Vanderbilt Journal of Transnational Law

Volume 43
Issue 1 *January 2010*

Article 2

2010

Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent

Kelly A. Gable

Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent

*Kelly A. Gable**

ABSTRACT

Cyberterrorism has become one of the most significant threats to the national and international security of the modern state, and cyberattacks are occurring with increased frequency. The Internet not only makes it easier for terrorists to communicate, organize terrorist cells, share information, plan attacks, and recruit others but also is increasingly being used to commit cyberterrorist acts. It is clear that the international community may only ignore cyberterrorism at its peril.

The primary security threat posed by the Internet is caused by an inherent weakness in the TCP/IP Protocol, which is the technology underlying the structure of the Internet and other similar networks. This underlying structure enables cyberterrorists to hack into one system and use it as a springboard for jumping onto any other network that is also based on the TCP/IP Protocol. Other threats to national and international security include direct attacks on the Internet and the use of the Internet as a free source of hacking tools. These threats will not be eradicated easily.

In the absence of feasible prevention, deterrence of cyberterrorism may be the best alternative. Without, at a minimum, a concerted effort at deterrence, cyberterrorism will continue to threaten national and international security. The most feasible way to deter cyberterrorists is to prosecute them under the international law principle of universal jurisdiction.

---

* Adjunct Professor of Public International Law, Drexel University Earle Mack School of Law. The Author wishes to thank Professor Duncan B. Hollis, Professor Paul B. Larsen, Professor David A. Koplow, Professor Daniel M. Filler, Professor Francis J. Gavin, Timothy S. Kearns, and Michael McGraw for their astute advice and helpful comments.

TABLE OF CONTENTS

I. INTRODUCTION

It is a cold December day, already dark, when Aidan Smith leaves his office to catch the train home. As he is leaving the building, the power suddenly cuts out, bringing the elevator he is in to a screeching halt on the ground floor. He presses the emergency button, and the doors open, begrudgingly, to let him out. Shaken, he heads for the train station. As he steps out into the street, he realizes it is much darker than usual—every building, every street light, every stoplight is dark. Only the headlights from passing cars light the sidewalk as he slowly makes his way to the train station. He finally arrives, but finds that the station is barely lit and is jammed with people waiting for trains that are not coming. Checking the news on his BlackBerry, he sees that Washington, D.C., New York, Chicago, and Los Angeles have simultaneously lost all electricity and that Al Qaeda replaced the White House website with a message proclaiming that they have hacked into and shut down these major power grids to cripple the U.S. economy, as the stock markets, airports, and banks cannot function without electricity. In short, Al Qaeda has caused a cyber-apocalypse.[1]

Although this situation is hypothetical, the possibility is disturbingly real. Hackers scan U.S. government computer systems literally thousands of times a day, looking for a way in.[2] In 2001, hackers successfully attacked an electric power grid in California and a seaport in Houston;[3] more recently, hackers planted malicious software in the U.S. power grid, oil and gas distribution computer systems, telecommunications networks, and computer systems of the financial services industry.[4] In March 2007, researchers at the Department of Energy's Idaho National Laboratory caused a

---

1. A cyber-apocalypse is "a cyber attack that could wreak havoc on the nation by bringing down critical information infrastructures." *See* BERNADETTE SCHELL & CLEMENS MARTIN, WEBSTER'S NEW WORLD HACKER DICTIONARY 78-79, 122 (2006) (explaining that a cyber-apocalypse easily could occur, given the rate at which hackers attempt to invade critical U.S. infrastructure facilities, and given the demonstrated weaknesses of those facilities).

2. Mike Mount, *Hackers Stole Data on Pentagon's Newest Fighter Jet,* CNN.COM, Apr. 21, 2009, http://edition.cnn.com/2009/US/04/21/pentagon.hacked/index.html; *see also* SCHELL & MARTIN, *supra* note 1, at 145 (noting that hackers, as they are commonly known and actually prefer to be called "crackers").

3. SCHELL & MARTIN, *supra* note 1, at xxvi.

4. According to Janet Napolitano, Director of the Department of Homeland Security, "the vulnerability of the nation's power grid to cyberattacks 'has been something that the Department of Homeland Security and the energy sector have known about for years.'" Jeanne Meserve, *Hackers Reportedly Have Embedded Code in Power Grid,* CNN.COM, Apr. 9, 2009, http://edition.cnn.com/2009/TECH/04/08/grid.threat/index.html.

generator to self-destruct, just to see if they could.[5] Although these attacks were narrower in scope and magnitude than the hypothetical scenario, they each demonstrate the vulnerability of critical U.S. infrastructure. The fact that each of these critical infrastructure systems is accessible via the Internet heightens (and arguably creates) this vulnerability.[6]

The Internet has revolutionized and exponentially increased the threat that terrorism poses to national and international security. The Internet not only makes it easier for terrorists to communicate, organize terrorist cells, share information, plan attacks, and recruit others,[7] but also is increasingly being used to commit cyberterrorist acts. In February 2009, the Director of National Intelligence testified before the Senate Select Committee on Intelligence that terrorist groups have expressed their intent to use cyber attacks against the United States.[8] Indeed, cyberterrorists and hackers attempt to penetrate Department of Defense computer systems thousands of times a day.[9]

Cyberterrorism has become one of the most significant threats to the national and international security of the modern state, and cyberattacks are occurring with increased frequency. Starting on July 4, 2009, a week-long cyberattack crippled numerous U.S. and South Korean websites, including those of the U.S. Departments of Transportation and Treasury; the U.S. Federal Trade Commission; the South Korean President's Office; the South Korean National Assembly; and U.S. Forces Korea.[10] Although the South Korean government initially believed that North Korea had perpetrated the attack, security experts later suggested that cyberterrorists operating in the United Kingdom may have been the source of the attack, which

---

5. Duncan B. Hollis, *E-War Rules of Engagement*, L.A. TIMES, Oct. 8, 2007, http://www.latimes.com/news/opinion/la-oe-hollis8oct08,0,5897172.story.

6. "Internet" and "cyberspace" are general terms that refer to the vast system of interconnected computers, what is in effect a network of networks. The Internet is distinct from an intranet, which is essentially a network of computers that are not connected to the Internet or are separated from the Internet in some way.

7. *See* Oscar Schachter, *The Decline of the Nation-State and its Implications for International Law*, 36 COLUM. J. TRANSNAT'L L. 7, 15 (1997) (noting that "new communication networks have also increased the power of lawless groups").

8. *See* Dennis C. Blair, U.S. Dir. of Nat'l Intelligence, Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence 39 (Feb. 12, 2009), http://intelligence.senate.gov/090212/blair.pdf ("Terrorist groups, including al-Qa'ida, HAMAS, and Hizballah, have expressed the desire to use cyber means to target the United States.").

9. Mount, *supra* note 2.

10. Martyn Williams, *U.K., Not North Korea, Source of DDoS Attacks, Research Says*, COMPUTER WORLD, July 14, 2009, http://www.computerworld.com/s/article/print/9135492/U.K._not_North_Korea_source_of_DDOS_attacks_researcher_says?taxonomyName=Cybercrime+and+Hacking&taxonomyId=82.

affected hundreds of thousands of personal computers across dozens of countries.[11]

Estonia was the target of a comparably massive attack from April to May 2007, when a multi-week wave of cyberattacks effectively shut down the country by disrupting the websites of the Estonian President and Parliament,[12] the vast majority of Estonian ministries, three of the country's six largest news organizations, and two of its major banks.[13] The attack on Estonia was so effective partly because Estonia has established an "e-government," conducting most of its basic governmental operations via the Internet.[14] For example, Estonians conduct more than 98% of their banking online,[15] pay their taxes online, and vote online.[16] Accordingly, these relatively simple attacks effectively brought the country to a halt for three weeks.

Other significant examples of cyberterrorism in the past few years include the theft of information regarding the new U.S. military stealth fighter jet, the hacking into the U.S. Air Force's air traffic control systems,[17] and Titan Rain, which is the codename given by

---

11. *Id.*

12. The attacks seem to have been precipitated by Estonia's removal of the Bronze Warrior statue, a World War II memorial in Tallinn recognizing Russian soldiers who died in the war; Estonia moved it because it regarded the statute as memorializing five decades of Soviet occupation. Tony Halpin, *Estonia Accuses Russia of "Waging Cyber War,"* TIMES (London), May 17, 2007, http://www.timesonline.co.uk/tol/news/world/europe/article1802959.ece; *see also* SUSAN W. BRENNER, CYBERTHREATS: THE EMERGING FAULT LINES OF THE NATION-STATE 1–6, 85–91 (2009) (describing the attack on Estonia); Duncan Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1024–1028 (2007) (describing the cyberattack on Estonia).

13. *See* Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, GUARDIAN (London), May 17, 2007, at 1, *available at* http://www.guardian.com.uk/world/2007/may/17/topstories3.russia (discussing the main targets of the cyber-attack on Estonia).

14. *Id.*; *see also* BRENNER, *supra* note 12, at 1–6, 85–91 (noting that Estonia "likes to call itself E-stonia").

