THE UNCHARTED WATERS OF CYBERSPACE: APPLYING THE PRINCIPLES OF INTERNATIONAL MARITIME LAW TO THE PROBLEM OF CYBERSECURITY

William M. Stahl[*]

TABLE OF CONTENTS

[*] J.D., University of Georgia, 2012; B.B.A., Emory University, 2007.

I. INTRODUCTION

The advent of the Internet has brought with it a fundamental change in the way nations and their citizens engage in global economic activity, manage critical infrastructure, and communicate with one another. Although the Internet is ubiquitous in modern society and plays a critical role in many aspects of everyday life, it was never intended to be used by so many and for the vast number of functions it performs today. To the contrary, the Internet was designed to allow a small group of scientists to share unclassified reports; it was not designed to transfer sensitive information securely.[1] Moreover, the Internet was not designed to allow for easy monitoring of user behavior and was not designed to protect against attacks originating from within the Internet itself.[2] That same inherent design persists today, largely unchanged, while the Internet's uses have evolved drastically.[3] The ease and anonymity with which people throughout the world can access information systems via the Internet, coupled with the Internet's inherently flawed design, have created a vulnerability to cyberattacks on an unprecedented scale.[4] Targets of cyberattacks are diverse, and the costs of such attacks are necessarily borne by consumers, private industry, and governments alike.[5] The frequency and sophistication of cyberattacks are likely to increase, as instructions for sophisticated attack methods are made more widely available to would-be attackers via the Internet, reducing the technical knowledge required to carry out an attack.[6]

All the same, the Internet has become vital in carrying out basic economic and governmental functions, including management of infrastructure[7] and the international financial network.[8] Cyberattacks pose a greater risk to

---

[1] HOWARD F. LIPSON, CARNEGIE MELLON SOFTWARE ENG'G INST., TRACKING AND TRACING CYBER-ATTACKS: TECHNICAL CHALLENGES AND GLOBAL POLICY ISSUES 13 (2002).

[2] *Id.* at 13–14.

[3] *See* Kelly A. Gable, *Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, 43 VAND. J. TRANSNAT'L L. 57, 67–69 (2010) (describing the Internet's historical purpose and the exponential increase in the types of devices with Internet access over the past two decades).

[4] *See id.* at 73–87 (describing threats the Internet poses to national and international security).

[5] *See, e.g.*, *id.* at 84–85 (noting the security threat the Internet poses to the international financial system and that a cyberattack on even one large U.S. bank would have a greater global economic impact than the terrorist attacks of September 11, 2001).

[6] *See* LIPSON, *supra* note 1, at 9–10 (noting the declining average technical knowledge of attackers versus the increasing sophistication of attacks over time).

[7] Walter Gary Sharp, Sr., *The Past, Present, and Future of Cybersecurity*, 4 J. NAT'L SECURITY L. & POL'Y 13, 14–15 (2010).

[8] Gable, *supra* note 3, at 76–77.

developed nations, where virtually all governmental operations require the support of computer systems.[9] That is not to say that lesser-wired nations will be shielded from collateral impact; with the convergence of today's commercial systems, a coordinated cyberattack against stock markets and banks could erode consumer confidence and effectively create a global financial crisis.[10]

The international community has a clear interest in developing a comprehensive, multilateral cybersecurity framework because the widespread use of the Internet in every aspect of daily life has created an almost "irreversible dependence" on its technological benefits,[11] and because the conceptual underpinnings of existing legal frameworks are not readily adaptable to threats emerging in cyberspace.[12] Many developed countries have taken steps toward developing comprehensive cybersecurity policy; however, these governments acknowledge that unilateral action will not suffice.[13] A recent U.S. government review of cybersecurity policy recognized the need for " 'a strategy for cybersecurity designed to shape the international environment and bring like-minded nations together on a host of issues, such as technical standards and acceptable legal norms regarding territorial jurisdiction, sovereign responsibility, and the use of force.' "[14] International cooperation is essential because the most devastating cyberattacks are often carried out using multiple computers simultaneously from around the globe, hampering the aggrieved nation's ability to pursue justice unilaterally as a result of jurisdictional issues.[15] Despite the fact that many attacks are carried out across multiple jurisdictions and often originate in foreign countries,[16] current international law does not recognize nations as duty bound to assist in investigating a cyberattack that allegedly originated within their jurisdiction.[17] As a result, nations attempting to develop and

---

[9] *See, e.g.*, *id.* at 77–78 (describing the dependence of the U.S. government on the Internet).

[10] *Id.* at 84.

[11] *Id.* at 64.

[12] *See* SUSAN W. BRENNER, CYBERTHREATS 6–7 (2009) (positing that cyberwarfare, cyberterrorism, and cybercrime differ from analogous activity in the physical world in a way that challenges the conceptual underpinnings of applicable legal regimes).

[13] *See, e.g.*, Jeffrey Hunker, *U.S. International Policy for Cybersecurity: Five Issues That Won't Go Away*, 4 J. NAT'L SECURITY L. & POL'Y 197, 197 (2010) (noting the U.S. government's view of cybersecurity as a global issue calling for international cooperation).

[14] Gable, *supra* note 3, at 89 (quoting EXEC. OFFICE OF THE PRESIDENT OF THE U.S., CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE, at iv (2009), *available at* http://www.whitehouse.govassets/documents/Cyberspace_Policy_Review_final.pdf).

[15] *Id.* at 101.

[16] *Id*.

[17] Christopher E. Lentz, Comment, *A State's Duty to Prevent and Respond to*

enforce cybersecurity measures often lack international support from nations where a given cyberattack likely originated.[18] Even when a victimized nation does receive cooperation from a foreign nation under, for example, a Mutual Legal Assistance Treaty (MLAT), evidentiary requests often take several months to be honored, if at all.[19] Since evidence of a cyberattack may be disposed of quickly, current international agreements like MLATs providing for law-enforcement cooperation operate too slowly to be effective.[20]

In the absence of codified law, nations attempting to enforce their cybersecurity regimes against foreign perpetrators have done so largely by analogy to international law governing military use of force and domestic criminal law.[21] Existing international cybersecurity agreements are narrow in scope, focusing on criminal activity in cyberspace, and fail to adequately account for cyberspace as a platform for terrorism and military action.[22]

The shortcomings of existing international law were apparent during the cyberattack perpetrated against Estonia in 2007. The attack on Estonia represents the best-known example of a coordinated cyberattack on a sovereign nation's critical infrastructure, and it illustrates the need for an international effort to coordinate cybersecurity policy.[23] The attack was debilitating, disrupting government communication support systems, and the online platforms of banks, retailers, and newspapers.[24] The damage inflicted by the attack necessitated a response from the Estonian government; however, the government could do very little in the absence of established procedures for international cooperation because the attacks originated in foreign jurisdictions.[25] The attack demonstrated that the Internet is a viable alternative to traditional modes of warfare and terrorism. It also reaffirmed

---

Cyberterrorist Acts, 10 CHI. J. INT'L L. 799, 800 (2010).

[18] *See* Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 201 MIL. L. REV. 1, 9 (2009) (noting several major states' refusal to participate in international efforts to curb cyberattacks and a belief among security experts that China and Russia sponsor such attacks to varying degrees).

[19] LIPSON, *supra* note 1, at 51 n.48.

