Brooklyn Journal of International Law

Volume 37 | Issue 3 Article 9

2012

An Adaptive Approach for an Evolving Crime: The Case for an International Cyber Court and Penal Code

Nicholas W. Cade

AN ADAPTIVE APPROACH FOR AN EVOLVING CRIME: THE CASE FOR AN INTERNATIONAL CYBER COURT AND PENAL CODE

INTRODUCTION

Technological innovation over the last half-century has bestowed revolutionary advantages upon humanity. Yet for all its brilliant progress, technology's constant state of development has also cultivated an evolving criminal field capable of inflicting unprecedented damage: cybercrime. To date, legislative efforts to fight the numerous forms of cybercrime, from localized mischief-making to highly destructive acts of cyberterrorism, have been largely inefficient and regularly outpaced by dynamic criminal tactics[1] and the mutations of cyberspace itself. As long as the global community continues to take insufficient action to address the threats posed by cybercriminals, the risk of a catastrophic cyberattack—with the potential to eradicate vast quantities of private records, dismantle corporate activities, and suspend entire governments—will persistently increase.[2]

Cybercriminals have been regarded as a serious threat to governments and state security since the dawn of the digital age, costing the global community billions of dollars each year.[3] Today, cybercriminals are playing a more prominent role in geopolitical affairs than ever before as they increasingly direct their focus to nontraditional targets in new and novel ways. In late August 2011, for example, a group of hackers successfully impersonated Google, the popular search engine and e-mail provider, and used their disguise to snoop on Internet users.[4] In an unrelated case from the latter half of 2011, a ruthless Mexican crime syndicate, Los Zetas, found itself in the crosshairs of Anonymous, a well-

---

1. *See, e.g.*, Christopher E. Lentz, Comment, *A State's Duty to Prevent and Respond to Cyberterrorist Acts*, 10 CHI. J. INT'L L. 799, 799–801 (2010); 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, 60–66 (2010).

2. *See, e.g.*, Charlotte Decker, Note, *Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime*, 81 S. CAL. L. REV. 959, 960–61 (2008).

3. *Id.* at 961–62; *see generally* Gable, *supra* note 1, at 59–66.

4. The targeted e-mail accounts belonged to people living in Iran. Neither the purpose of the attack, nor its focus on Iranian e-mail accounts, is clear. Somini Sengupta, *In Latest Breach, Hackers Impersonate Google to Snoop on Users in Iran*, N.Y. TIMES, Aug. 31, 2011, at B4.

known collective of hackers from across the globe.[5] After Los Zetas apparently kidnapped one of their hackers, Anonymous—which had illegally accessed confidential NATO documents only months before[6]—released a video on YouTube, the popular video sharing website, in which a masked figure criticized Los Zetas for its criminal behavior and pledged to release the identities of one hundred of Los Zetas' major contacts.[7] The Anonymous member was released within days.[8]

In addition to individuals and collectives perpetrating such novel cyberattacks, sovereign governments are engaging in potentially illegal online behavior with greater regularity. In November 2011, the United States accused China and Russia of using proxy computers and dispersed Internet routers in other countries to spy on Americans over the Internet.[9] The United States itself has admitted to considering the use of cyberattacks during its involvement in 2011's Libyan revolution[10] and may have utilized a computer worm to target uranium-enriching centrifuges in Iranian nuclear facilities.[11] Cybercriminals acting as government agents in such scenarios may be able to cause more widespread damage, and present even more challenging legal and logistical hurdles for law enforcement officials, than isolated actors.

As hackers' capabilities and resources continue to grow, and as more government operations increasingly occur online,[12] the scope of a single

---

5. Damien Cave, *After a Kidnapping, Hackers Take On a Ruthless Mexican Crime Syndicate*, N.Y. TIMES, Nov. 1, 2011, at A6.

6. *Hackers Gain Access to NATO Data*, N.Y. TIMES, July 22, 2011, at A7.

7. Cave, *supra* note 5, at A6.

8. Paul Wagenseil, *Anonymous wins victory in drug cartel fight*, MSNBC.COM (Nov. 4, 2011, 5:28 PM), http://www.msnbc.msn.com/id/45169382/ns/technology_and_science-security/t/anonymous-wins-victory-drug-cartel-fight/#.T2eVnXjs620.

9. Thom Shanker, *In Blunt Report to Congress*, *U.S. Accuses China and Russia of Internet Spying*, N.Y. TIMES, Nov. 4, 2011, at A4; *see also* Richard A. Clarke, Op-Ed., *How China Steals Our Secrets*, N.Y. TIMES, Apr. 3, 2012, at A27 (providing an overview of Congressional efforts to address cybercrime and noting that "Robet S. Mueller III, the director of the F.B.I., said cyberattacks would soon replace terrorism as the agency's No. 1 concern as foreign hackers, particularly from China, pentrate American firms' computers and steal huge amounts of valuable data and intellectual property").

10. Eric Schmitt & Thom Shanker, *U.S. Debated Cyberwarfare in Attack Plan on Libya*, N.Y. TIMES, Oct. 17, 2011, at A1.

11. Michael Totty, *The First Virus . . .*, WALL ST. J., Sept. 26, 2011, at R2; Tom Gjelten, *Security Expert: U.S. 'Leading Force' Behind Stuxnet*, NPR (Sept. 26, 2011), http://www.npr.org/2011/09/26/140789306/security-expert-u-s-leading-force-behind-stuxnet.

12. *See, e.g.*, Vivek Kundra, Op-Ed., *Tight Budget? Look to the 'Cloud'*, N.Y. TIMES, Aug. 31, 2011, at A27.

cyberattack's damage becomes increasingly daunting. Though the United States to date has managed to weather most of the cybercrimes perpetrated against it with relatively modest damage, other less fortunate nations provide ominous examples of what could be in store for the global community. In 2007, for one example, Estonia was effectively shut down for three weeks by a series of relatively simple cyberattacks that targeted government, media, and business websites.[13] Estonia made itself particularly vulnerable by being at the vanguard of adopting online processes—the government opted to conduct most of its operations over the Internet while individual Estonians conducted much of their personal affairs, including more than ninety-eight percent of their private banking, online.[14] Despite Estonia's stark example of the risks associated with taking state business online, the number of nations adopting Internet-based operations continues to grow.[15]

Owing perhaps to the ever-expanding list of potential targets, the frequency of cybercrimes is increasing. The U.S. Department of Homeland Security announced that there were eighty-six reported attacks on critical infrastructure computer systems in the United States between October 2011 and February 2012, an increase of seventy-five attacks from the same time-span the previous year.[16] These attacks were just a small part of the more than 50,000 cyberattacks reported to the agency since October 2011.[17]

Due to the uniquely global dimensions of cybercrime and the world's growing reliance on technology, the international community needs to adopt an international penal code for cybercrime and vest jurisdiction over this unique body of law in an international criminal court or tribunal. Such a code is necessary to provide a uniform set of definitions, norms, and standards, and to effectively regulate a crime—evolving faster than many legislatures can operate—that knows no territorial boundaries.

This Note seeks to examine the justification for this new approach and to evaluate the inherent difficulties in regulating cybercrime through traditional criminal systems.[18] Part I, in sections A and B, considers the de-

---

13. Lentz, *supra* note 1, at 799–800; Gable, *supra* note 1, at 61.

14. Gable, *supra* note 1, at 61.

15. *See, e.g.*, Kundra, *supra* note 12, at A27.

16. Michael S. Schmidt, *New Interest in Hacking as Threat to Security*, N.Y. TIMES, Mar. 13, 2012, at A16.

17. *Id.* The article also notes that a total of 10,000 attacks were reported the previous year. *Id.*

18. This Note will not discuss the important role that self-governance plays in Internet-based activities as it is focusing primarily on criminal activity intended to cause harm.

velopment of cybercrime and the current methods of combating it. Part I.C considers the historical use of universal jurisdiction and its applicability to cybercrime. Part I.D presents a brief survey of the strengths, weaknesses, and purposes of the International Criminal Court ("ICC"), which provides the most promising model for an international cybercrime court. Part II evaluates three proposals for tackling cybercrime at an international level: extending universal jurisdiction to encompass cyberspace, using traditional treaty law to bind states to domestic incorporation of international cybercrime codes, and finally, the preferred approach of adopting an international penal code under the jurisdiction of an international court or tribunal.

I: THE EVOLVING LANDSCAPE OF CYBERCRIME

Over the past fifty years, technological advancements have radically changed both personal and professional business activities.[19] Since its invention in the late 1940s, the computer has come to play such a dominant role in human culture that it may now be hard to imagine a world without its existence.[20] Springboarding off of the computer came the invention of the Internet and other networks that linked computers and computer systems together from around the globe.[21] Though capabilities to create worldwide computer networks like the Internet had been available since the 1960s, it was not until the end of the Cold War, when the United States government became less concerned about potential security vulnerabilities, that the Internet became widely available for public use.[22] Over the last fifteen to twenty years, the use and accessibility of the Internet have proliferated and web access has become a common feature of mainframe computers,[23] tablet computers, cell phones, and other portable

---

For a thorough discussion of property rights, self-regulation in cyberspace, and additional important issues relating to cyberlaw, see generally Nicolas Suzor, *The Role of the Rule of Law in Virtual Communities*, 25 BERKELEY TECH. L.J. 1817 (2010). *See also generally* Paul Schiff Berman, *Cyberspace and the State Action Debate: The Cultural Value of Applying Constitutional Norms to "Private" Regulation*, 71 U. COLO. L. REV. 1263 (2000); Henry H. Perritt, Jr., *Towards A Hybrid Regulatory Scheme for the Internet*, 2001 U. CHI. LEGAL F. 215.

19. *See, e.g.*, Decker, *supra* note 2, at 961.

20. Gable, *supra* note 1, at 67. Gable's article provides a helpful overview of the technological developments of both the computer and the Internet. *See generally id.*

21. *Id.* at 68.

22. *Id.* at 68–69.

23. One of the major factors in the proliferation of the Internet has been declining costs of both personal computers and connectivity. Decker, *supra* note 2, at 960. The increase in availability, coupled with the unparalleled rapidity of technological advance-

electronics like music players.[24] Today, mobile devices provide regular Internet access to as many users as stationary computers.[25]

Recently, a practice known as "cloud computing" has developed in which information is stored and accessed entirely through the Internet and other computer networks.[26] Businesses have shifted toward increasing reliance on cloud computing for the efficiency it can add in storing records, interfacing with customers, and cutting information technology infrastructure costs by eschewing the need to purchase and maintain requisite hardware.[27] Many individuals use cloud computing every day simply by accessing their e-mail or social networking websites; Google's popular e-mail system, "Gmail," and Facebook, the popular social networking site, are two primary examples of cloud computing products targeted toward the masses.[28] As with businesses, individuals often use cloud e-mail accounts because access is available on any computer and there is essentially no technological upkeep necessary—an individual does not have to download new software packages or upgrade computer hardware to keep e-mails up to date.[29] The allure of cloud computing has led to a rapidly expanding use of the practice across many sectors, including government.[30]

---

ment, has led to Internet access for an estimated seventy-five percent of Americans. *Id.* at 961.