15. See Kenneth Geers, Cyberspace and the Changing Nature of Warfare, SC Mag., Aug. 27, 2008, http://www.scmagazineus.com/Cyberspace-and-the-changing-nature-of-warfare/article/115929/ (noting that internet router attacks were also conducted on one of Estonia's Internet Service Providers, which is said to have disrupted government communications).

16. Michael Cross, *Whitehall Must Learn From Estonia's E-Government*, GUARDIAN (London), May 24, 2007, at 6, *available at* http://www.guardian.co.uk/technology/2007/may/24/society.insideit; *see also Marching Off to Cyberwar*, ECONOMIST, Dec. 4, 2008, at 20, *available at* http://www.economist.com/sciencetechnology/tq/displayStory.cfm?story_id=12673385 (noting that in 2000, Estonia's Parliament declared Internet access to be a human right).

17. These attacks occurred over the past two years, over which time hackers gained access not only to "data related to the design and electronics systems of the Joint Striker Fighter" the F-35 Lightning II, but also gained access to the Air Force's air traffic control systems, as a result of which they "were able to see such information as the locations of U.S. military aircraft in flight." Mount, *supra* note 2; *see also*

the U.S. government to a series of intelligence-gathering cyberattacks conducted by a group of Chinese hackers.[18] Furthermore, these are only the most publicized of examples—every day cyberterrorists attempt to undermine national and international security and wreak havoc in order to further their terrorist agendas. In a single day in 2008, for instance, hackers targeted the Pentagon with six million attempts to access its computer system.[19]

These attacks showcase a range of potential tools in the cyberterrorist's arsenal. Some may be relatively simple and low-tech; this also means they are relatively easy to deploy. They also highlight the potential damage that could be caused by more sophisticated attacks. In fact, cybersecurity has become so important that traditionally secretive organizations charged with protecting national security are speaking out about the threat.[20] Increasingly, it is clear that the international community may only ignore cyberterrorism at its peril.

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.[21] The United States has defined cyberterrorism as "a criminal act conducted with computers and resulting in violence,

---

Pentagon to Create Cyber-Defense Command, UNITED PRESS INT'L, June 24, 2009, http://www.upi.com/Security_Industry/2009/06/24/Pentagon-to-create-cyber-defense-command/UPI-79261245853207 (discussing attacks on U.S. computer networks).

18. *See, e.g.*, Nathan Thornburgh, *The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them)*, TIME, Aug. 29, 2005, at 34, *available at* http://www.time.com/time/magazine/article/0,9171,1098961,00.html (discussing efforts to track the Chinese hackers code-named Titan Rain); Nathan Thornburgh, *Inside the Chinese Hack Attack*, TIME, Aug. 25, 2005, http://www.time.com/time/nation/article/0,8599,1098371,00.html (discussing assaults on U.S. networks conducted by hackers based in China). Although these may be considered examples of cybercrime, as opposed to cyberterrorism, as the distinction lies in the actor's intent which is unknown, they are just as properly considered examples of cyberterrorism. *See* BRENNER, *supra* note 12, at 37–47 (describing cyberterrorism).

19. Arnaud de Borchgrave, *Commentary: Silent Cyberwar*, UNITED PRESS INT'L, Feb. 17, 2009, http:/www.upi.com/Emerging_Threats/2009/02/17Commentary-Silent-cyberwar/UPI-74141234886723.

20. James Jay Carafano & Eric Sayers, Outside View: New Cyber-Threats—Part 1, UNITED PRESS INT'L, Feb. 10, 2009, http://www.upi.com/Security_Industry/2009/02/10/Outside-View-New-cyber-threats-Part-1/UPI-96861234303408.

> U.S. Director of National Intelligence Mike McConnell raised this issue for the first time in February 2008 as part of his testimony on the 2008 Annual Threat Assessment. When asked if he believed the United States was prepared to deal with cybersecurity threats to the civilian and military infrastructure, McConnell noted that the country is 'not prepared to deal with it. The military is probably the best protected, the federal government is not well protected, and the private sector is not well protected.'

21. *See* SCHELL & MARTIN, *supra* note 1, at 87 (providing various definitions of the general term cyberterrorism).

destruction, or death of its targets in an effort to produce terror with the purpose of coercing a government to alter its policies," and it includes attacks on computer networks and transmission lines within that definition.[22] Put simply, cyberterrorism generally is understood as any terrorist act conducted in or by means of cyberspace or the Internet.[23] This definition is necessarily broad and includes everything from basic hacking and denial of service attacks to concerted efforts to unleash weapons of mass distraction or mass disruption.[24] Such a definition, however, is limited in application regarding the actor or actors and the intent behind the attack.

First, the term cyberterrorism refers only to terrorist actions taken by individuals, groups of individuals, or organizations such as Al Qaeda. To the extent that either a state or its agent was to act in similar ways,[25] it would be considered an act of aggression or use of force under international law, which may be considered cyberwarfare.[26]

Second, the term cyberterrorism refers only to those actions that are taken by terrorists with the intent or goal of causing destruction or inciting terror, generally for religious or political purposes,

---

22. *See id.* (noting definitions by the Department of Homeland Security and the Department of Defense).

23. BRENNER, *supra* note 12, at 37 (defining cyberterrorism similarly, as "using computer technology to engage in terrorist activity.").

24. *See id.* at 42–54 (providing a very broad definition of cyberterrorism and different ways in which cyberterrorism can help terrorists achieve their goals).

25. The Pentagon estimates that "more than 100 foreign intelligence services have tried to hack into U.S. networks." *Pentagon to Create Cyber-Defense Command*, *supra* note 17.

26. Cybercrime as a use of force under international law is, regrettably, beyond the scope of this article. For treatment of that issue, *see, e.g.*, BRENNER, *supra* note 12, at 65–70 (describing cyberwarfare more generally); Geers, *supra* note 15 (noting that internet router attacks were also conducted on one of Estonia's Internet Service Providers, which is said to have disrupted government communications); Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 890–99 (1999) (discussing international laws that govern the use of force and their applicability to computer network attacks). Parallels to and analysis of Information Operations also are informative, although cyberterrorism as defined here may or may not fit within the Information Operations framework, depending on how that framework is defined. Of course, this presumes that terrorists are rational actors, which may or may not be a valid assumption. Cyberterrorism may fit within the framework of Information Operations (IO) as defined by Hollis, *supra* note 12, at 1030 ("IO views these information networks as both new weapons for use in conflict and new targets for attack."), but perhaps not within the conception of Information Operations held by Rho (noting that " 'those activities that governments and military forces undertake to control and exploit the information environment via the use and the information component of national power'"). Jennifer J. Rho, *Blackbeards of the Twenty-First Century: Holding Cybercriminals Liable under the Alien Tort Statute*, 7 CHI. J. INT'L L. 695, 701 (2007) (quoting Daniel T. Kuehl, *Information Operations, Information Warfare, and Computer Network Attack*, *in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 35, 37 (Michael N. Schmitt & Brian T. O'Donnell eds., 2002)).

although financial gain to facilitate further attacks may be a secondary motivation.[27] It often is difficult to distinguish cybercrime from cyberterrorism during an attack, as the key distinction lies in the intent behind the attack.[28] Depending on his or her goal, a hacker could just as easily be a cyberterrorist as a cybercriminal.

The primary security threat posed by the Internet involves the TCP/IP Protocol, the technology underlying the structure of the Internet and other similar networks. This underlying structure enables cyberterrorists to hack into one system and use it as a springboard for jumping onto any other network that is also based on the TCP/IP Protocol. Other threats to national and international security include direct attacks on the Internet and the use of the Internet as a free source of hacking tools.

These threats are not easy to eradicate. One problem underlying the widespread use of the Internet is the concept of irreversible dependence on technology: once the benefits of technologies like the Internet are realized, it is impossible not to use them. The technologies become an indispensable crutch for those determining policy strategies, both for foreign policy determinations and daily governmental operations.

The cyberattacks on the Estonian, U.S., and South Korean governments, as well as the long list of similar attacks that came before them, have brought the issue of cyberterrorism prevention squarely before national governments and international organizations such as NATO, the Organization for Security and Cooperation in Europe (OSCE), the European Union, the United Nations, and the Council of Europe.[29] These institutions are beginning to take steps to improve international cooperation to combat cyberterrorism.[30] The OSCE recently established the Action Against Terrorism Unit.[31] Similarly, NATO established a Cooperative Cyber Defense Center of Excellence in Estonia.[32] The

---

27. *See* BRENNER, *supra* note 12, at 41 n.144 (discussing the secondary goals of cyberterrorists).

28. *Id.* at 37–47, 91–94.

29. *See infra* notes 32–36 and accompanying text (describing steps taken by national governments and international organizations in response to cyberterrorism).

30. It is possible, because of the difficulties in distinguishing cybercrime from cyberterrorism, that laws aimed at preventing and punishing cybercrime also may be effective against cyberterrorism.

31. *See* Counter-Terrorism Technical Assistance Programmes, Organization for Security and Co-operation in Europe, http://www.un.org/sc/ctc/directory/doa/OSCE.html (last visited Jan. 4, 2010) (discussing the role of the OSCE in combating terrorism); *see also infra* Part IV.A.2 (describing counter-terrorism efforts by international organizations).

