DERAILING THE DIGITALLY DEPRAVED: AN INTERNATIONAL LAW & ECONOMICS APPROACH TO COMBATING CYBERCRIME & CYBERTERRORISM[1]

*Jason A. Cody**

INTRODUCTION

Bound by no boundaries, invisible to interception, and impervious to the rules of any one nation, the digitally depraved wax brilliantly in the absence of a unified deterrent force in cyberspace. Into the second decade of Internet life—a duration akin to a millennium in the offline world—the international community continues to struggle with the issue of cybercrime. The criminal potential and the magnitude of cybercrimes parallel the growth of the Internet. To take just one example, over an eleven year period ending in 1999, the number of recorded computer security incidents grew by more than 133,000%.[2]

A new strain of cybercrime is also making its debut. With cyberterrorism, terrorists are asking, why hi-jack an airplane using a bomb and relying on unpredictable variables, when we

---

[1] Reprinted from and with the permission of the Michigan State University – DCL Journal of International Law. Jason A. Cody, *Derailing the Digitally Depraved: An International Law & Economics Approach to Combating Cybercrime & Cyberterrorism*, 11 MSU – DCL J. INT'L L. 231 (2002) (first publication).

*J.D. 2003, George Mason University School of Law. This Article was produced within the rich academic environment of the Mason community of law and economics. As always, I must also recognize the contributions of my partner, Amy Cody, to my personal, educational, and professional development through her love, friendship, and support. Views expressed and errors made herein are solely mine.

[2] Internet Denial of Service Attacks and the Federal Response: Joint Hearing Before the Crime Subcommittee of the House Judiciary Committee and the Criminal Justice Oversight Subcommittee of the Senate Judiciary Committee, 106th Cong. (2000) (statement of Senator Patrick Leahy) (stating that between 1988 and 1999, the number of recorded computer security incidents grew from 6 to over 8,000).

can sky-jack the entire airline industry from behind the comfort, safety, and predictability of our portable and unidentifiable computers. Countless other digital doom scenarios exist in which unseen cyberterrorists could wreak havoc at the stroke of a key or click of a mouse.[3] As this digital dilemma has no national boundaries, it is clearly international in scope. The question is whether the international community has a sufficient response to repel the growing threat of cybercrime, including cyberterrorism.

Creating a multilateral treaty to address cybercrime represents one possible solution. Indeed, on November 23, 2001, in Budapest, Hungary, the Council of Europe opened for signature the Convention on Cybercrime.[4] The Convention goes far to define international crimes, to provide for domestic criminal procedural law powers, and to further international cooperation involving cybercrimes.[5] However, inherent problems with treaty law suggest that it is not the only, and perhaps not the best, tool for solving problems in the dynamic world of cyberspace. To wit, formation of treaty law usually requires an extensive and cumbersome process of negotiation that may eventually yield formal codification.[6] By the time that states

---

[3] M. Cherif Bassiouni, *"Terrorism and Business" Forward: Assessing "Terrorism" into the New Millennium,* 12 DEPAUL L.J. BUS. 1 (2000) (describing some of the threats of cyberterrorism: "destroying corporate computer files, accessing private database entries, falsely manipulating the stock market, rerouting transportation systems, intercepting military communications, accessing personal email accounts, disrupting banking operations, and manipulating government files").

[4] Council of Europe, Convention on Cybercrime (Nov. 23, 2001), *available at* http://conventions.coe.int/Treaty/EN/cadreprincipal.htm (last visited Mar. 2002). The Convention was signed by thirty nations—Canada, Japan, South Africa, the United States, and 26 other countries—and awaits ratification by five member states before going into effect. Brian Krebs, *Thirty Nations Sign Cybercrime Treaty*, NEWSBYTES (Nov. 26, 2001), *available at* http://www.newsbytes.com (last visited Mar. 2002).

[5] Council of Europe, Convention on Cybercrime: Explanatory Report para. 16 (adopted Nov. 8, 2001), *available at* http://conventions.coe.int/Treaty/en/Reports/Html/185.htm) (last visited Mar. 2002).

[6] William J. Aceves, *The Economic Analysis of International Law: Transaction Cost Economics and the Concept of State Practice*, 17 U. PA. J. INT'L ECON. L. 995, 1066 (1996) (observing that

have actually "fixed" a solution to a problem, the realities giving rise to the original problem may have changed greatly (especially given the nature of cyberspace), or the answer may be the result of too much compromise. Economic analysis of law suggests that customary international law is a more flexible, efficient, and effective method for the development of international law capable of responding to cybercrime. This Article focuses on customary international law, rather than treaty law.

Unlike treaty law, customary international law is based upon state cooperation without the requirement of formal written agreements.[7] It is, in and of itself, a dynamic process that "minimizes the problems raised by transaction costs by allowing states to forego explicit negotiations and to function even in the absence of a formal structure."[8] Perhaps most importantly, customary international law is flexible and may be used by states to respond to new, dynamic problems, such as those that arise in the context of computers and the Internet.[9] The development of efficient customary international law, without more, is also challenged by real world circumstances. For example, states often have divergent interests in solving international problems such as cybercrime.[10] While capturing cybercriminals that threaten economic stability

---

"[w]hereas treaties require an extensive process leading to formal codification, customary international law does not").

[7] FRANCESCO PARISI, *Customary Law*, in THE NEW PALGRAVE DICTIONARY OF ECONOMICS AND THE LAW 572 (2002) (stating that international "customary rules can be regarded as an implied and often non-verbalized exercise of direct legislation by [states]").

[8] Aceves, *supra* note 5, at 1005.

[9] Anthea Elizabeth Roberts, *Traditional and Modern Approaches to Customary International Law: A Reconciliation*, 95 A.J.I.L. 757, 785 (2001) (stating that the "content of custom can change in view of new practice and principles in international law").

[10] Professor Parisi explains that "[w]hen appraising spontaneous sources of law [i.e., formation of customary international law] using game theory, one should consider the incentive structure of the originating environment as well as the possible role of strategic behavior in affecting the equilibrium outcome." Francesco Parisi, *The Cost of the Game: A Taxonomy of Social Interactions*, 9:2 EUR. J. L. & ECON. 99, 102 (2000).

may be worthwile, fighting cybercrime can be expensive, and easing rules relating to territorial sovereignty—a keystone of statehood—is a rather imposing notion.

Nevertheless, economics offers customary international law several tools that may be used to align the interests of states. These economic devices, namely, role reversability, reciprocity constraints, and articulation, create structures in which states' incentives become symmetrical.[11] Under symmetric incentive structures, states continue to pursue their individual economic interests, but they arrive at optimal solutions that promote the good of the entire international community.[12] Furthermore, customary international law continues to emerge in spontaneous fashion from the decentralized practice of states. This Article explains how these economic tools can assist states in developing dynamic and flexible customary international law that is sufficiently responsive to the scourge of cybercrime.

Part II of this Article first puts cyberspace into context by briefly describing its nature and evolution. Unencumbered by traditional geographical constraints and national laws, this Article next describes how the criminally adroit have found new opportunities to engage in worldwide, instantaneous, and low-cost cybercrime and cyberterrorism. Under Part III, this Article explains some basic principles of customary international law. Part III also highlights the strengths and weaknesses of customary international law, and concludes that *opinio juris* complicates its effectiveness as a means for responding to cybercrime. Finally, Part IV takes an international law and economics approach to combating cybercrime. Recognizing the challenges

[11] PARISI, *supra* note 6, at 574-576 (discussing the use of role reversability, reciprocity constraints, and articulation as means for achieving optimal customary international laws).

[12] PARISI, *supra* note 6, at 576 (discussing specifically how articulation theory provides an incentive for individuals to endorse customary rules that will benefit themselves, as well as the community at large).

that arise when states possess unique or hidden interests, this Article proposes three economic tools that may be used to align those interests. By employing these devices, this Article concludes, states may develop more efficient international customary law that maximizes the expected welfare of the entire international community.

I. CYBERCRIME

A. The Internet & Cyberspace

Before discussing crimes that occur on the Internet—and international law's ability to respond to such threats—a brief introduction to the nature of that forum is in order. The United States Supreme Court has explained, "The Internet is an international network of interconnected computers . . . [that] enables [] millions of people to communicate with one another and to access vast amounts of information from around the world."[13] It was originally designed by the U.S. Government to permit the military, defense contractors, and university researchers to have uninterrupted communication with one another notwithstanding any potential damages as a result of nuclear war.[14] By the early 1990s, this computerized network was opened up to the general public. Today, the Internet exists as an international forum in which individuals and organizations representing broad interests come together to share a variety of ideas and information.