[20] *Id.* at 51 & n.48.

[21] Sklerov, *supra* note 18, at 6.

[22] *See id.* at 5–10 (noting the prevailing view under international law that states must treat international cyberattacks as a criminal matter because of the constraints imposed by existing international law governing war).

[23] Scott J. Shackelford, *Estonia Three Years Later: A Progress Report on Combating Cyber Attacks*, J. INTERNET L., Feb. 2010, at 22, 22.

[24] Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED (Aug. 21 2007), http://www.wired.com/politics/security/magazine/15-09/ffestonia?currentPage=all.

[25] Sklerov, *supra* note 18, at 5, 8.

that the absence of a comprehensive international legal framework with the flexibility to cope with the complex nature of cyberspace has hampered efforts to deter such acts and prosecute those responsible.[26]

To prepare for and deter similar future attacks, the international community should use existing international legal instruments and principles as guidance in developing a comprehensive legal framework to combat cyberaggression. One such instrument is the United Nations Convention on the Law of the Sea (UNCLOS),[27] which, among other things, addresses the duty of sovereign states to combat piracy outside its jurisdiction, including in international waters.[28] Because UNCLOS governs legal relationships relating to the sea—which, like the Internet, transcends legal regimes based on traditional notions of territorial jurisdiction—UNLCOS's treatment of piracy and the obligations it imposes on states provide meaningful guidance in developing international obligations related to cybersecurity.

This Note calls for the development of an international legal framework addressing cybersecurity based on UNCLOS and the duties and obligations it imposes to combat piracy. Part II discusses the history of the Internet, the nature of weapons used in cyberattacks, recent examples of a cyberattack's destructive potential, and the legal challenges posed by cyberattacks. Part III discusses the status of the international community's efforts to formulate a response to the threat of cyberaggression, addresses the legal challenges posed by attempting to categorize a given cyberattack under existing legal definitions, and highlights legal challenges faced by nations attempting to operate within the limits of existing law, including domestic and international criminal law regimes and the law of war. Part IV identifies the similarities between the nature of piracy and cyberaggression, discusses the problems raised by the international community's ongoing efforts to combat piracy by way of international law, and advocates for the use of UNCLOS and its treatment of piracy as a viable blueprint for imposing international obligations to combat cyberaggression.

---

[26] *See id.* at 6–7 (noting the absence of a comprehensive international treaty addressing cybersecurity and discussing the resulting legal challenges that arise in situations like the Estonia attack).

[27] United Nations Convention on the Law of the Sea, Dec. 10, 1982, 1833 U.N.T.S. 397 [hereinafter UNCLOS].

[28] *Id.* art. 100.

II. BACKGROUND: THE SPECTER OF CYBERAGGRESSION AND RECENT ATTACKS

As the frequency and sophistication of cyberattacks continue to increase, cybersecurity has become one of the most pressing issues facing the international community and the modern state.[29] Additionally, as nations attempt to respond to these attacks, "the variable levels of malicious cyber activity" further aggravate the problem of determining an appropriate response.[30] Recent incidents demonstrate the diverse nature of cyberattacks and the international community's lack of an effective approach to incident deterrence and response.[31] These attacks also underscore the challenge of identifying the nature of a given attack and the parties responsible for the attack, and of developing a legal framework flexible enough to effectively counter the unique circumstances of a given cyberattack. The origin of the threat posed by cyberspace is found in the architecture of the Internet itself.

A. A Brief History of the Internet

The reasons for the creation and development of the Internet provide essential background for understanding the complex legal and technological challenges of combating cyberattacks. Originally known as ARPANET, the Internet was first developed in the 1960s by the Pentagon to create a system of interconnected computers for national security purposes.[32] In the mid-1980s, a common method of network communication known as TCP/IP Protocol was adopted as the Internet's standard for data transfers between computers,[33] and it was later used by the National Science Foundation to

---

[29] *See* Gable, *supra* note 3, at 60 (arguing that the Internet has exponentially increased the threat terrorism poses to international security and has become one the greatest threats to the security of the modern state); *see also* Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 192, 194–95 (2009) (noting the potential of a sophisticated, professionally coordinated cyberattack to destroy or damage much of a nation's infrastructure with effects similar to an electromagnetic pulse from a nuclear weapon).

[30] Jonathan A. Ophardt, *Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield*, 2010 DUKE L. & TECH. REV. 003, ¶ 7 (2010).

[31] Sklerov, *supra* note 18, at 4–7 (noting attacks on Georgia, the United States, and Estonia and the challenges faced by each nation in responding under existing international legal frameworks).

[32] Gable, *supra* note 3, at 67–68.

[33] LIPSON, *supra* note 1, at 5 n.4 ("A network protocol is a common language for communicating across a network. The protocol specifies the rules for data format and transmission." (emphasis omitted)).

establish connections between universities throughout the United States.[34] TCP/IP remains the foundation for network communications on today's Internet.[35]

Initially, the Internet was only accessible to governmental divisions, and their computers were presumed secure simply by virtue of their access to the network.[36] Since all Internet users at the time were known and trusted, TCP/IP Protocol's only goal was to facilitate communication, resulting in an insecure framework.[37] The National Science Foundation began to connect other countries to the Internet in 1988, and transferred control of the Internet to private entities in 1995.[38] Initially, the Internet was only accessible through mainframe and desktop computers, the locations of which were static and readily traceable, unlike the wide array of wireless devices that are used to access the Internet today.[39] As the Internet developed, many separate, smaller networks based on the same fundamental structure developed independently. The smaller networks were (and continue to be) used by corporations, banks, federal reserves, and many other organizations to transfer money and conduct business.[40]

Today's Internet is a network of networks, "comprised of a myriad of host computer systems joined together by communications links (wired and wireless)."[41] These host computer systems communicate with one another using TCP/IP network protocol, which dictates the format and method of transfer of data.[42] Computers use routers to transfer TCP/IP formatted data over the Internet.[43] These routers operate by identifying data's destination addresses and transferring that data to another router closer on the network to its destination until it reaches its destination.[44] The system of routers ensures that there are multiple paths data can take to reach its destination, which allows the system to continue to function in the event that communication links or routers are out of service.[45] The network of routers is not discerning; it transfers information from its origin to its destination but lacks the ability,

---

[34] Gable, *supra* note 3, at 68.
[35] LIPSON, *supra* note 1, at 5.
[36] Gable, *supra* note 3, at 78.
[37] *Id.*
[38] *Id.* at 68–69.
[39] *Id.* at 69.
[40] *Id.*
[41] LIPSON, *supra* note 1, at 7.
[42] *Id.*
[43] *Id.*
[44] *Id.*
[45] *Id.*

by virtue of its design, to ascertain the content of the data being transferred.[46] The routing system's structure was intended to ensure the Internet's continuing functionality in the event of an external attack, but it was not designed to prevent damage caused by the very data that it transfers.[47] The lack of focus on the security risks during the Internet's development, the exponential growth of Internet accessibility since its inception, and the existence of numerous parallel networks used by vital industries such as the financial sector are a large part of the challenges posed by modern cyberattacks.

