An Assessment of International Legal Issues in Information Operations*, 2nd edition, DOD, OGC, Nov. 1999.

the Federal Bureau of Investigation.[34] Funding has gone up from $1.14b in 1998 to $2.03b in FY2001 for intelligence and law enforcement efforts against cyber-attacks.[35]

Among its myriad applications, IT has a major role to play in the prevention, detection, and mitigation of cyber attacks. In essence, the United States' IT predominance is both a target and a weapon. Counterterrorist IW thus seeks to reduce the probability and scope of attacks against valued IT targets.[36] A passive defense against IW will not work, since even a single vulnerability given enough "free" attempts will compromise the system.[37] Defensive information technologies make the determination of an enemy's assets more difficult, thus complicating the task of setting up adequate defensive strategies.[38] Therefore, an active defense is paramount in which the attacker is forced to pay a price for targeting a system. Does such a philosophy of active defense, though, mean that self-defense against cyber attacks is justified – 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.

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

The Estonian public and private sector was the subject of a prolonged IW campaign beginning on April 27, 2007 and running for a period of several weeks.[39] The

---

[34] Joyner, *supra* note 15.
[35] Anthony H. Cordesman, *Defending America – Redefining the Conceptual Borders of Homeland Defense*, CSIS PUBLICATIONS, Feb. 14, 2001.
[36] There are several three primary modes of an IT attack: (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); (3) a trusted insider may be compromised. *Id.*
[37] Lin, *supra* note 18.
[38] Vizard, *War.com: A Hacker Attack Against NATO Uncovers a Secret War in Cyberspace*, POPULAR SCIENCE, July 1, 1999.
[39] The timeline of the attacks on Estonia was as follows. On April 26-27, the day of the government's decision to relocate the Soviet-era statue, the web sites of Parliament, the president and the prime minister are hit by a flood of junk messages and are shutdown. On April 30, several daily newspaper websites are brought down and a high-level meeting takes place with plans to protect vital services such as online

primary weapon deployed against the state included "distributed denial of service" ("DDOS") attacks, in which a target site is bombarded with so many bogus requests for information that it crashes.[40] Data from Arbor Networks Active Threat Level Analysis System shows that there were at least 128 unique DDOS attacks targeting internet protocols within Estonia.[41] Internet traffic increased from 20,000 packets to more than 4 million packets per second.[42] The attacks lasted from anywhere between one to 10 hours, and originated in as diverse of countries as Egypt, Peru, and Russia.

The cyber attack on Estonia is not the first time that DDOS attacks have been used against a country. The "Apolo Ohno" controversy at the 2002 Salt Lake City Olympics resulted in several U.S.-based servers being hit from machines that appeared to be based in South Korea.[43] Another episode involved the so-called "Titan Rain" series of cyber attacks on U.S. computer systems ongoing since 2003. These attacks were believed by the SANS Institute, a computer security training company, to be Chinese in

---

banking. On May 2, internet service providers from around the world succeed in blocking most of the incoming malicious data. On May 5, the Estonian government announces that the attacks originated in Russia. On Victory Day, May 9, botnet attacks begin which succeed in shutting down Estonia's largest bank's online portal leading to losses of more than $1m. In one case, the attackers sent a single huge burst of data to measure the capacity of the network. Then, hours later, data from multiple sources flowed into the system, rapidly reaching the upper limit of the routers. May 18 saw the last major wave of attacks, though small-scale assaults continued for several weeks. Mark Lander & John Markoff, *Digital Fears Emerge after Data Siege in Estonia*, N. Y. TIMES, May 29, 2007.

[40] *A Cyber Riot*, THE ECONOMIST, May 10, 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. Susan Brenner, *At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare*, 97 J. CRIM. L. & CRIMINOLOGY 379 (2007).

[41] Sean Kerner, *Estonia Under Russian Cyber Attack?*, SECURITY, May 18, 2007.

[42] 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 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. Definition from Whatis.com, available at: http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212736,00.html. Last visited: 4/18/2008.

[43] In 2002 at the Salt Lake City Games, Ohno won the gold medal in the 1,500-meter speed-skating race after South Korean Kim Dong-Sung was disqualified; soon after, several United States-based servers were hit with a DDOS. Robert Vamosi, *Cyberattack in Estonia – what it really means*, CNETNEWS.COM, May 29, 2007.

origin and were the result of military hackers trying to garner information on U.S. defense systems.[44] While the so-called "Solar Sunrise" attack involved a 1998 breach of the DOD computer systems, hidden through United Arab Emirates accounts. Yet it was not the UAE behind the attacks, but an Israeli teenager and two high school students from Cloverdale, California.[45] During the Kosovo Crisis, three 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 myriad U.S. state-sponsored efforts to disrupt Milosevic's command and control.[46] Later the "Moonlight Maze" attacks of 2001became 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.[47] But no country has ever before experienced a cyber attack on the scale of the 2007 assault on Estonia.

a. *Timeline of Estonian Cyber Attack*

The first full-scale cyber attack on a state broke amidst a furious row between Estonia and Russia over the removal of a Soviet-era statue and war graves from the

---

[44] B. Graham, *Hackers Attack Via Chinese Web Sites,* WASHINGTON POST, Aug. 25, 2005.

[45] Solar Sunrise was a series of DOD computer networks attacks which occurred from 1-26 February 1998. The attack pattern was indicative of a preparation for a follow-on attack on the DII. DOD unclassified networked computers were attacked using a well-known operating system vulnerability. The attackers followed the same attack profile: (a) probing to determine if the vulnerability exists, (b) exploiting the vulnerability, (c) implanting a program (sniffer) to gather data, and (d) returning 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. Porter Goss, *An Introduction to the Impact of Information Technology on National Security*, 9 DUKE J. OF COMP. & INT'L L. 391 (1999).

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

[47] Elinor Abreu, *Epic cyberattack reveals cracks in US defense*, CNN, May 10, 2001. Joyner, *supra* note 15.

center of the capital city, Tallinn.[48] Thousands of ethnic Russians Estonian rioted over the removal of what they view as a cherished reminder of wartime sacrifice.[49] The majority of Estonians though viewed the statute as a symbol of a hated foreign occupation. The majority of Russians did not. In Moscow, a Kremlin-youth movement surrounded and attacked the Estonian embassy prompting protests from the U.S., NATO, and the E.U. 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-fascist student group that has since grown to more than 100,000 members.[50] Feeling the Western pressure and following a deal brokered by Germany, the blockade soon ended. 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 though concentrated on shutting the sites down outright. By May 9th, when Russia and its allies commemorate 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.[51] 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. Mission-critical computers, including all telephone exchanges, were also

---

[48] 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. Davis, *supra* note 2.
[49] Economist, *supra* note 40.
[50] It is commonly thought that the group was formed as a reaction to the student protests leading to Ukraine's Orange Revolution in 2004. The official group website is: http://nashi.su/. Last visited: 4/18/2008.
[51] *Id.*

targeted. Estonia was very near a complete digital collapse on May 10th that would have shut off many vital services and caused massive, widespread social disruptions. Luckily Estonia's Cyber Emergecy Response Team ("ECERT") prevailed and Estonia avoided the worst case scenario that many feared all too likely. 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 "infblockade." "This may well turn out to be a watershed in terms of widespread awareness of the vulnerability of modern society," said Linton Wells II, the principal Deputy Assistant Secretary of Defense for networks and information integration at the Pentagon after the attack.[52] But who was to blame, and what can or should be done about it?

b. ***Determining Responsibility for the Estonian Cyber Attack***

Determining who was responsible 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 ran by Nashi su and other similar organizations. Yet it is exceedingly difficult to prove from where these attacks originated. Thousands of attacks came from untraceable private computers around the world. Most of these though were "script kiddies" who were goaded into attacking Estonian websites in Russian language chat rooms in which detailed instructions on how to launch botnet attacks were posted.[53] This is the equivalent of an army recruitment pitch complete with marching

---

[52] Shaun Waterman, *Who was behind Estonia's cyber attack?*, WORLD PEACE HERALD, Jun. 11, 2007. Available at: http://wpherald.com/articles/5127/1/Analysis-Who-was-behind-Estonias-cyber-attack/Crude-attack-unlikely-to-be-state-sponsored.html. Last visited: 01/28/2008.

[53] Botnet is a jargon term for a collection of software robots, or bots, which run autonomously and automatically on groups of zombie computers controlled remotely.

orders.[54] The ground troops were individuals using ping attacks; the air force was botnets; and the Special Forces were hackers using DDOS attacks. 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."[55]

The Russian government has offered no cooperation to Estonia in tracking down the true source of these botnets.[56] In many ways, the internet is the perfect platform for plausible deniability. An Estonian criminal investigation has been opened into the attacks under felonies of computer sabotage and interference with the working of a computer network, each punishable by up to three years in prison. Since many alleged hackers were Russian, Estonia submitted a request for bilateral investigation under the Mutual Legal Assistance Treaty ("MALT") between Estonia and Russia. Despite earlier promises of assistance though, the Russian Supreme Procurature refused assistance to Estonia under the treaty. This episode demonstrates the weaknesses of MALTs 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. Ultimately the only conviction from the cyber attack was on

---

[54] Davis, *surpa* note 2.

[55] This was not the first time that Russia had been accused of orchestrating IW. In fact, just a few weeks 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 shut down the opposition websites just as government authorities announced a change in venue for an upcoming opposition rally. With his site down, Kasparov had difficulty informing his followers of the change, and when they massed at the originally announced location, he was arrested for leading an illegal rally. Davis, *supra* note 2.

[56] Botnets are typically used for mass spam distribution, accounting for roughly half of the world's daily email flows. BBC News, *supra* note 3.

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.[57]

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 Russian security agencies directly.[58] In the report Mike Witt, deputy director of the U.S. Cyber Emergency Response Team ("USCERT"), surmised that botnets utilizing slave computers known as "zombies" had been operated by unknowing individuals, many of which in this case were in the U.S., and lacked the sophistication of the major powers. USCERT is the element within the Department of Homeland Security that "coordinates defense against and responses to cyber attacks across the nation."[59] In this instance, USCERT worked with the Forum of Incident Response and Security Teams to coordinate the global response to the attacks, such as it was. In contrast a well-known Russian hacker SpORaw believes that the most efficient online attacks on Estonia could not have been carried out without the blessing of the Russian authorities. He and others have argued that the hackers apparently acted under "recommendations" from parties in higher positions, as demonstrated with the chat room postings[60] and by the fact that on at least one Estonian site attackers replaced the homepage with the phrase "Hacked from

---

[57] Jeremy Kirk, *Student fined for attack against Estonian Web site*, IDG NEWS SERVICE, Jan. 24, 2008 (reporting that a 20-year-old Estonian student has been fined $1,642 for launching a cyber attack that crippled the websites of banks, schools, and government agencies).
[58] Waterman, *supra* note 52.
[59] US-CERT website: http://www.us-cert.gov/aboutus.html. Last visited: 01/28/2008.
[60] *Commissar of Nashi says he waged cyber attack on Estonian government sites,* SWISS BALTIC CHAMBER OF COMMERCE IN LITHUANIA NEWS, Jun. 6, 2007. Available at: http://www.sbcc-chamber.com/index.php?lng=en&page_id=60&news_id=888. Last visited: 01/28/2008.