From an international perspective, the Internet renders borders largely irrelevant.[15] This medium is often referred to as "cyberspace" because it has no physical location of its own and it

---

[13] Reno v. ACLU, 521 U.S. 844, 849-50 (1997).

[14] *Id*. at 850. The military program, Advanced Research Projects Agency Network (ARPANET), which began in 1969, served as a model for the development of a number of civilian computer networks. *Id*. These networks eventually came together to form what is now called the Internet.

[15] David R. Johnson and David G. Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1370 (1996) [hereinafter Johnson & Post] (stating that "[c]yberspace has no

is available to any person who has access to the Internet, regardless of their citizenship, or national borders.[16] In the words of one commentator, "More than any other technology, the Internet facilitates cheap, fast, and difficult-to-detect multi-jurisdictional transactions."[17] Thus, even though the Internet is often praised for its ability to "inform, educate, entertain and conduct business on a world-wide scale,"[18] it is also recognized as the vehicle for a great deal of potential harm. Because the threats are not bounded in the traditional sense, the interests of the entire international community are at stake—therefore, any solutions must be international in scope.

From an economic viewpoint, the Internet is efficient in that it allows its users to accomplish diverse tasks at virtually no cost.[19] Internet users have the ability to communicate and retrieve information worldwide using a variety of means such as electronic mail, list serves, chat rooms, and the Web.[20] With respect to crime, the "Internet fosters certain efficiencies that may make detection and subsequent prosecution considerably more difficult." [21] Moreover,

---

territorial based boundaries, because the cost and speed of message transmission on the Net is almost entirely independent of physical location").

[16] ACLU, 521 U.S. at 851. The Court also explained that the World Wide Web (Web) is the most well known category of communication over the Internet. *Id*. at 852. Essentially, the Web consists of documents stored in computers located throughout the world. *Id*.

[17] Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 IND. J. GLOBAL LEG. STUD. 475, 475 (1998).

[18] DAVID CAPITANCHIK & MICHAEL WHINE, *The Governance of Cyberspace: Racism on the Internet*, in LIBERATING CYBERSPACE LIBERTY, 237 (Pluto Press 1999) (noting that although the benefits of the Internet far outweigh the costs, the latter cannot be ignored).

[19] "Cyberspace presents unique opportunities for criminals to reduce their perpetration costs; the probability of success in inflicting a certain level of harm while holding expenditures constant is greater. Accordingly, the law should develop mechanisms to neutralize these efficiency advantages." Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1006 (2001).

[20] ACLU, 521 U.S. at 851 (calling the Web the "best known category of communication over the Internet").

[21] Michael Edmund O'Neill, *Old Crimes in New Bottles: Sanctioning Cybercrime*, 9 GEO. MASON L. REV. 237, 239 (2000) (also finding that "Cybercrime is unique [because] . . . it is often

computers have the ability to increase the expected return from criminal conduct and to decrease the fixed costs.[22] Primarily because the cost of using the Internet—i.e., the cost of entry—is so low, and its reach so broad, the Internet is a unique medium with unparalelled efficiency.[23]

B. A Vehicle for Cybercrime

Merely describing the nature of the Internet demonstrates its potential to be used for illicit purposes. Speaking of the Internet five years ago, the U.S. Supreme Court observed that "at any given time[,] 'tens of thousands of users are engaging in conversations on a huge range of subjects . . . [making it] no exaggeration to conclude that the content on the Internet is as diverse

---

a more efficient means by which to commit certain types of offenses"); Katyal, *supra* note 18, at 1006 (stating that the most important reason why cyberspace is a unique medium is that "the use of computers and other equipment is a cheaper means to perpetrate crime").

[22] O'Neill, *supra* note 20, at 239. Professor O'Neill illustrates the attractiveness of committing cybercrimes in the following manner:

> [B]ank robbers seeking to maximize their haul might be best directed to call upon Fort Knox. Fort Knox, however, is a wellguarded military base, and thus, the costs of breaking into its storied vaults are extraordinarily high. What if, an individual could attack a Forth Knox in cyberspace, however, at much less risk of either personal harm or detection by law enforcement? To the extent that computers, much as telephones once did, may reduce the costs and increase the expected benefits of crime, the law should develop appropriate deterrent mechanisms to neutralize these efficiency advantages.

Id. Ultimately, Professor O'Neill's article argues for taking measures to raise the costs of engaging in cybercrime. *Id*. at 288.

[23] One commentator notes that the Internet provides opportunity for previously marginalized viewpoints to access a much larger audiences than was ever before imagined. ADAM NEWEY, *Freedom of Expression: Censorship in Private Hands*, in LIBERATING CYBERSPACE LIBERTY, 13 (Pluto Press 1999) (stating also that the media is responsible for demonizing the Internet as "a haven for pornographers, terrorists and political exremists who can ply their poisonous trades with impunity"); Katyal, *supra* note 18, at 1112 (finding that the recent crimes committed on the Internet were a result of the advantages of computers that we all like: "their speed, efficiency, trustworthiness, and low startup costs").

as human thought.'"[24] Since human thought has long contemplated many means of criminal activity, crime occurring in the Internet forum comes as little surprise.[25]

With the growth of the Internet, however, came opportunities to commit more advanced and devastating computer crimes. The media has made most people aware of the potential for these types of crimes to wreak havoc within the Internet community. Two recent examples from 2000 are particularly illustrative. First, was the debilitating attack on the eight largest of the U.S.-based Internet companies.[26] In February of 2000, a hacker unleashed several computer programs that made thousands of simultaneous requests each minute to connect to the computer systems of the Internet companies.[27] Shutting down these companies for days, the attack was estimated to have caused over $1.2 billion in damages.[28]

Even more damaging was a virus reaching the entire Internet community and infecting over 45 million computers. The "I Love You" virus, originating from hackers located in the Philippines and affecting people throughout the world, was programmed to self-install on a

---

[24] ACLU, 521 U.S. at 852 (quoting the lower court, ACLU v. Reno, 929 F. Supp. 824, 835-42 (1996)).

[25] As one politician noted, "Unlawful activity is not unique to the Internet—but the Internet has a way of magnifying both the good and the bad in our society." Vice President Albert Gore, Jr. (Aug. 5, 1999) (quoted in The Electronic Frontier: *The Challenge of Unlawful Conduct Involving the Use of the Internet: A Report of the President's Working Group on Unlawful Conduct on the Internet* (Mar. 2000)).

[26] The companies whose network systems were targeted and debilitated include: Yahoo!, eBay, Buy.com, Amazon.com, E*Trade, MSN.com, CNN.com, and ZDNet.

[27] Internet Denial of Service Attacks and the Federal Response, Hearing before the Subcommittee on Crime of the House Committee on the Judiciary and the Subcommittee on Criminal Justice Oversight of the Senate Committee on the Judiciary, 106th Cong., 2d Sess. 35-37 (2000) (statement of Michael A. Vatis, Director, National Infrastructure Protection Center, Federal Bureau of Investigation) (describing the cyber attack).

[28] Russ Banham, *Hacking It*, CFO MAGAZINE 115 (Aug. 1, 2000).

computer's system files.[29] When a computer user generated an email, the virus caused the computer to forward an e-mail attachment to all of the addresses in the user's e-mail address book, thereby infecting all those who opened the attachment.[30] The aggregate economic damage of this crime was estimated to cost from $10 billion[31] to over $11 billion.[32]

The above mentioned crimes are considered "cybercrimes," which, if defined loosely, mean computer crimes committed over the Internet in cyberspace.[33] Most commentators recognize three types of cybercrime.[34] First, is where the computer itself is the target of the crime, such as when a hacker infects a specific computer or network with a virus (e.g., the attack on the Internet companies' systems). Second, a computer may be used as the instrument of a crime. For example, someone may use a computer to defraud consumers, to steal information from a competitor, or to embezzle money from an employer (e.g., the "I Love You" bug which

---

[29] Electronic Communications Privacy Act of 2000, Digital Privacy Act of 2000 and Notice of Electronic Monitoring Act, Hearings on HR 5018, HR 4987, and HR 4908 before the Subcommittee on the Constitution of the House Committee on the Judiciary, 106th Cong., 2d Sess (2000) (statement of Kevin DiGregory, Deputy Assistant Attorney General, Criminal Division, Department of Justice).

[30] *Id*.

[31] Rob Kaiser, *'Love Bug' Has Cousins; They Bite Too: Cyberattack Considered Most Disruptive Ever*, CHI. TRIB., May 6, 2000, at1.