24. Gable, *supra* note 1, at 68–69.

25. David J. Goldstone & Daniel B. Reagan, *Social Networking, Mobile Devices, and the Cloud: The Newest Frontiers of Privacy Law*, 55-SUM B. B.J. 17, 21 (2011).

26. *Id.* at 21. The exact definition of cloud computing is imprecise, though one clear component is that a user does not own any of the technology involved in operation. The National Institute of Standards & Technology defines it as a

> "model for enabling convenient, on-demand network access to a shared pool of configurable computing resources . . . that can be rapidly provisioned and released with minimal management effort or service provider interaction." Essentially, users store or share their information on the Internet and third-party providers maintain that information on remote servers owned or operated by the provider.

Ilana R. Kattan, Note, *Cloudy Privacy Protections: Why the Stored Communications Act Fails to Protect the Privacy of Communications Stored in the Cloud*, 13 VAND. J. ENT. & TECH. L. 617, 620–21 (2011) (internal citation omitted).

27. *Id.* at 622.

28. *Id.* at 618; *see also* Goldstone & Reagan, *supra* note 25, at 17.

29. Goldstone & Reagan, *supra* note 25, at 17.

30. *Id.* at 18. In a *New York Times* op-ed, Vivek Kundra, the Chief Information Officer for President Obama's administration from 2009–2011, promoted the administration's push into cloud technology. He writes that, "shortly after the Obama administration took office, we instituted a 'Cloud First' policy, which advocates the adoption of cloud serv-

These advancements have ushered in an era of unprecedented efficiency and speed in both personal and business-related Internet activity, but they have also created a user dependency on service providers to maintain and protect personal data.[31] As more personal information is conveyed over the Internet and stored in the cloud, everything from information on bank accounts to federal infrastructure, from personal e-mail to private photos, is increasingly vulnerable to cyberattack.[32] As a result, nearly every person could be victim to a cyberattack, whether they are individual Internet surfers, non-computer-using customers of Internet-using companies, or even citizens of cloud-embracing national governments.[33] Accordingly, governments strive to keep pace with technological advancements and to protect individuals, businesses, and themselves from cybercrime. However, these efforts have not always been sufficient to stem the tide of cybercrime proliferation.[34]

A. Definition of Cybercrime

One of the primary obstacles in combating cybercrime is defining it. No internationally recognized legal definition exists, though there are functional definitions that focus on general offense categories.[35] Cybercrime is, therefore, most accurately defined as crimes that are perpetrated over the Internet and that generally fall into two categories: first, those that target computers and information stored on computers, and second, those that use a computer to facilitate another crime.[36]

---

ices by government agencies and mandates the transition of at least three projects for every agency to the cloud by next summer [2012]." Kundra, *supra* note 12, at A27.

31. Kattan, *supra* note 26, at 623.

32. *See, e.g.*, Gable, *supra* note 1, at 68.

33. *Id.* at 59–63.

34. *See id.* at 74–77. *See generally* Haley Plourde-Cole, Note, *Back to* Katz*: Reasonable Expectations of Privacy in the Facebook Age*, 38 FORDHAM URB. L.J. 571 (2010); Miriam F. Miquelon-Weismann, *The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?*, 23 J. MARSHALL J. COMPUTER & INFO. L. 329 (2005).

35. Miquelon-Weismann, *supra* note 34, at 330–31 (drawing the functional defintions from a 1990 document produced by the UN Centre for International Crime Prevention, now integrated into the UN Office on Drugs and Crime); Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, Cuba, Aug. 27–Sept. 7, 1990, *International Review of Criminal Policy—United Nations Manual on the Prevention and Control of Computer Related Crime* ¶¶ 20–26, *available at* http://www.uncjin.org/8th.pdf.

36. Decker, *supra* note 2, at 964; Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1017 (2001).

When a cybercriminal targets a computer, (or, increasingly, someone's mobile device[37]) the computer may be victimized in ways analogous to many other traditional crimes,[38] not unlike a person who is assaulted while walking down a street or a house that is vandalized. Alternatively, the computer may be subjected to crimes that are unique to computers of the Internet era.[39] There are many crimes that fall into the latter category, though the average computer user may not be aware of the distinctions among all of them.

Most of these crimes utilize specific programs to damage software.[40] Viruses, perhaps the most well-known examples of malicious software (sometimes called "malware"[41]), are programs that modify other computer programs and can spread from one computer to another whenever a file is transmitted between them, be it via the Internet, traditional disk, or other means.[42] While viruses generally require human direction before travelling from one host computer to another, some can self-replicate and transfer themselves.[43] These self-replicating programs are called "worms."[44]

Today, viruses and worms often infect a computer through the user's e-mail. Unsolicited bulk e-mails from commercial parties, usually with no preexisting relationship to the recipient, are known as "spam" and are often the vehicle cybercriminals use to distribute their malicious soft-

---

37. See, for example, Nick Bilton, *Android Is No. 1 Target of Mobile Hackers*, N.Y.TIMES (Aug. 25, 2011, 9:39 AM), http://bits.blogs.nytimes.com/2011/08/25/android-number-one-target-by-mobile-hackers-report-says/?ref=anonymousinternetgroup, discussing hackers' preference for targeting phones that use Google's Android platform because of Google's lax screening procedures for new mobile applications.

38. Eric J. Sinrod & William P. Reilly, *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 177, 187–88 (2000).

39. Dominic Carucci, David Overhuls & Nicholas Soares, *Computer Crimes*, 48 AM. CRIM. L. REV. 375, 378 (2011). The article further differentiates between a computer being the object of a crime and the subject of a crime. Generally, a computer is an object of a crime when its hardware or its software is stolen. A computer is generally the subject of a crime in when it is targeted in other ways, including those listed above the line here. *Id.*

40. *See id.*

41. *Id.* at 379.

42. *Id.* Carucci, Overhuls, and Soares provide an extensive description of the varying kinds of malicious software that is highly informative and provides the foundation for much of the information located herein.

43. Sinrod & Reilly, *supra* note 38, at 221.

44. Carucci, Overhuls & Soares, *supra* note 39, at 379–80; Katyal, *supra* note 36, at 1024–25.

ware.[45] This can be similar to a "Trojan horse," a program that has a legitimate function but also contains hidden malicious coding.[46] Where spam is a specific e-mail crime, though, a Trojan horse can come from any type of file or program, such as word processors or music files.[47] Some malicious software programs, known as "logic bombs," may be designed to activate malicious programs upon the occurrence of a specific event or on a specific date, while remaining dormant in the meantime.[48]

Entire computer networks can be specifically targeted by additional kinds of malicious programs. "Sniffers" are programs that monitor and analyze network data and can be used to acquire confidential information including passwords, credit card numbers, and more.[49] "Web Bots" or "spiders" are similar, although they go the extra step of creating searchable indexes of the data passing through the network, often overwhelming that targeted network with requests for information.[50] Whether through the use of spiders or merely as a mischievous end in itself, many cybercriminals target websites or networks with "denial of service attacks," which debilitate sites by sending overwhelming numbers of simple requests for connectivity.[51]

It is important to note that each of the malicious software programs listed above has the potential to be used constructively.[52] For example, a virus could be designed to repair glitchy software while a sniffer could be used as a network security program.[53] However, cybercriminals are particularly adept at utilizing these programs to wreak havoc.[54] One important factor in the success of these cybercrimes is the cybercriminal's ability to use someone else's computer as an agent from which the cy-

45. Carucci, Overhuls & Soares, *supra* note 39, at 379.
46. Katyal, *supra* note 36, at 1026.
47. Carucci, Overhuls & Soares, *supra* note 39, at 380.
48. *Id.*
49. *Id.*
50. *Id.*
51. *Id.* at 380–81; Katyal, *supra* note 36, at 1026–27.
52. *See, e.g.*, Geoffrey A. North, *Carnivore in Cyberspace: Extending the Electronic Communications Privacy Act's Framework to Carnivore Surveillance*, 28 RUTGERS COMPUTER & TECH. L.J. 155, 162–63 (2002) (describing the FBI's use of a sniffer program called Carnivore to monitor a suspect's e-mail and Internet activity). Use of these devices by law enforcement has led to numerous debates regarding legal limits on Internet users' reasonable expectations of privacy, both in the U.S. and internationally. *See* Plourde-Cole, *supra* note 34; Kattan, *supra* note 26, *passim*.
53. *See, e.g.*, Carucci, Overhuls & Soares, *supra* note 39, at 380.
54. *See, e.g.*, Lentz, supra note 1, at 800.

bercriminal may then perpetrate more crimes with greater anonymity.[55] For example, one hacker could use a sniffer to track the e-mail addresses of thousands of employees in a particular company and then send each employee spam containing a self-replicating worm program designed to corrupt the user's computer in a number of different ways. Alternatively, a hacker could track each of the employees' e-mail account passwords, transcribing them into a spider-created database. Using these passwords, the hacker would then be able to deliver a denial of service attack to the company's network by overloading the system with requests to log into each e-mail account simultaneously. Such tactics can make policing the Internet and other networks exceptionally challenging.[56]

The second major category of cybercrime uses a computer to facilitate a separate, more traditional crime.[57] Cybercriminals often utilize one or more of the corrupting programs discussed above to glean information from potential victims or to disable security programs in furtherance of committing underlying, non-computer-related crimes.[58] Generally, there are four types of underlying crimes: identity theft or extortion, theft of intellectual property, fraud, and the possession or distribution of child pornography.[59] While these four crimes typically have straightforward statutory definitions, there are a number of areas, particularly those focusing on national security, where it remains unclear whether the use of a computer has led to, or alone constituted, a crime.[60] The confusion stems in equal part from the frequently evolving technological landscape and from the lack of uniformity in cybercrime statutes between international bodies.[61]

B. Legislation and Enforcement

Cybercrime poses unique challenges to law enforcement officials due to three major factors: first, the lack of territorial jurisdictional bounda-

---

55. Carucci, Overhuls & Soares, *supra* note 39, at 381.

56. *Id*. at 377. Katyal relates a specific denial of service attack, perpetrated by a fifteen-year-old Canadian citizen in 2000, which underscores the daunting and complex nature of these crimes. The hacker shut down some of the most popular websites, including Amazon.com, CNN.com, Yahoo!, and others, by utilizing remote computers to orchestrate the attack, as well as three "dummy" websites, making it very difficult for law enforcement to trace the attack. The FBI only learned of the hacker's identity after he began bragging about the success of his cybercrime in Internet chartrooms. Katyal, *supra* note 36, at 1027. For further discussion, see *infra* Part I.B of this Note.

57. Carucci, Overhuls & Soares, *supra* note 39, at 378.

58. *Id.*

59. *Id.* at 381; Decker, *supra* note 2, at 967–96.

60. *See, e.g.*, Decker, *supra* note 2, at 962.