Russia."[61] It is not the goal of this paper to determine whether the Estonian cyber attacks were in fact state-sponsored. Rather, an analysis of these attacks is meant to highlight the types of issues that arise when considering how best to form a legal regime to deal with cyber attacks going forward. These include 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 Attacks on Estonia*

What was a near disastrous attack for Estonia has been brushed off by U.S. officials, such as the former chief scientist of the Defense Advanced Research Project Agency ("DARPA"), who likened the attacks to "more of a riot than an attack."[62] That is not to say that the U.S. is unconcerned about cyber attacks, indeed quite the opposite is true. It makes little sense for an opponent to challenge the U.S. symmetrically. More likely avenues of challenge are asymmetric ones that exploit potential U.S. vulnerabilities, such as the civilian information infrastructure.[63] Defense assessments have laid out myriad challenges including interoperability, information systems security, and the culture of the intelligence community itself. The rate at which information systems are being relied on outstrips the rate at which they are being protected. The time needed to develop and deploy effective defenses in cyberspace is much longer than the time required to develop and mount an attack. At the same time, the DOD is prohibited by law and national policy from retaliating against cyber attacks if the goal was not the deterrence of future attacks. This gap is growing wider. In other words, cyber attack is

---

[61] Davis, *supra* note 2.

[62] This differential based on the IW capabilities of governments underscores the danger of anticipatory self-defense and a reactive legal regime to deal with cyber attacks. Shaun Waterman, *Who cyber smacked Estonia?*, UNITED PRESS INTERNATIONAL, Jun. 11, 2007.

[63] Steven Lambakis, et al., *Understanding 'Asymmetric' Threats to the United States*, NATIONAL INSTITUTE FOR PUBLIC POLICY, Sep. 2002 (analyzing asymmetric warfare and taking the position that the concept may be defined as different and challenging threats mired in legal and political constraints and vulnerabilities to new and old threats that are designed to offset U.S. strengths).

far easier than cyber defense, and the U.S., like Estonia and all countries in the Information Age, is right to be concerned about the continuing proliferation of these attacks.

In deciding how Estonia, and NATO, ought to respond to these cyber attacks the search for analogies is paramount given that cyber attacks are an unprecedented method of warfare. Some have surmised that the cyber attacks, to the extent that they were incited by Russia, amount to a test for NATO on its defenses to IW.[64] If this is the case, then NATO failed. Two NATO specialists were dispatched to Tallinn but little else was or could have been done given that so much of the internet is run by the private sector and international organizations. There are signs though 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.[65] Other proposals include the development of redundant networks of backup servers. Dealing with cyber attacks has never been in NATO's mandate, but if the increasing number and scale of cyber attacks is any indication, it soon could be integral to NATO's mission. This is especially true as Rein Lang, Estonia's justice minister, has complained that "international law is of little to no help" in dealing with cyber attacks.[66]

---

[64] Davis, *supra* note 2.
[65] *Bush, llves eye tougher tack on cybercrime*, AFP NEWS, Jun. 25, 2007.
[66] *Id.*

III. 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.[67] Two options exist. First, the international community can accept that cyberspace is an arena over which nations can and should exercise sovereignty through the effects doctrine. Second, the international community could determine that cyberspace is an information commons over which no state may claim jurisdiction.[68] 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 principle.

a. *Option 1: Regulating Cyberspace through the Effects Principle*

The general principle of sovereignty is fundamental to international law and relations, but not as directly to information technology.[69] As a practical matter though,

---

[67] Rosenau (1992) identifies six pillars that have traditionally upheld the autonomous state system: 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. JAMES N ROSENAU, GOVERNANCE WITHOUT GOVERNMENT: ORDER AND CHANGE IN WORLD POLITICS 1-29, 58-101 (1992).

[68] *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).

[69] Since Aristotelian antiquity, the term "sovereignty" has denoted a multitude of meanings dependent upon context, one's perspective and objectives. W. Reisman, *Sovereignty and Human Rights in Contemporary International Law*, 84 No. 4 AJIL 866 (Oct. 1990). First codified with the 1648 Treaty of Westphalia that ended the Thirty Years War, sovereignty became vested in the absolute monarch whose authority rested on divine mandate and history, but not the will of the people. S. Korff, *The Problem of Sovereignty*, 17 No. 3 THE AM. POL. SCIENCE REV. 404 (Aug., 1923). The 128 clauses of Westphalia that gave birth to this concept include, among much else, the principle of the sovereign states' monopoly on coercive force as well as the principles of nonintervention in internal affairs, consent as the basis of obligation to comply with international laws, and diplomatic immunity. *Id.* Taken together, these nascent international law provisions gave birth to the modern notion of territoriality. As the decades multiplied into centuries, sovereignty transitioned from an absolute right of monarchs to the supreme authority of states, eventually becoming established as "Westphalian sovereignty" that has to a large part since defined international relations. J. Jackson, *Sovereignty-Modern: A New Approach to an Outdated Concept*, 97 No.4 AJIL 782, 785 (Oct., 2003).

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. This principle is defined in the American *Restatement (Third) of Foreign Relations Law* in that "[i]nternational law recognizes that a nation has the ability to provide for rules of law with respect to conduct outside its territory that has or is intended to have substantial effect within its territory."[70] But cyberspace is not a normal arena over which states may exercise such control. It is contrary to international law, for example, if a nation were to destroy suspect shipping in international waters based on groundless suspicions. 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. Together, these regions constitute the sole exceptions to the system of Westphalian sovereignty that has long dominated international relations.[71] In the international commons, all of humanity is the sovereign under the Common Heritage of Mankind ("CHM") principle.[72] To the extent that cyberspace is a commons, though, it is one facing unique challenges and thus requiring exceptional regulatory solutions.[73]

---

[70] *See* 35 Sec. 301(9) cf. with *Restatement*, *supra* note 16, para. 402(1)(c).

[71] Although criticized, Westphalian territorial sovereignty remains central to both international relations and law, and as such it has a role to play 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." J. Jackson, *Sovereignty-Modern: A New Approach to an Outdated Concept*, 97 No.4 AJIL 782, 789 (Oct., 2003). From kings to citizens, to nations, the Communist Party, dictators, juntas, and theocracies, all have claimed to enjoy the benefit of sovereignty. The modern polity is known as the state, and the fundamental characteristic of authority within it is still sovereignty. *Id.* at 780.

[72] Although no universally agreed upon definition of the CHM principle has been reached by legal scholars or policymakers, a working definition would likely comprise five elements. First, there can be no private or public appropriation; no one legally owns common heritage spaces. J. Frakes, *Notes and Comments: The Common Heritage of Mankind Principle and the Deep Seabed, Outer Space, and*

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

From the Greek *cyber*, meaning "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."[74] However, unlike the physical world, cyberspace is an abstract reality of ideas, information, and logic. A cyber attacker entering this domain can anomalously shed ties of citizenship and cross sovereign boundaries without a trace, all the while masquerading as a real or fictitious entity.[75] Subsequent efforts to determine exactly which physical locations a virtual entity traversed are exceedingly difficult. 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), while current information systems are designed to have as many alternates and redundancies as possible to enhance reliably.[76] Though

---

Antarctica, 21 WIS. INT'L L.J. 409, 410 (2003). Second, representatives from all nations must manage resources since a commons area is considered to belong to everyone. The role of governments then is relegated to being a representative of the people. As popular management is practically unfeasible, a special agency to coordinate shared management must administer commons spaces in the name of all mankind. *Id* at 410. Third, all nations must actively share with each other the benefits acquired from exploitation of the resources from the commons heritage region. Private entities seeking profits would have to perform a service that benefited all of mankind. Equitable distribution is intrinsic to the principle, but the application is ambiguous necessitating a balance between economic benefit-sharing and environmental protection. Fourth, there can be no weaponry or military installations established in commons areas. Armed conflict is unlawful since every nation has a stake in maintaining the peace. Finally, the commons should be preserved for the benefit of future generations, and to avoid a "Tragedy of the Commons" scenario. G. Hardin, *The Tragedy of the Commons*, 162 SCIENCE 1243-1248 (1968).

[73] Anupam Chander & Madhavi Sunder, *The Romance of the Public Domain*, 92 CALIF. L. REV. 1331 (2004) ("With the rise of the Information Age, the flashpoint debates about property have moved from land to information. The public domain is now the cause célèbre among progressive intellectual property and cyberlaw scholars, who extol the public domain as necessary for sustaining innovation…This is the romance of the commons - the belief that because a resource is open to all by force of law, it will indeed be equally exploited by all.")

[74] Stephen J. Lukasik, *Protecting the global information commons*, 24(6) TELECOMMUNICATIONS POLICY 519-31 (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).

[75] *Id.*

[76] *Id.*

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, except in the form of anonymous, invisible radio waves or electrons.[77] 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."[78]

Yet even if sovereignty can be established over portions of the information commons through international negotiations,[79] it is very difficult to attribute a particular computer network attack ("CNA") to a foreign state despite it being legally permissible to do so under the effects principle for the reasons outlined above. Article 2(4) of the UN Charter limits its definition of uses of force to a specific territory. A breach of territorial integrity then signifies some threat to an unimpaired or unmarred condition, original perfect state, entireness, completeness, undivided or unbroken.[80] Cyberspace does not easily fit in with 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 in the same way that would be a flight through its airspace."[81] 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 being either

---

[77] DOD, *supra* note 33.
[78] *Id.*
[79] The purpose of international political theorizing 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. The Temple of Westphalia has been eroded by acid rain, flooded by rising waters, made porous by free information flows and the ever increasing rate of economic interdependence; but it remains standing. The intersection of the two, as stated by Rosalyn Higgins, is the domain of law. ROSALYN HIGGINS, TERRORISM AND INTERNATIONAL LAW 265 (1997).
[80] UN Charter, Art. 2(4).
[81] 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* (UK v. Alb.) ICJ Reports 1947-48, p.15, p.5.

internal (crime/terrorism) or external (war).[82] It is also unclear whether reparations are also due the victim of cyber attacks.[83] To answer these issues of attribution, it is necessary to institute a standard of state responsibility that recognizes the difficulties inherent in cyber law to definitively track down those responsible for cyber attacks. This will be addressed in Part V.