B. The Mechanics of a Cyberattack

The Internet's basic structure, the growing availability of Internet access, and decreasing access costs have resulted in essentially anonymous global access, which increasingly facilitates the availability, "assembly and use of cyber weaponry on a global scale."[48] Moreover, individual Internet use is difficult to trace because the original Internet was designed to facilitate information flow and collaboration as opposed to commercial and government purposes.[49] As a consequence, Internet Service Providers track Internet access based on overall usage, which does not involve monitoring the type of content sent or received by their customers.[50] Thus, cyberattackers can operate free from close scrutiny of their Internet use and behavior.[51]

Generally, cyberattacks are separated into three major categories: (1) "automated malicious software delivered over the Internet," (2) "denial-of-service[ ] attacks," and (3) "unauthorized remote intrusions into computer systems."[52] Recent high profile attacks perpetrated against Estonia, Georgia, and Iran[53] have involved a combination of these attack methods, but two types of attack are of particular importance because they are relatively easy to carry out and they are extremely effective. The first type utilizes malware,

---

[46] Sharon R. Stevens, *Internet War Crimes Tribunals and Security in an Interconnected World*, 18 TRANSNAT'L L. & CONTEMP. PROBS. 657, 660 (2009).
[47] LIPSON, *supra* note 1, at 14.
[48] Ophardt, *supra* note 30, ¶ 21.
[49] Stevens, *supra* note 46, at 660–61.
[50] LIPSON, *supra* note 1, at 13.
[51] *See id.* at 14–16 (explaining that advanced users can easily modify the content of information sent from an apparently trustworthy source or forge a source address, circumventing the Internet's only filtering mechanism).
[52] Sklerov, *supra* note 18, at 13–14.
[53] *See infra* Part II.*C* (describing these attacks).

which was traditionally classified as either a virus or worm.[54] Malware typically infects a computer system through e-mail or when a user visits infected websites, and the nature of its interaction with the system depends on whether it operates like a virus or worm.[55] For example, a virus cannot replicate itself until a user runs the infected program and can lay dormant until that occurs.[56] When it does, the virus replicates itself, infiltrates other programs on the host computer, and modifies them to carry out functions other than those originally intended.[57] Worms, on the other hand, are themselves programs and can replicate independently.[58] Worms can spread within a host computer system and also to any system connected to it by a network or the Internet.[59] As malware has grown more sophisticated it has been further classified by its specific function, common examples of which are "Trojan horses, rootkits, sniffers, exploits, bombs, and zombies."[60] Many cyberattacks involve another form of malware that allows multiple computers to be remotely controlled by—or "slaved" to the commands of—a single operator who can dictate the behavior of those computers.[61] Cyberattackers can effectively magnify the potential devastation caused by an attack by using this slaving technique.[62] This method of attack, used in the 2007 cyberattack on Estonia, "allow[s] a cyberattacker to implement a coordinated attack from numerous locations, including within the target network, with very limited warning for a nominal cost."[63]

The second frequently used method of cyberattack is known as a denial-of-service (DOS) attack.[64] A DOS attack is initiated from a single computer and overwhelms a target computer system with requests until the system can no longer function properly, denying users access to and use of the targeted system.[65] A DOS attack operates by paralyzing the target system's functionality, while malware operates by changing the function the target system is programmed to perform. Both methods capitalize on basic flaws in

---

[54] Symantec, the maker of popular Norton antivirus software, defines malware as "a category of malicious code that includes viruses [and] worms. . . . [which] utilize popular communication tools to spread." *Malware*, NORTON, http://us.norton.com/security_response/malware.jsp (last visited Nov. 21, 2011).

[55] Sklerov, *supra* note 18, at 14–15.

[56] *Id.* at 15.

[57] *Id.* at 14–15.

[58] *Id.* at 15.

[59] *Id.*

[60] *Id.*

[61] Ophardt, *supra* note 30, ¶ 20.

[62] *Id.*

[63] *Id.* ¶ 21.

[64] Sklerov, *supra* note 18, at 14.

[65] *Id.* at 16.

the Internet's architecture and are often used in conjunction with one another to maximize damage to the target system.[66] The recent cyberattacks on Estonia and Georgia offer vivid examples, as they were carried out using a combination of malware and DOS known as a Distributed Denial of Service (DDOS).[67]

In a DDOS attack, hackers use malware to take control of numerous computers and use the hijacked computers—referred to as "zombies"—to send a massive series of data packets to the targeted networks.[68] It is particularly difficult to track a DDOS attack to its original source because the owners of the hijacked computers are rarely aware that their systems are being used remotely to carry out a cyberattack.[69] A network of compromised "zombie" computers is often referred to as a "botnet."[70] In 2007, Vint Cerf, widely recognized as one of the fathers of the Internet, estimated that as many as 25% of networked computers worldwide, or 150 million computers, may be part of botnets.[71] Although hackers use other methods in carrying out attacks, malware, DOS, and DDOS used in recent, high profile attacks demonstrates the urgency of addressing cyberattacks and the challenges they pose for victimized nations.

C. The Cyberattacks on Estonia, Georgia, and Iran

In 2007, Estonian public and private sectors suffered a prolonged cyberattack campaign that lasted several weeks.[72] Estonia, formerly under the control of the USSR, decided to remove a Soviet statue built to commemorate victory over Nazi Germany from the town of Tallinn.[73] The decision sparked protests from ethnic Russians living in Estonia, and even angered Russian government-funded groups outside of Estonia.[74] Within days of the statue's removal, a coordinated cyberattack began.[75] The attack, which occurred in waves over several weeks, "disrupt[ed] the websites of the Estonian President and Parliament, the vast majority of Estonian ministries,

---

[66] *See* Gable, *supra* note 3, at 78–80 (arguing that the Internet's use of TCP/IP Protocol is responsible for its vulnerability to cyberattacks).
[67] BRENNER, *supra* note 12, at 1.
[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] Tim Weber, *Criminals 'May Overwhelm the Web,'* BBC NEWS (Jan. 25, 2007), http://news.bbc.co.uk/2/hi/business/6298641.stm.
[72] Shackelford, *supra* note 29, at 202–03.
[73] *Id.* at 205 & n.67.
[74] *Id.* at 205–06.
[75] Davis, *supra* note 24.

three of the country's six largest news organizations, and two of its major banks."[76] The crippling impact of the attack was due, in part, to the fact that the Estonian government conducts most of its basic operations using the Internet.[77] The prolonged disruption of critical websites caused widespread unrest and rioting; 150 people were injured and one Russian national was killed.[78] Although the attacks originated within Russian jurisdiction, Estonia was never able to link them directly to the Russian government.[79] However, the impression that Russia was behind the attacks during the ensuing chaos led some Estonian officials to advocate for an official request for assistance pursuant to Article V of the North Atlantic Treaty,[80] which requires members of the North Atlantic Treaty Organization (NATO) to assist an ally in the event of an armed attack.[81] Article V expressly states that such assistance may include use of "armed force" against the aggressor.[82] This marked the first time in NATO history that a member state sought assistance from NATO allies in response to an Internet-based attack on its infrastructure.[83]