61. *See, e.g.*, Gable, *supra* note 1, at 98, 100–04.

ries in cyberspace; second, the lack of uniform cybercrime statutes around the world; and third, the rapid and ongoing evolution of cybercrime.[62] Cybercriminals will continue to outpace law enforcement efforts if states do not tackle each of these interrelating factors.[63]

1. General Challenges

One of the most unique features about cybercrime is that it operates in a nonphysical realm that is free from territorial boundaries.[64] As mentioned in Part I.A, cybercriminals have the capability of targeting computers or networks anywhere in the world and may use third party computers or networks, located in wholly different locations from either themselves or their targets, as instruments.[65] Any country that is trying to prosecute a cybercriminal will find itself forced to contend with the fact that even a local hacker may have used, perhaps even inadvertently, Internet connections in other countries to perpetrate a local cybercrime. Additionally, the cybercriminal may reside in a country with conflicting, or nonexistent, cybercrime statutes.[66]

A notable example of this kind of enforcement challenge occurred in early 2000, when hackers used stolen credit card information to extort money from several American banks.[67] Upon investigation, the Federal Bureau of Investigation ("FBI") identified the suspected hackers as two Russian nationals living in Russia.[68] However, the United States did not have a mutual legal assistance treaty ("MLAT") with Russia that would have allowed for the countries to extradite the suspects to the United States.[69] The FBI eventually tricked the hackers into coming to the United States under false pretenses, monitored their computer activity during their time in America, and then used the information gleaned from

62. *See* Susan W. Brenner & Joseph J. Schwerha, IV, *Transnational Evidence Gathering and Local Prosecution of International Cybercrime*, 20 J. MARSHALL J. COMPUTER & INFO. L. 347, 369–75 (2002); Decker, *supra* note 2; Miquelon-Weismann, *supra* note 34; Amalie M. Weber, *The Council of Europe's Convention on Cybercrime*, 18 BERKELEY TECH. L.J. 425, 446 (2003).

63. Gable, *supra* note 1, at 98.

64. Miquelon-Weismann, *supra* note 34, at 334; Carucci, Overhuls & Soares, *supra* note 39, at 417.

65. Carucci, Overhuls & Soares, *supra* note 39, at 417.

66. Miquelon-Weismann, *supra* note 34, at 335; Carucci, Overhuls & Soares, *supra* note 39, at 417.

67. Weber, *supra* note 62, at 427–28.

68. *Id.*

69. *Id.*

watching the suspects' online movements to arrest them.[70] Any efforts to limit these kinds of transnational law enforcement obstacles will necessarily rely heavily on the existence of shared statutory definitions of cybercrime terminology and the existence of domestic laws in each participating country that will allow for international cooperation.[71]

Establishing such cooperative relationships can be a herculean task as the definitions for cybercriminal statutes vary from state to state in both substance and semantics.[72] This challenge has two components. First, translators struggle to accurately maintain the same meaning of a statutory definition or phrase in each state's official language.[73] Second, the connotative definition of a crime may vary significantly from one culture to the next.[74]

A recent event in Iran provided an illuminating example of the ever-present variances in legal doctrine. Iranian security forces arrested, and in some instances physically beat up, seventeen young men and women who participated in a squirt-gun fight that had been organized on Facebook.[75] In a statement that might seem absurd to Western sensibilities, one of Iran's lawmakers stated that Iranian security forces had to "stop the spreading of these morally corrupt actions," referring to simple squirt-gun fights.[76] Though Internet-based activities played a secondary role to the "criminal" acts of these Facebook users, this episode reveals the challenges in identifying uniform definitions for cybercrimes. A government that is deeply conservative, ideologically extreme, or facing popular unrest may be more likely to consider a cybercrime that which is

---

70. *Id.* Weber explains that the two cybercriminals attacked American banks and credit card businesses repeatedly, broke into secured files, and extracted credit card and merchant identification numbers. They used this information to demand that their victims pay for "security 'consulting services,'" which resulted in large damages for the victims. The FBI, after having its request for assistance snubbed by Russian authorities, used a ruse in which it made the Russian hackers false job offers. While the hackers were in the United States for their "interviews," the FBI used its own software to monitor the hackers' communications with their computer servers in Russia to learn their passwords and online identification information, and then accessed the hackers' own files to acquire sufficient proof to make an arrest. *Id.*

71. *See, e.g.*, Jennifer J. Rho, Comment, *Blackbeards of the Twenty-First Century: Holding Cybercriminals Liable under the Alien Tort Statute*, 7 CHI. J. INT'L L. 695, 710 (2007).

72. Miquelon-Weismann, *supra* note 34, at 353.

73. *Id.*

74. Lama Abu-Odeh, *A Radical Rejection of Universal Jurisdiction*, 116 YALE L.J. (Pocket Part) 393, 394 (2007).

75. Farnaz Fassihi, *Iran's Wet Blankets Put a Damper on Water-Park Fun*, WALL ST. J., Aug. 31, 2011, at A1.

76. *Id.*

innocuous in many other countries, such as using social media to organize rallies or protests.[77] Such a discrepancy can, in turn, affect international cooperation. A state may refuse to extradite, investigate, or provide any other kind of assistance to another nation if the two disagree over what modes of online conduct are criminal.[78]

In some instances, states will be incapable of effective international cooperation because statutory and treaty law often lags far behind what is needed to effectively combat cybercrime.[79] States may lack the resources, technology, or procedures to effectively regulate cyberspace.[80] Even in technologically advanced countries like the United States, which have taken a more active stance on legislating against cybercrime, differences of opinion about how best to legislate are abundant.[81] For example, juveniles or first time cybercriminals—committing only minor acts of mischief—may find themselves prosecuted under highly punitive statutes that were intended to deter large scale cybercrimes.[82] A more ubiquitous challenge lies in the time-consuming nature of legislative processes, which hamstring states' ability to prosecute cybercrime whenever a new technology spawns a new form of crime.[83] Treaties and MLATs are subject to similar obstructions, perhaps to an even greater degree.[84]

These three major impediments—jurisdictional disputes, lack of uniform definitions, and the gradual pace of legislation and treaty forma-

---

77. *See* Abu-Odeh, *supra* note 74, at 394; *see also* H. Brian Holland, *The Failure of the Rule of Law in Cyberspace?: Reorienting the Normative Debates on Borders and Territorial Sovereignty*, 24 J. MARSHALL J. COMPUTER & INFO. L. 1, 32 (2005). Indeed, several countries have issued bans on social media and specific technologies, particularly in times of political turmoil. Syria, for example, banned certain Facebook features following the Tunisian revolution that launched the "Arab Spring" in 2011. Khaled Yacoub Oweis, *Syria tightens Internet ban after Tunis unrest—users*, REUTERS (Jan. 26, 2011, 11:40 PM), http://in.reuters.com/article/2011/01/26/idINIndia-54427520110126. Similarly, the Democratic Republic of the Congo banned text-messaging after a disputed election led to voter outrage and calls for organized protest. Thomas Hubert, *DR Congo election: Deaf anger at ban on texting*, BBC NEWS (Dec. 14, 2011, 2:14 PM), http://www.bbc.co.uk/news/world-africa-16187051. Even more recently, an Egyptian court made it a crime for Egyptians to view Internet pornography. Amro Hassan, *Court bans Internet pornography in Egypt*, L.A. TIMES: WORLD NOW BLOG (Mar. 29, 2012, 7:09 AM), http://latimesblogs.latimes.com/world_now/2012/03/court-bans-internet-porn-in-egypt.html.

78. Brenner & Schwerha, *supra* note 62, at 357–58.

79. Miquelon-Weismann, *supra* note 34, at 335.

80. Weber, *supra* note 62, at 427–28.

81. Decker, *supra* note 2, at 976–77.

82. Carucci, Overhuls & Soares, *supra* note 39, at 378–79.

83. *See* Miquelon-Weismann, *supra* note 34, at 335.

84. Weber, *supra* note 62, at 443.

tion—can stymie states' effective cybercrime prevention either individually or in conjunction with each other. To date, cybercrime prevention efforts have failed to sufficiently tackle all three factors simultaneously, resulting in a patchwork of cybercrime statutes that leaves gaps for cybercriminals to utilize as "safe data havens."[85] Nevertheless, states have made significant efforts to create anti-cybercrime laws.

2. Preventative Efforts in the United States

In the United States, the first federal laws criminalizing unauthorized access to computers were passed in 1984.[86] The original set of laws comprised several provisions within the Comprehensive Crime Control Act, a general crime statute.[87] Over the next two and a half decades, the computer crime provisions were expanded and recodified five times, most recently in 2008, resulting in what is now known as the Computer Fraud and Abuse Act ("CFAA").[88] The CFAA protects computers used in interstate or foreign commerce or communications by prohibiting seven acts of computer-related crime.[89] Because the law has sought to keep up with the quick clip of cybercrime's development, each of the five major expansions of the CFAA has significantly broadened the scope and jurisdiction of the statute.[90] Though several Circuit Courts have narrowed the application of the law, and despite a required threshold of $5,000 in damage,[91] some legal scholars argue that the CFAA has become dangerously broad in that it potentially grants the United States government jurisdiction over every Internet-connected computer in the world.[92] Oth-

85. Miquelon-Weismann, *supra* note 34, at 336.

86. Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1561 (2010). Kerr's article provides a detailed and comprehensive legislative history of the Computer Fraud and Abuse Act, carefully examining each of the major amendments to the bill over the last quarter century. *Id.*

87. *Id.*

88. Fraud and Related Activity in Connection with Computers, 18 U.S.C. § 1030 (2006) (effective Sept. 26, 2008); *see* Kerr, *supra* note 86, at 1561–71; *see also* Carucci, Overhuls & Soares, *supra* note 39, at 392–96.

89. Carucci, Overhuls & Soares, *supra* note 39, at 392–94. The seven specific acts that CFAA prohibits, which are discussed in more detail in Carucci, Overhuls, and Soares's articles are generally 1) accessing and/or transmitting computer files without authorization; 2) obtaining private information without authorization; 3) intentionally accessing a government computer without authorization; 4) accessing a protected computer with intent to defraud; 5) knowingly, recklessly or negligently damaging a protected computer through hacking; 6) knowingly trafficking in passwords with intent to defraud; and 7) transmitting a threat to cause damage or to extort something of value. *Id.*

90. Kerr, *supra* note 86, at 1561.

91. Carucci, Overhuls & Soares, *supra* note 39, at 395.

92. *See generally* Kerr, *supra* note 86, at 1561.

ers, however, warn that CFAA is still not broad enough to sufficiently combat cybercrime because of its inapplicability to as-yet-undeveloped forms of cybercrime and because of its minimum monetary requirement.[93] These contrasting views reveal one of the major tensions in legislating against cybercrime, namely the balancing of individual users' privacy rights with the public's interest in maintaining cybersecurity.[94]

The United States has complemented the CFAA with a slate of additional statutes designed to target more specific cybercrimes.[95] Among these are the Control the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM"), which focuses primarily on curtailing spam; the Electronic Communications Privacy Act ("ECPA") and Stored Communications Act ("SCA"), which protect, among other private data, e-mail accounts, voicemail accounts, and television signals; and various copyright, fraud, child pornography, identity theft, and even cyber-bullying statutes.[96] This body of law, taken together, seeks to address four basic needs created by cybercrime: "protection of privacy, prosecution of economic crimes, protection of intellectual property and procedural provisions to aid in the prosecution of computer crimes."[97]

Other countries have tried to employ differing approaches to combating cybercrime, but with little success.[98] Germany and France initially tried to hold Internet Service Providers ("ISPs") liable for the content they were transmitting, while Cuba has simply limited Internet access to 200,000 citizens.[99] Yet most industrialized countries are now adopting statutes, similar to the CFAA, that target unauthorized access to computers and private information by focusing on the four needs identified in

---

93. *See, e.g.*, Decker, *supra* note 2, at 1010.