Consequently, sovereignty should not act as a bar on regulating the information commons.[84] Nations have every right to protect their sovereign interests through the effects principle. But given that cyberspace is interpreted by many as a commons territory, it would be prudent to setup an international organization tasked with regulating the commons in the guise of other CHM areas, similar to the United Nations Commission on the Limits of the Continental Shelf ("CLCS") under UNCLOS. This body could regulate cyber security like in 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, i.e. cyber security, through extensive cooperation, while also mutually respecting one another's independence and the increasingly important role of non-state actors.[85] This system of

---

[82] Brenner, *supra* note 40.

[83] Depending on the context, reparations are often due a nation whose rights under international law were violated by another nation. *Case Concerning the Factory at Chorzow* (Claim for Indemnity), PCIJ Series C, No. 13-1, July 26, 1927.

[84] 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 73 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.

[85] *See generally* FRED DALLMAYR, ALTERNATIVE VISIONS: PATHS IN THE GLOBAL VILLAGE 64 (1998) (arguing that Frankfurt School philosopher Jurgen 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 Nietzche and Heidegger, alternatively view the humanist project of reason and progress as fundamentally flawed. Bunn-Livingstone's intersubjectivity is one way in which to make constructive progress with diverse groups expressing everything from radical relativism to xenophobia. There is, according to this view, much more that unites than divides us, a sentiment in

mutual autonomy in the context of international collaboration to dissuade, 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 as an application of state *control* but about state *authority*.[86] 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 has tested traditional conceptions of sovereignty, so too is IW forcing a reinterpretation of the "use of force" and "armed attack" under the U.N. Charter.[87]

IV. ANALOGIZING PEACETIME RESPONSES TO CYBER ATTACK IN INTERNATIONAL LAW

Little controversy exists regarding whether the use of chemical and biological weapons should be viewed as forms of force within the classic meaning of armed attacks in international law. Much more contentious to date has been the question of in which box to place IW, since it similarly poses the threat of widespread destruction but with unconventional tactics; the same end with modern means. Cyber attacks that directly and intentionally result in non-combatant deaths and destruction do breach modern prohibitions on the use of force.[88] However, the literature to date has been silent as to what is the appropriate legal analogy to use as a baseline from which to consider regulatory responses to IW. It will be argued that the broad-based and extraordinary

---

keeping with the transition from absolute to popular sovereignty). A more moderate viewpoint is expounded by Michael Mann, who asserts 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 VIRGINIA L. REV. 437 (1929).

[86] J. Thomson, *State Sovereignty in International Relations: Bridging the Gap between Theory and Empirical Research*, 39 No. 2 INTERNATIONAL STUDIES QUARTERLY 213, 225 (Jun., 1995).

[87] Joyner, *supra* note 15.

[88] *Id*.

nature of a 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 capabilities to launch IW.[89] Thus, other international law regimes must be considered to develop an appropriate international response to this dire threat in the absence of a comprehensive international treaty on cyber security.

Both Russia and the United States have publicly made statements regarding the similarity and necessary military response to IW and nuclear war. The Russians have stated: "An attack against the telecommunications and electronic power industries of Russia would, by virtue of its catastrophic consequences, completely overlap with the use of weapons of mass destruction.[90] In fact, a Russian policymaker recently published a critique in the aftermath of the Estonian cyber attack that "Russia reserves the right to respond to an information warfare attack *with nuclear weapons*" [emphasis added].[91] On the other hand, former CIA Director John Deutch ranks information warfare "a close third behind the proliferation of weapons of mass destruction and the use by terrorists of a nuclear, biological, or chemical weapon."[92] Although the U.S. has not as brazenly argued that IW is tantamount to a nuclear exchange, Deutch's meaning is clear. These incendiary statements point to the extreme danger that great powers see in IW, as well as

[89] Though there is some question about the scale of IW necessary to bring about effects analogous to a nuclear war.
[90] Joyner, *supra* note 14.
[91] DOD, *supra* note 33.
[92] Mann, *Cyber-threat Expands with Unchecked Speed*, AVIATION WEEK AND SPACE TECHNOLOGY, July 8, 1996, at 64.

the extraordinary harm that could result in not laying out an appropriate legal framework from the outset to deal with cyber attacks.

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*? 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 that will be considered is inadequate in one way or another to the task, including communications law, space law, the law of the sea, and other applicable accords. Yet by fitting together strands of these various regimes it is possible to graft together two appropriate legal frameworks – one applicable in peace-time and another that is activated after an armed attack occurs. This is necessary to ensure that legal principles are seamlessly applied to avoid gaps in humanitarian protection,[93] as well as to guard against the continued propagation of cyber attacks. As has been stated though, a new comprehensive international regime that builds on these treaties would be preferred to the currently available system.

a. *The Analogy of Nuclear War*

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. The U.S. argued in the case that nuclear weapons cannot be banned in the abstract, but rather each case must be examined individually. Ultimately the Court stated that the threat or use of nuclear weapons "would generally be

[93] Kenneth Watkin, *Controlling the Use of Force: A Role for Human Rights Norms in Contemporary Armed Conflict*, 98 AJIL 1 (Jan. 2004).

contrary to the rules of international law applicable in armed conflict, and in particular the principles and rules of humanitarian law." But "in view of the current state of international law, and of the elements of fact at its disposal, the court cannot conclude definitively 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."[94] The ICJ went on to state that:

> [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.[95]

The United States, while taking the position that there is no *per se* rule banning the use of nuclear weapons, acknowledges that the use of such weapons is subject to the law of armed conflict, including the rules of proportionality, necessity, moderation, discrimination, civilian immunity, neutrality, and humanity.[96] As has been noted, some of the effects of nuclear weapons can be similar to a worst case cyber attack on a state. In an all-out attack, *all* critical infrastructure could be disabled or destroyed, leaving the victim nation completely helpless and its population terrorized or worse.

Cyber attacks on the scale of 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.

---

[94] Nuclear Weapons Advisory Opinion ¶ 105. E., at 36, 35 I.L.M. at 835.
[95] Nuclear Weapons Advisory Opinion ¶ 95, at 32, 35 I.L.M. at 829.
[96] *On the Unlawfulness of the Use and Threat of Nuclear Weapons*, Report of the Foreign and International Law Committee of the New York County Lawyers' Association, available at: http://www.nuclearweaponslaw.com/JournalsReport/NYCLA_Report.pdf. Last visited: Feb. 24, 2008.

maintains, so too should cyber attacks. Even though the ICJ did not declare all nuclear weapons illegal, the logic of its holding that "methods and means of warfare…which would result in unnecessary suffering to non-combatants, are prohibited"[97] is just as applicable to cyber war as it is to nuclear war. Cyber attackers are in fact conceivably even more responsible for non-combatant casualties than is 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. Even the lowest yield weapons result in substantial collateral damage.[98] Yet the ICJ has refused to rule such low-yield nuclear weapons illegal. As this decision indicates, there is as of yet little to no customary international law pertaining to the use of cyber attacks beyond the basic principle laid out in the *Nicaragua Case* that " every sovereign State [has a right] to conduct its affairs without outside interference...[this] is part and parcel of customary international law."[99]

Custom according to the *North Sea Continental Shelf Case* requires "widespread and representative participation provided it include[s] that of [the] States whose interests were specially affected."[100] State practice in the aftermath of cyber attacks seems to

---

[97] Nuclear Weapons Advisory Opinion ¶ 95, at 32, 35 I.L.M. at 829.
[98] Robert W. Nelson, *FAS Public Interest Report - Low-Yield Earth-Penetrating Nuclear Weapons*, FEDERATION OF AMERICAN SCIENTISTS, Apr. 19, 2008. Available at: http://www.fas.org/programs/ssp/nukes/new_nuclear_weapons/loyieldearthpenwpnrpt.html. Last visited: 4/20/2008.
[99] 1968 I.C.J. 4, para. 202.
[100] North Sea Continental Shelf (Fed. Rep. of Gem / Den. v. Neth.), 1969 ICJ 41 (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 (*opinion juris*)." Andrew T. Guzman, *Why LDCs Sign Treaties that Hurt Them: Explaining the Popularity of Bilateral Investment Treaties*, 38 VIRGINIA JOURNAL OF INTERNATIONAL LAW 639, 646 FN 20 (1996). *See also* Statute of the International Court of Justice, June 26, 1945, art. 38, 59 Stat. 1055, 3 Brevans 1179, *reprinted in* INTERNATIONAL LAW: SELECTED DOCUMENTS 27 (Barry E. Carter & Phillip R. Trimble eds., 1991 ("The Court…shall apply…international custom, as evidence of a general practice accepted as law."; Concerning the Continental Shelf (Libya v. Malta) 1985 I.C.J. 13, 29 (June 3) ("It is of course axiomatic that the material

suggest widespread condemnation but no consensus on how to respond, or even at what level a cyber attack becomes an armed attack. Due to this lack of custom, several treaty regimes will be examined in kind that 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 be called upon until a comprehensive treaty on cyber security is implemented.

b. ***The Analogy of Space Law and the Antarctic Treaty System***

Outer space is inherently similar to cyberspace; both are incredibly large and resource rich areas of the international commons.[101] Neither outer space nor cyberspace may be nationalized under international law.[102] Space and telecommunications systems are also intertwined, including in such functions as: communications relay, imagery collection, missile warning, navigation, weather forecasting, and signals intelligence.[103] However, the limitations inherent in applying space law[104] to cyberspace are illustrated in

---

of customary international law is to be looked for primarily in the actual practice and *opinion juris* of states…").

[101] In the outer space context, gold has now been discovered on asteroids, Helium-3 on the Moon, and magnesium, cobalt and uranium on Mars. The first wave of space tourists are preparing for launch in 2008 courtesy of Virgin Galactic. New industries promising unlimited energy could be developed, necessitating a well-defined legal regime. In cyberspace, internet service protocols and domain names are similarly valuable real estate in the Information Age.

[102] The OST, dubbed 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." OST Preamble; Interview with Steve Doyle, Executive Vice President, Clean Energy Systems in Sacramento, CA (Oct. 2, 2007).

[103] DOD, *supra* note 33.