Although the Estonian government claims to have proof that the earliest attacks originated from Russian government computers, the nature of a DDOS attack makes determining the original source of the attack difficult.[84] Moreover, hackers who use botnets continue to develop increasingly sophisticated command structures that make the task of tracing an attack to the original source nearly impossible.[85] One development is the use of tiered command and control, which allows users of botnets to distribute functions "across many different, geographically dispersed computer servers [unlike] earlier versions, which had a single point of command."[86] It is evident, though, that unaffiliated individuals "who were goaded into attacking Estonian websites in Russian-language chat rooms" were responsible for at least part of the attacks.[87] Their estimated involvement in the attack, however, is only a fraction of the estimated one million zombie computers used to overload Estonian websites and governmental systems.[88] A

---

[76] Gable, *supra* note 3, at 61.
[77] *Id.*
[78] Shackelford, *supra* note 29, at 194.
[79] Sklerov, *supra* note 18, at 8.
[80] Shackelford, *supra* note 29, at 194.
[81] North Atlantic Treaty art. 5, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243.
[82] *Id.*
[83] Shackelford, *supra* note 23, at 25.
[84] BRENNER, *supra* note 12, at 1.
[85] *Id.* at 2.
[86] *Id.*
[87] Shackelford, *supra* note 29, at 207.
[88] BRENNER, *supra* note 12, at 2.

subsequent U.S. government investigation found that it is not likely that Russian security agencies were responsible for the attacks, but rather politically driven hackers[89] Although there is no indisputable evidence implicating the Russian government's direct involvement in the attack, it coincided with a political dispute between Estonia and Russia, and several Estonian websites were replaced with Russian propaganda.[90]

It is clear, however, that a number of Russian computers were used in the attack, but Russia has refused to assist Estonia's criminal investigation despite Estonia's request for assistance.[91] Russia's refusal to cooperate only compounds Estonia's already difficult task of identifying and prosecuting the responsible parties, is representative of the unique jurisdictional obstacles posed by cyberattacks, and illustrates the pressing need for an international framework that facilitates, or even mandates, cooperation. Without Russian cooperation, which is not required by existing international law,[92] Estonia's criminal investigations have been, for the most part, unsuccessful.[93]

While political upheaval predated the cyberattack on Estonia, a cyberattack against Georgia in 2008 immediately preceded Georgia's armed conflict with Russia over the disputed territory of South Ossetia.[94] The attack was designed to disrupt the Georgian government's ability to communicate, demonstrating that a cyberattack can complement traditional armed conflict.[95] The DDOS attack on Georgia began weeks before the armed conflict, and it "overloaded and effectively shut down Georgian servers."[96] A DDOS attack can be enormously effective in disrupting an enemy's ability to coordinate defense measures in preparing for an armed conflict, transmit emergency communications to its citizens, and communicate with the outside world.[97] The attack on Georgia is an example of the crucial role that cyberattacks may play in future instances of armed conflict. Cyberattacks are a cost effective alternative or complement to traditional warfare, as the cost of initiating a cyberattack relative to developing, producing, and using traditional weaponry is nominal. If states can " 'fund an entire cyberwarfare campaign for the cost of replacing a tank

---

[89] Shackelford, *supra* note 29, at 208.
[90] *Id.* at 205–06.
[91] *Id.* at 204, 208.
[92] Lentz, *supra* note 17, at 800.
[93] *See* Shackelford, *supra* note 29, at 208 (noting that only one conviction has resulted from the attack).
[94] John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES, Aug. 13, 2008, at A1.
[95] *Id.*
[96] *Id.*
[97] *See, e.g.*, Ophardt, *supra* note 30, ¶ 6 (describing the impact of DDOS during the attack on Georgia).

tread,' "[98] it is likely to gain favor as a viable complement or alternative to traditional warfare.

The source of the cyberattack on Georgia, as with Estonia, is still the subject of debate.[99] Evidence suggests that a Russian criminal organization was responsible for the attack with the support of the Russian government, but the difficulty in sorting through an attack perpetrated using numerous computers throughout the world makes it impossible to be certain.[100] The lack of consensus on who initiated the attack underscores the challenge of determining who should ultimately be held responsible for initiating a cyberattack.

Cyberattacks, however, do not always result in noticeable interference with the targeted computer system. In 2010, Iranian officials discovered malicious software, known as Stuxnet, with the ability to reprogram a host computer system, on networks used to manage their industrial infrastructure, including their much-maligned nuclear facilities.[101] While the cyberattacks perpetrated against Estonia and Georgia disrupted the targeted operating systems, Stuxnet was ostensibly introduced into Iran's critical infrastructure systems to assess the Iranian nuclear threat and destroy the facility if necessary.[102] Iranian officials believe it had been operating in Iran's computer systems for almost a year before discovery, and it also proved difficult to remove from the system, copying itself into several versions to evade removal.[103] Unlike the attacks on Estonia and Georgia, Stuxnet was introduced to a computer's operating system using a USB port, illustrating that even systems that are not connected to the Internet are vulnerable to exploitation.[104] While Stuxnet did not take control of the nuclear facility, which it was more than capable of doing, the damage it caused delayed the facility's opening by several months.[105] Stuxnet has also been found in other infrastructure systems in India, Pakistan, and Indonesia raising concerns that once sophisticated malware is released into a network, it can spread unpredictably and fall into even more dangerous hands.[106] Clearly, the

---

[98] Markoff, *supra* note 94 (quoting Bill Woodcock, research director of organization that tracks Internet traffic).

[99] *Id.*

[100] *Id.*

[101] *Stuxnet Worm Hits Iran Nuclear Plant Staff Computers*, BBC NEWS (Sept. 26, 2010), http://www.bbc.co.uk/news/world-middle-east-11414483.

[102] Caroline B. Glick, *Column One: The Lessons of Stuxnet*, JERUSALEM POST (Oct. 1, 2010), http://www.jpost.com/Opinion/Columnists/Article.aspx?id=189823.

[103] *Id.*

[104] *Id.*

[105] *Id.*

[106] *Id.*

prospect of an unknown party gaining control of a nation's nuclear facility by way of a cyberattack reinforces the gravity of the threat posed by cyberaggression. If a hostile nation were able to seize control of a nuclear facility in this manner, a threatened nation would find it difficult to justify retaliation by force under existing international law.[107]

Although the cyberattack on Iran was not carried out using the Internet like the cyberattacks on Estonia and Georgia, in all cases, the victimized nations were unable to attribute responsibility for the attack. Each example demonstrates the inherent difficulty of determining responsibility for a cyberattack, the nature of the attack, and the intentions of those responsible.[108] For example, the Estonia attack, which originally appeared to be a state-sponsored cyberattack by Russia, was relatively unsophisticated and well within the capabilities of mere civilians.[109] Such ambiguity surrounding the perpetrators and their intentions is a significant obstacle to any victimized nation's ability to defend itself, and current legal regimes do little to address the problem.[110] The problem, at its core, is evidentiary; a nation under attack must properly attribute the attack before choosing a course of action but rarely has immediate access to the necessary evidence, which is often in a foreign jurisdiction and can be destroyed quickly and easily.[111] Gathering evidence of an attack, which is ephemeral by nature, is further hampered by cross-border law enforcement's reliance on international agreements that were not designed with the unique problems of cyberaggression in mind.[112]

III. EXISTING INTERNATIONAL LAW ADDRESSING CYBERSECURITY

As previously stated, no comprehensive international legal framework addressing cybersecurity exists.[113] International efforts to address the issue have been narrow in scope, focusing primarily on data privacy regulations and human rights,[114] at the expense of a broader effort to define and

---

[107] *See infra* Part III.*C* (explaining the application of the law of war to cyberaggression).