94. *See generally* Kattan, *supra* note 26, *passim*; Goldstone & Reagan, *supra* note 25, *passim*; Plourde-Cole, *supra* note 34, *passim*.

95. Carucci, Overhuls & Soares, *supra* note 39, at 396–410.

96. *Id.*; *see also* Control the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat 2699 (2003) (codified at 15 U.S.C. §§ 7701–7713 and 18 U.S.C. § 1937 (2006)); Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2510–2521, 2701–2710, 3121–3126 (2006)).

97. Carucci, Overhuls & Soares, *supra* note 39, at 418.

98. *Id.* at 417–18.

99. *Id.* However, Cuba has been unsuccessful in completely restricting Internet access. This is primarily because those who have been permitted access, typically doctors or academics, often sell their access information on the black market. *Cuba and the internet: Wired, at last*, ECON. (Mar. 3, 2011), http://www.economist.com/node/18285798. However, the Cuban government may be embracing a different approach to limiting Internet access, given that Venezuela recently spent seventy million dollars to connect a 1,000-mile fiber-optic cable between itself and the island in March 2011. *Id.*

the U.S. statutes listed above.[100] One of the ongoing challenges facing all countries, though, is the procedural and logistical challenges that stem from pursuing cybercriminals who operate in a world free from jurisdictional boundaries.[101]

3. Europe's Convention on Cybercrime

The Council of Europe's Convention on Cybercrime ("the Convention") marks the most ambitious international effort to combat cybercrime to date.[102] The Convention was drafted in 2001 in an effort to address those specific jurisdictional challenges that came about with the evolution of the Internet and to facilitate greater cooperation between nations fighting cybercrime.[103] It entered into force in January 2004 and, as of April 2012, the Convention had been ratified by thirty-three countries, including the United States.[104]

Each signatory to the Convention agrees to three obligations: first, to criminalize certain computer-related conduct by statute; second, to establish investigative and electronic-evidence gathering procedures; and third, to assist in broad, international efforts to prosecute cybercriminals, including cooperation with fugitive extradition efforts.[105] In addition to laying out suggested norms and standards for domestic cybercrime laws and MLATs between party states, the Convention provides uniform definitions of at least four terms indelibly linked to cybercrime: "computer system," "computer data," "service provider," and "traffic data."[106]

In this way, the Convention has made important progress in addressing many of the challenges that plague cybercrime prevention.[107] The four definitions listed at the outset of the Convention mark some progress in

---

100. *Id.* at 418.

101. Miquelon-Weismann, *supra* note 34, at 335; Weber, *supra* note 62, at 425.

102. *See, e.g.*, Gable, *supra* note 1, at 93.

103. Weber, *supra* note 62, at 425–26.

104. *Convention on Cybercrime*, COUNCIL OF EUROPE, http://www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=01/11/2011&CL=ENG (last updated Jan. 1, 2011) [hereinafter *Cybercrime*, COUNCIL OF EUROPE].

105. Miquelon-Weismann, *supra* note 34, at 329–30.

106. Council of Europe, Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185 [hereinafter Convention on Cybercrime]. These definitions, listed at the beginning of the convention, were drafted as a direct result of the United Nation's identification of "uniformity in law and consensus over definitional terms as two of the impediments that had to be overcome in order to achieve meaningful cooperation and successful enforcement." Miquelon-Weismann, *supra* note 34, at 338.

107. *See generally* Miquelon-Weismann, *supra* note 34; Weber, *supra* note 62, at 445–46.

unifying terms across languages.[108] Similarly, the document calls for parties to the Convention to criminalize four categories of crime and lists nine specific actions that should be criminalized.[109] Both of these provisions streamline cooperation and enforcement processes, as do the additional provisions that call for signatories to establish a minimum set of standardized legal procedures and to coordinate with each other by means of MLATs and other agreements.[110]

Perhaps the most important feature of the Convention, and the reason for its growing list of participants,[111] is that it allows participating states to retain a sense of total sovereignty.[112] All of the obligations placed on signatories require only the creation of domestic law, not subjugation to extraterritorial legislation,[113] and while MLATs come with ratification of the Convention, they do not supersede preexisting treaties.[114] Furthermore, parties to the convention have the right to make reservations that limit their adherence to certain provisions or MLATs.[115] National governments find the Convention's deference to their own sovereignty reassuring and may be drawn toward it, and future treaties on cybercrime, because of this.[116]

However, the Convention still falls far short of addressing all of the challenges of fighting international cybercrime. At a fundamental level,

---

108. Miquelon-Weismann, *supra* note 34, at 338.

109. Weber, *supra* note 62, at 431. The first category of crimes focuses on protecting privacy rights and specifically proscribes illegal access, illegal interception, data interference, system interference, and misuse of devices. The second category outlaws fraud and forgery. The third category centers on content-related crimes, namely child pornography-related offenses. The fourth category deals with copyright protections, as well as supplemental provisions relating to all of the aforementioned activities, such as corporate liability standards and laws that forbid the aiding and abetting of cybercrime. *Id.*

110. Weber, *supra* note 62, at 433–34.

111. As of December 1, 2011, the following countries had ratified the Convention: Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Italy, Latvia, Lithuania, Moldova, Montenegro, the Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Switzerland, the former Yugoslav Republic of Macedonia, Ukraine, United Kingdom, and the United States. *Cybercrime*, COUNCIL OF EUROPE, *supra* note 104.

112. Weber, *supra* note 62, at 442.

113. Convention on Cybercrime, *supra* note 106.

114. Weber, *supra* note 62, at 441–42.

115. *Id.* at 443.

116. Miquelon-Weismann, *supra* note 34, at 354; *see also* David J. Scheffer, *Staying the Course with the International Criminal Court*, 35 CORNELL INT'L L.J. 47, 59–60 (2002) (describing how the incorporation of the complementarity principle played a major role in convincing the Clinton administration to sign the Rome Statute by addressing fears of forfeited sovereignty).

the Convention's deference to national sovereignty prevents the treaty from adequately addressing one of the three major challenges of fighting cybercrime listed earlier: obstructive jurisdictional boundaries.[117] Because not every state in the world is a party to the Convention, and because signatories can water down their own commitment through the use of reservations, safe data havens for cybercriminals will continue to exist throughout the world.[118] Furthermore, the treaty's reliance on local legislation undermines the Convention's progress in harmonizing terminology and criminal statutes—a party to the Convention may simply not meet its obligation to criminalize each of the listed actions, thereby reducing the efficacy of the treaty.[119] The reasons for not enacting a particular law may vary, but the fact remains that the Convention offers no enforceable standards to which participating parties must conform.[120]

The Convention has two other significant weaknesses. First, it fails to provide uniform procedural rules regarding privacy and other due process rights for cybercrime suspects.[121] Even with mutual assistance between two Convention signatories, where both have met all of the obligations laid out by the treaty, there may still be a conflict when one of those two states has more invasive cyber search and seizure statutes than the other.[122] The potential—indeed likelihood—of such discrepancies does much to subvert the sense of cooperation the Convention is designed to foster, as participating countries will balk at full participation in the treaty if they are not guaranteed what they consider fair treatment for their citizens by other states.[123] Second, the Convention, like all treaties, is more difficult to amend than domestic legislation and therefore is still subject to another one of the major obstacles of cybercrime prevention—obsolescence in the face of a rapidly changing environment.[124]

For these reasons, the Convention marks the best effort to date to combat cybercrime yet still falls short of establishing the necessary legal tools and authority to overcome the three major obstacles of traditional territorial jurisdiction, disharmonious definitions of cybercrime terms, and rapid technological advancement.[125] Due to the ever-growing threat

117. Miquelon-Weismann, *supra* note 34, at 359; Weber, *supra* note 62, at 443.
118. Weber, *supra* note 62, at 443–44.
119. *Id.* at 442–43.
120. Miquelon-Weismann, *supra* note 34, at 353–54.
121. *Id.* at 340–41.
122. *Id.*; *see also* Brenner & Schwerha, *supra* note 62, at 350.
123. Miquelon-Weismann, *supra* note 34, at 360.
124. Weber, *supra* note 62, at 443.
125. *Id.* at 445–46. *See generally* Miquelon-Weismann, *supra* note 34.

that cybercrime poses to international security, though, law enforcement agencies are bridging many of the legal gaps at an operational level.[126]

4. The Growing Role of Multinational Task Forces

Whether working through informal, mutually beneficial relationships or through formal mechanisms like Interpol and MLATs, law enforcement agencies are finding methods to work together in order to prosecute cybercriminals to a greater, though still limited, extent than the Convention allows.[127] At a hearing before the United States House Financial Services Committee's Subcommittee on Financial Institutions and Consumer Credit in September 2011, an assistant director of the FBI's Cyber Division testified that strategic discussions between the United States and major allies have "resulted in increased operational coordination on intrusion activity and cyber threat investigations."[128] He added that the United States "currently [has] FBI agents embedded full-time in five foreign police agencies to assist with cyber investigations," and that the FBI has "trained foreign enforcement officers from more than [forty] nations in cyber investigative techniques over the past two years."[129] Similarly, the U.S. Secret Service operates twenty-three offices abroad[130] and deploys 1,400 agents trained in its Electronic Crimes Special Agent Program throughout the world.[131] When testifying to the United States Senate Committee on the Judiciary, a Deputy Special Agent in Charge of the Secret Service's Criminal Investigative Division endorsed such multinational field work and said that "the personal relationships that have been established in those countries [where the Secret Service operates offices] are often the crucial element to the successful investigation and prosecution of suspects abroad."[132] In addition to multinational task forces, law

126. Decker, *supra* note 2, at 1005. See also Brenner & Schwerha, *supra* note 62, at 394, which, written just before the initial development of multinational task forces, calls for just such an integration of law enforcement efforts as an important tool in fighting cybercrime.

127. *See generally* Brenner & Schwerha, *supra* note 62; Carucci, Overhuls & Soares, *supra* note 39, at 419.

128. *Cyber Security: Threats to the Financial Sector: Hearing Before H. Fin. Serv. Comm. Subcomm. on Fin. Insts. & Consumer Credit*, 112th Cong. 8 (2011) (statement of Gordon M. Snow, Assistant Director, Cyber Division, Federal Bureau of Investigation).

129. *Id.*

130. *Cybercrime: Updating the Computer Fraud and Abuse Act to Protect Cyberspace and Combat Emerging Threats: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. 4 (2011) (statement of Pablo A. Martinez, Deputy Special Agent in Charge, Criminal Division, U.S. Secret Service).

131. *Id.*

132. *Id.*

enforcement agencies are increasingly turning to private and nonprofit corporations, particularly those that have international copyright enforcement programs, for assistance in combating cybercrime.[133]

These collaborative efforts exemplify the most promising methods to prevent and prosecute cybercrime. The increased flexibility, rapid response capabilities, and diverse populations within multinational task forces make them better equipped to overcome the three major obstacles of international cybercrime than treaties or any other regulatory mechanism. Yet their efforts are still restricted by the red tape of jurisdictional limits and mercurial relations between states.