[104] Since its inception after the launch of *Sputnik* in 1958, space law has created a whole new field of legal terminology that has challenged national governments and international institutions to redefine ideals for space operations. This is made evident by the five principal space law treaties signed between 1967 and 1981. These were the first international treaties to employ the terms "mankind" and "people" rather than "states," "nations," or "international community," and affirmatively recognized the quasi-subject status of non-governmental organizations. Space law considers the welfare of people as the beginning and end of all human activity and 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, and thereby raising the profile of non-state actors in ways that are now being challenged as technology opens up the final frontier.

space law's failure to address whether the legal regime applies during armed conflict.[105] There exists also no legal prohibition against developing and using space weapons besides the placement of nuclear weapons into orbit.[106]

The military use of space was not completely forbidden by the 1967 U.N. Outer Space Treaty, as can be observed 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 weapons of mass destruction were prohibited in space in this treaty with the passage, "States Parties to the Treaty undertake not to place in orbit around the earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction, install such weapons on celestial bodies, or station such weapons in outer space in any other manner."[107] But even this limitation applies only to the Moon and other celestial bodies and not the empty space in between.[108] Thus there is currently no legal regime prohibiting weapons being placed in the void between bodies. In *Vision for 2020*, a 1998 government report, explains that the role of the United States Space Command ("USSC") will be to dominate "the space dimension of military

---

[105] 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. If both nations had objectively analyzed the situation beforehand, they likely would have wished to prevent espionage on this scale. Since both countries were already engaging in this practice, though, 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." Chicago Convention, Art. 89.

[106] In 1989 a US Congressional study called 'Military Space Forces: The Next 50 Years,' was envisioning the day when aerospace corporations would "mine the sky" for profit. The study cited US 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).

[107] BIN CHENG, STUDIES IN INTERNATIONAL SPACE LAW 517 (1997).

[108] *Id.* at 529.

operations to protect U.S. interests and investment…It's politically sensitive, but it's going to happen," says General Joseph Ashy, Commander-in-Chief of the US Space Command. "Some people don't want to hear this, and it sure isn't in vogue, but absolutely—we're going to fight in space …That's why the US has development programs in directed energy and hit-to-kill mechanisms."[109] This statement underscores the Bush Administration's desire to maintain the United State as the world's foremost space power at the expense of multilateral cooperation.

International efforts to limit the spread of space weapons have been just as happenstance as those aimed at forming a legal regime to deal with cyber attacks. Russia and China have publicly stated their wish for such a treaty, but the United States has demurred.[110] The rationale commonly given by the U.S. is that it wants to maintain its space dominance. Similar efforts to crystallize a treaty for cyber attacks have also failed for the same reasons. Like 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, and there has been little support for the Russian initiative to date. 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 30 are in space. Barring a major conflict, most states do not expect or have the resources to be either an attacker or a defender in space in the near future. With information systems though, nearly all states can reasonably expect to be both. This has

---

[109] COLLINS, *supra* note 107.
[110] John Borland, *Russia, China Propose Space Arms Treaty*, WIRED, Feb. 12, 2008 (arguing that Russia and China have been pushing for talks on this issue since the beginning of the decade, largely against resistance from the United States which wishes to maintain its dominance in space).

been shown to be true not only in Estonia, but across the world as cyber attacks continue to proliferate.

Space law provides an example of the principle that an area of the international commons can in fact be regulated to bar the most egregious military weapons systems. The problem with applying such an approach to cyber attacks though is that it is the aggregate scale of seemingly innocent intrusions that can aggregate into the equivalent of 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 amalgamation of coordinated attacks that can result in a total collapse of infrastructure – a national death by a thousand cuts.

Rather than banning only the most egregious weapons, then, perhaps it is possible to regulate all hacking that could rise to the level of 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. In effect, the ATS sets aside Antarctica as a scientific preserve, establishes freedom of scientific investigation, and bans military activity on the continent.[111] The main objective of the ATS[112] 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."[113]

---

[111] These 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.

[112] Like the deep seabed and the Arctic, the continent of Antarctica is an enormous expanse of undeveloped land that contains substantial mineral deposits. Unlike the deep seabed and similar to the Arctic though, 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.

[113] Preamble of the Antarctic Treaty, text available at the National Science Foundation website: http://www.nsf.gov/od/opp/antarct/anttrty.jsp. Last Visited: 10/06/07.

Imposing such a freeze on developing new software capable of malicious attacks though, even if was possible, stifles innovation in the same way that shutting down the generative nature of the internet would. 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 needed to meet new challenges as they arise. Subsequent ratification by national legislatures would thereafter pose a significant problem, unless that power was written into the mandate of the committee outright. On the surface then, it appears 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.

c. ***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. Modern communications law is crafted by the International Telecommunications Union ("ITU"), a specialized UN Agency for information communication technologies.[114] Article 35 of the ITU Charter prohibits "harmful interference" defined in Annex 2 as "interference which endangers the functioning of a radio navigation service or of other *safety services* or seriously degrades, obstructs or repeatedly interrupts a radio communication service operating in accordance with the Radio Regulations [emphasis added]."[115] This passage could be used to hold those states that use cyber attacks to "endanger…safety services" responsible under international law. "Safety services" conceivably includes public services such as health, police, and public

[114] *See* ITU website: http://www.itu.int/net/about/index.aspx. Last visited: Feb. 24, 2008.
[115] ITU Charter, Art. 35.

transport, all of which are sectors vulnerable to cyber attacks. Though, the lack of mandatory enforcement mechanisms limits the ability of this regime to hold states accountable.

There are also provisions giving governments wide discretion in regulating private activity that may appear dangerous to the security of the State.[116] This includes "cut[ing] off any private telecommunications which may appear dangerous…or contrary to state laws, to public order, or to decency."[117] Unlike space law or the ATS, Article 38 does have an exception for military activities,[118] 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.[119] State practice though asserts that these treaties are thought not to apply during international armed conflicts.[120] Critically, international communications law currently contains no direct and specific prohibition against the conduct of information operations by military forces, even in peacetime. As a result, though Articles 35 and 38 of the ITU are potentially useful in developing felony statutes to deal with state-sponsored IW perpetrators, the regime has little utility in crafting a comprehensive legal framework to deal with state-sponsored cyber attacks that have risen to the level of an armed attack.

---

[116] DOD, *supra* note 33.
[117] ITU Charter, Art. 19.
[118] ITU Charter, Art. 38.
[119] DOD, *supra* note 33.
[120] *Id.*

i. *U.S. Cyber Law Applied to Information Warfare*

Cyber law is a relatively new phenomenon. It has to be – in 1988, there were only sixty thousand computers connected to the internet, all at research institutions.[121] 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.[122] The attack exposed difficulties in U.S. law that would make the prosecution of cyber attackers exceedingly difficult.[123] As a direct result, USCERT was founded. Its largely successful track record though is not entirely a commentary on its ability, but goes more to the fact that there have been so few major malicious viruses and worms since 1988.[124]

As the threats posed by cyber attacks grow, it is prudent to look to and analogize from applicable domestic as well as international law. U.S. law does possess certain principles that are applicable to cyber attacks. For example, consider vicarious liability. This is a form of strict secondary liability that arises under the common law doctrine of agency, i.e., *respondeat superior*. Under this theory, the principal is responsible for the acts of the subordinate. In a broader sense, a third party that has the "right, ability, or duty to control" the activities of a violator but refuses or neglects to do so may in some circumstances be held responsible for the violator's actions.[125] Applied to cyber attacks, this principle may hold companies liable for a CNA that knowingly or negligently fail to provide sufficient cyber security for the persons or resources, including infrastructure,

---

[121] JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 36 (2008).
[122] *Id.*
[123] U.S. GENERAL ACCOUNT OFFICE, GAO/IMTEC-89-57, VIRUS HIGHLIGHTS NEED FOR IMPROVED INTERNET MANAGEMENT (1989).
[124] ZITTRAIN, *supra* note 121 at 44.
[125] Meyer v. Holley, 537 U.S. 280 (2003).

under their care. The fact that most of the critical infrastructure in the U.S. is privatized signifies that this principle of tort law and other related common law doctrines could prove decisive in developing a U.S. legal regime to deal with cyber attacks.

Several recent precedents may be used to begin laying 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.[126] This case stands for the proposition that, 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 acts. Similarly, in *Fonovisa v. Cherry Auction, Inc.* the court held that vicarious liability existed because the defendants had control over direct infringers of U.S. law, and it had a direct financial interest in the infringing activity.[127] Together, these cases place the onus of 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 as this would violate the first amendment and activate intermediate scrutiny according to the court in *Ctr. for Democracy & Tech. v. Pappert*.[128] Nor do companies have secondary liability for

---

[126] 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).
[127] Fonovisa v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996).
[128] Ctr. for Democracy & Tech. v. Pappert, 337 F. Supp. 2d 606 (E.D. Pa. 2004).

providing internet services if they have no knowledge of the violation or infringement, as the court held in *Hendrickson v. eBay, Inc*.[129]

In addition to case law, several U.S. criminal statutes could also be used as a rubric for cyber attacks. For example, the U.S. has passed felony statutes criminalizing violation of international accords dealing with international radio or wire communications.[130] Maliciously interfering with satellite transmissions is a felony in the U.S.,[131] similar to wire fraud.[132] These statutes could be expanded to include 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 criminalize the various forms of cyber attacks.[133] 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 deconstructed any online ethical code that once existed. This is evidenced by the fact that 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

---

[129] Hendrickson v. eBay, Inc., 165 F. Supp. 2d 1082 (C.D. Cal. 2001).
[130] *See* 47 USC 502 (stating that "Any person who willfully and knowingly violates any rule, regulation, restriction, or condition…made or imposed by any international radio or wire communications treaty or convention, or regulations annexed thereto, which the United States is or may hereafter become a party, shall, in addition to any other penalties, provided by law, be punished, upon conviction thereof by a fine of not more than $500 for each and every day during which such offense occurs.").
[131] 18 USC § 1367.
[132] 18 USC. § 343.
[133] 18 U.S.C.§ 2331 (2000). For more definitions, *see, e.g.*, Mohammad Iqbal, *Defining Cyberterrorism*, 22 J. MARSHALL J. COMPUTER & INFO. L. 397 (2004).

criminal acts.[134] 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.[135] The right advanced worm released today making use of botnets and zombie networks could infect and crash every computer connected to the internet simultaneously.[136] How it is possible to avoid such an eventuality?

Cyber attacks expose the weaknesses of a generative network, i.e., networked computers that retrieve and install code from sources anywhere on the network.[137] The current system is analogous to nibbling food from hundreds of different people, some established vendors, some street peddlers.[138] 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.

d. ***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 when President Truman issued a proclamation stating that the natural resources of the seabed and subsoil of the U.S. continental shelf

---

[134] ZITTRAIN, *supra* note 121 at 45.
[135] *Id.* at 47.
[136] *Id.* at 52.
[137] *Id.* at 38.
[138] *Id.* at 55.

were exclusively U.S. property.[139] The practice was followed by nations around the world, [140] giving birth to the customary international law concept of the continental shelf since codified by four Geneva Conventions, beginning with UNCLOS I in 1958.[141] 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 held from 1973 to 1982. Finally 320 Articles were adopted with a roll call of 130 votes to four, with 17 abstentions and 160 nations overall participating.[142] UNCLOS III was setup to regulate the use, exploration and exploitation of all living and non-living resources of the international sea and the seabed extending in an "Area" beyond territorial waters.[143] Nevertheless, technology transfer requirements and other fixed fees were imposed to ensure access for developing countries to the deep seabed.