[108] BRENNER, *supra* note 12, at 6 ("What was, and remains, ambiguous is what kind of attack it was, and who was responsible.").

[109] *Id.*

[110] *See* Sklerov, *supra* note 18, at 7 (noting that a nation's response to an attack under current law requires a conclusive identification of the attacker, which is virtually impossible during an attack because it requires time and cooperation from the state of origin).

[111] LIPSON, *supra* note 1, at 51.

[112] *Id.*

[113] Lentz, *supra* note 17, at 800.

[114] Sean Kanuck, *Sovereign Discourse on Cyber Conflict Under International Law*, 88 TEX. L. REV. 1571, 1581 (2010).

differentiate various levels of cyberaggression and codify an international approach to deal with its challenges.[115] These shortcomings may be due, in part, to the nature of cyberaggression, which "challenge[s] the conceptual categories we have so far used to avoid chaos and maintain order in our societies and in our lives."[116] Without a comprehensive international definition of the types of cyberaggression, nations will continue to face challenges in assessing the legality of their response to a given attack.[117] Finally, because there is no international body authorized to investigate and prosecute cyberaggression without limitation based upon the attack's location, nations resort to legal systems founded on the principle of territorial jurisdiction in crafting a response to cyberattacks.[118] Nations' efforts are hampered by the fact that international law recognizes no duty to assist other nations in investigating cyberaggression absent an explicit agreement to the contrary among the parties.[119]

A. Defining Cyberaggression and Its Impact on Applicable Law

Cyberattacks often do not closely resemble traditional criminal activity; it is often difficult to establish that the conduct at issue is criminal, as opposed to an act of war or terrorism.[120] In the context of cyberspace, "states generate crime and terrorism as well as war, and individuals wage war in addition to committing crimes and carrying out acts of terrorism."[121] Cyberattacks largely "defy the simple categorization of traditional weaponry currently used in international law,"[122] making it difficult for nations to apply the traditional definitions of crime, terrorism, and warfare as understood under existing law. Traditional classifications of crime, terrorism, and warfare break down because "[b]y giving nonstate actors access to a new, diffuse kind of power, cyberspace erodes nation-states' monopolization of the ability to wage war and effectively levels the playing field between all actors."[123]

Victimized nations seeking to take action under the current international legal framework must first determine the source and nature of a

---

[115] *Id.* at 1571.
[116] BRENNER, *supra* note 12, at 6.
[117] *See* Kanuck, *supra* note 114, at 1585 (noting that in the absence of comprehensive international law governing cyberspace, international legal norms are created unilaterally by states).
[118] Gable, *supra* note 3, at 100.
[119] Lentz, *supra* note 17, at 800.
[120] BRENNER, *supra* note 12, at 70.
[121] *Id.*
[122] Ophardt, *supra* note 30, ¶ 21.
[123] BRENNER, *supra* note 12, at 70.

cyberattack.[124] In doing so, a nation must equate a cyberattack to either a traditional armed attack, or to a criminal act.[125] Attributing a physical attack perpetrated with traditional weaponry to those responsible involves a two-prong analysis;[126] it is determined whether another nation (as opposed to individuals or other non-state groups) was responsible for the attack, and if not, the attack is addressed as a criminal matter.[127] Historically, the evidence indicating that another nation perpetrated a physical attack, thus constituting an act of war, was relatively clear.[128] An attack involved physical destruction that only another nation had the resources to inflict, and soldiers wearing the uniform of the aggressor nation carried out the attack.[129] The circumstances surrounding most cyberattacks rarely produce such clear evidence.[130] By nature, cyberwarfare "represents a disaggregation of combatants. . . . and requires significant geographic dispersal of assets. . . . [where] [t]he identity and location of attackers are masked."[131] Moreover, nations without sophisticated cyberspace capabilities or those wishing to further disguise the attack's source may contract with for-hire enterprises across the world that are willing to carry out cyberattacks against " 'legitimate' targets."[132] Identifying responsible parties is further complicated by the rapid advancement in computer technology, which creates an almost continuous learning curve that places law enforcement at an extreme disadvantage in their attempts to attribute responsibility for an attack.[133] The technological challenges cyberspace poses, coupled with the problem of anonymity, "exponentially increase[ ] the complexity of the cross-jurisdictional investigative challenges."[134] Furthermore, a nation must show that a cyberattack qualifies as an "armed attack" in the context of internationally accepted rules of warfare in order to respond with force,[135] otherwise nations are forced to rely upon criminal proceedings.

---

[124] *Id.*
[125] *Id.*
[126] *Id.* at 74.
[127] *Id.* at 74–75.
[128] *Id.* at 75.
[129] *Id.*
[130] Ophardt, *supra* note 30, ¶ 51.
[131] *Id.*
[132] *Id.* ¶ 15.
[133] BRENNER, *supra* note 12, at 28–29.
[134] *Id.* at 29.
[135] Sklerov, *supra* note 18, at 50–52.

B. Existing International Criminal Law Addressing Cybercrime

If a nation is unable to attribute a cyberattack to a foreign nation or its agents, as was the case with the Estonia attack, the law of war prohibits the use of force in response, and the aggrieved nation is left to pursue the attackers under criminal law.[136] Nations pursuing criminal matters internationally must depend on treaties and agreements that operate very slowly,[137] thwarting efforts to assert jurisdiction over cyberattackers based on the concept of territorial jurisdiction.[138] Under the theory of territorial jurisdiction, the ability of a nation to apply its laws to a given crime is based on the physical locations of the origin and target of the attack.[139] As the recent cyberattack on Georgia demonstrates, while the location of the target is readily apparent, cyberspace presents challenges to this notion of jurisdiction because the location of the origin is often indeterminate. Despite these challenges, a victimized nation may attempt to prosecute those responsible for an attack in accordance with the international agreements proscribing criminal cyber activity.

The Council of Europe's Convention on Cybercrime[140] is the only multilateral, legally binding instrument that addresses criminal activity in cyberspace.[141] The Convention on Cybercrime has five main purposes: "(1) harmonization of substantive criminal law on cybercrime; (2) harmonization of criminal procedure; (3) facilitating mutual legal assistance; (4) codifying international law, with an emphasis on territory-based jurisdictional rules; and (5) providing for a legal framework to enable development and understanding of the issues related to cybercrime."[142] The Convention aims to protect society against cybercrime and focuses on criminal activities such as "copyright infringement, computer-related fraud, child pornography, and offenses related to breaches of network security."[143] Although the Convention identifies specific prohibited conduct, it is left to the parties to the Convention to unilaterally determine the elements of prohibited conduct and the best method of enforcement adopted in each party's domestic

---

[136] *Id.* at 6.
[137] LIPSON, *supra* note 1, at 51.
[138] Gable, *supra* note 3, at 100.
[139] *Id.*
[140] Convention on Cybercrime, Nov. 23, 2001, T.I.A.S. No. 13,174, 2296 U.N.T.S. 167.
[141] Jon P. Jurich, *Cyberwar and Customary International Law: The Potential of a "Bottom-Up" Approach to an International Law of Information Operations*, 9 CHI. J. INT'L L. 275, 283 (2008).
[142] Stevens, *supra* note 46, at 685–86.
[143] Jurich, *supra* note 141, at 283.