[32] *eVirus Signs Marketing and Sales Contract*, BUSINESS WIRE, Aug. 1, 2000.

[33] The Department of Justice defines "computer crimes" as "any illegal act for which knowledge of computer technology is essential for successful prosecution." NATIONAL INSTITUTE OF JUSTICE, U.S. DEPARTMENT OF JUSTICE, COMPUTER CRIME: CRIMINAL JUSTICE RESOURCE MANUAL 3 (1989); Katyal, *supra* note 18, at 1004 (defining "cybercrimes" as "all sorts of crimes committed with computers – from viruses to Trojan horses; from hacking into private e-mail to undermining defense and intelligence systems; from electronic thefts of bank accounts to disrupting web sites").

[34] *See generally Id.*; *see also* Patricia L. Bellia, *Chasing Bits Across Borders*, 2001 U. CHI. LEGAL F. 35, n.11 (2001) (stating that the three types of criminal conduct involving computers include the computer (1) serving as the target of a crime, (2) serving as a tool for committing a crime, and (3) being used incidentally to the crime); see also O'Neill, *supra* note 20, at 242-43 (describing the three types of cybercrimes).

used other computers to spread a virus).[35] Finally, a computer may be incidental to a crime or store evidence of a crime. For instance, a bank robber may use a computer to store records pertaining to past robberies or plans for future robberies.

C. The Definitive Cybercrime—Cyberterrorism

In addition to the above-mentioned types of cybercrime, the idea of "cyberterrorism" is gaining recognition.[36] As a preliminary matter, the international community has had trouble enough attempting to define "terrorism,"[37] let alone its offspring, "cyberterrorism."[38] For instance, the United States,[39] the United Kingdom,[40] and the United Nations[41] all define terrorism

---

[35] Also in 2000, the Federal Bureau of Investigations discovered that Russian hackers were using their computers and the Internet to break into computer networks of banks, Internet service providers, and other companies located in the United States. Bellia, *supra* note 33, at 39-40; Jack L. Goldsmith, *The Internet and the Legitimacy of Remote Cross-Border Searches*, 2001 U. CHI. LEGAL F. 103 (2001).

[36] One commentator, coming from a military point of view, describes what he terms "cyberwar." Mark R. Jacobson, *War in the Information Age: International Law, Self-Defense, and the Problem of "Non-Armed" Attacks*, 2 MERSHON CENTER, THE OHIO STATE UNIVERSITY (2001). By waging cyberwar, a perpetrator has the ability to wage low-cost attacks against an enemy that may significantly damage military operations, national security, and a nation's overall economic stability. *Id*.

[37] *See, e.g.*, General Assembly Official Records, 28th session 7-8 (Suppl. No. 28, 1973); *see also* Bassiouni, *supra* note 2, at 6 (referring to a definition of "terrorism" and stating that “legal labels are of little relevance unless they conform to the manifestations of an actual phenomenon, are capable of conveying the predictability of deterrence, and result in a consistent application"); OPPENHEIM'S INTERNATIONAL LAW, vol. I, part 1, §122 (Sir Robert Jennings & Sir Arthur Watts editors, 9th ed. 1992) (stating that "[p]rogress towards general and more binding international anti-terrorist measures has [] been hindered by difficulties over . . . the definition of 'terrorism', which must, in the eyes of some but not all states, take account of the purposes for which a *prima facie* terrorist act is committed"); MALCOLM N. SHAW, INTERNATIONAL LAW 803 (4th ed. 1997) (stating that the first problem that international law encounters in addressing terrorism is in defining it).

[38] Professor Bassiouni states that cyberterrorism "consists of computer generated attacks against adverse entities, whether civilian, corporate, or governmental, which affect aspects of our professional and personal lives and impacts on national and international security." Bassiouni, *supra* note 2, at 14.

[39] The Federal Bureau of Investigation defines "terrorism" as "the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian

in slightly different terms. One commentator has come up with the following working definition: "the calculated employment or the threat of violence by individuals, subnational groups, and state actors to attain political, social, and economic objectives in violation of law, intended to create an overwhelming fear in a target area larger than the victims attacked or threatened."[42]

Aside from the teenage hacker who may disrupt a company's website, the possibility that "cyberterrorists" will use computers to commit crimes that result in death or mass destruction is real. Discussing the threat of cyberterrorism, a U.S. ex-Terrorism Czar said, "I'm talking about people shutting down a city's electricity, . . . 911 systems, . . . telephone networks and transportation systems. You black out a city, people die. Black out lots of cities, lots of people

---

population, or any segment thereof, in the furtherance of political or social objectives." U.S. DEPARTMENT OF JUSTICE, FBI, TERRORISM IN THE UNITED STATES 34 (1988). However, the United States Department of State defines "terrorism" as "premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents", usually intended to influence an audience, and "international terrorism" as "terrorism involving citizens of the territory of more than one country." 22 U.S.C. § 2656f(d) (1994).

[40] In the United Kingdom, the government defines "terrorism" as "the use or threat, for purposes of advancing a political, religious, or ideological course of action which involves serious violence against any person or property, endangers the life of any person, or creates a serious risk to the health or safety of the public or a section of the public." Mark Matfield, *Terrorism Bill Passes Second Reading*, RDS NEWSLETTER, Jan. 2000, at 8-9.

[41] Although the United Nations (UN) has resolved to combat terrorism, it has found defining terrorism difficult, primarily due to political reasons. Yonah Alexander, *Terrorism in the Twenty-First Century: Threats and Responses*, 12 DEPAUL BUS. L.J. 59, 64 (2000). Nevertheless, at the end of 1999, the UN decided that terrorism includes,

> Criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes are in any circumstances unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious, or other nature, that may be invoked to justify them.

International Convention for the Suppression of the Financing of Terrorism, G.A. Res. 109, U.N. GAOR, 6th Comm., 54th Sess., 76th mtg., Agenda Item 160, U.N. Doc. A/54/109 (1999).

[42] Alexander, *supra* note 40, at 65.

die. It's as bad as being attacked by bombs . . . ."[43] Echoing the same sentiment, one commentator noted that "bombing the right junction station might shut down an air traffic control network or phone-communications for a large city, but inserting a computer virus which shuts down or overloads the system could accomplish the same ends."[44]

Like the Internet, terrorism—whether cyber or not—is also a low-cost and efficient tool that knows no national boundaries.[45] In addition, cyberterrorism consists of low-intensity conflict and is especially effective for its ability to project psychological intimidation in its targets.[46] Consider this: "a well-coordinated attack with about thirty computer experts strategically placed around the globe and with a budget of approximately 10 million dollars, could bring the United States, the only superpower, to its knees."[47] Such realities give nations, big or small, substantial cause for worry. Without an adequate, efficient, and international response to the threat of cybercrime, including cyberterrorism, such worries will not ease anytime soon.

Effectively combating cybercrime—say national scholars, national leaders, and national law enforcement officials—will depend greatly upon the ability of the international community

---

[43] Tim Weiner, *The Man Who Protects America From Terrorism*, N.Y. TIMES, Feb. 1, 1999, at A3 (quoting Richard Clarke, who also described the potential for devastation as the "electronic Pearl Harbor").

[44] Jacobson, *supra* note 35, at 8 (concluding that "[a]ggression no longer needs to be 'armed' in the traditional sense, nor does it have to be physically destructive in order to constitute a legitimate threat to a nation—the Walls of Jericho can thus be taken down with a laptop").

[45] Alexander, *supra* note 40, at 85-86 (describing Internet warfare as a low-cost "equalizer" weapon for terrorists, and stating that hacker websites result in the "democratization" of tools used for disruption and destruction in that forum).

[46] *Id*. at 65 (tracing the development of "terrorism" back to the Zealot Sicarii and the Hashashin in the Middle East between the first and second centuries respectively); *see also* Bassiouni, *supra* note 2 (noting that cyberterrorism is "capable of generating higher levels of insecurity and likely a more harmful impact on society" than traditional terrorist attacks).

[47] Alexander, *supra* note 40, at 86.

to cooperate in detecting, preventing, and deterring potential cybercriminals, as well as prosecuting and punishing those who commit cybercrimes.[48] More specifically, the international community must develop international standards regarding extradition, mutual legal assistance, transfer of criminal proceedings, transfer of prisoners, seizure and forfeiture of assets, and recognition of foreign penal judgments.[49] This Article does not attempt to make specific recommendations for achieving each objective. Nonetheless, this Article does address the threat of cybercrime in broadstroke by examining how international law and economics may contribute to achieving such objectives.