Developed nations eschewed being forced to give up their technological edge or share the benefits of development, and so the U.S., Federal Republic of Germany, the U.K. and most other nations elected not to sign UNCLOS III.[144] As the deep seabed mining provisions of UNCLOS proved ultimately unsatisfactory to the industrialized world, after Guyana became the 60th nation to ratify the agreement in 1993 (under Article

---

[139] The continental shelf is defined as the "seabed and subsoil of the submarine areas that extend beyond a coastal state's territorial sea throughout the natural prolongation of its land territory to the outer edge of the continental margin, or to a distance of 200 nautical miles from the baselines from which the breadth of the territorial sea is measured where the outer edge of the continental margin does not extend up to that distance." Penelope Warn, *Arctic Scramble: International Law and the Continental Shelf*, AM. SOC. OF INT'L L., Oct. 1, 2007.

[140] Between 1946 and 1950, Argentina, Chile, Peru and Ecuador all extended their sovereign rights to a 200 nautical mile (370 km) distance. Other nations extended their territorial seas to 12 nautical miles (22 km). By 1967 only 25 nations still used the old 3 nautical mile (6 km) limit, 66 nations had set a 12 nautical mile (22 km) territorial limit, and eight had set a 200 nautical mile (370 km) limit. *Id.* at 15.

[141] 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.

[142] *Id.*

[143] *Id.* at 18.

[144] L. CALUDE, STATES AND THE GLOBAL SYSTEM: POLITICS, LAW AND ORGANIZATION 117 (1988).

308 the accord would then enter into force 12 months later) 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, and doing away with most mandatory technology transfers and instituting various international legal obligations in their place.

As applied to cyber attacks, UNCLOS[145] Article 19 states the customary international law obligation for nation's territorial sea not to engage in activities "prejudicial to the peace, good order, or security of the coastal State."[146] This includes the collection of information, or for propaganda, or in any way interfering with any systems of communications. Article 113 requires domestic criminal legislation to punish willful damage to submarine cables.[147] 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 as well does not specify its status in war-time.[148] Nor does it include enforcement mechanisms.

---

[145] Ultimately, 320 Articles were adopted with a roll call of 130 votes to four, with 17 abstentions and 160 nations overall participating. These margins were not reflected with actual ratifications. UNCLOS III established unequivocally the concept of the EEZ in international law. States have the benefit of exploring, exploiting and managing all natural resources within their EEZ. By claiming the EEZ, the state can enforce its fishing rights within the zone and can even build artificial islands, such as offshore oil platforms. The EEZ does not prevent the passage of foreign vessels through its waters, and foreign states may lay submarine pipes and cables within the zone, but outside territorial waters.

[146] UNCLOS, Art. 19.

[147] UNCLOS, Art. 113.

[148] 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.

Nonetheless, UNCLOS is also important as an example of a regime which was unsuccessful until it recognized the needs of the private sector, as well as doing away with 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.

e. ***Analogizing other Applicable Accords***

Numerous bilateral and multilateral treaties dealing with everything from legal assistance, extradition, diplomatic relations, friendship, to status of forces agreements include elements that impact on the prosecution of cyber attackers. The U.S. is a party to dozens of Mutual Legal Assistance Agreements ("MALT"), beginning with Switzerland in 1977, which could be used to seek criminal prosecution of those found responsible for cyber attacks, especially those MALTs termed broadly enough to cover *all* law enforcement investigations.[149] The problem with this approach though, would be to treat a cyber attack as analogous to terrorism, meaning the IHL framework drops away unless state-sponsored terrorism is included within the regime.[150] There are often no enforceable obligations under these treaties. The U.S. is also a party to more than 100 bilateral extradition treaties. Without such accords national governments often will have neither an international obligation nor the domestic authority to deliver custody of an

[149] An example is the US-Canada MALT: 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.
[150] JOHN MURPHY, STATE SUPPORT OF INTERNATIONAL TERRORISM: LEGAL, POLITICAL, AND ECONOMIC DIMENSIONS 128 (1989).

individual for prosecution.[151] 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 returned to in part V.

The 1961 Vienna Convention on Diplomatic Relations enshrines the right of inviolability of the premises of a diplomatic mission,[152] its archives,[153] private residences and property,[154] and its *communications*.[155] 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.[156] 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 MALTs and extradition treaties would apply to

---

[151] DOD, *supra* note 33.
[152] 1961 Vienna Convention, Art. 2.
[153] 1961 Vienna Convention, Art. 24.
[154] 1961 Vienna Convention, Art. 30.
[155] 1961 Vienna Convention, Art. 27.
[156] DOD, *supra* note 33.

make perpetrators accountable in various jurisdictions.[157] If the attack is directed against a foreign mission or embassy, than 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.

V. ARMED ATTACKS IN INFORMATION WARFARE

Under what circumstances can a CNA be considered an act of war? International law requires that for self-defense to be permissible there must be an attack so egregious that the victim would be justified in responding in kind.[158] This conception rules out preemptive or aggressive self-defense in most instances. U.N. General Assembly Resolution 2625 (hereinafter "UNGA 2625") declares that "A war of aggression constitutes a crime against the peace…States have a duty 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 State."[159] Yet it is not UNGA 2625 that

[157] It should be noted, though, that the Estonian-Russian MALT proved entirely ineffective, since Russia refused to honor the treaty in this instance.
[158] UN Charter, Art. 2(4).
[159] UNGAR 2625.

governs the use force – that is defined by the U.N. Charter itself. The question then is whether and to what extent CNAs constitute a use of armed force.[160]

The U.N. Charter was envisioned to cover such situations as the presence of troops, and the use of traditional military weapons or another nation's territory; not simultaneous multimodal network attacks on a state emanating from around the world. 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 clearly prohibits international intervention through the use of armed force, but withholds comment on other, more subtle forms of subversive coercion that do not involve a perceived threat of armed force.[161] State practice has shown though that such coercion or other forms of "aggression" do not activate Article 2(4) protections. Therefore, the only way for a state to have a right of self-defense in response to a CNA would be if that attack rose to the level of an armed attack. Using the Estonia case study, the main legal hurtles in pursuing a self-defense rationale are (1) proving that the cyber attack raised 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 recognized under traditional IHL.[162] IW is an expansive category of military activities. It includes physical attacks on information systems by traditional military means,

---

[160] In 1974, the General Assembly defined the term aggression as "the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, 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 (1974).
[161] Joyner, *supra* note 14.
[162] The debate about what constitutes an armed attack can be framed in reference to the 9/11 attacks. Some authors maintain that these attacks on the US were armed attacks under the meaning of the UN 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. Watkin, *supra* note 93.

psychological operations, military deception, and electronic welfare operations such as jamming.[163] IW is not the first arena of high technology to be applied to the IHL framework. Even futuristic electro-magnetic pulse weapons and directed-energy lasers, micro-wave devices, and high energy radio frequency 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 far easier than at any point in history since global communications has essentially made distance and geographic boundaries irrelevant to the conduct of computer network attacks.[164]

The potential for cyber attacks to disrupt and destroy a society was witnessed in Estonia. In a worst case scenario, CNAs could indeed cripple a society, shut down vital public services, and lead to the utter breakdown of public order. Property damage and loss of life would be on the order of a traditional military attack. The question thus turns on a definition of "force,"[165] which could be interpreted strictly in accordance with the text, or with the broad object and purpose of the U.N. Charter.[166] Although it is a contentious issue, it may be stated with some confidence that the boundaries of "force" do not precisely coincide with armed force only.[167] What matters then are the ends sought, not the means. For example, "a CNA specifically intended to directly cause

---

[163] DOD, *supra* note 33.
[164] *Id.*
[165] Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885 (1999).
[166] Vienna Convention on the Law of Treaties, May 23, 1969, art. 31(1), 1155 U.N.T.S. 331 (1969). Analysis based on both UN Charter travaux and text leads to an interpretation excluding economic, and for that matter political, coercion from Article 2(4)'s prescriptive sphere. *See* Doc. 784, I/1/27, 6 U.N.C.I.O. Docs. 331, 334, 609 (1945).
[167] Schmitt, *supra* note 165.

physical damage to tangible property or injury or death to human beings is reasonably characterized as a use of armed force and, therefore, encompassed in the [Article 2(4)] prohibition."[168] Thus it is theoretically possible for a CNA to rise to the level of an armed attack. The CNA itself is only an instrument to carry out that attack in the same way that any other weapon would be.

Second, the 1986 Libya attack precedent held that states which unwittingly, or permissively, allow their territory to be used to carry about attacks are committing an act of aggression.[169] The problem then becomes one of attribution, i.e., 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 were shown to have been located in the U.S. 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 heat of a cyber attack with a society's infrastructure falling down by the second? For such a legal regime to be functional, the doctrine of state responsibility for cyber attacks would have to be restructured and sufficiently defined.

a. ***State Responsibility for Cyber Attacks***

The speed and anonymity of cyber attacks makes "distinguishing among the actions of terrorists, criminals, and nation states difficult."[170] Simultaneously, the instances of state-sponsored terrorist acts have increased since the end of the Cold

---

[168] *Id*. 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.*
[169] UNGAR 41/38 on Nov. 20, 1986.
[170] The White House, The National Strategy to Secure Cyberspace 19, 64 (2003), available at http://www.whitehouse.gov/pcipb/ ("Cyber attacks cross borders at light speed..."); Brenner, *supra* note 40.

War.[171] 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 acted on its behalf in committing criminal or terrorist acts. A nation-state might even be able to "conceal its involvement in self-interested cyber attacks by encouraging 'civilian' cybercriminals and cyberterrorists to conduct their operations from within its borders since the fog of 'civilian' cyberattacks would obscure the purpose and origins of the state-sponsored attacks."[172] Consequently should the cyber attack on Estonia be characterized as: a cybercrime, with Russian Nashi hackers orchestrating a coup; cyberterrorism by a group pursuing idiosyncratic ideological goals; or cyberwarfare, a virtual sortie by Russian intelligence operatives?[173] Determining this distinction will also dictate the appropriate response, including the extent to which civilian law enforcement or the military should be involved.

Cyberterrorism consists of using computer technology to engage in terrorist activity, distinguishable from cybercrime since "crime is personal, while terrorism is political."[174] Classic conceptions of terrorism are discernible from warfare, which is not

---

[171] *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"). In the discussion above "state-sponsored crime" denotes state involvement in the commission of conventional crimes, such as the theft of intellectual property. Brenner, *supra* note 40.