32. *See* Press Release, North Atlantic Treaty Organization, NATO Opens New Centre of Excellence on Cyber Defence (May 14, 2008), http://www.nato.int/docu/update/2008/05-may/e0514a.html (discussing the formal establishment of a Cooperative Cyber Defence Centre of Excellence to conduct research and training on

European Union also recently launched the Critical Information Infrastructure Protection Initiative.[33] The United Nations Security Council and General Assembly have enacted resolutions to address terrorism or cyberterrorism.[34] Possibly the most significant enactment is the Council of Europe's enactment of the Convention on Cybercrime,[35] which is the first multilateral convention to address cybercrime.

These domestic and international organizations have made significant progress merely by taking these preliminary steps, but more must be done. The international community must recognize that, as a result of the fundamental insecurities inherent in the architecture of the Internet, none of these actions will prevent cyberterrorism completely. Without a complete overhaul (or at least a significant retrofit) of the very structure of the Internet, these legal, policy, and technological methods will serve only to mitigate the potential effects of cyberterrorism.

In the absence of feasible prevention, deterrence of cyberterrorism may be the best alternative. A longstanding concept of international law—universal jurisdiction—is one way to deter cyberterrorism. The likely effect can be seen by drawing analogies to other international crimes for which universal jurisdiction is recognized and by applying various rationales for universal jurisdiction. The borderless and transnational nature of the Internet and cyberterrorism complicates the application of territorial jurisdiction.[36] The asynchronous pairing of territorial jurisdiction and borderless cyberterrorism means that territorial jurisdiction

---

cyber warfare); *see also infra* Part IV.A.2 (describing counter-terrorism efforts by international organizations).

33. *See Commission Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection, Protecting Europe From Large Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience,* at 2–3, COM (2009) 149 final (Mar. 30, 2009) (discussing an initiative to strengthen critical information infrastructures); *see also infra* Part IV.A.2 (describing counter-terrorism efforts by international organizations).

34. *See infra* notes 184–87 (providing examples of resolutions enacted by the United Nations Security Council and General Assembly).

35. Convention on Cybercrime, *opened for signature* Nov. 23, 2001, Eur. T.S. No. 185, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm; *see also infra* Part IV.A.2 (detailing the requirements and significance of the Convention).

36. Not all scholars would agree with the characterization of the Internet as borderless and/or transnational. *See, e.g.*, JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD vii-ix (2006) [hereinafter GOLDSMITH & WU I] ("[T]he Internet . . . is conforming to local conditions. The result is an Internet that differs among nations and regions that are increasingly separated by walls of bandwidth, language, and filters."); Jack Goldsmith & Timothy Wu, *Digital Borders*, LEGAL AFF., Jan.-Feb. 2006, at 40, 40–41 [hereinafter Goldsmith & Wu II] (discussing the view that the Internet "is splitting apart and reflecting national borders").

likely would be a less effective deterrent than universal jurisdiction. Without, at a minimum, a concerted effort at deterrence, cyberterrorism will continue to threaten national and international security. This Article argues that the most feasible way to accomplish deterrence is to prosecute cyberterrorists under the international law principle of universal jurisdiction.

Part II of this Article provides a brief history of the Internet, as understanding the Internet's origins is important to understanding the nature and extent of the threat the Internet poses to national and international security. It also explains cyberterrorism in the context of the development of intelligence, as viewing the issue in context is important to understanding the problem of cyberterrorism and its potential solutions.

Part III of this Article describes the threats to national and international security that the Internet and cyberterrorism pose and the ways in which the Internet provides the very tools that cyberterrorists need. It describes the ramifications of this technology and argues that, as a result of fundamental insecurities inherent in the structure of the Internet, it will be impossible to prevent cyberterrorism in a meaningful way without a major change in the Internet's structure or its mode of operation.

Part IV of this Article then evaluates various current legal, policy, and technological methods of preventing cyberterrorism, including encryption and firewalls on the technological side and various governmental initiatives on the legal and policy side. Many of these are still nascent, but none of these legal, policy, or technological methods can prevent cyberterrorism completely.

Part V of this Article questions whether cyberterrorism—if it cannot be prevented—can be deterred and whether international law can provide a meaningful deterrent. It examines whether territorial jurisdiction would serve as an effective deterrent to cyberterrorism and determines that, due to the nature of territorial jurisdiction and of cyberterrorism, territorial jurisdiction would not be an effective deterrent. It then examines whether universal jurisdiction exists for prosecuting cyberterrorists under international law, analyzes how cyberterrorism fits the various rationales for universal jurisdiction, and draws analogies to other international crimes for which universal jurisdiction is recognized. It determines that universal jurisdiction is likely to be the most effective deterrent to cyberterrorism.

This Article concludes that, although the inherent structure of the Internet is such that cyberterrorism cannot be completely prevented without massively restructuring the Internet, consistent and effective prosecution using the principle of universal jurisdiction may create a sufficient deterrent to cyberterrorism. Although deterrence is far from an ideal solution, a layered approach of defense, deterrence, and mitigation can reduce the threat of cyberterrorism substantially.

II. HISTORICAL BACKGROUND

Examining the history and the technology behind the Internet and its sister networks is key to understanding the threats to national and international security that the next Part describes. Similarly, reviewing the history of intelligence is important to understanding the historical context for cyberterrorism. The similarities and distinctions drawn from those histories and examined in this Part enable a further understanding of the threats modern cyberterrorism poses.

A. *A Brief History of the Internet and Its Sister Networks*

Inherent in all communication is a certain measure of insecurity, which exists in direct proportion to the size and complexity of the information infrastructure. The Internet demonstrates this most clearly. As a network of networks, the Internet exponentially compounds the problems ordinarily faced by a single network. As a result of certain technological decisions made during its early days, the Internet creates major security problems for networks that are even indirectly linked to it.

The "birth" of the Internet occurred in the late 1960s,[37] but similar systems of interconnected computers had already been in existence for about ten years.[38] The computer had been created almost two decades before the Internet, in 1946, when the Electronic Numerical Integrator And Calculator (ENIAC) was first demonstrated at the University of Pennsylvania.[39] Like the Internet, the computer had its origins in national defense.[40] Exactly who can

---

37. National Science Foundation, NSF and the Birth of the Internet—1960s, www.nsf.gov/news/special_reports/nsf-net/textonly/60s.jsp (last visited Jan. 4, 2010) (discussing that the Internet was "born" on October 29, 1969 at 10:30 p.m., when the first message was sent between computers at UCLA and Stanford as part of the ARPANET, created by the Advanced Research Projects Agency of the U.S. Department of Defense). *But see* Susan W. Brenner, *Law In An Era of Pervasive Technology*, 15 WIDENER L.J. 667, 730–33 (2006) (agreeing that the ARPANET went online in 1969, but stating that changing the core protocol to TCP/IP in 1983 technically is the birth of the Internet).

38. KATIE HAFNER & JOHN MARKOFF, CYBERPUNK: OUTLAWS AND HACKERS ON THE COMPUTER FRONTIER 277–78 (1991).

39. *See* SCOTT MCCARTNEY, ENIAC: THE TRIUMPHS AND TRAGEDIES OF THE WORLD'S FIRST COMPUTER (1999) (describing the development of the ENIAC computer); Asaf Goldschmidt & Atsushi Akera, John W. Mauchly and the Development of the ENIAC Computer, An Exhibition in the Department of Special Collections, Van Pelt Library, University of Pennsylvania, http://www.library.upenn.edu/exhibits/rbm/mauchly/jwmintro.html (last visited Jan. 4, 2010) (discussing an exhibition in 1996 to commemorate the fiftieth anniversary of the ENIAC computer).

40. *See* Daniel F. Burton, Jr., *The Brave New Wired World*, 106 FOREIGN POL'Y 22, 26 (1997) ("It was designed to calculate firing trajectories for artillery shells."); *see also* National Science Foundation, *supra* note 37 (discussing that, according to common

take credit for creating the Internet is unclear, as at least three individuals have been named "the father of the Internet" for their respective contributions.[41] What is clearer is that it was the ARPANET, created by the Pentagon's Advanced Research Projects Agency (ARPA), that ultimately became the world-wide system known today as the Internet.

TCP/IP, the underlying protocol of the Internet, was adopted as the core protocol of the ARPANET in 1983.[42] In 1984, the National Science Foundation established connections with most major universities based on the TCP/IP Protocol.[43] Although they had considered using an international standard being developed called OSI networking, the TCP/IP Protocol was already developed and ready, so they adopted it for future use.[44] Because all of the potential users were known and trusted—indeed, the users of the early Internet were the designers themselves—security of the protocol was not a serious concern.[45]

The end of the Cold War significantly reduced international tensions and removed any lingering doubts that the U.S. government might have held about opening the Internet to the American public and beyond.[46] Thus, in 1988, the National Science Foundation began to connect other countries to the Internet.[47] In 1991, the first World

---

belief, the Internet was created as an emergency communication measure to enable the government to continue to operate in the event of nuclear war).