laws.[144] The Convention also does not purport to set out universal standards for prosecuting acts of cyberaggression nor does it require a particular punishment for a given act.[145] Moreover, the Convention does not compel signatories to enforce one another's domestic laws, relying instead on international cooperation.[146] The practical implications of the Convention's use of domestic law and cooperation enforcement were apparent when the creator of the "Lovebug" virus, which caused ten billion dollars (U.S.) of damage globally was apprehended.[147] Although the perpetrator was apprehended, authorities were unable to criminally prosecute him because the domestic law of the Philippines, the perpetrator's domicile, did not prohibit his conduct, even though he had violated the law of the victimized nations.[148] Thus, given the Convention's relatively few signatories, and the fact that the Convention is not recognized as reflecting customary international norms,[149] a victimized nation attempting to prosecute attackers residing in a country that is not party to the Convention will have to rely on an independent agreement in order to pursue criminal charges against perpetrators located within the nonmember state's borders.[150] The challenge presented by the domestic differences across nations regarding scope of jurisdiction outside of their borders is exacerbated by the fact that, under the Convention, member nations are allowed to exempt their own jurisdictional rules from the Convention regime.[151] Most importantly, the Convention does not recognize universal jurisdiction as a means for prosecuting cybercrime cases.[152]

Similarly, the Group of 8 (G8),[153] which is comprised of eight world-leading market economies, addressed computer-related crimes in the *G8 Recommendations on Transnational Crime*.[154] The recommendations call for international cooperation in investigating cybercrime, review of substantive and procedural domestic law to ensure criminal sanctions are in place, and

---

[144] *Id.* at 283–84.
[145] *Id.* at 284.
[146] *Id.*
[147] Stevens, *supra* note 46, at 686.
[148] *Id.*
[149] Jurich, *supra* note 141, at 289.
[150] *Id.*
[151] Stevens, *supra* note 46, at 687.
[152] *Id.* at 688.
[153] The Group of 8 is composed of Canada, France, Germany, Italy, Japan, Russia, the United Kingdom, and the United States. *G8 Research Group: About Us*, G8LIVE.ORG, http://g8live.org/about/ (last visited Nov. 21, 2011).
[154] GROUP OF 8, G8 RECOMMENDATIONS ON TRANSNATIONAL CRIME (2002), *available at* http://www.canadainternational.gc.ca/g8/ministerials-ministerielles/2002/transnational_crime-criminalite_transnationale.aspx?lang=eng&view=d.

adoption of the European Council's Convention on Cybercrime.[155] These recommendations, however, lack specific implementation guidelines and they do not have binding effect.

The U.N. has been working toward developing a comprehensive approach to combating cybercrime as well.[156] The U.N. published the *United Nations Manual on the Prevention and Control of Computer-Related Crime*[157] in 1995, which "examines the law governing cybercrime and the need for international cooperation in cybercrime investigations."[158] In 2000, the U.N. General Assembly adopted Resolution 55/59,[159] which called on member nations to further develop comprehensive domestic policy regarding computer-related crime.[160] Although Resolution 55/59 reflects U.N. recognition of cybercrime as an issue of import, it offers only broad policy recommendations which lack the specificity to further harmonize the domestic criminal law of member states.[161]

C. Cyberaggression and the Law of War

The rules of warfare as applied to cyberwarfare are based on principles of law established by the U.N. Charter.[162] The law of war has traditionally been considered in two separate parts: law governing conflict management before war is actually declared, and law governing the use of force once war has been declared.[163] The former, known as *jus ad bellum*,[164] dictates how and by what justification a state may use force to respond to a perceived threat.[165] *Jus ad bellum* is comprised of "those established 'conflict management' norms and procedures that dictate when a state may—and may not—legitimately use force as an instrument of dispute resolution."[166] Prior to

---

[155] *Id.* pt. IV, sec. D.

[156] Susan W. Brenner & Joseph J. Schwerha IV, *Transnational Evidence Gathering and Local Prosecution of International Cybercrime*, 20 J. MARSHALL J. COMPUTER & INFO. L. 347, 363 (2002).

[157] UNITED NATIONS, UNITED NATIONS MANUAL ON THE PREVENTION AND CONTROL OF COMPUTER-RELATED CRIME (1995).

[158] *Id.*

[159] Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-First Century, G.A. Res. 55/59, U.N. Doc. A/RES/55/59 (Jan. 17, 2001).

[160] Brenner & Schwerha, *supra* note 156, at 363.

[161] *See id.* (noting that the resolution identifies several areas of focus for member nations but does not set forth specific guidelines in these areas).

[162] U.N. Charter arts. 2, 39–51.

[163] Sklerov, *supra* note 18, at 27.

[164] *Id.*

[165] David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SECURITY L. & POL'Y 87, 87 (2010).

[166] *Id.*

World War II, sovereign nations had a legal right to declare war unilaterally but were expected to announce their intentions.[167] The U.N. Charter was ratified following the war and "has redefined and codified 'contemporary *jus ad bellum* in its entirety' and has become the starting point for all *jus ad bellum* analyses."[168] *Jus ad bellum* operates as a set of rules that help states determine if "use of force" is a lawful response to a perceived threat or acts of aggression perpetrated by another nation.[169] The U.N. Charter imposes an obligation on the UN Security Council to maintain peace (Article 39), prohibits threats and uses of force (Article 2(4)), and provides for the right of self-defense (Article 51).[170] Article 2(4) of the U.N. Charter requires all Member States to "refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state."[171] In addition to the UN Charter, customary international law allowing for the use of self-defense requires that a nation show a necessity that is "instant, overwhelming, leaving no choice of means, and no moment for deliberation. . . . [and] that there was a necessity, present and inevitable, for attacking."[172] In short, a nation's use of aggressive force is "a crime against peace that has been outlawed by the international community," and is only excusable if the force used "is an exercise of [a nation's] inherent right of self-defense," or if it is authorized by the U.N. Security Council.[173]

Under the U.N. Charter, as it pertains to cyberattacks, it is unclear whether a cyberattack perpetrated by one nation against another rises to the level of a use of force necessary to trigger a nation's right of self-defense.[174] Moreover, the U.N. Charter's "use of force" doctrine does not cover the actions of terrorists and other non-state actors,[175] who are often behind cyberattacks. Since acts of cyberaggression are not amenable to traditional classification under internationally accepted rules of warfare, it is generally accepted that nations must treat international cyberattacks as a criminal matter.[176] Thus, even in the event that a nation or its agents perpetrate a cyberattack, under the current international legal regime, absent

---

[167] BRENNER, *supra* note 12, at 62–63.
[168] Sklerov, *supra* note 18, at 27 (quoting THOMAS C. WINGFIELD, THE LAW OF INFORMATION CONFLICT 33, 37–38 (2000)).
[169] WINGFIELD, *supra* note 168, at 33.
[170] U.N. Charter arts. 2, 39, 51.
[171] *Id.* art. 2, para. 4.
[172] Stevens, *supra* note 46, at 672 (citation omitted).
[173] WINGFIELD, *supra* note 168, at 38.
[174] Sklerov, *supra* note 18, at 31.
[175] Stevens, *supra* note 46, at 676.
[176] Sklerov, *supra* note 18, at 6.

unsanctioned unilateral action, the victimized nation would likely be forced to resort to criminal prosecution to obtain justice.