[172] Brenner, *supra* note 40.

[173] *Id.*

[174] *Id.*

supposed to target civilians.[175] IW consists of nation-states' using cyberspace to achieve 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."[176] 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.[177] Yet it is too simple to state that "If we conclude with some confidence that an attack did not 'come from a nation-state actor, we inferentially assign it to the cybercrime/cyberterrorism category and embark upon the tasks of determining precisely what it is and who is responsible for it."[178] 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.

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 launching an attack on another state to identify themselves, though this convention is apparently honored more in the breach than in its realization.[179] The International Law Commission ("ILC") Draft Articles elaborate on this basic law by adding that "the conduct of any State organ shall be considered an act of that state under international law."[180] An organ includes "any person

---

[175] *See* U.N. Office of the High Comm'r for Human Rights, Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, available at http://www.unhchr.ch/html/menu3/b/92.htm. Last visited: 4/18/2008.
[176] Brenner, *supra* note 40.
[177] *Id.*
[178] *Id.*
[179] *See* Hague Convention No. III Relative to the Opening of Hostilities art. I, Oct. 18, 1907, 36 Stat. 2259, 2271, T.S. 598; Brenner, *supra* note 40.
[180] Draft ILC Articles, Art. 4(1).

or entity which has that status in accordance with the internal law of the State."[181] Such an official body cannot avoid responsibility by claiming that the actor exceeded their authority.[182] 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.[183] 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.[184] But as has been stated, cyber attacks of the type that we have seen and will likely to continue to be prevalent are typically not at the public behest of an official state organ. As such, the international law doctrine of attribution in fact is essential ground for regulating cyber attacks.

The relevant ILC section regulating attribution in fact states that "The conduct of a person or group of persons shall be considered an act of 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 State in carrying out the conduct."[185] There are currently two standards for interpreting this provision in international law – the doctrines of effective and operational control. The effective control doctrine, originating in the ICJ *Nicaragua* case, held that a country's control over paramilitaries or other non-State actors can only

[181] Draft ILC Articles, Art. 4(2).
[182] Draft ILC Articles, Art. 7.
[183] Examples of such accords include: 1970 Declaration on Principles in International Law; 1965 Declaration on the Inadmissibility of Intervention in the Domestic Affairs of State.
[184] Joyner, *supra* note 14.
[185] Draft ILC Articles, Art. 8.

be established if the actors in questions act in "complete dependence" on the State.[186] In contrast, the operational control doctrine is illustrated in the International Criminal Tribunal for the Former Yugoslavia *Tadic* case. That 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.[187]

The distinction between the *Nicaragua* and *Tadic* standards is whether or not the State must be in direct control of operational planning. Dr. Marc Weller, Director of the European Centre for Minority Issues, argues 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.[188] The ICJ has consistently used the more restrictive *Nicaragua* standard in its jurisprudence. For example, in the *Bosnian Genocide* decision,[189] the Court adopted *Nicaragua* in deciding that Serbia was ultimately not responsible for the genocide at Srebrenica.[190] Yet given the secretive nature of CNAs, the *Tadic* standard of attribution should apply in cyber attacks. It should not be necessary to prove complete governmental control of a CNA, just operational control. It is far too easy for governments to hide their IW operations under the *Nicaragua* standard. If the *Tadic* standard were used instead, it is possible that even the well-document Russian incitement to the cyber attack on Estonia would be sufficient to satisfy state attribution. In a future

---

[186] Case Concerning the Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) 1986 I.C.J. Rep. 392 (Jun. 27).
[187] Prosecutor v. Tadic, Case No. IT-94-1-I, Decision on the Defense Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 (Oct. 2, 1995).
[188] Telephone Interview with Marc Weller, Director of the European Centre for Minority Issues, in Kosovo (Mar. 14, 2008).
[189] The Application of the Genocide Convention Case (Bosnia and Herzegovina v. Serbia and Montenegro), 2007 I.C.J. 140 (Feb. 26) (*Hereinafter* "the *Bosnian Genocide* case").
[190] The Srebrenica Massacre was the July 1995 killing during the Bosnian War of an estimated 8,000 Bosniak 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.

comprehensive legal regime, that would be sufficient to grant Estonia 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.

i. Proposal: Incitement to Genocide through Cyber Attack

Once attribution is satisfied for victims of the most horrific cyber attacks it may be possible to use the incitement to genocide rubric to bring those responsible to justice in the International Criminal Court or another appropriate forum. There is already recognition that cyber attacks should be considered as under the IHL framework, and that those who break these laws in a cyber attack should be guilty of war crimes.[191] It is only one inferential step further to argue that it is also possible for cyber attackers to be guilty of genocide in the most horrific cases, which has at its focus the destruction of national groups. The Genocide Convention defines 'genocide' as the inchoate commission of "any…acts committed with intent to destroy, in whole or in part, a national, ethnical, racial or religious group."[192] The Convention does not quantify the proportion of a population that needs to be destroyed before genocide can legally be said to have occurred.[193] Nor does Article IX expressly impose an obligation on States to prevent, or

---

[191] 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) (noting that the misuse of cyber attacks could subject U.S. authorities to war crimes charges).

[192] 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; (e) Forcibly transferring children of the group to another group. Convention on the Prevention and Punishment of the Crime of Genocide, December, 9 1948, 78 U.N.T.S. 277.

[193] 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 international responsibility of the State is incurred. *Bosnian Genocide, supra* note 4, at 166; Scott Shackelford, *Holding*

be held accountable for, genocide.[194] That is, until the ICJ established such an obligation in its recent *Bosnian Genocide* decision.

For the first time in legal history, of the four genocide cases that have come before the ICJ, the Court unequivocally held in *Bosnian Genocide* that States can be found responsible for genocide, rather than simply have to punish the individual perpetrators.[195] A state using a weapon of mass destruction capable of destroying a national group, such as would occur in worst case scenario cyber attack, could thus be liable for genocide if it had the requisite specific intent to destroy the group to which the victims belonged.[196] Three Rwandan media leaders were recently found guilty of incitement to genocide for publishing and broadcasting words and pictures that produced and promoted ethnic atrocities, by Trial Chamber I of the International Criminal Tribunal for Rwanda.[197]

States that sponsor or launch cyber attacks designed to produce similar atrocities should also be found liable for this crime. 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 reach this most horrific of international crimes, nor would proving

---

States Accountable for the Ultimate Human Rights Abuse: An Analysis of the ICJ Bosnian Genocide Decision, 14 NO. 3 HUM. RTS. BRIEF 30 (2007).

[194] Article IX 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 State 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 1, art. IX.

[195] Trial of Pakistani Prisoners of War (Pakistan v. India) 1973 I.C.J. Rep. 328 (Dec. 15); *Bosnian Genocide* case, *supra* note 4; Legality of the Use of Force Case (Yugo. v. United Kingdom) 1999 I.C.J. 124, 132 (Order of 2June 1999); 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).

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

[197] 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 A.J.I.L. 325 (Apr. 2004).

specific intent be a simple matter. It should also be noted that the prevention of incitement to genocide remains muddied by divergent practice and confused jurisprudence.[198] Nevertheless the option exists of using the Genocide Convention as a vehicle to bring justice to nations that experience genocide as a result of a massive and deadly state-sponsored IW campaign.

b. *Cyber Attacks and Self-Defense*

Provided that the attack is actual or the threat is imminent and without any alternative choice of means, the victim state of a cyber attack may lawfully invoke self-defense to justify reasonable, necessary, and proportional measures to safeguard its security under Article 2(4) if that attack reaches the level of an armed attack.[199] Coercion not involving armed force does not violate Article 2(4) or result in action under Article 39. As such, "it does not follow that states may react unilaterally pursuant to Article 51.[200] The purpose of this section of the U.N. Charter is the maintenance of international peace and security.[201] Uses of force that endanger that international stability fall within Article 2(4)'s scope.[202] Threats of force, or economic coercion, do not fall under the gambit of Article 2(4) protection. Since cyber attacks are not 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, i.e., analogous to an attack by traditional military forces.

---

[198] William Schabas, *The Genocide Convention at Fifty*, SPECIAL REPORT 41, UNITED STATES INSTITUTE OF PEACE, Jan. 7, 1999. Available at: http://www.usip.org/pubs/specialreports/sr990107.html. Last visited: 4/18/2008.
[199] U.N. Charter art. 2, para 4.
[200] Schmitt, *supra* note 165.
[201] *Id.*
[202] 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. *Id.*

A valid exercise of self-defense would require irrefutable proof of aggression to satisfy state responsibility and to justify any sort of retaliation.[203] Forcible retaliation as retribution is not permitted under international law. The notion of preemptive or anticipatory self-defense permits a state to defend itself in the event of 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.[204] No strict prohibition precludes a government using cyber-force preemptively as long as the perceived threat is demonstrated to be real and immediate, and the criteria of proportionality and necessity are adhered to in the application of computer-generated coercion.[205] Whether the international community would accept such a use of force depends entirely on context.[206] 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 may only respond with force in self-defense if the CNA was intended to directly cause physical destruction or injury.[207]

In addition to Article 51 protections, the UNSC is also legally able to determine whether an attack would constitute a Chapter VII threat to international peace and security.[208] This power extends to calling upon member states to apply "measures not involving the use of armed forces" including the "complete or partial interruption

---

[203] Joyner, *supra* note 15.
[204] Letter from Daniel Webster to Lord Ashburton (Aug. 6, 1842), *reprinted in* 2 JOHN MOORE DIGEST OF INTERNATIONAL LAW 411-12 (1906). The Caroline incident involved a Canadian insurrection in 1837. After being defeated, the insurgents retreated into the United States where they recruited and planned further operations. The Caroline, a naval vessel, was being used by the rebels. British troops crossed the border and destroyed the vessel. Britain justified the action on the grounds that the United States was not enforcing its laws along the frontier and that the action was a legitimate exercise of self-defense. *Id.* at 409-11.
[205] Joyner, *supra* note 15.
[206] Schmitt, *supra* note 165.
[207] *Id*.
[208] U.N. Charter art. 1, para. 2.

of…telegraphic, radio, or other means of communications."[209] The U.S. Department of Defense has stated though that "A computer network attack that caused widespread damage, economic disruption, and loss of life could well precipitate action by the Security Council."[210] The U.N. though was noticeably silent regarding the attacks on Estonia.[211] The fact that such action was not forthcoming in the aftermath of the Estonian CNA speaks to 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. The general expectation is that a nation whose interests are damaged by the private conduct of an individual who acts within the territory of another nation will notify the government of that nation and request its cooperation in putting a stop to such conduct.[212] The appropriate response when a state, and not a private individual, is behind such an act remains unclear. As does differentiating these two scenarios – as has been stated, it is not as if the cyber attacker will be wearing the military uniform of the sponsoring hostile government (a situation discussed in sub-part (c) below).