C. Universal Jurisdiction

One innovative approach toward combating cybercrime calls for granting every nation the right to prosecute cybercriminals under a universal jurisdiction theory.[134] Such an approach offers immediate benefits as a powerful deterrent and as a means to reduce many of the restrictions that stem from traditional territorial jurisdiction.[135] It is helpful, then, to briefly explore the historical usage of this rare legal principle.

Universal jurisdiction grants any state the right to prescribe, adjudicate, and enforce a law against a person regardless of that person's nationality, the nationality of any victim, or the location at which the crime was committed.[136] Incumbent upon extending jurisdiction to such an expan-

---

133. *Id.* Carucci, Overhuls, and Soares provide only one example of a private organization working with law enforcement agencies, a software industry trade group called the Business Software Alliance, but they refer to multiple unnamed groups, as well. Carucci, Overhuls & Soares, *supra* note 39, at 419.

134. *See, e.g.*, Gable, *supra* note 1, at 104–17.

135. *See generally id.*; Rho, *supra* note 71, at 709–10.

136. M. Cherif Bassiouni, *Universal Jurisdiction for International Crimes: Historical Perspectives and Contemporary Practice*, 42 VA. J. INT'L L. 81, 89 (2001). Kenneth C. Randall offers a more detailed definition of universal jurisdiction by describing jurisdiction in this way:

> [it] refers to a state's legitimate assertion of authority to affect legal interests. Jurisdiction may describe a state's authority to make its law applicable to certain actors, events, or things (legislative jurisdiction [sometimes called "prescriptive jurisdiction"]); a state's authority to subject certain actors or things to the processes of its judicial or administrative tribunals (adjudicatory jurisdiction); or a state's authority to compel certain actors to comply with its laws and to redress noncompliance (enforcement jurisdiction). A state may not legally assert legislative, adjudicatory, or enforcement jurisdiction over all persons and things within the state's power and control.

Kenneth C. Randall, *Universal Jurisdiction under International Law*, 66 TEX. L. REV. 785, 786 (1988).

sive degree is the belief that allowing a state the authority to prescribe and adjudicate a certain crime, or set of crimes, on behalf of the international community is instrumental in preserving world order.[137]

For the most part, universal jurisdiction stems from customary law and not from treaties between nations.[138] Because customary law is, generally, a set of rules and norms that affects every state—and creates a sense of legal obligation on all states to conform to that set of rules—universal jurisdiction, when applied to a specific crime, governs the entire community of nations regardless of any country's express willingness to be bound by it.[139]

One of the major obstructions to the expansive use of this legal tool is that states must voluntarily relinquish some sovereign power.[140] Because states are hesitant to give up any jurisdictional power, the global community must unquestionably consider a crime worthy of universal jurisdiction before such broad prosecutorial authority will be enforced. Since the middle of the twentieth century, the "heinousness principle" has been the standard used to justify universal jurisdiction over crimes that are "profoundly despised throughout the world."[141]

Unsurprisingly, universal jurisdiction is rarely applied.[142] The first, and to date most prominent example of universal jurisdiction was the global

---

137. Bassiouni, *supra* note 136, at 88.

138. Anthony J. Colangelo, *Constitutional Limits on Extraterritorial Jurisdiction: Terrorism and the Intersection of National and International Law*, 48 HARV. INT'L L.J. 121, 132 (2007).

139. *Id.* at 130–32. Colangelo provides a more detailed definition of customary international law and describes it as being made up of

> two components: (i) a general state practice, and (ii) a belief or intent to act with legal purpose, or what is often called opinio juris. Customary law is universal in its application and is therefore theoretically binding on all states . . . . By contrast, [treaty law] results from formal agreements among states and binds only those states parties to the treaty.

Id. at 131.

140. Eugene Kontorovich, *The Piracy Analogy: Modern Universal Jurisdiction's Hollow Foundation*, 45 HARV. INT'L L.J. 183, 184–85 (2004); *see also* Christopher Harding, *The International and European Control of Crime*, *in* RENEGOTIATING WESTPHALIA 183, 190 (Christopher Harding & C.L. Lim eds., 1999) (noting that the rise in international criminal prevention efforts in Europe toward the end of the twentieth century is "to some extent associated with the weakening of the state structure"); *see also* Christopher Harding & C.L. Lim, *The Significance of Westphalia: An Archaeology of the International Legal Order*, *in* RENEGOTIATING WESTPHALIA, *supra*, at 1, 8 (questioning why states would "contrary to their own immediate self-interest, [accept] a limitation of their own sovereignty" by recognizing international human rights).

141. Kontorovich, *supra* note 140, at 205; *see also* Gable, *supra* note 1, at 108.

142. *See, e.g.*, Bassiouni, *supra* note 136, at 82.

prosecution of piracy[143] that began in earnest in the seventeenth century.[144] Any nation was allowed to try and execute pirates caught on the high seas regardless of the nationality of the vessel the pirates chose to attack or the original nationality of the pirates.[145] Though piracy was governed by universal jurisdiction before the advent of the heinousness principle, any state that prosecuted pirates was nevertheless considered to be preserving world order on behalf of the international community.[146]

The crime of piracy easily lent itself to universal jurisdiction for two interrelated reasons. First, the high seas were extraterritorial spaces that most nations valued as a "global commons" essential for commerce.[147] As a general rule, each state's jurisdiction on the high seas was limited to its own citizens and its own vessels.[148] Thus, in order to adequately protect the communal safety of the high seas, an exception was made to the usual jurisdictional rules and states were allowed uniquely broad authority when prosecuting pirates.[149] Second, pirates voluntarily eschewed their own nationalities and disregarded the laws of all nations, thus making pirates, in the truest sense, outlaws.[150] As the influential, eighteenth century British jurist William Blackstone wrote, a pirate "'declare[ed] war against all mankind' and thus 'all mankind must declare war against him.'"[151]

For centuries, piracy stood alone as the only crime that was governed by universal jurisdiction. Slowly, slave trading became the second.[152] It

---

143. Gable notes, "although there does not seem to be a definitive definition of piracy, it [is generally] defined as an act committed by non-state actors aboard a vessel on the high seas or outside of any state's jurisdiction." Gable, *supra* note 1, at 108. Kontorvich offers a more specific definition, stating that while each nation has different statutory descriptions, "the crime of piracy consists of nothing more than robbery at sea." Kontorovich, *supra* note 140, at 191.

144. Kontorovich, *supra* note 140, at 190.

145. *Id.*; Colangelo, *supra* note 138, at 144–45; Randall, *supra* note 136, at 791–98.

146. James D. Fry, Comment, *Terrorism as a Crime against Humanity and Genocide: The Backdoor to Universal Jurisdiction*, 7 UCLA J. INT'L L. & FOREIGN AFF. 169, 175 (2002).

147. Kontorovich, *supra* note 140, at 190.

148. Randall, *supra* note 136, at 793.

149. *Id.*

150. Colangelo, *supra* note 138, at 144–45; Randall, *supra* note 136, at 791.

151. Colangelo, *supra* note 138, at 144. In the famous U.S. Court of Appeals for the Second Circuit case *Filartiga v. Peña-Irala*, the court adopted similar language to Blackstone when discussing the act of torture, conforming to the practice of linking crimes newly held to be under universal jurisdiction to piracy. 630 F.2d 876, 890 (2d Cir. 1980). The court held that "the torturer has become like the pirate and slave trader before him *hostis humani generis*, an enemy of all mankind." *Id.*

152. Bassiouni, *supra* note 136, at 112.

was during the aftermath of World War II, though, that the heinousness principle came into effect and that universal jurisdiction was extended over a slate of new crimes, including genocide, war crimes, and crimes against humanity.[153] There exist additional crimes, like the hijacking of planes, which have been universally condemned but have not yet reached an accepted status under customary law to be governed by universal jurisdiction.[154]

Proponents of expanding the usage of universal jurisdiction emphasize its power to prevent crimes through its immense scope and applicability to potential criminals all over the world.[155] In almost every instance where a theorist seeks to justify extending universal jurisdiction over a new crime, the basis for the extension is the crime's similarity to piracy.[156] Currently, the crime (or class of crimes) that appears to enjoy the most popular justification for universal jurisdiction, and which is most successfully analogized to piracy, is terrorism,[157] though even it stands a slim chance of facing true universal prosecution.

Any expansion of universal jurisdiction is met with persuasive opponents. Critics rightly challenge a number of factors, aside from the sacrifice of state sovereignty,[158] which will be discussed in some detail in Part II.A of this Note. However, one standout criticism regarding universal

---

153. Kontorovich, *supra* note 140, at 194, 204–05; *see also* Randall, *supra* note 136, at 800.

154. Bassiouni, *supra* note 136, at 115–34.

155. Gable, *supra* note 1, at 108.

156. Kontorovich, *supra* note 140, at 204–06.

157. Colengelo writes,

> Like pirates, terrorists, and in particular al Qaeda and those like al Qaeda, also have opted out of the "law of society": they "acknowledge obedience to no government whatever and act in defiance of all law," such as the law distinguishing between military and civilian targets . . . and their acts potentially target all states . . . . [B]y "throwing off his national character" in committing his illegal acts of war, the terrorist has, like the pirate, exposed himself to the enforcement jurisdiction of all states. He too wages a lawless war under the color of no state's authority.

Colangelo, *supra* note 138, at 145 (internal citations and punctuation omitted). Many theorists suggest that universal jurisdiction should be applied to a wider array of legal fields, such as drug-related crimes. *See, e.g.*, Anne H. Geraghty, *Universal Jurisdiction and Drug Trafficking: A Tool for Fighting One of the World's Most Pervasive Problems*, 16 FLA. J. INT'L L. 371 (2004). Other scholars have pushed for universal regulation to cover specific, more controversial issues like in vitro fertilization and embryonic regulation. *See, e.g.*, Sherylynn Fiandaca, Comment, *In Vitro Fertilizations and Embryos: The Need for International Guidelines*, 8 ALB. L.J. SCI. & TECH. 337, 395 (1998).

158. *See, e.g.*, Kontorovich, *supra* note 140; Abu-Odeh, *supra* note 74.

jurisdiction over cybercrime, discussed above, is the unresolved set of limitations that stem from a lack of a unified set of cybercrime definitions.[159] Universal jurisdiction proponents point out that even piracy lacks specific international definitions.[160] Theorists on both side of the debate of universal jurisdiction note, under different lines of argument, the troubling fact that if the same acts that generally satisfy the elements of piracy are committed under the auspices of a sovereign state, they are considered acts of privateering, an act neither subject to universal jurisdiction nor universally condemned.[161]

Still, because cybercrime is a uniquely global problem, the debate over whether it should be globally prosecuted via universal jurisdiction becomes a fundamentally important question. As this Note will explore more fully in Part II.A, expanding universal jurisdiction to some degree over cybercrime will be an important element of any effective preventative legislation.