IV. AN INTERNATIONAL APPROACH TO STRENGTHENING GLOBAL CYBERSECURITY

A. International Regimes Combating Maritime Crime and Piracy

The Internet poses legal challenges similar to those encountered in maintaining order in the use of the world's oceans. UNCLOS, which imposes law and order in the seas, entered into force based on "the notion that all problems of ocean space are closely related and needed to be addressed as a whole."[177] Similarly, the Internet is shared globally and the consequences of actions taken by an Internet user in one jurisdiction can be borne globally. As a result, the legal challenges posed by cyberaggression are similar in many respects to the problems posed by piracy and other criminal activity on the high seas. UNCLOS specifically addresses piracy by defining conduct that constitutes piracy[178] and describing the duties of all nations with respect to combating piracy.[179] For example, UNCLOS balances the territorial jurisdiction of nations with the concept of universal jurisdiction. Article 105 provides that "[o]n the high seas, or in any other place outside the jurisdiction of any State, every State may seize a pirate ship or aircraft" and that "[t]he courts of the State which carried out the seizure may decide upon the penalties to be imposed."[180] Moreover, if a vessel engaged in piracy is captured in international waters by a nation that does not have criminal law that applies beyond their territorial borders, other nations that do have such criminal law may prosecute the pirates based on universal jurisdiction.[181]

B. Universal Jurisdiction

While there has been some debate among state officials and scholars over whether the doctrine of universal jurisdiction applies to acts of piracy,[182]

---

[177] Barry Hart Dubner, *Recent Developments in the International Law of the Sea*, 36 INT'L LAW. 721, 724 (2002).
[178] UNCLOS, *supra* note 27, art. 101.
[179] *Id.* art. 100.
[180] *Id.* art. 105.
[181] Barry Hart Dubner & Karen Greene, *On the Creation of a New Legal Regime to Try Sea Pirates*, 41 J. MAR. L. & COM. 439, 459 (2010).
[182] *See, e.g.*, Eugene Kontorovich, *The Piracy Analogy: Modern Universal Jurisdiction's Hollow Foundation*, 45 HARV. INT'L L.J. 183, 186 (2004) (challenging the generally accepted

many scholars argue that universal jurisdiction is clearly established as a means for prosecuting such acts.[183] The history of the international community's treatment of piracy suggests that there is universal jurisdiction over acts of piracy.[184] In fact, pirates have been prosecuted based on the principle of universal jurisdiction as early as the sixteenth century.[185] Although international law generally requires some nexus between the crime and the forum of prosecution in order to justify jurisdiction,[186] international jurisdiction over crimes such as piracy is an exception.[187] Such an exception exists because " 'every state has an interest in exercising jurisdiction to combat egregious offenses that states universally have condemned,' "[188] of which piracy is one. Some experts argue that the current legal regime only requires nations to prosecute piracy arising in their jurisdiction under their own laws[189] because crimes constituting piracy have never been prosecuted in an international tribunal, and the definition and prosecution of piracy have been left to respective national law.[190] Despite the fact that an act of piracy has never been tried before an international tribunal, prosecutions of piracy based on universal jurisdiction are well documented.[191] Proponents of universal jurisdiction over piracy conferred by international law find support for their argument in post-World War II international agreements and the opinions of international tribunal judges.[192] One expert, Kenneth Randall, notes:

> The historic universal jurisdiction over piracy has been used to justify universal jurisdiction over modern-day international offenses. Judges in the post-World War II prosecution of war criminals, in international tribunals and those organized by occupying authorities, relied on universal jurisdiction in their opinions. The precedent of universal jurisdiction over piracy

---

view that piracy was universally cognizable because of its heinousness).

[183] Dubner & Greene, *supra* note 181, at 448.

[184] *Id.*

[185] *Id.* at 449.

[186] *Id.*

[187] *Id.*

[188] *Id.* at 448 (quoting Kenneth C. Randall, *Universal Jurisdiction Under International Law*, 66 TEX. L. REV. 785, 788 (1988)).

[189] ALFRED P. RUBIN, THE LAW OF PIRACY 375–76 (2d ed. 1988).

[190] *Id.*

[191] Eugene Kontorovich & Steven Art, *An Empirical Examination of Universal Jurisdiction for Piracy*, 104 AM. J. INT'L L. 436, 436 (2010) ("We found that of all the clear cases of piracy punishable under universal jurisdiction, international prosecution occurred in no more than 1.47 percent [of cases].").

[192] Dubner & Green, *supra* note 181, at 450.

> similarly was important to drafting post-War humanitarian treaties . . . .[193]

Further evidence that universal jurisdiction over piracy exists is found in UNCLOS, in which "[t]he concept of universality principle is one of several legal concepts by which piracy . . . [is] elevated to the top tier of the normative hierarchy of international law."[194] At the very least, universal jurisdiction grants nations the right, but not the obligation, to punish pirates captured outside of the nation's territorial waters.[195]

Given such evidence that universal jurisdiction exists, Professor Dubner notes, "The problem is not that jurisdiction is unattainable, but rather that no country is exercising jurisdiction."[196] A recent study of maritime incidents occurring between 1998 and 2009 identified 1,158 incidents of piracy cognizable under universal jurisdiction.[197] Nonetheless, international prosecution occurred in only 1.47% of cases.[198] An explanation offered for the low prosecution rate is the naval and judicial costs of prosecution to the capturing nation where the incident itself did not affect that nation directly.[199] Developing nations tend to incur lower prosecution costs than developed nations, which helps explain why pirates are often transferred to countries like Kenya for prosecution, even when victimized ship has the same country of origin as the capturing ship.[200] Despite its infrequent use, some experts believe that universal jurisdiction over acts of piracy is "a prototype to which should be assimilated in time all crimes universally recognized as offenses against society."[201] The fact that nations are permitted to prosecute acts of piracy under the principle of universal jurisdiction, but often choose not to, does not undermine its application to cyberaggression.

Acts of cyberaggression, like piracy, are carried out in an environment where jurisdiction is unclear. A legal framework conferring universal jurisdiction over some acts of cyberaggression may help to resolve some of the jurisdictional issues raised by attacks such as the one on Estonia. Universal jurisdiction could be extended to cybercrime if the international community recognizes cybercrime as a universally condemned egregious

---

193 *Id.* (quoting Kenneth Randall).
194 *Id.*
195 *Id.* at 449.
196 *Id.* at 450–51.
197 Kontorovich & Art, *supra* note 191, at 437.
198 *Id.* at 436.
199 *Id.* at 450.
200 *Id.*
201 Dubner & Greene, *supra* note 181, at 442 (citation omitted).

offense.[202] Thus, a comprehensive, universally accepted definition of the spectrum of cybercrime would facilitate application of universal jurisdiction.