One option to resolve the convoluted 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 defense mode," as

---

[209] 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.").
[210] DOD, *supra* note 33.
[211] *The View from the UN*, THE BALTIC TIMES, Dec. 5, 2007, available at: http://www.baltictimes.com/news/articles/19430/. Last visited: 06/12/2008.
[212] DOD, *supra* note 33.

termed by the Department of Defense.[213] Such a regime would need to include: (a) a statement of general criteria to be applied; (b) identification of officials or agencies that will be involved in making the decision; and (c) procedures to be followed.[214] What is required is a test of reasonableness of self-defense that is both subjective and objective. Still it is far from clear to what extent the world community will regard computer network attacks as "armed attacks" or "uses of force," and hence it is difficult to foresee how doctrines of self-defense and countermeasures could be used to apply to such situations. Interpretations ultimately turn more on the consequences of such an attack. If the Estonia cyber attack is any judge, then the international community would not have condoned an, however infeasible, Estonian armed attack against Russia. What is unclear is how the collective perspective would have changed if the cyber attack succeeded in bringing the entire country to a halt, ruining the economy, and leading to widespread unrest, rioting, and potentially a spate of tragic deaths.

c. *The Intersections of International Humanitarian and Human Rights Law*

In order to determine what combination of IHL and IHRL should be considered in grafting a legal regime to deal with cyber attacks that rise to the level of an armed attack, it is necessary to investigate the intersections in these two distinct bodies of law.

---

[213] A useful conceptual chart of this normative framework is offered by Michael Schmitt: "(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 165.

[214] DOD, *supra* note 33.

International human rights law and international humanitarian law differ in their formulation, structure, application, and enforcement. Rene Provost has argued that the distinctions between the two regimes are far from merely "semantic and contextual,"[215] but areas of overlap exist. Since WWII, increased 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. The question then naturally arises, is each system a clearly-defined, or amorphous, legal entity crafted to meet specific and distinct societal needs during peace and armed conflict?

The unique threat posed by non-state actors, combined with the lack of a consensus on the legal categorization of conflict, creates conditions in which the criminal law enforcement and armed conflict paradigms overlap. This overlap affects the applicability of human rights law, which is most commonly associated with law enforcement, and humanitarian law, which applies during armed conflict.[216] Human rights conventions generally do not impose obligations on individuals. Though if there is an applicable treaty or *erga omnes* customary law obligation, then states must protect these rights *at all times*.[217]

In contrast, IHL was created to protect members of specific groups during limited types of armed conflicts. These include: inter-state conflicts, national liberation armed

---

[215] RENE PROVOST, AID AND INTERVENTION: INTERNATIONAL HUMAN RIGHTS AND HUMANITARIAN LAW 343 (2002).
[216] Watkin, *supra* note 93.
[217] As the *North Sea Continental Shelf Case* demonstrated, 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 it must not be capable of attracting reservations. This principle was altered by the *Nicaragua (Merits) Case* in which the key question became, do customary rules apply when both states are also subject to a treaty covering the same grounds. The Court decided that: "…there is 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 185.

conflicts, non-international armed conflicts, and internal armed conflicts. The provisions of the 1907 Hague Convention, the 1949 Geneva Conventions, and the 1977 Additional Protocols protect the rights of identified subgroups, including combatants, POWs, and unarmed civilians.[218] Yet although IHRL and IHL were originally designed to be active in different circumstances, there is a chance for cross-fertilization between these two bodies of law 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."[219] A common starting point of both IHRL and IHL is respect for human values and the dignity of the human person – the core of fundamental standards which are applicable at all times, and from which no derogation is permitted.[220] The point of departure for IHL is that it requires the balancing of humanity with military necessity.

The nature and scale of violence in interstate conflict has had a distinct impact on how force is controlled in IHL. The internal use of force is normally dealt with under a human rights paradigm.[221] IHL, on the other hand, applies to international and non-international armed conflict. Though the relationship between the two is much more complex than this simple division of responsibilities.[222] For example, IHRL does apply during armed conflicts, as the ICJ decided in the *Nuclear Weapons Advisory Opinion*, whereas determining whether there has been an arbitrary deprivation of the right to life is determined by IHL acting as *lex specialis*.[223] There is now an elaborate system of law of war treaties governing many aspects of the conduct of modern warfare, from permissible

---

[218] *Id.*
[219] PROVOST, *supra* note 215 at 341.
[220] Watkin, *supra* note 93.
[221] *Id.*
[222] *Id*.
[223] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996, p. 226.

weapons to the treatment of POWs and non-combatants.[224] A gap in the literature to date is whether these regimes also apply to IW.

i. *Applying IHL to Cyber Attacks*

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. There are several IHL norms that are due special consideration in the IW context. These include: (1) the paramount distinction between combatant and non-combatants; (2) between civilian and military infrastructure; (3) and the prohibition against disproportionate attacks. Each norm will be addressed in turn.

First is the distinction between combatants and non-combatants. Only members of a nation's regular armed forces are entitled to use force against the enemy according to the combatant privilege enshrined in the Hague Conventions.[225] Combatants must follow laws of war, but failing to do so does not remove "combatant" status.[226] Given the absence of traditional combatant status including the wearing of identifying insignia in IW, would the Hague Conventions apply to captured cyber attackers? The language of Protocol I, Article 44 that these 'soldiers' did not distinguish themselves as combatants by uniform or by carrying arms openly during or in preparation for the engagement, most likely 'combatant' status would be stripped by a tribunal. Instead, cyber attackers captured in the IHL context would be prosecuted as prisoners of war. In particular, given the nature of cyber warfare, it may be possible to prosecute those accused under Protocol I, Article 37 provisions for prohibiting perfidy. Specifically cyber attackers disguise their

[224] The U.S., for example, is party to 18 law of war treaties.
[225] Protocol I, Art. 43.
[226] Protocol I, Art. 44.

attacks on state and civilian networks alike as innocent requests for information, in the same manner as a soldier who feigns civilian status would be prosecuted under Article 37(c).[227]

Second, the laws of war maintain a distinction between military and civilian personnel, objects and installations, and limit attacks to military objectives.[228] Protocol I, Article 52.2 states that "military objectives are limited to objects which are effective contributions to military action and whose destruction offers a military advantage."[229] In other words, infrastructure that makes no direct contribution to the war effort is immune from deliberate attack. To illustrate using the Estonia case study, the fact that everything from banks to broadcasters to government services and air-traffic control was attacked signifies that this cyber attack failed to discriminate between military and civilian targets and thus, in an armed conflict, would have ran afoul of Protocol I, Article 51(4). The attacking state could counter, as NATO did when it attacked the Serbian TV towers that were used to broadcast propaganda that perpetuated genocide during the Kosovo conflict, that these facilities were used for command and control and thus were in fact military objectives.[230] Though this is a fine line, the widespread and wholly indiscriminate nature of this broad cyber attack is inconsistent with this ICTY precedent. Given that the internet is essential to the functioning of Estonian society, from banking and shopping to voting, and that the purpose of the attacks was to terrorize the populace, in an armed

---

[227] "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, Art. 37.
[228] Protocol I, Art. 48.
[229] Protocol I, Article 52.2.
[230] Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia. The Attack on the RTS (Serbian Radio and TV Station) in Belgrade on 23/4/99. Available at: http://www.un.org/icty/pressreal/nato061300.htm. Last visited: 06/12/2008.

conflict these attacks ran afoul of the laws of war. Recognizing this nature of cyber attacks, the DOD has stated that targeting analysis must be conducted for CNAs just as it traditionally has been conducted for attacks using traditional weapons.[231] This distinction did not occur in Estonia.

Third, IHL prohibits disproportionate attacks. The law of war places much of the responsibility for collateral damage on a defending force that has failed to properly separate military targets from noncombatants and civilian property.[232] The law of proportionality is codified in Protocol I, Article 51 in which "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]."[233] Implicit in this principle then is the balancing act that occurs, measuring military advantage against 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 treaties existing under IHL for certain limited responses to cyber attacks.[234] In fact, according to the DOD, "The law of war is probably the single area of international law in which current

---

[231] DOD, *supra* note 33.
[232] *Id*.
[233] Protocol I, Art. 54.
[234] For example, the Hague Convention Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land 1907, articles 8 and 9 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."

legal obligations can be applied with the greatest confidence to information operations."[235] This fact is especially important given how many treaties lose affect during armed conflicts.[236] Collectively, these principles form the basis of non-derogable norms that should be applied with the greatest confidence to IW.

ii. *Information Warfare, International Criminal 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."[237] Increasingly the use of force during armed conflict is being assessed through the perspective of human rights law especially in the aftermath of the September 11, 2001 attacks.[238] This is true even though as some authors have argued that "some 95 percent of all the problems and challenges posed by criminals and hackers will have to be dealt with in the same way as other criminal activities, to be dealt with by law enforcement, and treated as normal actuarial losses and 'cost of doing business.'"[239] It has also been argued that ninety percent of the burden of preventing cyber attacks lays on the private sector. This introduces significant expense and problems of coordination among businesses, international organizations, and governments, which is especially troubling given the checkered history of international efforts to criminalize cyber terrorism.[240]

---

[235] DOD, *supra* note 33.
[236] 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 215 at 289.
[237] Watkin, *supra* note 93.
[238] *Id*.
[239] CORDESMAN, *supra* note 46.
[240] *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.

The first efforts to coordinate efforts to stem cyber crime and terrorism stretch back nearly three decades. As a result of urging by then Assistant U.S. Attorney General Telly Kossack, Interpol began harmonizing disparate national legislation on cyber crime for Interpol in 1981.[241] Progress was slow, but quickened 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 "safe havens" anywhere in the world.[242] This was articulated on May 11, 2004 when the G8 issued a Justice and Home Affairs Communiqué stating: "Continuing to strengthen domestic laws…[t]o truly build global capacities to combat terrorist and criminal uses of the Internet, all countries must continue to improve laws that criminalize misuses of computer networks and that allow for faster cooperation on Internet-related investigations."[243]

Various other regional and UN initiatives have sense been enacted to deal with cyber attacks through harmonizing divergent national laws. The Council of Europe's Convention on Cybercrime came into force on July 1, 2004, providing another vehicle through which to harmonize divergent state cyber crime laws. 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 (2001).[244] Similarly, the Organization of American States

---

[241] Stein Schjolberg, Chief Judge, Moss Tingrett Court, Norway. "Law Comes to Cyberspace," *A presentation at the 11th UN Criminal Congress,* Apr. 18-25, 2007, Bangkok, Thailand. Workshop 6: Measures to combat computer-related crime.
[242] It should be noted that since then only one G8 member, Russia, has been accused of harboring cyber attackers (those from the Estonian attacks).
[243] *G8 Justice and Home Affairs Communiqué*, Washington DC, May 11, 2004, para. 10.
[244] Convention on Cybercrime. Budapest, 23.XI.2001.