II. CUSTOMARY INTERNATIONAL LAW

A global problem as large and as encompassing as cybercrime must find a solution within the framework of international law. Although international law has no criminal system of its own, from its beginnings, it has served to keep the peace among nations.[50] Without constitutive

---

[48] *See, e.g.*, Bassiouni, *supra* note 2 (recommending enhanced international cooperation to effectively combat all forms of terrorism); Bellia, *supra* note 33, at 100 (arguing that states must develop a legal framework for evaluating cross-border data searches that takes into account the customary international problems of conducting unilaterally); Howard L. Steele, *The Web That Binds Us All: The Future Legal Environment Of The Internet*, 19 HOUS. J. INT'L L. 495, 517 (1997) (stating that cyberspace is in dire need of uniform and centralized rules, and calling upon the governments of the world to unite and to cooperate in developing an international criminal approach to cybercrime); Michael A. Sussman, *The Critical Challenges From International High-Tech And Computer-Related Crime At The Millennium*, 9 DUKE J. COMP. & INT'L L. 451, 488-89 (1999) (arguing that governments must work together to stay ahead of the next generation of criminal activity by updating domestic laws relating to extradition, and cooperating with locating and identifying cybercriminals); Alexander, *supra* note 40, at 95 (arguing for states to develop credible responses and capabilities to minimize future terrorist threats).

[49] Consider the fact that "[i]ndividual electrons can easily, and without any realistic prospect of detection, 'enter' any sovereign's territory." Johnson & Post, *supra* note 14, at 1372. For this reason, Johnson and Post argue that cyberspace should be recognized as a distinct place for purposes of legal analysis). *Id*. at 1378.

[50] SHAW, *supra* note 36, at 12-13 (explaining that Mespotamian rulers of Lagash and Umma signed a treaty around 2100 B.C. which defined international boundaries, and that a thousand years later Ramses II of Egypt and the king of the Hittites signed an international treaty to establish eternal peace and brotherhood).

documents to rely upon, international law nevertheless sets forth the body of rules that are legally binding on states in their interactions with each other.[51] Formal and material sources of international law[52] provide evidence of the existence of consensus among states regarding accepted rules or practices, which are legally binding on each state. This Article will explore the ability of customary international law to combat the plague of the Internet that is cybercrime.[53]

A. General Principles

A primary source of international law is found in state custom. By one account, customary international law may be regarded as an "implied and often non-verbalized exercise of direct legislation by the members of society," which constitutes "a spontaneous norm."[54] Such deduction is made based upon the fact that the international legal system identifies customary law in the form of established norms, rather than by creating customary law through some exercise of sovereign authority.[55] To wit, customary international law is formed and has the force of law because of the practice and behavior of states, not because of any legislated or

---

[51] OPPENHEIM, *supra* note 36, at § 1.

[52] Article 38 of the Statute of the International Court of Justice provides for four sources of international law: (1) international conventions (treaties); (2) international custom; (3) general principles of law recognized by civilized nations; and (4) judicial decisions and teachings of the most highly qualified publicists of the various nations. Article 38 sets forth a definitive statement of the sources of international law. INTERNATIONAL LEGISLATION, *The Permanent Court of International Justice* 601 (Hudson 1943).

[53] The focus of this Article is the decentralized emergence of customary international law as an effective response to cybercrime. Therefore, this Article will not critique the recent European Council's Convention on Cybercrime, which was signed November 23, 2001, in Budapest, Hungary.

[54] PARISI, *supra* note 6, at 572.

[55] *Id.* (explaining that "[T]he legal system 'finds' the law by recognizing social norms, but does not 'create' the law"); Robert D. Cooter, *Law, Economics, & Norms: Decentralized Law for a Complex Economy: The Structural Approach to Adjudicating the New Law Merchant*, 144 U. PA. L. REV. 1643, 1648 (1996) (stating that, in medieval times, "English judges allegedly tried to discover those rules that already existed among the merchants, and then selectively enforced them," rather than dictating conformity to rules to which the merchants should conform).

written rules.[56] Thus, the two elements of customary international law consist of (1) state practice, and (2) *opinio juris vel necessitatis* (*opinio juris*).[57] Finally, customary international law—like the common law and unlike statutory law—is a dynamic process of creating law that is universal in application,[58] which is especially relevant to addressing the threat of cybercrime given the objective of implementing an international solution.

B. State Practice

In determining whether a state practices a certain custom, courts consider the duration, the consistency, the repetition, and the generality of a particular practice. No hard-and-fast rules have evolved regarding a time element.[59] However, the International Court of Justice has elucidated basic rules regarding continuity and repetition. For example, a customary rule must accord with a "constant and uniform usage practised by the States in question."[60] Furthermore, state practice must be "extensive and virtually uniform."[61] However, the uniformity rule is not

---

[56] Professor Cooter noted well the distinction between custom and statutory law such as treaty law when he remarked, "Customs arise, while laws are made." *Id*. at 1655.

[57] Essentially, *opinio juris* means a state's "sense of legal obligation." RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 102(2) (American Law Institute 1987).

[58] *See, e.g.*, ANTHONY D'AMATO, THE CONCEPT OF CUSTOM IN INTERNATIONAL LAW (Cornell University Press 1971) [hereinafter D'AMATO—CUSTOM].

> [T]he ultimate power of customary international law is that it binds all states irrespective of their consent to specific rules. Thus it constitutes a default law—a law that applies to every dispute whenever a more specific treaty does not (for whatever reason of interpretation or clausula rebus sic stantibus) provide a sufficiently clear text to settle the dispute. There is no source of international law other than customary law that provides this kind of comprehensive default rule.

ANTHONY D'AMATO, INTERNATIONAL LAW ANTHOLOGY 52 (Anderson Publishing Co. 1994) [hereinafter D'AMATO—ANTHOLOGY].

[59] SHAW, *supra* note 36 at 59-60 (stating that states usually specify a time-scale for the acceptance of a practice as a customary rule).

[60] Asylum Case (Colom. V. Peru), 1950 I.C.J. 266, at 276 (Nov. 20).

[61] North Sea Continental Shelf (F.R.G. v. Den.; F.R.G. v. Neth.), 1969 I.C.J. 3, at 43 (Feb. 20).

absolute: the state practice requirement will be satisfied if "consistent with [customary] rules, and . . . [if] inconsistent with a given rule, [it] should generally have been treated as [a] breach[] of that rule."[62] Repetition may even be completely unnecessary under certain circumstances (i.e., customary international law may be created in a single act or spontaneously).[63] Thus, to the extent that customary law is capable of quickly responding to the crime committed in cyberspace, it is a valuable tool to combat cybercrime.[64]

Finally, the courts consider whether a state practice is general. The generality requirement implicitly means that the state practice must be generally accepted practice in the international community.[65] The general application, however, does not require every state to observe or accept the practice.[66] In fact, even if a practice is limited to just a couple of states, it may still constitute customary international law as applied to those two states.[67] In such cases,

---

[62] Military and Paramilitary Activities (Nicar. V. U.S.), 1986 I.C.J. 14, at 98 (June 22). For a critique of the International Court of Justice's application of custom in the Nicaragua case, *see* Anthony D'Amato, *Trashing Customary Law*, 81 AM. J. INT'L L. 101 (1978).

[63] *E.g.*, Bin Cheng, *United Nations Resolutions on Outer Space: "Instant" International Customary Law?*, 5 INDIAN J. INT'L L. 23 (1965) (discussing the rapid evolution of customary law in new areas such as outerspace); *see also* PARISI, *supra* note 6, at 6 (stating that state practice should emerge out of spontaneous behavior).

[64] OPPENHEIM, *supra* note 36, at § 10 (stating that while custom is normally a relatively slow process, under certain circumstances, customary rules may develop quickly, such as was the case with custom relating to the continental shelf and the exclusive economic zone).

[65] *See* SHAW, *supra* note 36, at 63 (concluding that "for a custom to be accepted and recognised it must have the concurrence of the *major powers* in that particular field") (emphasis added). Professor Shaw views international law as permitting all states to participate in its formation, but as conferring greater weight to views expressed by states based upon each state's relative power and role within the international community. *Id*.

[66] IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 6 (Clarendon Press 4th ed. 1990) (stating that "universality is not required, but the real problem is to determine the value of abstention from protest by a substantial number of states in face of a practice followed by some others").