D. The ICC

One relatively recent development in international criminal law has been the establishment of the ICC.[162] Though this institution is still in its infancy, its creation has been a landmark development in international criminal law.[163] Given the global nature of cybercrime, there can be little doubt that international judicial bodies of some form will play at least a limited role in the prevention and prosecution of cybercrime.[164] Any practical solution to the growing threat of cybercrime should therefore include a role for a judicial body similar in design to the ICC.

Representatives from a majority of the world's countries, gathered at the United Nations Diplomatic Conference of Plenipotentiaries in 1998, outlined the structure and powers of the ICC in what is now known as the

---

159. *See, e.g.*, Abu-Odeh, *supra* note 74, at 394.

160. *See* Gable, *supra* note 1, at 108; *see also* Kontorovich, *supra* note 140, at 191.

161. Kontorovich, *supra* note 140, at 218–22; Colangelo, *supra* note 138, at 145.

162. *See generally* Remigius Oraeki Chibueze, *The International Criminal Court: Bottlenecks to Individual Criminal Liability in the Rome Statute*, 12 ANN. SURV. INT'L & COMP. L. 185 (2006); James F. Alexander, *The International Criminal Court and the Prevention of Atrocities: Predicting the Court's Impact*, 54 VILL. L. REV. 1 (2009).

163. See, for example, Chibueze, *supra* note 162, at 187, stating that the creation of the ICC "was one of the remarkable achievements of the twentieth century."

164. *See, e.g.*, Miquelon-Weismann, *supra* note 34, at 360–61 (advocating for the passage of a proposed "Treaty to Establish a Constitution for Europe," which would improve upon the Convention on Cybercrime by providing "for the right to an effective remedy and to a fair trial, presumption of innocence and right of defense, principles of legality and proportionality of criminal offenses and penalties, and the prohibition against double jeopardy").

Rome Statute.[165] The Rome Statute calls for a court that would have jurisdiction over "the most serious crimes of concern to the international community"[166]—including genocide, war crimes, and crimes against humanity—and that would be situated in The Hague, the Netherlands.[167] The treaty entered into force and established the ICC in 2002, with 121 countries participating as of July 1, 2012.[168]

The idea of an international criminal court was not entirely a novel one when the Rome Statute was drafted.[169] Beginning with the Nuremburg Trials after World War II, which criminally prosecuted high-ranking Nazi officials for atrocities, the international community has moved steadily in the direction of holding individuals liable for violations of international laws (where before only state-actors might have been held liable for acts of genocide or war crimes).[170] The trend continued throughout the twentieth century, resulting in the creation of specific international criminal tribunals, modeled to an extent on the Nuremburg Trials, for atrocities committed in association with the conflicts in Yugoslavia and Rwanda.[171] These tribunals were generally ad hoc, rendering jurisdiction over only a specific country or over a specific series of events.[172] Establishing a permanent court with potential jurisdiction over all countries was, in many ways, a natural next step.[173]

Because the potentially universal reach of the ICC was a concern for many of the parties involved in drafting the Rome Statute, they reached a series of compromises that limited the ICC's jurisdiction in at least three significant ways.[174] First, the ICC may only exercise its jurisdiction in a particular matter if one or more of the parties has consented, either through ratification of the Rome Statute or by being a citizen (over the

165. Chibueze, *supra* note 162, at 185; Alexander, *supra* note 162, at 2–3.

166. Statute of the International Criminal Court, July 17, 1998, 2187 U.N.T.S. 90 [hereinafter Rome Statute].

167. Alexander, *supra* note 162, at 2.

168. *ICC at a Glance*, INT'L CRIMINAL COURT, http://www.icc-cpi.int/Menus/ICC/About+the+Court/ICC+at+a+glance/ (last visited Apr. 24, 2012).

169. *See* Johan D. ven der Vyver, *Personal and Territorial Jurisdiction of the International Criminal Court*, 14 EMORY INT'L L. REV. 1, 4–9 (2000).

170. *Id.* at 4–9.

171. These tribunals were officially titled the International Criminal Tribunal for the Former Yugoslavia ("ICTY") and the International Criminal Tribunal for Rwanda ("ICTR"). IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 569–71 (6th ed. 2003). As of late 2008, the ICTY had rendered judgments in sixty-seven cases and was proceeding on forty-five more; the ICTR had judged thirty-seven with thirty-seven additional cases in progress. Alexander, *supra* note 162, at 12–13.

172. Alexander, *supra* note 162, at 12.

173. *See id.* at 2–3.

174. ven der Vyver, *supra* note 169, at 2, 60–65.

age of eighteen) of a state over which the ICC held previously-vested authority by treaty.[175] Second, and perhaps most importantly, the ICC must adhere to a policy of complementarity, meaning that it must remain a court of last resort that only reviews an issue if no preexisting domestic legal organism can, or will, hear it.[176] Last, the United Nations Security Council retains the power to request that the ICC defer any investigation or prosecution for one year, a request that may be renewed for additional year-long intervals.[177]

The ICC has the potential to be an extremely effective criminal deterrent and prosecutorial mechanism.[178] However, proponents of the ICC worry that its power is diluted though treaty compromises to a point of being nearly moot.[179] The restrictions, listed above, on its ability to hold jurisdiction over various claims and issues put damaging limits on the court's purposes, they argue.[180] The notion of complementarity, in particular, may allow states to protect their own nationals from ICC prosecution by retaining domestic jurisdiction,[181] and the Security Council's effective blocking power allows states that are not party to the Rome Statute, including the United States, to prevent the court from reaching certain individuals.[182] These jurisdictional handcuffs reveal the major weakness of the ICC: its reliance on states for enforcement and validity.[183] The ICC lacks police or military forces, let alone its own source of funding, and so it cannot apprehend suspects or enforce its own orders.[184] It is therefore subject to the political whims of a state when requesting that state arrest or surrender a defendant.[185] The ICC may also be unable to functionally assist a weak state that seeks assistance in corralling criminals within its borders.[186]

---

175. Rome Statute, *supra* note 166.

176. Alexander, *supra* note 162, at 19; ven der Vyver, *supra* note 169, at 66–71.

177. Chibueze, *supra* note 162, at 199–200.

178. Alexander, *supra* note 162, at 19; ven der Vyver, *supra* note 169, at 9–10.

179. Chibueze, *supra* note 162, at 187; Jack Goldsmith, *The Self-Defeating International Criminal Court*, 70 U. CHI. L. REV. 89, 91–92 (2003).

180. *See generally* Chibueze, *supra* note 162.

181. Complementarity provides a comfort to states participating in the Rome Statute similar to the deference to national sovereignty featured in the Cybercrime Convention. Complementarity certainly played a key role in garnering enough support to ratify the Rome Statute from the earliest stages of its inception. *See* JANN K. KLEFFNER, COMPLEMENTARITY IN THE ROME STATUTE AND NATIONAL CRIMINAL JURISDICTIONS 79–80 (2008).

182. Chibueze, *supra* note 162, at 217–18.

183. Alexander, *supra* note 162, at 11.

184. *Id.*

185. *Id.*

186. *Id.*

Ultimately, the success or failure of the ICC has yet to be seen.[187] Too little time has passed for any substantive analyses to be made about the court's effectiveness—to date only fifteen cases have been brought to the court[188] and the court reached its first verdict in March 2012.[189] For the ICC to have a long-term effect, the international community needs to demonstrate a stronger consensus in support of the court's legitimacy and the barriers to its operation need to be removed.[190]

II: THREE APPROACHES TO TACKLING CYBERCRIME ON AN INTERNATIONAL LEVEL

The application and prosecution of criminal law in the international arena always presents practical challenges.[191] The issues of national sovereignty, multinational cooperation, and a lack of enforcement mechanisms, discussed in Part I of this Note, are just the beginning of the list of issues that plague any international efforts to regulate crime. Though cybercrime is uniquely suited to international regulation, many of these same historical obstacles continue to exist.[192]

An analysis of three distinct approaches to international regulation of cybercrime can highlight the way the international community's perception of international regulation—particularly with regard to international courts—should evolve. The first approach calls for universal jurisdiction over cybercrime. The second approach relies on states' domestic ratification of cybercrime statutes that are drafted by international bodies. The third approach is the most radical, and yet the most pragmatic, calling for

---

187. *See id.* at 55.

188. *All Cases*, INT'L CRIMINAL COURT, http://www.icc-cpi.int/Menus/ICC/Situations+and+Cases/Cases/ (last visited Mar. 18, 2012); Alexander, *supra* note 162, at 15.

189. Marlise Simons, *Congolese Rebel Convicted of Using Child Soldiers*, N.Y. TIMES, Mar. 15, 2012, at A12. The ICC found Thomas Lubanga guilty of "recruiting and enlisting boys and girls under the age of 15 and using them in war." *Id.* This first conviction was not an overwhelming success for the court, though. The three-year trial was "halting [and] arduous," ending with the three judges, two of whom wrote dissenting opinions, harshly criticizing the prosecution for having been "negligent and ha[ving] delegated investigations to unreliable paid go-betweens who had encouraged witnesses to give false testimony." *Id.*

190. Alexander, *supra* note 162, at 27. Though there have been critics of the ICC from the outset, a significant group of anti-ICC scholars and practitioners point to its slow start as evidence that the court, by its very structure, is incapable of effectively prosecuting international crimes. *See, e.g.*, Elena Baylis, *Reassessing the Role of International Criminal Law: Rebuilding National Courts through Transnational Networks*, 50 B.C. L. REV. 1, *passim* (2009); Goldsmith, *supra* note 179, *passim*.

191. *See, e.g.*, ven der Vyver, *supra* note 169, at 8.

192. *See generally* Holland, *supra* note 77.

an international penal code for cybercrime regulated by an international court and enforced by multinational task forces. As may often be the case with a technology-based issue, traditional legal tactics, including the first two approaches to cybercrime discussed here, are quickly becoming antiquated and fail to meet challenges posed by a dynamic, expansive, and rapidly mutating species of crime.[193]

A. Universal Jurisdiction for Cybercrime

Extending universal jurisdiction over cyberspace and cybercrime can be very attractive at first glance, though careful examination reveals that it fails to address many of the problems presented by cybercrime and, if applied, may create new areas of concern.[194]

In her article "Cyber-Apocalypse Now: Securing The Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent," Kelly A. Gable forcefully lays out the value of universal jurisdiction over cybercrime, with particular focus on the major crimes that may be labeled terrorist acts.[195] The pivotal value of universal jurisdiction, as she argues, is in its impact as a deterrent.[196] Physical prevention being nearly impossible for multiple logistical and practical reasons,[197] deterrence becomes the most viable solution to the challenge of would-be cybercriminals.[198] Universal jurisdiction alone, she argues, can provide the level of deterrence necessary because its broad reach can surmount many of the practical challenges of locating, and then prosecuting, cybercriminals by potentially stripping cybercriminals of any data safe-havens.[199]

Yet the very broadness of universal jurisdiction makes it a controversial approach to any crime.[200] Though, as mentioned in Part I.B of this Note, its application has expanded significantly since the end of World

---

193. David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, *passim* (1996); Weber, *supra* note 62, at 443, 446.

194. *See, e.g.*, Gable, *supra* note 1, at 105; Rho, *supra* note 71, at 699.