41. Those three individuals are: Vinton Cerf, for designing TCP/IP (with Robert Kahn); Tim Berners-Lee, for conceiving the key protocols of the World Wide Web; and Paul Baran, for his prior invention of packet switching and routed digital computer networks survivable under attack. *See* GOLDSMITH & WU I, *supra* note 36, at 36–37, 52 (discussing the work of Vinton Cerf and Tim Berners-Lee); George Gilder, *Inventing the Internet Again*, 159 FORBES ASAP 106–14 (June 2, 1997) (discussing the work of Paul Baran).

42. Barry M. Leiner et al., *A Brief History of the Internet: Proving the Ideas*, INTERNET SOC'Y, Dec. 10, 2003, http://www.isoc.org/internet/history/brief.shtml.

43. *See* National Science Foundation, NSF and the Birth of the Internet—1980s, www.nsf.gov/news/special_reports/nsf-net/textonly/80s.jsp (last visited Jan. 4, 2010) (discussing the development of computers in the 1980s).

44. *See id.* (quoting an excerpt from a video transcript of George O. Strawn's discussion of OSI networking).

45. *See, e.g.*, Jonathan L. Zittrain, *The Generative Internet*, 119 HARV. L. REV. 1974, 1989–90 (2006) ("[A]buse of the network was of little worry because the people using it were the very people designing it—a culturally homogenous set of people bound by their desire to see the network work.").

46. *See* National Science Foundation, Science and Engineering Indicators 2006, Overview, S&T: The Global Picture, http://www.nsf.gov/statistics/seind06/c0/c0s1.htm (last visited Jan. 4, 2010) ("The demise of the Cold War political order precipitated more open borders just as the Internet became a tool for unfettered worldwide information dissemination and communication.").

47. Guy Basque, *Introduction to the Internet*, *in* THE ELECTRONIC SUPERHIGHWAY: THE SHAPE OF TECHNOLOGY AND LAW TO COME 9 (Ejan Mackaay et al. eds., 1995). *But see* SCHELL & MARTIN, *supra* note 1, at xx (listing 1991 as the key year). That same year, Robert Tappan Morris, then a graduate student at Cornell University, unleashed the first Internet worm. Zittrain, *supra* note 45, at 2003–05.

Wide Web page launched.[48] Finally, in April 1995, the National Science Foundation shifted control of the Internet to numerous private, regional networks.[49] Over the past fifteen years, the accessibility of the Internet has expanded exponentially—once available only on mainframe and desktop computers, it now is available on cell phones and handheld devices that are usable in any location.

Even at the early stages, however, the Internet was not the only computer network in use. There are multiple computer networks around the globe that were built using the same fundamental structure. International banks, federal reserves, intergovernmental organizations, nongovernmental organizations, and multinational corporations use many of these sister networks to transfer money and conduct international trade.[50] This interrelationship is quietly undermining national and international security, including that of the international financial system.[51]

In many ways, the Internet and its sister networks seem new on the scene. Thus, one might consider that cyberterrorism also is a new development. In some ways, however, the concepts of intelligence and of hacking have been around forever.

B. *A Brief History of Intelligence*

Although cyberterrorism is a relatively new topic of investigation, the underlying fundamentals have existed for centuries. In fact, the actions themselves have remained almost perfectly constant—it is the way in which those actions are executed and the motivation behind them that have changed.

The most significant aspect of constancy is that cyberterrorism is, in some ways, merely a new form of intelligence. Intelligence is a broad term that includes all methods of secret communications and methods to reveal those secret communications, such as spying,

---

48. The first world wide web page was launched on August 6, 1991 by Tim Berners-Lee. National Science Foundation, NSF and the Birth of the Internet—1990s, www.nsf.gov/news/special_reports/nsf-net/textonly/90s.jsp (last visited Jan. 4, 2010).

49. *See* National Science Foundation, A Brief History of NSF and the Internet, http://www.nsf.gov/news/special_reports/cyber/internet.jsp (last visited Jan. 4, 2010) (discussing the privatization conducted by the NSF).

50. *See, e.g.*, 2 JAMES W. CORTADA, THE DIGITAL HAND: HOW COMPUTERS CHANGED THE WORK OF AMERICAN FINANCIAL TELECOMMUNICATIONS, MEDIA AND ENTERTAINMENT INDUSTRIES 37 (2006) (discussing the use of electronic funds transfer systems in the banking industry); *see also* Zittrain, *supra* note 45, at 1975 ("[T]he Internet has been designed to serve both as a means of establishing a logical network and as a means of subsuming existing heterogeneous networks while allowing those networks to function independently—that is, both as a set of building blocks and as the glue holding the blocks together.")

51. *See* Zittrain, *supra* note 45, at 2003 (discussing the vulnerabilities of a decentralized Internet).

counterintelligence, and encryption[52] These concepts are so old that no one really knows when or where they originated. Many ancient societies, including those of Ancient Greece and Rome, developed methods of secret communication.[53] In the United States, encryption and other intelligence methods have been used since the days of the Founding Fathers.[54] Such methods are equally common today, though they have grown in complexity and acquired the umbrella term "intelligence."[55]

Signals intelligence is the type of intelligence that is most relevant with respect to the Internet and strategies for securing the

---

52. The term "encryption" refers to one of many possible ways to alter data so as to make it unintelligible to all but specified individuals. Many such methods currently exist, in various forms. Encryption methods are generally divided into two categories: "weak" and "strong." The two terms are rather self-explanatory—"weak" encryption is easily breakable, whereas "strong" encryption is difficult to solve. There is an important difference between "key length" and "bit length." A bit is "the most basic unit of computer data. It stores one of two possible states, represented by 0 or 1." Philip R. Zimmermann, *Cryptography for the Internet,* SCI. AM., Oct. 1998, at 110, 112, *available at* http://www.philzimmermann.com/docs/SciAmPRZ.pdf. The key is the sequence of random numbers used to encrypt a block of data, or a given number of bits. There is a direct correlation between the key size and the difficulty level of cracking the code. *Id.*

53. *See, e.g.,* SIMON SINGH, THE CODE BOOK 8–9 (2000) for a discussion of the existence of evidence that the Spartans used a system of secret writing called the *scytale* in 400 BC. (The scytale is a tool used to encrypt and decrypt messages whereby a strip of paper, leather, papyrus, etc., is wound around a rod and a message is written on it. When unwound, the strip of paper, etc., will contain a seemingly meaningless string of letters, enabling the message to be transmitted secretly. When the recipient wraps the paper around a rod of the same diameter, however, the message is easily read. Julius Caesar used a simple letter substitution method in his secret correspondence, which is now known as a Caesar cipher. Essentially, the alphabet is shifted by a certain number of letters, which is the key. For example, if the key were 5, the encoded alphabet used to write the message would be FGHIJ, etc., instead of ABCDE, etc.). *See also* JEFFREY HOFFSTEIN ET AL., AN INTRODUCTION TO MATHEMATICAL CRYPTOGRAPHY 1–2 (2008) (describing the Caesar cipher); SINGH, *supra,* at 48 (also describing use of the Caesar cipher).

54. *See, e.g.,* Rachel Emma Silverman, *Two Centuries On, a Cryptologist Cracks a Presidential Code,* WALL ST. J., July 2, 2009, at A.1, *available at* http://online.wsj.com/article/SB124648494429082661.html (describing the recent work of Lawren Smithline to solve a code sent by Robert Patterson to President Thomas Jefferson in 1801).

55. *See, e.g.,* CHARLES D. AMERINGER, U.S. FOREIGN INTELLIGENCE: THE SECRET SIDE OF AMERICAN HISTORY (1990) (distinguishing between three types of intelligence: human intelligence, otherwise known as human espionage or traditional spying; photographic intelligence; and signals intelligence, including hacking and encryption.); Norman J.W. Goda, *Tracking the Red Orchestra: Allied Intelligence, Soviet Spies, Nazi Criminals, in* RICHARD BREITMAN ET AL., U.S. INTELLIGENCE AND THE NAZIS 293 (2005) (discussing one example of human intelligence, the Soviet Rote Kapelle ("Red Orchestra"), a spy network that permeated German-occupied Europe in the early days of World War II); ROBERT F. KENNEDY, THIRTEEN DAYS: A MEMOIR OF THE CUBAN MISSILE CRISIS 23–25 (1962) (describing how photographic intelligence was important in the Cuban Missile Crisis of 1962, when American U-2 spy planes revealed the locations of Soviet missiles in Cuba).

Internet. It encompasses everything related to encoding communication, either human or electronic.[56] Almost every major power, including the United States, has used signals intelligence.[57] Historically, signals intelligence has played a critical role, especially on an international level.[58] In particular, the concept and practice of encryption and decryption has long played an integral role in U.S. foreign policy. For example, President Roosevelt and Secretary of State Cordell Hull used the MAGIC system of decoding Japanese communication transmissions during negotiations prior to the bombing of Pearl Harbor and thus were able to tailor their response to Japanese actions with the benefit of more complete information.[59]

In contrast to this aspect of constancy, the methodology and motivation behind the hacking and codebreaking that underlie cyberterrorism have changed significantly over time. First, the motivation behind such intelligence has changed. The original Hacker Ethic was a code of conduct "that championed the free sharing of information and demanded that hackers never harm the data they found."[60] That original Hacker Ethic is no longer the norm, however; cyberterrorism has become a serious threat to national and international security, as cyberterrorists seek to advance religious or political agendas. The methods of intelligence are also in transition. Instead of using Enigma machines, as in World War II, encryption is increasingly based upon complex mathematics and digital computer systems.[61] As a result, hacking is following suit, incorporating more technological aspects and fewer quintessentially human skills.[62]

---

56. *See* Judson Knight, *SIGINT (Signals Intelligence), in* ENCYCLOPEDIA OF ESPIONAGE, INTELLIGENCE, & SECURITY, http://www.espionageinfo.com/Se-Sp/SIGINT-Signals-Intelligence.html (last visited Jan. 4, 2010) (defining signals intelligence).