[67] *Rights of Passage over Indian territory (Port . v. Indian),*1960 I.C.J. No. 12 at 39-40. (Judgment of Apr. 12 in 1960).

the practice is considered to have specific application, rather than general application.[68] In the Internet realm, specification application of state practice may assist in addressing certain instances of cybercrime, but it is obviously less meaningful than practice of general applicability, which would bind all states to a custom.

C. Opinio Juris

The second requirement of customary international law is that each state view a certain practice as legally obligatory, as opposed to a mere usage performed out of "courtesy, morality, or fairness."[69] It is this subjective belief in owing a legal obligation that turns usage into a custom.[70] The International Court of Justice, has on three occasions, interpreted the *opinio juris* requirement rather strictly. For example, in the *Lotus case*, the *North Sea Continental cases*, and the *Nicaragua case*, the International Court of Justice rejected a presumption of *opinio juris.* Instead the Court required evidence of a belief that the practice was obligatory.[71] Obviously, a strict interpretation of the *opinio juris* requirement would tend to fasten customary law to a rigid

---

[68] OPPENHEIM, *supra* note 36, at § 10 (noting that state practice that is not general in application, may nonetheless be considered a customary rule of law; only it would be of "particular rather than general application").

[69] BROWNLIE, *supra* note 64, at 7 (distinguishing *opinio juris* from usage); *see also* MARK W. JANIS, AN INTRODUCTION TO INTERNATIONAL LAW (Aspen Law & Business ed., 3rd ed. 1999) (finding that while a state will rarely make a formal expression regarding *opinio juris*, jurists and judges frequently provide evidence of a state's belief that it owes a legal obligation to abide by certain state practices).

[70] SHAW, *supra* note 22, at 67 (observing that states act in certain ways out of a sense of legal duty). The following example may be useful to distinguish norms from regularities:

> [M]en take off their hats when they enter a furnace room or a church. Taking off your hat to escape the heat is different from taking off your hat to satisfy an obligation. The former is a regularity and the latter a norm. A regularity results from an inclination, whereas a norm imposes an obligation.

Cooter, *supra* note 54, at 1656.

[71] *S.S. "Lotus,"* 1927 P.C.I.J., (Ser. A) No. 10, 28 (1927); *North Sea Continental shelf (W. Ger. v. Den., W. Ger. v. Neth.)*, 1969 I.C.J. 3, 51-52 (Feb. 20); *Military and Paramilitary Activities In and Against Nicaragua*, (Merits) (Nicar. v. U.S.), 1986 I.C.J. 14 (Nov. 26)

and potentially outdated rule, which is contrary to the very idea of customary international law as an organic and continuously growing source of international law.[72] To the extent that the courts view evidence of *opinio juris* liberally, customary law may serve as a viable tool to protect the interests of the international community against cybercrime.

To summarize, the fact that customary international law applies universally throughout the international community makes customary international law especially well-suited to address legal issues arising in the context of the Internet. Furthermore, customary law has, on occasion, been quick to develop when previously unaddressed issues of international concern arise, as was the case with the development of custom regarding outerspace law. Probably not detrimental to its applicability to cybercrime, but definitely weighing against it, the fact that "custom is normally a relatively slow process for evolving rules of law."[73] Finally, the more rigidly the courts interpret *opinio juris*, the less useful customary international law can be used as a tool to end cybercrime. With the help of economic principles, the rest of this Article attempts to fine tune customary international law to meet the needs of states fighting cybercrime.

III. APPLYING INTERNATIONAL LAW & ECONOMICS TO COMBAT CYBERCRIME

"International law is the product of its environment."[74] It is a system that regulates and defines the rights and obligations of states as they interact with each other.[75] International law

---

[72] *See generally* SHAW, *supra* note 36, at 69 (noting that the courts must take a flexible view of the *opinio juris* and connect it to outward manifestations of state practice). The International Court of Justice itself stated that "reliance by a State on a novel right or an unprecedented exception to the principle might, if shared in principle by other States, tend towards a modification of customary international law." M. AKEHURST, *Custom as a Source of International Law,* BRITISH YEARBOOK OF INTERNATIONAL LAW 32-4 (1974-5) (quoting *Military and paramilitary activities(Nicar. v. U.S.),* 1986 I.C.J. 14 (June 27).

[73] OPPENHEIM, *supra* note 36, at 10.

[74] SHAW, *supra* note 36, at 36.

developed as a result of the customary notions of international relations. In order for international law to endure, it must adapt to the prevailing realities of the cyber age. Somewhat differently, economics is concerned with determining which laws are the most efficient.[76] An economically efficient law is one that provides for achieving a goal (transaction) at the least possible cost.[77] In the international domain, economic analysis of law provides a behavioral theory that predicts how actors—in this case, states interacting in the international community—will respond to different structures of the international legal regime.[78] As this article stresses, an economic approach to international law, as this Article stresses, can assist states in developing optimal solutions that address the cybercrime problem.

---

[75] *Id*. at 37 (explaining that the purpose and determining factor of international law in its development is to serve the needs and characteristics of the international political system).

[76] Aceves, *supra* note 5 at 1061 (concluding that economic analysis of law suggests that efficiency, by way of customary international law, will help to create international institutions).

[77] *E.g*., O'Neill, *supra* note 20, at n.14 (stating, "By 'efficient,' I adopt the traditional economic definition of efficiency to mean that crimes involving the Internet reduce costs to potential criminals while at the same time increasing their expected gains").

[78] ROBERT COOTER & THOMAS ULEN, LAW AND ECONOMICS 3 (Addison-Wesley ed., 2d ed. 1997) [hereinafter Cooter & Ulen] (generalizing that "economics provides a behavioral theory to predict how people respond to changes in laws").

> [Economic analysis of law] tries to explain and predict the behavior of participants in and persons regulated by the law. It also tries to improve law by pointing out respects in which existing or proposed laws have unintended or undesirable consequences, whether on economic efficiency, or the distribution of income and wealth, or other values. It is not merely an ivory-tower enterprise, at least in the United States, where the law and economics movement is understood to have influenced legal reform in a number of important areas.

RICHARD A. POSNER, *Values and Consequences: An Introduction to Economic Analysis of Law*, in CHICAGO LECTURES IN LAW AND ECONOMICS 190 (Eric Posner ed., Foundation Press 2000); PARISI, *supra* note 6,at 1 (stating that a "fundamental insight of the economic analysis of law is the notion that legal sanctions are 'prices' set for given categories of legally relevant behaviour").

A. An Economics Approach to Customary International Law

Economic analysis provides that decentralized market processes are comparatively more efficient than centralized processes.[79] In this respect, customary law, which is created voluntarily and spontaneously, is a highly efficient process for creating rules of international cyberlaw.[80] Historically, traditions of international economic law can be traced back to the law merchant and sets of principles used to resolve conflicts involving jurisdictions.[81] Presently, the international community is challenged by similar problems that must be resolved to in order to rid the Internet of cybercrime.[82] Because customary international law permits states to cooperate in the absence of formal written agreements, it minimizes the transactions costs associated with

---

[79] *See, e.g.*, Aceves, *supra* note 5, at 1061 (stating that "customary international law allows states to reap the benefits of a formal relationship without the limitations imposed by a formal agreement"). Moreover, Aceves recognizes that international custom establishes expectations that guide economic transactions without the need for costly safeguards, which contributes to the economic efficiency of international cooperation. *Id*.

[80] Professor Cooter's argument is especially apropos to emerging international cyberlaw:

> [C]entralized law, like socialism, is not even plausible for a technologically advanced society. . . . [e]fficiency requires decentralization to become more important, not less, as economies become more complex. Specifically, efficiency requires that as economies develop, the enforcement of custom . . . becomes more important . . . .

Cooter, *supra* note 54, at 1646.

[81] Joel R. Paul, *Interdisciplinary Approaches to International Economic Law: The New Movements in International Economic Law*, 10 AM. U.J. INT'L L. & POL'Y 607, 609-610 (1995). For a traditional account of the "law merchant" that arose during medieval times, *see* Cooter, *supra* note 54, at 1646-50.