Like piracy,[203] however, it is difficult to define cybercrime because it is often unclear whether the perpetrators are affiliated with or sponsored by sovereign nations or criminal organizations.[204] Universal jurisdiction necessitates international agreement on the nature of illegal cyberactivity that separates criminal cyberactivity from cyberwarfare. The inadequacy of UNCLOS's definition of piracy is a notable shortcoming of the convention,[205] and is instructive on the importance of a carefully constructed international definition of cybercrime. A comprehensive definition of cybercrime would require intense international cooperation, given the burgeoning cyberwarfare operations pursued by many nations, including several world powers.[206] One legal scholar, Susan Brenner, has developed a plausible method for distinguishing between various types of cybercrimes.[207] Brenner separates cyberaggression into three categories: cybercrime, cyberterrorism, and cyberwarfare.[208] Dividing cybercrime into manageable components could facilitate the development of international law governing the rights and duties of nations with respect to each category of activity. This approach would help to address the shortcomings of present international cybersecurity law, and is in line with an ongoing shift toward "a model of indirect state responsibility" in international law.[209] Cybercrime is an international problem with international consequences, and an effective response demands its recognition as a category of offenses that are universally condemned.

C. The Prospect of a U.N. Agency Regulating Cybersecurity

If members of the international community were able to develop a convention structured after UNCLOS, mandating international cooperation on cybersecurity and applying universal jurisdiction to acts of cyberaggression, the benefits would be palpable. One such benefit would be

---

[202] *Id.* at 448 (noting that every state is interested in fighting egregious offenses, and the collective sentiment regarding a particular offense provides the basis for universal jurisdiction).

[203] *See* RUBIN, *supra* note 189, at 376 (noting that the definition of piracy under international law is unclear).

[204] BRENNER, *supra* note 12, at 7–8.

[205] *See, e.g.*, Dubner & Greene, *supra* note 181, at 457–61 (discussing the limited scope of UNCLOS's definition of piracy).

[206] Sklerov, *supra* note 18, at 9.

[207] Lentz, *supra* note 17, at 809.

[208] *Id.*

[209] Sklerov, *supra* note 18, at 60.

an opportunity to create a U.N. agency comparable to the International Maritime Organization (IMO)[210] whose purpose would be to ensure the safety and security of the Internet.

The IMO was created pursuant to the adoption of the Convention on the International Maritime Organization,[211] which entered into force in 1958. The purpose of the IMO as stated in Article 1(a) of the Convention is to facilitate cooperation among governments in order to ensure that the "highest practicable standards in matters concerning maritime safety" are in place.[212] The IMO also maintains detailed records of all incidents of piracy,[213] which supports the IMO's policy recommendations and efforts to develop new law when the need arises.[214] One such legal instrument is Resolution A.738(18), which was intended to facilitate States' duties to cooperate in the repression of piracy under Article 100 of UNCLOS.[215] Generally, Resolution A.738(18) encouraged intergovernmental cooperation in all aspects of piracy prevention and solidified the IMO's antipiracy strategy. The IMO's "strategy consist[s] of compilation and distribution of periodical statistical reports, piracy seminars and field assessment missions to regions affected by piracy and the preparation of a code of practice for the investigation and prosecution of the crime of piracy."[216]

An agency similar in function to the IMO dedicated to tracking incidents of cyberaggression and fostering cooperation between member nations would help to consolidate the international effort to monitor and deter cyberaggression. Moreover, such an agency would help to legitimize the international legal regime that created it, and would provide sound policy rooted in empirical evidence.

D. The Prospect of an International Cybercrime Tribunal

Although international maritime law has not established an international tribunal to prosecute acts of piracy, some experts believe that creating such a

---

[210] *Introduction to IMO*, INT'L MAR. ORG., http://www.imo.org/About/Pages/Default.aspx (last visited Nov. 21, 2011).

[211] Convention on the International Maritime Organization, Mar. 6, 1948, 9 U.S.T. 621, 289 U.N.T.S. 48 (entered into force Mar. 17, 1958).

[212] *Id.* art. 1(a).

[213] Kontorovich & Art, *supra* note 191, at 437.

[214] *See* About IMO: Conventions, INT'L MAR. ORG., http://www.imo.org/About/Conventions/Pages/Home.aspx (last visited Nov. 21, 2011) (explaining that the IMO is most involved with facilitating the adoption and implementation of proposed conventions).

[215] U.N. Secretary-General, *Oceans and the Law of the Sea: Rep. of the Secretary-General*, para. 188, U.N. Doc. A/56/58 (Mar. 9, 2001), *available at* http://www.un.org/Docs/journal/asp/ws.asp?m=%20A/56/58 (follow "English" link).

[216] *Id.* para. 192.

tribunal would provide a long-term solution to combating piracy.[217] Employing an international tribunal with respect to acts of cyberaggression would ensure that offenses are not treated differently across jurisdictional lines. At the very least, the existence of an international tribunal with universal jurisdiction over acts of cyberaggression would deter such acts and provide a venue for prosecution where nations otherwise often refuse to prosecute such acts. As with piracy, it may be difficult to compel nations to prosecute acts of cyberaggression in the absence of an international tribunal, where the concept of universal jurisdiction confers a right but does not impose an obligation to prosecute such crimes.[218] It has been suggested that "while every state should retain the *right* to redress piracy, the United Nations could create an ad hoc tribunal to have the *obligation* to redress piracy."[219] As has been suggested for handling the prosecution of piracy under UNCLOS, an international agreement addressing acts of cyberaggression could allow nations to retain the right to redress cybercrime, while creating an international tribunal that has an obligation to prosecute cybercrime. This type of tribunal would help to preserve national autonomy, while providing nations and private actors with an international forum for redressing their grievances. Since cybercrime, like piracy, has a large impact on private actors who are often the victims of these types of crimes, allowing private actors to pursue justice via access to an international tribunal would encourage nations to bring domestic policies in line with international standards.[220] The availability of an international cybercrime tribunal could also lessen nationalistic resistance to international standards by empowering private actors with the ability to seek international redress for economic injury inflicted by acts of cybercrime.

V. CONCLUSION

The current international legal regime governing cybersecurity fails to provide a comprehensive, effective framework for dealing with the unprecedented challenges posed by the various forms of cyberaggression. However, the international legal framework governing piracy, even with its shortcomings, provides a basis for an analogous regime governing international cybersecurity.

The recent cyberattacks on Estonia, Georgia, and Iran demonstrate the shortcomings of both international criminal law governing cybercrime and

---

[217] Dubner & Greene, *supra* note 181, at 452.
[218] *Id.* at 449.
[219] *Id.* at 452.
[220] *Id.* at 453.

the absence of international law addressing cyberterrorism and cyberwarfare. In a world where internet commerce is increasingly important to the growth of the global economy, nations cannot afford to shape cybersecurity law unilaterally in furtherance of provincial interests at the expense of a concerted international effort to develop uniform cybersecurity law. As the economic futures of nations become ever more intertwined, international consensus on issues like cyberaggression is essential to global security and economic well-being.

Analogizing cyberthreats to the concerns that spawned cooperation in developing international maritime law is a useful starting point for analyzing and developing an international response that is necessary to meaningfully address global cybersecurity. Without an international agreement that defines the spectrum of cyberaggression, provides for some form of universal jurisdiction over perpetrators, and establishes an international organization focused on cybersecurity policy, the threat to international security posed by cyberaggression will continue to grow. To that end, the mere existence of an international cybercrime tribunal would go a long way toward encouraging cooperation on the development of international norms relating to cybercrime, while allowing nations to retain some level of autonomy in the development and enforcement of domestic cybersecurity policy.