195. "Roughly defined, cyberterrorism refers to efforts by terrorists to use the Internet to hijack computer systems, bring down the international financial system, or commit analogous terrorist actions in cyberspace . . . Depending on his or her goal, a hacker could just easily be a cyberterrorist as a cybercriminal." Gable, *supra* note 1, at 62–63.

196. *Id.* at 105.

197. These reasons include, among others, the political, religious and ideological nature of the criminal's motives, along with challenges pinpointing, geographically, a "location" of a crime that may utilize multiple computer systems in multiple countries. *Id.* at 100–05.

198. *Id.* at 105.

199. *Id.*

200. Kontorovich, *supra* note 140, at 184.

War II,[201] the international community has identified compelling reasons to be cautious in allowing its proliferation.[202] Specifically, two sets of hurdles arise when considering the application of universal jurisdiction to cybercrime: first, proponents must justify the use of such unusually expansive prosecutorial power to the international community, and second, they must address the many practical implications in actually pursuing cybercriminals without regard for territorial boundaries.[203]

At the outset, proponents of applying universal jurisdiction to cybercrime must first persuade the international community that the crimes have reached a level of heinousness on par with other crimes granted such an unusual international distinction, such as genocide or crimes against humanity.[204] "Heinous" crimes, as discussed, are generally defined in vague terms, such as those crimes that are "shocking to the conscience."[205] Gable successfully argues that the very extreme acts of cyberterrorism—those that are of such a scale that entire financial or national security systems may be dismantled—may meet this standard.[206] However, any crime that falls short of this conscience-shocking standard may present difficult questions over whether the crime in question truly warrants being subject to universal jurisdiction.[207] This dilemma also brings up the corollary practical concerns regarding the need for uniform terminology and definitions discussed earlier.[208]

Most proponents of universal jurisdiction for cybercrime draw the common analogies to piracy as a method of justification,[209] suggesting that the Internet is like the high seas—a valuable "global commons" essential for commerce. For many of the reasons discussed in Part I.C, however, the historic crime of piracy on the high seas may fail to provide an accurate analogy for cybercrime. States were more comfortable with universal jurisdiction for piracy because pirates were readily identifiable as nonstate actors and because their impact was limited to one ship at a

---

201. *See* Fry, *supra* note 146, at 176.

202. *See, e.g.*, Bassiouni, *supra* note 136, at 82.

203. *See, e.g.*, Abu-Odeh, *supra* note 74, at 394. Abu-Odeh, a universal jurisdiction skeptic, suggests that universally prosecuted laws are likely to be promulgated by countries that are either economically or militarily powerful. She questions the impact of such laws, which she suggests would be pro-Israel, and their correlating procedures on Palestinians. *Id.*

204. *See, e.g.*, Kontorovich, *supra* note 140, at 205–06.

205. *Id.* at 206.

206. Gable, *supra* note 1, at 118.

207. *See, e.g.*, Kontorovich, *supra* note 140, at 206–07.

208. *See supra* Parts I.B & I.C.

209. *See, e.g.*, Gable, *supra* note 1, at 116; Kontorovich, *supra* note 140, at 184.

time.[210] Pirates, put simply, did not present the kind of identification and capture challenges posed by today's frequently anonymous cybercriminals, nor were they capable of dismantling entire countries through their plundering.[211] Unlike a physical capture on the high seas, law enforcement agencies may have to contend with cybercriminals hiding out in a host country while their criminal presence is manifested only on the "high seas" of the Internet.[212] Furthermore, the piracy analogy again raises the question of uniform definitions, as highlighted by the example of privateering.[213] Because neither the heinousness standard nor the piracy analogy provide decisive justification for universal jurisdiction, it is unlikely that the international community will be easily convinced that cybercrime meets historical standards for expanding this broad prosecutorial power.

Assuming that universal jurisdiction could be justified, though, the questions of terminology and definition become pivotal.[214] Genocide, for example, may be able to pass muster as a crime worthy of universal jurisdiction because it is universally understood and definable in every language without substantial controversy.[215] Yet cybercrime, or cyberterrorism, can present challenges by being more controversial in definition. The term "terrorism," alone, may not be easily defined as it lacks meaning in any uniform legal sense.[216] The adage of "one man's terrorist is another man's freedom fighter" highlights the subjectivity of the definition of terrorism[217] and, as the Iranian squirt-gun fight episode demonstrated, the same subjectivity may apply to cybercrime, generally.[218]

Norming these standards and defining exactly what constitutes cybercrimes or acts of cyberterrorism—something eminently important to the enforcement of universal jurisdiction—will not be an easy task. There is strong probability that those definitions and norms would be generated

---

210. Rho, *supra* note 71, at 715.

211. *See* Kontorovich, *supra* note 140, at 204–07, 210.

212. Rho, *supra* note 71, at 705.

213. Kontorovich, *supra* note 140, at 210–23.

214. Miquelon-Weismann, *supra* note 34, at 338.

215. *See, e.g.*, Bassiouni, *supra* note 136, at 120.

216. Fry, *supra* note 146, at 182.

217. *Id.* Gable makes an unconvincing response to this argument, simply calling the adage absurd for its inapplicability to crimes such as genocide and stressing that it "has outlived its usefulness." Gable, *supra* note 1, at 114.

218. Lentz notes that the rapid pace of the cyberspace's evolution will guarantee that any "workable definition [of cyberterrorism] would quickly grow stale." Lentz, *supra* note 1, at 809–10. He suggests that while large, catastrophic terrorist acts might be easily and universally identifiable, midlevel attacks require some kind of agreement, presumably based on an international consensus, to identify them as "terrorist acts." *Id.*

by the world's more affluent countries, therefore reflecting a limited legal perspective.[219] This kind of political orientation in the actual prosecution of cybercrimes marks an additional concern about the practicality of simply extending jurisdiction beyond territorial borders.

Procedural concerns constitute yet another set of challenges. Even presuming that universal jurisdiction allows for one country to prosecute an identifiable defendant under a clear set of cybercrime statutes, current domestic court structures may not be equipped to handle the unique scope of such cases.[220] A cybercriminal may attack a global network with a virus that can self-replicate and adapt to various computer systems and programs,[221] making the nature and temporal extent of the harm difficult to specify with precision. In the event of such an attack, there may be millions of victims located just within the prosecuting nation's boundaries,[222] not to mention the number of victims that could be affected worldwide on an ongoing basis. Such a vast and complicated case could overwhelm a nation's judicial resources and few procedural mechanisms exist that could effectively control the scope and complexity of these legal actions.[223]

On balance, providing states with universal jurisdiction is impractical as a sole solution to combating cybercrime, though it is an approach that acknowledges many important realities. Gable successfully presents the importance of deterrence in preventing the attacks of would-be cybercriminals and correctly suggests that universal jurisdiction has a role to play in the larger efforts to combat cybercrime.[224]

B. Domestic Adoption of International Statutes

The creation of broad, multinational treaties—premised on traditional notions of territorial sovereignty—provides a less radical solution to dealing with cybercrime on an international level, though the very structure of such an approach threatens to limit its practicability.[225] The Convention on Cybercrime provides a model for this tactic and highlights the

---

219. Abu-Odeh, *supra* note 74, at 394. Abu-Odeh suggests that an important concern stems from the application of universal jurisdiction to the Israeli-Palestinian conflict. She predicts that universal jurisdiction would lead to widespread prosecution of "Palestinian Terrorism" but less vociferous prosecution of "Israeli Terrorism" because of Israel's influence with more affluent countries. *Id.*

220. Rho, *supra* note 71, at 715.

221. *Id.*

222. *Id.*

223. *Id.*

224. Gable, *supra* note 1, at 118.

225. *See generally* Miquelon-Weismann, *supra* note 34; Weber, *supra* note 62, *passim*.

important strengths and inherent weaknesses in relying on treaties to address transnational cybercrime.[226]

Multinational treaties can go far in making the initial strides of establishing norms and creating customary international law.[227] Moreover, they can facilitate the domestic internalization of rules among participating states while still allowing each state to retain sovereignty.[228] At the most fundamental level, such treaties (building primarily off of the Cybercrime Convention and UN Security Council resolutions against terrorism and other grave criminal acts) can articulate the existence of state duties to prevent and respond to cybercrime.[229] Without treaties to lead the way on these fronts, nations may struggle to identify the proper avenues through which they can combat cybercrimes that touch so many different jurisdictions and actors.[230]

Yet the value of treaties that rely on domestic legislation is limited to these first normative steps. As discussed in Part I.B, such treaties bind only member parties, who may still exert nonuniform efforts to comply.[231] For example, both Nation A and Nation B might criminalize the same cyberactivity in line with a cybercrime treaty to which they are both members, but they may vary in their approach to computer monitoring measures.[232] Alternatively, Nation A might move rapidly to enact universally agreed upon legal standards but will have the effectiveness of their efforts frustrated by a slower moving legislature in Nation B.[233] Inconsistencies such as these will keep cooperation between member states problematic, particularly with regard to evidence sharing or extradition provisions.[234]

Furthermore, a treaty that is too deferential to the sovereignty of participating states is unlikely to resolve important jurisdictional dilem-

---

226. Miquelon-Weismann, *supra* note 34, at 334–35.

227. Weber, *supra* note 62, at 445.

228. *See, e.g.*, Miquelon-Weismann, *supra* note 34, at 340–41.

229. Lentz, *supra* note 1, at 816.

230. Jennifer J. Rho provides one example of the way the United States might fight international cybercrime on its own. She suggests that the Alien Tort Statute, 28 U.S.C. § 1350 (2006), might serve as the legal vehicle to prosecute claims, but concedes that this approach is limited in that it relies either on treaty law or customary international law for standing and generally may not apply for criminal prosecutions. She suggests, ultimately, that the "Convention on Cybercrime's approach may be the best path to take." Rho, *supra* note 71, at 717.

231. Weber, *supra* note 62, at 443–44.

232. Miquelon-Weismann, *supra* note 34, at 340–41.

233. Weber, *supra* note 62, at 428.

234. Lentz, *supra* note 1, at 820–22.

mas.[235] The Convention on Cybercrime, for example, is silent on the proper course of action when more than one country in the treaty has a valid jurisdictional claim over a particular act of cybercrime.[236]

Ultimately, for such treaties to be successful they require universal participation and binding provisions regarding the rules and procedures to which states should adhere in passing their own legislation.[237] However, states would undoubtedly balk at such a powerful treaty and, even if they agreed to sign and ratify it, would undermine the treaty's value through the insertion of numerous reservations that exempted them from the most stringent provisions.[238] A multinational treaty, then, will play an important role in mounting an initial international effort to fighting cybercrime, but it will fail if it relies entirely on domestic action for enforcement.

C. Vesting Jurisdiction in an International Court

The most promising method of preventing and prosecuting cybercrime marries the use of universal jurisdiction and multinational treaties, but goes the extra step of vesting jurisdiction over an international penal code on cybercrime in an international judicial body. By vesting jurisdiction over cybercrime in a court modeled after the ICC, the international community can ensure that the authority of articulating definitions and standards will rest within single entity that can adapt in tandem with this ever-evolving field of crime.