57. *See, e.g., id.* (describing the joint operation of signals intelligence, in the form of a communications intercept program, by the United States, United Kingdom, Canada, Australia, and New Zealand).

58. The "Berlin Tunnel" of 1955–1956, is an example of signals intelligence collection. The Berlin Tunnel was a joint wiretap undertaking by the United States and Great Britain of Soviet and East German communications, in which American and British intelligence services dug a tunnel below Berlin to tap directly into the telecommunications cables. *See, e.g.*, Caryn E. Neumann, *Berlin Tunnel, in* ENCYCLOPEDIA OF ESPIONAGE, INTELLIGENCE, & SECURITY, http://www.espionageinfo.com/Ba-Bl/Berlin-Tunnel.html (last visited Jan. 4, 2010) (describing use of the Berlin Tunnel by American and British intelligence to collect information from Soviet communications).

59. JONATHAN G. UTLEY, GOING TO WAR WITH JAPAN: 1937–1941, at 145, 151 (1985).

60. Stephen Stockwell, *We're All Hackers Now: Doing Global Democracy, in* THE ART OF SERIOUS PLAY. THE SERIOUS ART OF PLAY—CURIOSITY, CREATIVITY, CRAFT AND CONNECTEDNESS IN THE DIGITAL AGE: PROCEEDINGS OF THE CREATEWORLD 08 CONFERENCE 21, 24 (Michael Docherty & Darryl Rosin eds., 2008), *available at* http://www.auc.edu.au/myfiles/uploads/Training/CW08/CW08_Proceedings.pdf.

61. For the evolution of encryption, see generally SINGH, *supra* note 53.

62. *See, e.g., infra* notes 63–66 and accompanying text (describing the use of computers to attack websites).

In fact, intelligence methods actually are becoming less elegant. Brute force is becoming important in decrypting codes, as teams of computers, often connected by the Internet, combine forces to attempt to break the strongest encryption.[63] Cyberterrorists increasingly are using similar groups of computers and netbots to bombard websites in denial of service (DoS) attacks, which essentially are attempts to flood a website with so many requests that the website shuts down.[64] Similarly, a distributed denial of service (DDoS) attack involves the use of a large number of malware-infected computers, known as "zombies" or "bots," to simultaneously visit a website in an effort to flood the server and overwhelm it, causing it to shut down and deny access.[65] In a more advanced DoS or DDoS attack, cyberterrorists use electromagnetic interference in the form of current or voltage surges to destroy computer hardware.[66] This type of advanced DoS attack would be particularly effective against electrical grids and pipeline systems.[67] Cyberterrorists used the more basic type of DoS

---

63. *See, e.g.*, THOMAS CALABRESE, INFORMATION SECURITY INTELLIGENCE: CRYPTOGRAPHIC PRINCIPLES AND APPLICATIONS 266, 485 (2004) (discussing the use of brute-force attacks to break the encryption of passwords stored on a system).

64. *See, e.g.*, U.S. Computer Emergency Readiness Team, National Cyber Alert System, Cyber Security Tip ST04-015, Understanding Denial of Service Attacks, http://www.us-cert.gov/cas/tips/ST04-015.html (last visited Nov. 15, 2009).

> In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. The most common and obvious type of DoS attack occurs when an attacker 'floods' a network with information. When you type a URL for a particular web site into your browser, you are sending a request to that site's computer server to view the page. The server can only process a certain number of requests at once, so if an attacker overloads the server with requests, it can't process your request. This is a 'denial of service' because you can't access that site.

See also SCHELL & MARTIN, *supra* note 1, at 127 (describing the strategy of flooding).

65. *See, e.g.*, U.S. Computer Emergency Readiness Team, *supra* note 64.

> In a distributed denial-of-service (DDoS) attack, an attacker may use your computer to attack another computer. By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer. He or she could then force your computer to send huge amounts of data to a web site or send spam to particular email addresses. The attack is 'distributed' because the attacker is using multiple computers, including yours, to launch the denial of service attack.

See also BRENNER, *supra* note 12, at 1–3 (describing the use of zombie and bot programs); SCHELL & MARTIN, *supra* note 1, at 102 (describing the DDoS cyberattack).

66. *See* Geers, *supra* note 15 (explaining that critical infrastructure is connected to and dependent on the internet).

67. Tyler Williams, *Cyber Security Threats to Pipelines and Refineries*, PIPELINE & GAS J., Nov. 2007, http://www.oildompublishing.com/PGJ/pgjarchive/Nov07/cyber.pdf.

and DDoS attacks both against the United States and South Korea and in the attack against Estonia.[68]

III. THE THREATS TO NATIONAL AND INTERNATIONAL SECURITY POSED BY INTERNATIONAL DEPENDENCE ON THE INTERNET

The Internet is arguably the most significant development in the history of communications because it connects individuals, institutions, and everything in between to an unprecedented degree.[69] Dependence on information technology, especially the Internet, is increasing exponentially on both national and international levels. Cyberspace affects every aspect of daily life—from the most serious, such as linking networks of computers that control critical national infrastructure,[70] such as electric power grids and military infrastructure, to the most mundane, such as providing people's primary means of communication through platforms like e-mail, Facebook, and Twitter.[71] The Internet has become a global platform

---

68. *See, e.g.*, John Sudworth, *New "Cyber Attacks" Hit South Korea*, BBC NEWS, July 9, 2009, http://news.bbc.co.uk/2/hi/asia-pacific/8142282.stm (describing the attacks against the United States and South Korea). BRENNER, *supra* note 12, at 1–3 (noting that an estimated one million zombie computers were used in the attack on Estonia and further noting that, increasingly, this is a fairly average number).

69. The National Science Foundation says that "the Internet has changed our society in ways not seen since the invention of the printing press." National Science Foundation, *supra* note 37. Having had a hand in the creation of the Internet, however, it may be a bit biased.

70. The U.S. government defines "critical infrastructure" as "systems and assets, whether physical or virtual, so vital to nations that their incapacity or destruction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters." U.S. GOV'T ACCOUNTABILITY OFFICE, CONTINUED FEDERAL EFFORTS ARE NEEDED TO PROTECT CRITICAL SYSTEMS AND INFORMATION, GAO DOC. NO. GAO-09-835T, at 3 n.4 (2009).

71. *See* President Barack Obama, Remarks on Securing Our Nation's Cyber Infrastructure (May 29, 2009), http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/ (arguing that cyberspace is the foundation for "the classified military and intelligence networks that keep us safe"); GOV'T ACCOUNTABILITY OFFICE, CONTINUED FEDERAL EFFORTS ARE NEEDED TO PROTECT CRITICAL SYSTEMS AND INFORMATION, GAO DOC. NO. GAO-09-835T (noting the central place that information systems have in American infrastructure). *See also* Carafano & Sayers, *supra* note 20 ("Over the past quarter-century, the cyberspace domain has rapidly expanded to dominate almost every aspect of human interaction. Americans now depend on cyberspace more than ever to manage their banking transactions, investments, work and personal communication, shopping, travel, utilities, news and even social networking."); Hollis, *supra* note 12, at 1030 (noting the pervasiveness of the Internet).

for sharing information and for conducting global trade and investment with few limitations or filters.[72]

Unfortunately, the Internet also has become a global platform for cyberterrorism, which poses a direct threat to the national security of all states and, by extension, to international security. The Internet has become a key tool in terrorists' arsenals. Terrorists use the Internet to distribute propaganda, recruit and train new followers, and build and maintain virtual communities of terrorists.[73] People visit terrorist websites that glorify terrorist acts and host virtual training camps tens of thousands of times per day.[74] The Internet also enables terrorists to raise and transfer funds and to plan attacks.[75] Most importantly, the Internet provides cyberterrorists with a new target that arguably is bigger than any physical target. Without ever having to build a bomb or sacrifice themselves,[76] cyberterrorists can bring down the critical infrastructure of an entire state, disrupt the global economy, and instill fear and chaos among billions of people.

These threats are not new, however, nor are the government's attempts to recognize and respond to them. Almost from the moment the Internet became available to the public, the U.S. government recognized the importance of information networks and their potential to yield disastrous consequences. The White Paper on Information Infrastructure Assurance of December 1995 recognized that critical U.S. infrastructures such as the banking, credit, and Federal Reserve systems, and the stock exchanges each depend heavily on information networks like the Internet that are vulnerable to network-based attacks.[77] That same White Paper estimated that (admittedly underreported) U.S. business losses from cybercrimes

---

72. And, as will be discussed, disturbingly little security. Carafano & Sayers, *supra* note 20.

73. Raphael F. Perl, Head, Action Against Terrorism Unit, Org. for Sec. & Coop'n in Eur., Terrorist Use of the Internet: Threat, Issues, and Options for International Cooperation, Remarks at the Second International Forum on Information Security 2 (Apr. 7–10, 2008), *available at* http://www.osce.org/documents/cio/2008/04/30594_en.pdf.