[82] *See, e.g.*, Goldsmith, *supra* note 34, at 104 (arguing that international law principles of territorial sovereignty do not prohibit the United States from conducting searches and seizures on computer networks located within the territory of another country); *cf.* Bellia, *supra* note 33 (arguing for, in most instances, obtaining permission from a state prior to conducting a cross-border search into sovereign territory). *But see* Johnson & Post, *supra* note 14, at 1367 (arguing that traditional international law regarding territorial borders is inappropriate to govern cyberspace, which requires creating a new and independent doctrine of law).

negotiating bi- or multi-lateral treaties.[83] Thus, on its face, customary international law appears to provide an efficient means for responding to cybercrime.[84]

1. Symmetrical Cybercrime Interests

In a perfect digital world, each state is confronted with symmetrical conditions and preferences. Here, the incentives of each state are perfectly aligned with other states.[85] For example, states concerned about cyber-crime may each regard permission prior to chasing digital data across borders as an unnecessary hindrance to combating cybercrime. Under this scenario, an international cybercrime custom would emerge to which all states would agree. Regardless of the custom, each state expects the same levels of costs and benefits to create and adhere to such custom. Therefore, in creating international custom relating to cybercrime, each state has an incentive to agree to rules that not only maximize its benefits, but also incidentally maximize the welfare of the entire international community.[86]

---

[83] ACEVES, *supra* note 5, at 1005 (arguing that customary international law minimizes transaction cost problems by permitting states to bypass formal negotiations and to operate in an environment lacking formal structure).

[84] Speaking of the efficiency of custom, Aceves states, "Custom establishes expectations regarding certain behavior. In turn, these expectations can guide economic transactions without the need for costly safeguards [inherent in treaty law]. Through this process, custom may contribute to economic efficiency." ACEVES, *supra* note 5, at 1062. Aceves, further declares that customary international law is well-equipped to accept changes in practice and the need for modification of custom; it can even modify existing treaty obligation. *Id*. at 1061.

[85] Francesco Parisi, *The Cost of the Game: A Taxonomy of Social Interactions*, 9:2 EUROPEAN JOURNAL OF LAW AND ECONOMICS 3 (2000) [hereinafter *The Cost of the Game*] (stating that in games involving perfect incentive alignment, "there is no temptation to defect unilaterally because there are safeguards that eliminate all the payoff advantages of unilateral defection"). Such alignment also ensures that emerging customary international law will arrive at an equilibrium point that optimizes the parties' incentives. *Id*.

[86] Goldsmith and Posner set forth for strategic positions that allegedly capture the behavioral regularities of customary international law. Jack L. Goldsmith and Eric A. Posner, *A Theory of Customary International Law*, 66 U. CHI. L. REV. 1113, 1121-28 (1999) [hereinafter Goldsmith & Posner]. The first strategic position is "coincidence of interests," which means that states engage in certain usages because "each obtains private advantages form a particular action []

2. Asymmetrical Cybercrime Interests

In the real digital world, however, states are unlikely to have perfect incentive alignment. One reason is because customary international law and law enforcement relating to cybercrime constitute public goods. In the context of cybercrime, the public goods problem arises because each individual state faces a private cost and generates a public benefit when it engages in creating and enforcing customary international rules that address cybercrime.[87] Without reframing the public goods problem, states will produce and enforce suboptimal levels of customary international law in response to the threat of cybercrime.[88] In fact, a state confronted with a public goods problem will only create or enforce customs addressing cybercrime to the extent that its marginal cost of doing so is less than or equal to the marginal benefit that it expects in return.[89]

---

irrespective of the action of the other." *Id*. at 1122. This position inherently recognizes that incentives are in perfect alignment, although not as a result of state action. Nevertheless, perfect incentive alignment does not depend upon the states intending to benefit the general welfare; as Goldsmith and Posner argue, states may achieve such result merely by pursuing their own self interest. *Id*. at 1176-77.

[87] *See generally* PARISI, *supra* note 6, at 22-24 (discussing some of the general failures of customary law, and specifically addressing collective action problems in customary legal regimes). Professor Parisi also notes that one of the inherent problems with customary international law is that it constitutes a public good *per se*. *Id*. at 23.

[88] COOTER & ULEN, *supra* note 77, at 40-41. Cooter and Ulen provide an example of the public defense problem by examining who would purchase national defense: the authors conclude,

> As a result of the presence of free riders and the high cost of distinguishing nonpaying from paying beneficiaries, it is not likely that the private company will be able to induce many people to purchase defense services. If private profit-maximizing firms are the only providers of national defense, too little of that good will be provided.

Id.

[89] *See also* PARISI, *supra* note 6, at 23 (stating that if "left to private initiative, punishers would be willing to enforce norms only to the point which the private marginal cost of enforcement equals its private marginal benefit," which is less than the public marginal benefit). With respect

Where states have diverse interests, and the probability of future interaction with respect to a subject such as cybercrime is high, each state's discount factor bears on the likelihood of an optimal solution. Under game theory,[90] a discount factor is a function of both (1) a state's time preference and (2) the probability of future interactions.[91] First, the more that a state prefers quick resolution of an international problem, the less it values future resolution of such problem. In cybercrime cases, state law enforcement agents must be able to search and seize electronic data before it is destroyed, which may be done at the click of a mouse.[92] Therefore, states responding to cybercrime will generally have a high preference for time, and they will be less interested in trading present payoff (i.e., the chance to catch a cybercriminal now) for an expected increase in future payoff (i.e., the less likely chance to catch a cybercriminal at some future date). In other words, states pursuing cybercrime beyond their borders will be less likely to cooperate with states viewed as unlikely to permit them digital entry into their sovereignty; thus, the pursuing states have a low discount factor.

Second, the greater the probability that states will interact in the future, the greater the expected value of future cooperation.[93] A state that believes it will interact with other states in

---

to law enforcement of customary international law, Professor Parisi suggests delegating such responsibility to a centralized authority to achieve optimal levels of public benefit. *Id.*

[90] Game theory may be thought of as "a set of tools and a language for describing and predicting strategic behavior." RANDAL C. PICKER, *AN INTRODUCTION TO GAME THEORY AND THE LAW IN CHICAGO LECTURES IN LAW AND ECONOMICS*, *supra* note 77, at 30 (emphasis omitted).

[91] PARISI, *supra* note 6, at 8 (stating that the discount factor is a function of (1) the players' time preference, and (2) the probability of future interactions).

[92] Bellia, *supra* note 33, at 55-56 (stating that two problems that law enforcement encounters in attempting to obtain cybercrime evidence are (1) "more and more evidence will be located across international borders," and (2) "electronic evidence can so easily be lost or destroyed").

[93] COOTER & ULEN, *supra* note 77, at 36 (stating that "[i]f the same players play the same game according to the same rules repeatedly, then it is possible that cooperation can arise"). Furthermore, if a game is to be repeated, i.e., if states are to interact, an indefinite number of times, the optimal strategy calls for conditional cooperation. ROBERT M. AXELROD, THE

the future—as the result of it pursuing a cybercrime abroad or because another state may seek to pursue a cybercrime within its borders—will be more willing to develop efficient customary rules relating to cybercrime. Conversely, if a state believes that future interaction is unlikely, or that a "one-shot" interaction is likely, it has no incentive to cooperate because doing so will not increase the expected value of future cooperation.[94] As the expectation of future interaction of any one state is unknown and may not be generalized, the discount factor for this element is unknown. "Only where there is a relatively large discount factor, do long-run optimization strategies become evolutionarily stable."[95]

Several other misalignments of cybercrime interests may exist in the international community. For example, states that are economically less dependent upon technology have less incentive to create rules in which cybercriminals are effectively deterred and punished. To go

---

EVOLUTION OF COOPERATION 13-14 (Basic Books ed. 1984) (explaining that if a party cooperated in the last round of play, the opposing party would cooperate on the next round of play, and vice versa—this is called a "tit-for-tat" strategy); Goldsmith & Posner, *supra* note 85, at 1125-27 (applying Axelrod's tit-for-tat strategy to customary international law cooperation).

[94] Addressing investment decisions that are made during agency games, professor Cooter noted that if a "game is played only once, the agent's best more is to appropriate [the principal's investment]. Knowing this, the principal's best move is not to invest. The *one-shot game* of investment has a unique solution, which is unproductive." Cooter, *supra* note 54, at 1658 (emphasis added).