The Convention on Cybercrime, with its efforts to create a short list of universal definitions and its growing list of member parties, provides an important starting point in formulating an international penal code for cybercrime. In her article, "The Council of Europe's Convention on Cybercrime," Amalie M. Weber articulates the values of establishing such a code: "It could be changed more easily as technology develops . . . states could better maintain consistency between their own legislative schemes and the model code [and, finally,] the process of developing such a model code might yield superior solutions to the jurisdictional problems permeating cybercrime legislation."[239] A detailed and specific penal code for cybercrime would also alleviate many of the definitional discrepancies that currently limit effective cooperation between various enforcement agencies and would help web users know more precisely what response their actions are likely to bring from regulators worldwide.[240]

---

235. Miquelon-Weismann, *supra* note 34, at 327.
236. *Id.* at 327.
237. Weber, *supra* note 62, at 444.
238. *Id.* at 441.
239. *Id.* at 445.
240. Holland, *supra* note 77, at 32.

An international penal code would require an extraterritorial regulatory power for enforcement and review.[241] Because cyberspace exists without regard to territorial boundaries, universal jurisdiction proponents are correct to view the web as akin to the high seas. Unlike the high seas, though, this is a unique and dynamic realm that requires its own system of legal rules and regulatory processes that can evolve along with the space itself.[242] The potential scope of harm in cyberspace, as mentioned earlier, far exceeds the amount of harm that a single pirate ship might cause on the seas.[243] Thus, tasking individual nations with the duty to regulate cybercrime through universal jurisdiction may fail to address the potentially global implications of a single crime and the potentially competing interests of different states in prosecuting that crime. Moreover, a single state, as discussed earlier, may be overwhelmed by the sheer volume of victims, the complexity of the issues, or other procedural hurdles unique to a major cybercrime.[244]

The structure of the ICC serves as an ideal template for an international court or tribunal holding jurisdiction over cybercrime for at least four compelling reasons. First, the ICC's potential to reach various criminal actors is already internationally (though admittedly not universally) sanctioned. As long as either a cybercriminal or that criminal's victims are citizens of a country that is party to the Rome Statute, the ICC may have jurisdiction over the matter.[245] The international community's landmark creation of the ICC, with its novel jurisdictional scope and structure, suggests that the creation of a similar court focused on cybercrime is not too far-fetched.

Second, a complementarity provision and a focus on only the most serious international crimes, again modeled on the ICC, will ensure that states may continue to exercise jurisdiction over less major cybercrimes or those that only affect domestic actors. An international cybercrime court would exercise jurisdiction over only those cases that affect global classes of victims (those with populations that are enormous, dispersed

241. *Id.* at 9.

242. Holland, *supra* note 77, at 8 (providing an illuminating and comprehensive summary of the views of professors David R. Johnson and David Post, who articulated the unique view of cyberspace as essentially its own territory, and the competing arguments of Jack L. Goldsmith, who challenges their assertions that traditional jurisdictional boundaries are inadequate for effective regulation of cyberspace); *see also* Johnson & Post, *supra* note 193, *passim*.

243. *See supra* Part II.A.

244. *Id.*

245. Chibueze, *supra* note 162, at 187.

across multiple nations, or both), truly heinous crimes or terrorist acts, or even impermissible cyberattacks between states.

Third, an international cybercrime court, much like the Supreme Court in the United States, would have the ability to provide authoritative and final interpretations over the international penal code and thus could quickly adapt the law when necessitated by technological advancements. Should a cybercriminal utilize a new technology to perpetrate a harmful act in an as-yet inconceivable manner, the court would play the critical role of interpreting the international cyber penal laws to evaluate whether the criminal's actions fall within the international community's definitions of illegal conduct. Moreover, the international can be structured to be more liberal with regard to the procedural and privacy rights of defendants than many national court systems,[246] again increasing the likelihood of state participation in an international cybercrime court.

Finally, the rulings of such a court would benefit from the preexisting multinational cybercrime task forces, which will be able to act as the court's otherwise-lacking enforcement mechanism.

The proposal's benefits reveal themselves when considered against a hypothetical situation in which, for example, a cybercriminal, in violation of one of the international cyber penal laws, launches a malicious Trojan Horse through individuals' Facebook accounts. If the cybercriminal was an American, and substantially all of the victims were also Americans, then American courts would exercise jurisdiction over the case. However, in the more likely case that the class of victims contained individuals—including corporations and other organizational groups—from various countries, the international court would exercise jurisdiction over the matter. Multinational law enforcement teams would coordinate the investigation into the precise extent and nature of the harm and would locate, arrest, and detain the criminal. A scenario in which one country accuses another of cyberespionage or a coordinated cyberattack provides a second helpful hypothetical. Before the states escalate to armed conflict, the international court would have the opportunity to rule on whether the actions of the accused nation constituted a violation of the international penal laws and then propose a solution.

Of course, vesting jurisdiction over cybercrime in an international cybercrime court or tribunal would still present a host of challenges. The creation of such a court would surely mirror and perhaps surpass the current hurdles the ICC faces in terms of speed, relevance, and authority

246. Harding, *supra* note 140, at 206. Harding notes that "protective rules [such as double jeopardy] have of course a variable application and resilience at the national level . . . but are increasingly capable of being invoked at the international level." *Id.*

mentioned in Part I.D above. Beyond these initial challenges, implementing this Note's proposal would face at least three specific obstacles. First, states will be hesitant to sacrifice sovereignty to an international body. Some optimists may argue that placing the power to regulate cybercrime in an international court would not necessarily be an extreme act because the regulatory participation of non-state and multi-state entities, in addition to transnational common law-making, may already be blurring the traditional boundaries of jurisdiction.[247] However, giving an international cybercrime court complete regulatory power would be a truly unprecedented shift in international law and will be a hard pill for many sovereign states to swallow. Second, significant efforts would be required to draft both an international penal code and an international treaty creating an international court or tribunal with specific power of review over cybercrimes. As discussed above, the lack of uniformity in cybercrime definitions and the sluggish nature of treaty-making guarantee that producing such documents will be exceptionally difficult. Finally, the new international court will be reliant on independent states to provide enforcement and funding, requiring a mechanism to ensure cooperation between states.[248] Though state enforcement agencies are increasingly working together via multinational taskforces to combat cybercrime, binding them to such efforts may, again, run counter to states' traditional notions of sovereignty.

Still, there is ample support for the belief that a specialized cybercrime court could serve as the most effective answer to cybercrime. The United States may have already blazed the trail in recent years by creating federal courts with specialized jurisdiction, most notably the United State Court of Appeals for the Federal Circuit, which holds exclusive appellate review over almost all patent cases in country.[249] Congress created the Federal Circuit and granted it review over the nation's patent appeals in large part to harmonize the widely divergent approaches to patent law that had evolved in different regions of the United States.[250] By allowing a court to specialize in one area of the law, particularly one that is based on complex and predominantly nonlegal underlying concepts, its judges

---

247. Paul Schiff Berman, *The Globalization of Jurisdiction*, 151 U. PA. L. REV. 311, 534–35 (2002).

248. Weber, *supra* note 62, at 445.

249. RICHARD A. POSNER, THE FEDERAL COURTS: CHALLENGE AND REFORM 6 (1996). Additional specialized courts in the United States include, among others, the Court of International Trade, the United States Tax Court, and the United States Court of Military Appeals. 13 CHARLES ALAN WRIGHT ET AL., FEDERAL PRACTICE AND PROCEDURE § 3508 (3d ed. Supp. 2011).

250. POSNER, *supra* note 249, at 252–53.

can develop an expertise that will be more likely to result in consistent and practical rulings.[251] The success of the Federal Circuit in promulgating a consistent judicial gloss for patent law is likely to be repeated by a cybercrime court. The probable emergence, and then prominence, of "technocratic" judges[252] on a cybercrime court may also alleviate concerns about the courts' inherent biases toward one kind of legal system or set of policies,[253] reduce the chances that judges with no technical savvy will permit overly intrusive search and seizure practices, and perhaps even position it to hear civil cases[254] in addition to criminal.

The ever-evolving and growing threat of cybercrime may serve as a catalyst that pushes the international community to break away from its traditional hesitancy to sacrifice state sovereignty to international organizations. Conceivably, a truly global cyberattack of unprecedented, but plausibly catastrophic, proportions could usher in a rapid global response that could result in an international cybercrime court gaining jurisdiction over an international cyber penal code. States should act responsibly to take decisive action on this issue before such a cyberattack occurs.

CONCLUSION

Cybercrime is a new and rapidly evolving form of crime that is uniquely suited to international regulation and multinational enforcement. Though universal jurisdiction and treaty-based approaches may be effective in combating cybercriminals to a certain extent, such efforts

---

251. Edward K. Cheng, *The Myth of the Generalist Judge*, 61 STAN. L. REV. 519, 549 (2008).

252. In his article exploring the policy-making role of ICC judges, Jared Wessel notes, specifically within the realm of humanitarian law, that "the line between the administrative technocrat and the public international legal mind becomes blurred, if not irrelevant" because of the role technocratic bodies have played in addressing global political issues like terrorism. Jared Wessel, *Judicial Policy-Making at the International Criminal Court: An Institutional Guide to Analyzing International Adjudication*, 44 COLUM. J. TRANSNAT'L L. 377, 439–40 (2006).

253. Such biases in international courts may derive from the nationality of judges, their personal philosophical approach to the role of international adjudicatory bodies, or from the political realities that stem from their court's reliance on the cooperation and support of the sovereign governments they may be presiding over. *See* Jacob Katz Cogan, *International Criminal Courts and Fair Trials: Difficulties and Prospects*, 27 YALE J. INT'L L. 111, 115, 135–36 (2002).

254. While this Note is focused primarily on criminal law, Moritz Keller provides an interesting analysis of the role the International Court of Justice can play in handling Internet-based civil cases, with a particular focus on international e-commerce laws. *See generally* Moritz Keller, *Lessons for The Hague: Internet Jurisdiction in Contract and Tort Cases in the European Community and the United States*, 23 J. MARSHALL J. COMPUTER & INFO. L. 1 (2004).

will be most effective in the context of establishing an international cybercrime penal code and vesting jurisdiction over that body of law in an international cybercrime court. While this solution admittedly faces daunting challenges, the preexisting and growing presence of multinational taskforces lends an enforcement mechanism that has heretofore been absent in most international courts—an exception to the norm that makes placing authority in a new international court at once more feasible and, therefore, potentially objectionable to sovereign states. Anything short of this level of action, however, will continue to leave the world in an ever-more precarious position in which cybercriminals threaten to harm individuals, cripple global economies, and disable entire nations.

Nicholas W. Cade[*]

* B.A., Colby College (2008); M.S.T., Pace University (2010); J.D., Brooklyn Law School (expected 2013); Editor-in-Chief, *Brooklyn Journal of International Law* (2012–2013). I owe a special tribute to all of the teachers and professors who played a role in my education and personal growth; whether directly or indirectly, they have each made profound contributions to this Note. I would also like to thank the staff of the *Brooklyn Journal of International Law* for their assistance in preparing this Note for publication. Finally, for her unwavering faith and unending support, I dedicate this Note to Christina Evriviades. All errors or omissions are my own.