74. *Id.*

75. *Id.*

76. It should be noted that some terrorists may be deterred from cyberterrorism specifically because it does not offer the opportunity for self-sacrifice and, therefore, martyrdom. Regardless, the threat of cyberterrorism remains severe, as demonstrated by incidents to date. Furthermore, prosecution under universal jurisdiction may have an even stronger deterrent effect on those motivated by martyrdom, as the cyberterrorist likely will have few such opportunities while in prison. *But see* Bradley K. Ashley, Anatomy of Cyberterrorism: Is America Vulnerable? 22 (Feb. 27, 2003) (unpublished manuscript, on file with the U.S. Air Force), *available at* http://www.au.af.mil/au/awc/awcgate/awc/ashley.pdf (arguing that the absence of suicide missions is one incentive of sustained cyberterror operations).

77. U.S. SEC. POLICY BD., FED'N OF AM. SCIENTISTS, WHITE PAPER ON INFORMATION INFRASTRUCTURE ASSURANCE (1995), http://www.fas.org/sgp/spb/whitepap.html.

totaled $5 billion in 1995.[78] As a result, the Clinton administration created the Presidential Commission on Critical Infrastructure Protection and the Presidential Information Technology Advisory Council, among other similar committees.[79]

The second Bush administration also took several actions against cyberterrorism. Former President George W. Bush created the Department of Homeland Security, which was tasked with (among other things) cybersecurity.[80] In February 2003, the White House released the National Strategy to Secure Cyberspace, which was intended to "provide[] a framework for protecting this infrastructure that is essential to our economy, security, and way of life."[81] Little from the National Strategy was implemented, however, in part because the administration could not agree on how to structure the authorization to do so and in part because it was determined that the administration did not have sufficient credibility or political capital to do so.[82] On January 8, 2008, the Bush

---

78. *Id.* Those, of course, were the halcyon days; losses today are exponentially higher. *See Digital Warriors: Professor Pens Book About The New Battlefield—Cyberspace*, REUTERS, Apr. 23, 2009, http://www.reuters.com/article/pressRelease/idUS181528+23-Apr-2009+PRN20090423.

> 'In 2004, the Federal Bureau of Investigation estimated that cybercrime cost U.S. citizens about $400 billion, and in July 2007 FBI Director Robert Mueller said he believes only about one-third of cybercrime in the U.S. is actually reported to the FBI,' Brenner said. 'I have heard cybercrime estimates are much, much higher than the figure cited for 2004 . . . . It will continue to increase until governments begin to create realistic disincentives for cybercriminals.'

79. U.S. Department of Justice, Computer Crime and Intellectual Property Section (CCIPS), Critical Infrastructure Protection, http://www.usdoj.gov/criminal/cybercrime/critinfr.htm (last visited Nov. 15, 2009).

80. *See generally* Exec. Order No. 13,228, 66 Fed. Reg. 51,812 (Oct. 10, 2001) (establishing the Office of Homeland Security and charging the organization with protection of information systems); Exec. Order No. 13,260, 67 Fed. Reg. 13,241 (Mar. 21, 2002) (providing for implementation of information security measures); Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002) (creating the department). The National Cybersecurity Division of the Office of Cybersecurity and Communications "works collaboratively with public, private and international entities to secure cyberspace and America's cyber assets." U.S. Department of Homeland Security, National Cybersecurity Division, Mission, http://www.dhs.gov/xabout/structure/editorial_0839.shtm (last visited Jan. 4, 2010).

81. THE WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE 4 (2003), *available at* http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf.

82. David E. Sanger, John Markoff & Thom Shanker, *U.S. Steps Up Effort on Digital Defenses*, N.Y. TIMES, Apr. 27, 2009, at A1, *available at* http://www.nytimes.com/2009/04/28/us/28cyber.html. Indeed, the Cyberspace Policy Review published by the Obama administration recognizes up front that the United States still "needs a strategy for cybersecurity designed to shape the international environment and bring like-minded nations together on a host of issues, such as technical standards and acceptable legal norms regarding territorial jurisdiction, sovereign responsibility, and the use of force." THE WHITE HOUSE, CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS

administration established the Comprehensive National Cybersecurity Initiative (CNCI) through Homeland Security Presidential Directive 23 and National Security Presidential Directive 54.[83] The CNCI was an effort to identify current and emerging cyber threats, protect vulnerable infrastructure, and determine how to respond to cybercriminals.[84]

The Obama administration has acknowledged, perhaps more adroitly than the previous administrations, the threat that cyberterrorism poses to U.S. and global infrastructures. As President Obama said, cybersecurity is

> a matter of public safety and national security. We count on computer networks to deliver our oil and gas, our power and our water. We rely on them for public transportation and air traffic control. Yet we know that intruders have probed our electrical grid and that, in other countries, cyber attacks have plunged entire cities into darkness. Our technical advantage is a key to America's military dominance. But our defense and military networks are under constant attack. Al Qaeda and other terrorist groups have spoken of their desire to unleash a cyber attack on our country—attacks that are harder to detect and harder to defend against. Indeed, in today's world, acts of terror could come not only from a few extremists in suicide vests but from a few keystrokes on the computer—a weapon of mass disruption.[85]

Similarly, the head of the National Security Agency, Lieutenant General Keith Alexander, described cyberspace as "the new national security frontier."[86]

These critical infrastructures, and all who depend upon them, are plagued by a very serious problem: these technological media are historically insecure. The combination of the world's dependence on technology with the fallibility of such systems has profound effects on the state of national and international security. As global financial markets increasingly rely upon information technology to operate on

---

INFRASTRUCTURE iv (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

83. Each of those Presidential Directives is classified. *See* JOHN ROLLINS & ANNA C. HENNING, COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE: LEGAL AUTHORITIES AND POLICY CONSIDERATIONS, CONG. RESEARCH SERV. DOC. NO. R40427, at 1 (2009), *available at* http://www.fas.org/sgp/crs/natsec/R40427.pdf ("The Homeland Security Presidential Directive 23 and National Security Presidential Directive 54 establishing the CNCI are classified."). *See also* Press Release, U.S. Dep't of Homeland Sec., Fact Sheet: Protecting Our Federal Networks Against Cyber Attacks, Apr. 8, 2008, http://www.dhs.gov/xnews/releases/pr_1207684277498.shtm (stating that the directive formalized continuing efforts to protect federal information systems from attack).

84. ROLLINS & HENNING, *supra* note 83, at 2.

85. President Barack Obama, *supra* note 71. *See also Obama Creates Top Job for Guarding Online Security: Speech by U.S. President Barack Obama* (CNN Internet broadcast May 29, 2009), *available at* http://edition.cnn.com/2009/POLITICS/05/29/cyber.czar.obama/index.html#cnnSTCVideo (detailing the threat of cyber terrorism).

86. *Pentagon to Create Cyber-Defense Command, supra* note 17.

even the most basic level, their interconnectedness and vulnerability are becoming ever more salient.[87]

As will be explained in detail, the Internet poses a three-pronged threat to national and international security. The clearest manifestation of this threat is the capacity to exploit an inherent weakness in the structure of the Internet to "island-hop," or jump from computer to computer and network to network, accessing more critical data and more vulnerable networks.[88] This easily can be accomplished once an attacker has "spoofed" his or her way onto a network.[89] As a result of the structure of the Internet and related networks, cyberterrorists can gain access to systems and networks that are not necessarily considered vulnerable. Second, the Internet is utterly incapable of protecting information from sufficiently persistent and knowledgeable cyberterrorists. Finally, the Internet provides cyberterrorists with the tools that they need to carry out direct attacks on the Internet and use the Internet as a springboard to attack other networks.

In fact, the insecurity of the Internet and its sister networks is such that a cyberterrorist with enough knowledge and the right tools can bring the entire system crashing down.[90] This looming danger is related to the very accessibility that makes the Internet revolutionary because, increasingly, key aspects of critical public infrastructure are connected or accessible via the Internet. In the United States, "[v]irtually all federal operations are supported by computer systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions, deliver services to the public,

---

87. Diffie and Landau explain the trend toward an increasing dependency on information technology for conducting business:

> The rising importance of intellectual property has expanded the role of electronic communications in business . . . A larger and larger fraction of our commerce is in information, so delivery of goods and services by electronic media is becoming more and more common. To support this delivery, the media themselves are becoming more unified, (which is) commonly referred to as the development of a 'Global Information Infrastructure.'

WHITFIELD DIFFIE & SUSAN LANDAU, PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION 5 (1998).

88. This is discussed in greater detail in Part IV.A *infra*.

89. Spoofing is defined as the "appropriation of an authentic user's identity by non-authentic users, causing fraud or attempted fraud, in some cases, and causing critical infrastructure breakdowns in other cases. Spoofing can also target nonuser-based entities. For instance, an IP address can be spoofed to appropriate the identity of a server and not a human (user)." SCHELL & MARTIN, *supra* note 1, at 298.