[95] PARISI, *supra* note 6, at 8. Similar to Parisi's analysis, Goldsmith and Posner assert that states presented with a bilateral prisoner's dilemma may achieve cooperation over time if three conditions are met: (1) the states must have sufficiently low discount rates; (2) the game (interaction) must continue indefinitely; and (3) the payoffs from defection must not be higher than the payoffs from cooperation. Goldsmith & Posner, *supra* note 85, at 1124-27. The second requirement that the game continue "indefinitely" is significant. This is so because if a game is played for a fixed number of times (say 20), each party will work backward from 20 and determine that their best strategy is to defect from the rules as soon as possible; the parties cannot do better by changing their strategy so long as the other party maintains the original strategy. COOTER & ULEN, *supra* note 77, at 35-36. The net result is that the parties reach a nash equilibrium, where surplus equals zero. *Id*. at 35. However, when a game is repeated for an indefinite number of times, the optimal strategy involves cooperating as a condition of the previous player's cooperation ("tit-for-tat" strategy). AXELROD, *supra* note 92, at 13-14.

further, some states may even benefit from loose national rules relating to cybercrime, and strict rules relating to territorial sovereignty, which would effectively create a refuge for cybercriminals. Put somewhat differently, states that opt out of international customs relating to cybercrime may permit by default the development of a market for cybercrime.[96]

Asymmetric or unknown state interests present obvious challenges to international cooperation in preventing and deterring cybercrimes, and in subsequently punishing cybercriminals. Nevertheless, states seeking to induce a socially optimal level of cybercrime custom in international law may employ several economic tools to align diverse interests.

3. Creating Symmetrical Cybercrime Interests

As was demonstrated above, perfect incentive alignment among states would be a rare occasion. Incentives can be aligned, however, once states agree to a framework in which certain conditions reduce the likelihood of uncooperative behavior. Three methods described below—

---

[96] Like a market for lemons, a market for cybercrimes may emerge in countries that fail to heed international cybercrime customs and laws. For example, imagine a potential cybercriminal who has the means and ability to conduct cybercrime from any location in the world—after all, cybercrime can be profitable. Further imagine that the cybercriminal is aware that ten of the eleven states comprising cyberworld have agreed to certain customary law sanctions that increase the cost of committing cybercrime. One state held out for whatever reasons. Finally, assume that potential victims of cybercrime have no way of knowing from which state a cybercrime will occur. See Johnson & Post, supra note 14, at 1371 (noting that the "Net enables transactions between people who do not know, and in many cases cannot know, each other's physical location"). In other words, the cybercrime market (on the Internet) is comprised of large information asymmetries between the criminals and the victims. Obviously, our imagined cybercriminal, and all of her associates, would prefer to conduct her cybercriminal enterprise from the state lacking customary international cybercrime laws, where the expected future gains are greatest. *See* George A. Akerlof, *The Market for 'Lemons': Quality and Uncertainty and the Market Mechanism*, 84 QUARTERLY JOURNAL OF ECONOMICS 488, 488-500 (1970) (arguing that in the market for used cars, there exists informational asymmetry between car sellers and buyers which results in car quality uncertainty and correlative price averaging); T. Markus Funk & Daniel D. Polsby, *The Problem of Lemons and Why We Must Retain Juvenile Crime Records*, 18 CATO JOURNAL 75, (1998) (arguing that expunging juvenile offender records, like the market for lemons problem, creates information asymmetries that are likely to result in judges sentencing career criminals too leniently and first time offenders too severely).

namely, role reversability, reciprocity constraints, and articulation—can help align state interests so that efficient customs of international cyberlaw may emerge.

a. State Role Reversability

One mechanism for aligning states' interests is to impose role reversability constraints upon each state.[97] Advocates of the law and economics school often use the example of the law merchant to demonstrate the effect of role reversability on the emergence of efficient customary international law. In medieval times, traveling merchants conducted business abroad in a capacity as both buyer and seller. In establishing customary norms, merchants sought to protect both their interests as buyer and their interests as seller.[98] Because they knew that any rule having a positive effect on one set of interests (e.g., seller interests) could negatively effect their interests on the other side of the equation (e.g., buyer interests), merchant law evolved which took into equal consideration the interests of buyers and sellers.[99] The crux of role reversability is that "an otherwise conflicting set of incentives [is changed] into one that converged toward symmetrical and mutually desirable rules."[100]

In the same way, role reversability could be used to align each of the states the cybercrime interests. Take for example, international law concerning territorial sovereignty on the one hand, and a state's need to pursue cybercrimes being perpetrated from abroad on the other. A large debate surrounds the issue of when a state may independently perform cross-

---

[97] PARISI, *supra* note 6, at 9 (asserting that "role reversability and stochastic symmetry induce each member to agree to a set of rules that benefits the entire group").

[98] *See* Cooter, *supra* note 54, at 1647 (defining "new law merchant" as norms created within business communities—for instance, those norms created around certain technologies—and outside of a legislature).

[99] *Id*.

[100] PARISI, *supra* note 6, at 10.

border data searches without violating international law.[101] One forceful argument concludes, "In the criminal context, [] customary international law generally prohibits law enforcement officials from one country from exercising their functions—such as conducting searches or making arrests—in the territory of another state without that state's permission."[102] Without a supplemental rule, such custom seriously impedes any state's ability to quickly respond to cybercrime.

On the other side, however, is the United States, which recently manifested its views on the issue by engaging in a remote cross-border search and seizure of electronic data located on computers located in Russia.[103] Even though the United States had a strong interest in obtaining evidence and in capturing cybercriminals before it was too late, if asked, its government would be unlikely to advocate a rule in which states were permitted to transgress territorial sovereignty at will. Clearly, the United States would object—as did most of the international community in the Alvarez-Machain kipnapping[104]—if the roles were reversed.

---

[101] *See, e.g., Fighting Cybercrime – What are the Challenges facing Europe? Meeting Before the European Parliament* (Sept. 19, 2000) (remarks of Kevin DiGregory, Deputy Assistant Attorney General, Criminal Division, U.S. Dep't of Justice) (*available at* http://www.usdoj.gov/criminal/cybercrime/EUremarks.htm) (last visited Mar. 2002).

[102] Bellia, *supra* note 33, at 48. As professor Bellia recognizes, *id*. at n.41, the international law doctrine of self-defense constitutes an exception to this rule. In general and under limited and proportional constraints, a state may employ self-defense if it is attacked by another state. OPPENHEIM, *supra* note 36 at § 127; United Nations Charter, art. 51, (providing that each state has an "inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations").

[103] While investigating a Russian group suspected of hacking several U.S.-based companies, FBI agents obtained Russian passwords and used them to download evidence directly from computers located in Russia. The FBI's investigation was the first instance in which a state publicly acknowledged that it conducted a cross-border data search and seizure without the permission of the state in which the data investigation and seizure was performed. Bellia, *supra* note 33, at 39-40.

[104] It should be noted that the U.S. is no stranger to controversial cross-border search and seizures. *See, e.g., United States v. Alvarez-Machain*, 504 U.S. 655, 657-58 (setting forth the

Similar to the case of the traveling merchant, states will seek rules that protect two distinct sets of interests. At times, states will want to protect their territorial sovereignty interests; while at other times, they will want expedient rules that permit pursuing cybercrime transgressions that originate from abroad. The development of efficient rules of customary international law relating to cybercrime depend, in part, on a successful system in which spontaneous and decentralized decisions are made by state actors.[105] Over time, as states engage in interactions involving cybercrime, their roles will reverse, and international cybercrime customs will emerge and be followed by states acting in pursuit of their economic interests.[106]

b. State Reciprocity Constraints

A second, and perhaps stronger, method of converging the interests of states is by inducing reciprocity constraints.[107] So for instance, if Goldsmith and Posner are correct in

---

facts and circumstances under which the United States Drug Enforcement Agency entered Mexican territory, kidnapped a Mexican citizen, and brought him to trial in the United States, all without the permission of the Mexican government). *See generally* Jimmy Gurule, *Terrorism, Territorial Sovereignty, and the Forcible Apprehension of International Criminals Abroad*, 17 HASTINGS, INT'L & COMP. L. REV. 457 (1994) (discussing the international outcry against the U.S. kidnapping of a Mexican citizen without the prior permission of the Mexican government).

[105] Goldsmith & Posner, *supra* note 85, at 1132 (arguing that states may spontaneously cooperate, and that such cooperation may "evolve" into a behavioral regularity as a result of states pursuing their own interests).

[106] *See, e.g.*, L.L. FULLER, THE MORALITY OF LAW 24 (Yale University Press rev. ed. 1969) (stating that role reversability promotes duties that will be recognized and accepted by parties, "not only in theory, but in practice"). Although states may have an incentive to breach rules following role reversal, the reputational costs of doing so often outweigh such behavior. PARISI, *supra* note 6, at 11. *But see* Goldsmith & Posner, *supra* note 85, at 1135 (rejecting the idea that reputation would cause a state to comply with customary international law, except in tit-for-tat and related game strategies). In fact, Goldsmith and Posner "insist that the payoffs from cooperation or deviation are the *sole determinants* of whether states engage in the behavioral regularities that are labeled norms of [customary international law]." *Id*. at 1132 (emphasis added).