("OAS") approved on April 28-30, 2004 a resolution which stated that member states should "evaluate the advisability of implementing the principles of the 2001 Council of Europe Convention on Cybercrime and consider the possibility of acceding to that convention…Based on the Council of Europe Convention on Cybercrime and the UNGAR, we may reach our goal of a global legal framework against cybercrime."[245] Another subsequent UNGAR was adopted in 2000 on combating the criminal misuse of information technologies. The language in this non-binding resolution includes the passage that "States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies…legal systems should protect the confidentiality, integrity, and availability of data and computer systems from unauthorized impairment and ensure that criminal abuse is penalized."[246] Together, these regional initiatives and accords have made important progress in the fight to unify diverse national cyber criminal law into the beginnings of a global regime regulating cyber terrorism.

International efforts are also underway to enshrine cyber attacks in 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 conference recommended that a review conference pursuant to the article 123 of the Statute of the ICC consider such crimes with the view of their inclusion in the list within

---

[245] Website of the Organization of American States: www.oas.org. Last visited: 01/28/2008.
[246] Dec. 4, 2000 (A/res/55/63). Available at : http://daccessdds.un.org/doc/UNDOC/GEN/N00/563/17/PDF/N0056317.pdf?OpenElement. Last visited: 01/28/2008.

the jurisdiction of the Court.[247] Cyber attacks and serious cybercrimes should be included by amendment in 2009 in accordance with articles 121 and 123.[248] If this were to occur, the international community would no longer have to lurch from attack to attack on a case-by-case basis, but instead be confident in a multilateral response to cyber attack already rooted in the international system.

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 raises to the level of an armed conflict, do not fit in nearly with either paradigm. A threatened use of weapons of mass destruction by a transnational terrorist group may not be amenable to a human rights review approach, for example. Even so, classifying global terrorism may be an easier case study than IW given that most terrorist attacks have a tangible harm. As such, aggressive acts in cyberspace can only be assessed by their consequences.[249]

Similar to the debate surrounding IW, concerns exist that shifting counter terrorism from a crime control to a conflict model would displace 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. One aspect of human rights related to IW is that of privacy. A potential patchwork of privacy protections could include the right to expect and enjoy physical privacy; privacy of personal information; privacy of communications and space; and

---

[247] Rome Statute U.N. Doc. A/CONF.183/9 of 17 July 1998, Art. 123.
[248] Defined by the Council of Europe Cybercrime Convention of 2001.
[249] 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 88.

freedom from surveillance. Thus there is an inherent need for compromise between individual civil and political rights, on the one hand, and economic and national security interests on the other.

VI. Summary of the Present Legal Regime and a Proposal Going Forward

Neither IHL, nor IHRL, or any of the other treaty systems or legal principles discussed in this paper serves as a standalone analogue to deal with state-sponsored IW. Yet the international community is already being confronted with situations in which cyber attacks are being state-sponsored to a greater or lesser extent. In the case of the Estonian assault for example, the preponderance of available evidence points to some degree of Russian involvement in inciting and carrying out the cyber attack on Estonia. But regardless of the level of Russian involvement, the cyber attack did not rise to the level of an armed attack required to activate IHL. Nevertheless, it should not be possible for states that sponsor cyber attacks to avoid responsibility. This necessitates the creation of a two-tiered system in international law for response to cyber attacks, a default state which is active during peace-time and another which is engaged in an international armed conflict.

The capacity for existing treaty frameworks to form a useful legal regime to deal with cyber attacks that do not reach the level of an armed attack may be illustrated by using the Estonian case study. The attack disrupted the functioning of government, and thus the "safety services" referred to in Article 35 of the ITU. If Russia were attributed blame for the cyber attack then, it would be in breach of the ITU Charter and Estonia could receive reparations or seek other enforcement actions available under international law. The Estonian government could also hold liable those companies most affected by

cyber attacks if it was determined that 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. Similarly Estonia could invoke UNCLOS, since it is a coastal state, which is relevant 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 sent subversive code through submarine cables to a coastal state would be in breach of their customary and international law obligations. 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 UNSC under its Chapter VII authority to regulate breaches of international peace and security. Finally, Estonia could use MALTs, extradition treaties, and potentially eventually the ICC to bring those responsible to justice in the victim nation if the host nation be unwilling or unable to prosecute those responsible (as was the case with Russia after the Estonian cyber attack). 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.[250] Both regimes have much to

[250] 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. Watkin, *supra* note 93. Theodor Meron has noted that "because human rights law, or at a minimum its non-derogable core, continues to apply in times of armed conflict, gaps in protection under the law of war can be filled in some circumstances." *Id.* There is an ongoing tension between efforts to incorporate humanitarian standards into non-international armed conflicts and the view of states that such

offer in forming a final regulatory system. For example, it may be possible to graft on IHL's proportionality principle to IHRL. A solely human rights framework is insufficient since it would not address the relative importance of objects and people, or the proportionate assessment regarding the number of non-combatant casualties. Moreover, command responsibility is well-established under IHL – commanders should apply the same IHL principles to computer attacks that they do to the use of bombs and missiles.[251] Another important distinction between IHRL and IHL in terms of controlling the use of force is that the former seeks review of every use of lethal force by agents of the state, while the latter is based on the premise 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 controlling how such a policy is implemented.[252]

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 have a positive impact on the regulation of the use of force during armed conflict.[253] The Appeals Chamber's decision in *Tadic*, the Statute of the ICTR, and the Rome Statute of the ICC have recognized the need to expand the reach of the accountability process under IHL to conflicts of all types,[254] as has had the

---

conflicts involve the legitimate suppression of criminal activity. *Id.* The challenge lies in separating incidents that are simply criminal in nature from those that form part of the armed conflict.

[251] Reynolds, *supra* note 191.

[252] *Id.*

[253] Watkin, *supra* note 93.

[254] *Id.*

Inter-American Court of Human Rights which has applied 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 that IHL should be applied.[255] The ECHR has reached a similar conclusion in *Ergi v. Turkey*.[256]

The dual track legal framework described above is applicable to CNAs that do not rise to the level of an armed attack as well as those that do. Yet the regime is by no means preferable to the adoption of a comprehensive treaty dealing exclusively with cyber security. Such a regime 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.[257] An example is the Cyber Crime Pact Council of Europe December, 2000.[258] Another is the 2000 Proposal for an International Convention on Cyber Crime and Terrorism drafted at Stanford University (hereinafter "Stanford Proposal").[259] The findings of the Stanford Proposal include several points arguing for greater international cooperation in combating cyber attacks:

---

[255] IACHR, Report No. 55/97 (Case 11.137, Abella v. Argentina), in Annual Report of the CIDH 1997, OEA/Ser.L/V/II.98, doc. 7 rev., April 13, 1998, at 307. See also, A. Cançado Trindade, Tratado de Direito Internacional dos Direitos Humanos, Vol. I, 1st ed. (Sérgio A. Fabris ed. 1997) at 269-80 (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.

[256] ECHR : Ergi v.Turkey Publication: 1998-IV, no. 81 (holding that "the responsibility of the State is not confined to circumstances when there is significant evidence that misdirected fire from agents of the State has killed a civilian. It may also be engaged where they fail to take all feasible precautions in the choice of means and methods of a security operation mounted against an opposing group with a view to avoiding and, in any event, to minimizing, incidental loss of civilian life.").

[257] An Assessment of International Legal Issues in Information Operations, DOD, OGC, May 1999.

[258] Cyber Crime Pact Council of Europe, Dec. 2000.

[259] Stanford Treaty Proposal, *supra* note 29.

> Cyber criminals exploit weaknesses in the laws and enforcement practices of States, exposing all other States 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.[260]

Article 12 of the Stanford Draft proposes an international Agency for Information Infrastructure Protection ("AIIP"). The AIIP is intended to serve as a formal structure in which interested groups will cooperate through 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.[261] 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.[262] This underscores the fact that most international cooperation dealing with international information operations law has emphasized the need to cooperate on international

---

[260] *Id.*

[261] The Stanford Proposal states that all States 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. Stanford Treaty Proposal, *supra* note 29.

[262] 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. States 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 29.

criminal efforts to detract 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 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 make use of the effects principle as a mechanism for bypassing 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 better 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, i.e., 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 nature 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 the UNCLOS saga has taught should be avoided lest the commons 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.[263]

International law is greatly influenced by events – after all, "The life of the law has not been logic; it has been experience."[264] 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.[265] Just as much of an impetus is the United States' refusal to negotiate to prohibit these weapons so as 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.

CONCLUSION

The form and functioning of an ultimate international regime dealing with cyber attacks will depend largely on how the international community reacts 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 in its mechanism. This

[263] 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.
[264] DOD, *supra* note 33.
[265] *Id*.

does not put aside state responsibility, but instead focuses international attention first and foremost 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. Afterwards, attribution and state responsibility will have to be determined, as has been argued by using the *Tadic* standard rather than *Nicaragua*.

There is little likelihood that the international legal system will soon operate a coherent body of "information operations" law. More needs to be done to precisely define the criteria used to distinguish between normal transborder data flows from other cyber activities that may constitute a cyber attack.[266] In some areas, such as the law of war, existing legal principles can be applied with considerable confidence once a cyber attack reaches the level of an armed attack. As far as active defense as self-defense – it is far from clear where the international community will come out.[267] The main failings of existing international treaties that touch on cyber law 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 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 an imperfect regime, the international community should use all of the tools at its disposal to begin dealing with the issue of cyber attacks. Nations are increasingly making use of the weapons potential of cyberspace, making the likelihood of

[266] Joyner, *supra* note 15.
[267] DOD, *supra* note 33.

attacks increase. Emblematic of this trait, the U.S. Air Force adopted a new mission statement in 2005 "to fight in air, space, and cyberspace."[268]

The best way to ensure a comprehensive approach to lessening the occurrence of IW is through a new international accord dealing exclusively 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 United States should drop its opposition to such a treaty regime. Without such an organization, the international community will lurch from case-to-case with the worry that next time, the case of Estonia may resemble merely a step along the way to Net War Version 2.0. When IW reaches the scale of nuclear war, a new and distinct regime incorporating elements of existing international law, notably IHL, is required lest nations risk systemic infrastructure crashes that not only will cripple societies, but could quite possible shake the Information Age to its foundations.

[268] Mitch Gettle, *Air Force Releases New Mission Statement*, Air Force Print News, Dec. 8, 2005. Available at: http://www.af.mil/news/story.asp?storyID=123013440. Last visited: 4/20/2008.