90. For a more technical explanation of the fundamental insecurity than is provided in this article, *see generally* Steven T. Bellovin, *A Look Back at "Security Problems in the TCP/IP Protocol Suite,"* Dec. 2004, http://www.cs.columbia.edu/~smb/papers/ipext.pdf (outlining the vulnerabilities of TCP interfacing).

and account for their resources without these cyber assets."[91] As a result, ineffective security controls can expose a broad array of government operations and assets to significant risk, including the threat that critical infrastructure could be disabled.[92] Ironically, the necessary knowledge and tools are readily available on the Internet.

There is no good outcome to cyberterrorist attacks. The best-case scenario would involve damage limited to bad publicity and international embarrassment because government websites were hacked. The seemingly inevitable worst-case scenario includes the theft of classified information, the collapse of the international financial system, major breaches of national and international security and, potentially, war.[93]

A. *Jumping from Network to Network – The Fundamental Insecurity of the TCP/IP Protocol*

The first and most glaring threat is the fundamental lack of security incorporated into the TCP/IP Protocol suite, the structure upon which the Internet is based. The TCP/IP Protocol essentially serves as the "language" of cyberspace—it is the technology by which information moves from computer to computer and server to server.[94] When the Internet was born at the height of the Cold War, only divisions of the government had access to the system.[95] As a result, the early Internet did not need to be secure; indeed, by being connected to the system, a computer was presumed to be secure.[96] The only goal was to make communication between those government agencies as easy and as immediate as possible. As a result, the very framework on which the Internet is built, the TCP/IP Protocol, is inherently insecure.[97]

The primary insecurity of the TCP/IP Protocol is that it allows access to other networks also based on the TCP/IP Protocol. This insecurity opens the Internet, and any network or computer

---

91. GOV'T ACCOUNTABILITY OFFICE, CONTINUED FEDERAL EFFORTS ARE NEEDED TO PROTECT CRITICAL SYSTEMS AND INFORMATION, GAO DOC. NO. GAO-09-835T, at 2 (2009).

92. *Id.*

93. Some might say that this position is naïve, that we already are in a state of information warfare, and that of course many of the attacks come from foreign governments. *See generally* DOROTHY DENNING, INFORMATION WARFARE & SECURITY 62–76 (1999) (chronicling the current uses of information warfare in state-sponsored international conflict). Although this may be true from a policy perspective, from a legal perspective an act of aggression or use of force has significant consequences.

94. *Id.* at 16.

95. National Science Foundation, *supra* note 37.

96. *See* HAFNER & MARKOFF, *supra* note 38, at 278–79 (portraying the early Arpanet as an intimate and insular community of elite scientists).

97. SCHELL & MARTIN, *supra* note 1, at 311 (noting that the TCP/IP Protocol is "known for its lack of security on many of its layers").

connected to it, to a number of security threats that cannot be solved with encryption alone.[98] The TCP/IP Protocol operates by a sequence of communications between the sending computer or network and the receiving computer or network, known as a "three-way handshake."[99] Essentially, Computer 1 tells Computer 2 that it wants to communicate. Computer 2 responds that it is willing to communicate. Computer 1 then sends Computer 2 a message confirming that they are going to communicate.[100]

Theoretically, this process must be followed completely in order to open a connection, but there is a process error in the way TCP operates. "If two connections are opened in a short time, many TCP stacks pick the initial sequence number for the second connection by adding some constant to the sequence number used for the first."[101] An attacker can easily exploit this common system error, especially if he or she has already spoofed (i.e., faked) a user's login name and password and can thus use them to open a legitimate connection to the network. Once that connection is open, he or she can note the sequence number used and then use it to send the third message to the network and open a new, anonymous connection whereby he or she can attack undetected.[102] The attacker can then jump, not only from computer to computer, but from network to network, which is known as "island-hopping."[103] With determination and a bit of luck, the criminal can find a "back-door" into a network and cause significant damage, especially if his or her actions go undetected.[104] This type of springboard attack is possible with any network based on the TCP/IP Protocol.[105] Thus, networks that are thought to be

---

98. The U.S. government recognizes this insecurity. *See, e.g.*, GAO DOC. NO. GAO-09-835T, *supra* note 70, at 2 ("Computer resources could be used for unauthorized purposes to launch attacks on other computer systems.")

99. *See* SCHELL & MARTIN, *supra* note 1, at 319–20 (describing the operations of TCP/IP Protocol).

100. *See id.* (using "Alice" as Computer 1 and "Bob" as Computer 2).

101. Steve Bellovin, *Network and Internet Security, in* INTERNET BESEIGED: COUNTERING CYBERSPACE SCOFFLAWS 117, 122 (Dorothy E. Denning & Peter J. Denning eds., 1997).

102. *Id.*

103. SCHELL & MARTIN, *supra* note 1, at 183–84 (defining "island-hopping" as "crack[ing] one system and then us[ing] it as a 'launching pad' for cracking other systems").

104. *Id.*

105. *See* U.S. Computer Emergency Readiness Team, National Cyber Alert System, Technical Cyber Security Alert TA04-111A, Vulnerabilities in TCP, http://www.us-cert.gov/cas/techalerts/TA04-111A.html ("Since the TCP/IP Initial Sequence Number vulnerability (VU#498440) has been proven more viable of an attack, any services or sites that rely on persistent TCP sessions could also be affected by this vulnerability.") (last visited Jan. 4, 2010); John McCormick, *TCP Reset Spoofing a Serious Flaw With Routers: Protect Yourself*, TECH. REPUBLIC, May 3, 2004, http://articles.techrepublic.com.com./5100-10878_11-5201771.html (noting the vast extent of TCP vulnerability).

separate and therefore secure because they are not connected to the Internet may not be as safe as originally thought.

The infamous 1994 infiltration of the Citibank system by Russian hackers who penetrated the Citicorp electronic banking system used by corporate customers for electronic funds transfers illustrates the feasibility of this springboard tactic.[106] Having somehow acquired the proper authorization, the hackers obtained the identification numbers and passwords for the accounts of three banks.[107] They then dialed into Citicorp's network from an office in St. Petersburg and transferred over $10 million to their own accounts.[108] Similarly, in 1995 and 1996, an attacker from Argentina hacked into a U.S. university system and used that as a springboard to computer networks at the Naval Research Laboratory, NASA, and Los Alamos National Laboratory that contained sensitive research information regarding weapons and command and control systems.[109] Though these may not have been considered examples of cyberterrorism, it is easy to see how these actions could be taken for the purpose of destabilizing governments and/or the international financial system.

This ability to use the Internet as a springboard creates an entirely different type of problem. Protecting one company's network and the information therein is in and of itself an extremely difficult task; protecting the entire Internet and the myriad of networks that may or may not be connected to it is much more complex. Indeed, as the most salient problems lie in the very design and foundation of the Internet itself, such problems are almost impossible to solve. This threat is severe and significantly worse than most people realize.

B. *Direct Attacks on the Internet*

The Internet's second major insecurity is that, due to its inherently insecure structure, it is vulnerable not just as a springboard for jumping from network to network but to other types of cyberattacks as well. Cyberterrorists can attack the Internet itself using DoS or DDoS attacks, shutting down critical infrastructure or launching any number of other attacks.[110] Although encryption has long been touted as the blanket solution to the security of the

---

106. DENNING, *supra* note 93, at 55–56.

107. *Id.*

108. *Id.*

109. U.S. GOV'T ACCOUNTABILITY OFFICE, INFORMATION SECURITY—COMPUTER ATTACKS AT DEPARTMENT OF DEFENSE POSE INCREASING RISKS, GAO DOC. NO. GAO/AIMD-96-84, at 25 (1996).

110. *See generally* Richard Garnett & Paul Clarke, *Cyberterrorism: A New Challenge for International Law*, *in* ANDREA BIANCHI & YASMIN NAQVI, ENFORCING INTERNATIONAL LAW NORMS AGAINST TERRORISM 465 (2004) (describing various ways terrorists target the internet).

Internet, even strong encryption is inadequate to solve such a complex problem.[111] Many types of attacks still can be carried out, including eavesdropping, password sniffing, data modification, Trojan horses,[112] and spoofing. Although some of these types of attacks have been longstanding, such as eavesdropping, spoofing, and Trojan horses, they remain relevant: for example, Trojan horses were used in the Titan Rain attacks.[113] Encryption alone has not eliminated these grave threats.[114]

"Eavesdropping" is exactly what it sounds like: a third party "listens in" on the communications of two parties with neither the knowledge nor the consent of either party.[115] This is usually done with a packet sniffer,[116] which is a program for monitoring network packets of information that come to and from a particular computer. Usually, a computer on a local-area network (LAN) will only receive packets of information that are addressed specifically to it, but with some LAN technologies, it is possible to operate the modem, router, or other network interface in "promiscuous mode,"[117] which allows the computer to receive all incoming information, regardless of whether or not it is properly addressed to that computer.[118]

Password sniffing is also done with a packet sniffer, but whereas the goal of eavesdropping is to gain access to particular information, the goal of password sniffing is to acquire log-in names and passwords that can be used to gain direct access to other computers.[119] This can be even more dangerous, because by using this login information, a cyberterrorist not only has access to all files on that computer but also would have access to the entire network to which that computer belongs.