[107] It is important to note that reciprocity constraints may only help to align interests where states have an incentive to unilaterally defect in pursuit of higher payoffs that are available outside of customary international law. PARISI, *supra* note 6, at 14.

believing that reputational effects have little do with compliance with customary international law, a state may be tempted to ignore custom in exchange for a higher payoff.[108] States may eliminate the incentive to pursue opportunities that are sub-optimal by binding their strategic choices to those of other states.[109] Professor Parisi explains that the key to the reciprocity principle is embodied in the age old ideal of "do unto others as you would have done to you."[110]

Without reciprocity constraints, states will not achieve the best solution to combat the threat of cybercrime. For example, states pursuing digital evidence of crimes committed in cyberspace must act quickly before data is lost or destroyed. In contrast, states from which permission is sought to collect evidence have traditionally required such requests to proceed through an often formal and cumbersome process, which is not conducive to capturing invisible and fleeting cybercriminals.[111] In addition, the state withholding its permission is better off under the status quo because it expends no energy or resources in providing legal assistance.

---

[108] *See generally id.* at 11-16 (arguing that reciprocity constraints may be used to align parties' interests "[w]hen unilateral defection promises higher payoffs and there is no contract enforcement mechanism" to prevent opportunistic behavior and sub-optimal strategies).

[109] *Id*.

[110] *Id*. at 14 (citing Exodus 21:23 and the Code of Hammurabi paras. 108 and 127) (quotes are author's and are added for emphasis). In meting out retribution, however, states are limited by their reciprocal strengths. *Id*. The same holds true today. SHAW, supra note 36, at 63 (stating that "for a custom to be accepted and recognised it must have the concurrence of the *major powers* in that particular field") (emphasis added); Goldsmith & Posner, *supra* note 85, at 1123 (explaining that in one of the four strategic positions that capture behavioral regularities of customary international law, "coercion" describes equilibrium in which a large state issues a threat to a small state, the small state heeds the threat, and the large state does not punish the small one).

[111] Bellia, *supra* note 33, at 50 (explaining that states requesting evidence from other states have historically relied upon letters rogatory, which are evidentiary requests issued by a court located in one country to a court located in another country via diplomatic assistance). Bellia concludes that even if the process of obtaining letters rogatory were not slow and cumbersome, they are not well-suited to cybercrimes because courts may only issue them in pending cases. *Id*. In practical terms, this means that law enforcement of one state would have already identified and charged certain suspected cybercriminals. Obviously, these letters do not assist in determining who to bring charges against.

Also adding to the expense of legal assistance in the area of cybercrime requires developing technical expertise. Finally, with the growth of the Internet, "more and more evidence will be located across international borders."[112] These costs suggest that the state from which permission is requested can achieve a higher payoff by stonewalling.

Automatic reciprocity constraints would induce states to arrive at an optimal cybercrime outcome because a state's incentive to behave opportunistically would be eliminated. Analyzing the problem from an *ex ante* perspective—that is to say before cybercrimes occur—each state will create customary rules that it would like to be applied to it regardless of the circumstances (i.e., regardless of whether the state was requesting legal assistance or whether the state was presented with a request for legal assistance). If a state established rules taking into account, and hoping to benefit from, only one set of probabilistic circumstances, it may be gambling unwisely. This will happen because if in the future converse circumstances exist, reciprocity will dictate applying the same opportunistic rule previously established by the state, against the same state. Therefore, states confronted with the possibility of being in either of two situations—requesting permission from a state or considering a request for permission from a state—will create international cyberlaw custom that is socially optimal.[113]

c. State Articulation

A third technique for aligning the interests of states involves in requiring states to clearly articulate their intentions to follow certain international customs. As professor D'Amato explains the theory, articulation requires states to make an *objective* (notice the element of subjectivity is

[112] *Id.* at 55.

[113] PARISI, *supra* note 36, at 16 (concluding that "iterated interactions with role reversability, reciprocity constraints, and structural integration facilitate the emergence and recognition of customary law").

removed) statement or expression[114] regarding the legality of particular international customs either prior to engaging in state practice or at the same time the state begins to engage in state practice.[115] The purpose of articulation theory is to fix the primary challenge that the *opinio juris* requirement presents to the spontaneous formation and continuous development of customary international law[116]—the requirement that a state produce evidence that another state believes it is obliged to perform a specific state practice.[117] In application, articulation theory crystalizes.

International law emerging to address cybercrime would benefit greatly if states articulated customs that they intend to apply. Consider once more the issue of territorial sovereignty in cyberspace. Viewing the problem *ex ante*, states have an incentive to "articulate and endorse norms that maximize their expected welfare."[118] The incentive arises because states must base their decisions on unforeseen events and some probability that they will be on either

---

[114] D'AMATO—CUSTOM, *supra* note 57, at 18 (stating that articulating statements or expressions may come in the form of a published article, an announcement to an international body, through diplomatic relations, or through any other effective means of public communication).

[115] D'AMATO—ANTHOLOGY, *supra* note 57, at 66 (Anderson Publishing Co. 1994). More formally, articulation is the requirement "that an objective claim of international legality be articulated in advance of, or concurrently with, the act which will constitute the qualitative element of custom." *Id*.

[116] *Id.* at 17 (observing that articulation is an attempt by legal theorists and practitioners to address one of the primary problems with *opinio juris*—namely the circular requirement "that [states] must believe that a practice is already law before it can become law"). Professor Parisi also finds that the *opinio juris* "requires the existence of a mistake for the emergence of custom: the belief that an undertaken practice was required by law, when instead, it was not." Parisi, *supra* note 6, at 16. *See also* Goldsmith & Posner, *supra* note 85, at 1115 (replacing traditional explanations of customary international law based on *opinio juris* for the idea that customary international law emerges as a result of states pursuing their own self-interested policies within the international political environment).

[117] *Military and Paramilitary Activities In and Against Nicaragua*, (Merits) (Nicar. v. U.S.), 1986 I.C.J. 14 (Nov. 26) (requiring evidence of a state's subjective belief that it owed an obligation to follow certain custom, rather than mere evidence of state practice).

[118] PARISI, *supra* note 6, at 18 (arguing also that *ex ante* norms, consistent with economic analysis of law, should be given greater weight in the adjudication process).

side (or on both sides) of the issue at some future date.[119] No state knows in advance whether it will need to pursue evidence of a cybercrime in another state, or whether a foreign state will seek evidence of a cybercrime within its digital borders. So, for instance, based on articulation, the following customary rule might emerge: a state may pursue digital evidence of a cybercrime located in another state's territory so long as it notifies the appropriate jurisdictional authorities of its activities and investigates in good faith. The example, although perhaps not arriving at "the" solution, demonstrates that states will articulate rules that tend to maximize the expected welfare of the entire international community,[120] rather than one side's narrow interests.

The primary benefit of articulation is that it eliminates the guesswork associated with the *opinio juris* requirement.[121] Consistent with the goals of economics, articulation improves the efficiency of international customary law by reducing the transaction costs associated with creating and following such laws. Similarly, articulation of customary law prior to engaging in state practice, puts other states on notice of the articulating state's state practice intentions. In these ways, customary international law is allowed to grow and to respond to new challenges such as those that have arisen in the fight against cybercrime.

---

[119] In this respect, articulation aligns the interests of states in the same way that role reversability and reciprocity constraints do.

[120] PARISI, *supra* note 6, at 18. On the other hand, rules articulated after states already disagree about a specific application of customary international law, i.e., post disagreement rationalization, are more likely to reflect the strategic biases of each party.

[121] *Id.* at 17-18 (stating that the guessing process inherent in *opinio juris* is removed when "states articulate desirable norms . . . that they intend to follow and be bound by").

CONCLUSION

If any international issue is ripe for a "transnational" solution, it is the enigmatic and borderless disease of cybercrime.[122] This Article argues that any "cyberlaw" solution seeking to deny the digitally depraved of the ability to employ the Internet as a vehicle of criminal enterprise must be international in scope. In addition, due to the nature of the Internet, which is in a state of continuous flux and evolution, any response by states hoping to stop cybercrime must also be flexible and capable of evolving. Customary law presents the most efficient and effective means for the international community to address cybercrime. By borrowing principles from economics to align states' interests for purposes of forming cybercrime rules, states may achieve optimal customary international law that maximizes the welfare of the entire international community.

[122] *See* PHILIP JESSUP, TRANSNATIONAL LAW 2 (1956) (envisioning "transnational law" that embodied "all law which regulates actions or events that transcend national frontiers").