Both eavesdropping and password sniffing are relatively low-level attacks, in that they attempt to gain access to information but not to modify it. Data modification, also known as tampering, is the unauthorized modification of data or software on a computer or network.[120] Attacks of this type are particularly serious when the perpetrator is able to obtain root access to the network, which gives the attacker the power to issue any command and to alter or delete any information on the system.[121] This can result not only in

---

111. DENNING, *supra* note 93, at 309–10.
112. *See* SCHELL & MARTIN, *supra* note 2, at 328-29 (defining "Trojans").
113. Carafano & Sayers, *supra* note 20.
114. DENNING, *supra* note 93, at 309-10.
115. *See* SCHELL & MARTIN, *supra* note 1, at 107 (defining "eavesdropping").
116. *See id.* at 292 (defining "packet sniffer").
117. *See id.* at 255–56 (defining and describing "promiscuous mode network interface").
118. *Id.*
119. DENNING, *supra* note 93, at 184.
120. *Id.* at 151.
121. *See* SCHELL & MARTIN, *supra* note 1, at 273 (defining "root").

information being changed, such as the destination account number for an electronic funds transfer, but also in computer or network shut-down, such as a major electricity grid. Due to the availability of specialized hacking tools, obtaining root access to a system, and therefore affecting critical infrastructure, is relatively easy.

Spoofing attacks are concentrated on impersonating a particular user or computer, usually in order to launch other types of attacks.[122] Spoofing is often committed in connection with password sniffing; after obtaining a user's log-in and password, the spoofer will log in to the computer and masquerade as the legitimate user. The cyberterrorist typically does not stop there, instead using that computer as a bridge to another, hopping in this fashion from computer to computer. This process, called "looping," effectively conceals the spoofer's identity, especially because he or she may have jumped back and forth across various national boundaries.[123]

Even more disturbing is the possibility of misleading entire governments into believing that another, potentially hostile government is attempting to infiltrate its networks. Imagine that a cyberterrorist perpetrates an attack on the network maintained by the U.S. Treasury and steals millions of dollars, transferring the money to his own account to be used for funding further terrorist activities.[124] He has used the spoofing technique, however, which causes the U.S. government to believe the Russian government to be behind the attack and to accuse them of the attack. The Russian government denies the accusation and is insulted at the seemingly unprovoked hostility. Tensions between the governments escalate and boil over, potentially resulting in war. Though this may be only a hypothetical example, it is frighteningly plausible. In fact, it may have been used in the attacks on U.S. and South Korean websites—the South Korean government initially was so certain that North Korea was behind the attack that it publicly accused the North Korean government, despite already tense relations.[125] Similarly, in the 2007 attack on Estonia, Estonian authorities were so certain that the Russian government was behind the attack that they not only publicly accused them but requested military assistance from NATO in responding to the attack.[126] It was later determined that Russia was not behind the attack and that at least some of the attackers were located in Brazil and Vietnam.[127]

---

122. *See id.* at 298 (defining "spoofing").

123. DENNING, *supra* note 93, at 218.

124. *See* BRENNER, *supra* note 12, at 41 n.144 (noting that terrorists have secondary financial agendas).

125. *See, e.g.*, Williams, *supra* note 10 (illustrating the confusion felt by American officials when tracing hackers who used looping techniques).

126. BRENNER, *supra* note 12, at 133.

127. BRENNER, *supra* note 12, at 5–6, 133.

Another possibility exists, however, which is even more disturbing due to its more subversive nature. In the previous example, only certain actors' identities were altered. Imagine, however, that the attacker presents the victim with an alternative version of the entire Internet, tricking the victim into using the false interface without knowing that he or she is giving his or her attacker valuable information, such as log-in names, passwords, and account numbers. Researchers at Princeton University have shown how the entire Internet can be spoofed by intercepting all web traffic to and from a victim, showing the victim an edited version, and squirreling away the victim's passwords.[128] Encryption actually harms the victim in this situation because it effectively establishes a secure channel to the attacker's computer.[129] As described by Professor Susan Brenner, cyberterrorists could then use the false website to make bomb threats of other similarly disruptive threats, causing evacuation of entire cities; mass chaos; potential death and destruction; and almost certain erosion of public confidence in the government, without even having to build a bomb.[130]

C. *The Internet As Hacker's Toolbox*

The third way the Internet threatens national and international security is its use as a resource to find and acquire the tools needed to attack separate networks. The Internet essentially functions as a free, communal toolbox, providing hackers and cyberterrorists with software, commands, and other tools.[131] In fact, many of the programs used to locate and exploit the vulnerabilities of a particular computer or network are available free for download from publicly accessible websites and require little technical knowledge to implement.[132] Simply putting "hacker tools" into any search engine yields thousands of websites ready to provide the information.[133] Thus, not only are transactions, research, and other actions taken through the Internet insecure, but the Internet provides the very keys used to commit acts of cyberterrorism.

---

128. DENNING, *supra* note 93, at 265.

129. *Id.*

130. *See* BRENNER, *supra* note 12, at 46–47 (describing such a potential attack on the San Francisco Bay Area Rapid Transit system).

131. DENNING, *supra* note 93, at 206–7.

132. *Id. See also* Carolyn Meinel, *Appendix A: How Do Hackers Break Into Computers?*, *in* SCHELL & MARTIN, *supra* note 2, at 373, 373–80 (discussing various ways that hackers break into computers).

133. When the Author ran this search in Google, it yielded approximately 44,900,000 results.

D. *The Particular Vulnerability of Networks in the International Financial System*

Threats to the international financial system constitute one of the more serious threats posed by cyberterrorism.[134] This threat is so salient largely due to the ease of jumping from the Internet to the networks of the international financial system. Most of those aspects of the international financial system that do not operate via the Internet use separate networks that are based on the same protocol as the Internet—the TCP/IP Protocol. As a result of the inherent insecurity of the TCP/IP Protocol, as discussed, it is remarkably easy to attack any network that is based on that protocol.

The international financial system is such a large target for cyberterrorists because of the substantial rewards that cyberterrorists stand to gain—from stealing large amounts of money to fund other terrorist acts, to crushing the global economy by shutting down the international financial system,[135] to more subtly affecting international markets by eroding consumer confidence. As Mike McConnell, the former Director of National Intelligence, succinctly stated, "what backs up [international markets] is confidence—an accounting system that is reconcilable."[136] By crashing stock markets and eroding consumer confidence in banks, cyberterrorists could effectively recreate the global economic crisis through which the world has been suffering for the past year. Indeed, as Mr. McConnell warned former President George W. Bush, if even one large American bank were successfully attacked, "it would have

---

134. The international financial system is a complex system of controlling trade and investment, and can be construed very loosely to incorporate everything and anything dealing with money. For the purposes of this article, the term refers primarily to the international banking sector and the international investment and trade industries, especially the electronic fund transfers that are integral to these sectors of the international financial system. The word "international" could easily be omitted without altering the meaning, as these aspects of the global economy are inherently international, and have been almost since their inception.

135. Perl, *supra* note 73, at 2–3.

> [C]yber terrorism could also aim at inflicting economic costs, at times where communications and information exchange is essential to the functioning of our societies and to the global economic system. A central goal of Al-Qaeda inspired terrorists is to cause economic damage, not only physical damage. Increasingly therefore, I am convinced that communication networks are likely to become the target of terrorist cyber attacks seeking to paralyze our societies and economies.

Id.

136. Sanger, Markoff, & Shanker, *supra* note 82.

an order-of-magnitude greater impact on the global economy" than that of the attacks on September 11, 2001.[137]

The Internet poses a serious security threat to the international system. First, as a result of their similar construction, it is possible to "island-hop" from the Internet to the parallel VANs (value-added networks) used by the international financial system. Cyberterrorists would be able to access the networks on which the international financial system is based by exploiting the common structure of both the Internet and the separate networks over which most banks and clearing houses of the international financial system do not send electronic fund transfers. Once a cyberterrorist has established a connection on one of the systems, he or she can exploit the weakness in the TCP/IP Protocol to "jump" to the other. As sensitive information is accessible via the Internet, it is feasible that cyberterrorists could gain access to the information and use it to the detriment of the entire global economy.

One of the more important systems of the international financial system, due to the volume of daily transactions, is Fedwire, operated by the U.S. Federal Reserve System. In 2008, Fedwire processed an average of approximately 521,000 payments, with an average value of approximately $ 2.7 trillion, each day.[138] Another key system is the Clearing House Interbank Payment System (CHIPS), founded by some of the largest commercial banks,[139] which processes over $2 trillion each day.[140] Since at least 2005, CHIPS has been available via the TCP/IP Protocol, opening it up to the kind of network-to-network jumping attacks described above.[141] Electronic Data Interchange (EDI),[142] a separate network that also is based on the

---

137. *Id.*

138. FEDERAL RESERVE BD., FEDWIRE FUNDS TRANSFER SYSTEM: ASSESSMENT OF COMPLIANCE WITH THE CORE PRINCIPLES FOR SYSTEMICALLY IMPORTANT PAYMENT SYSTEMS 10 (2009), *available at* http://www.federalreserve.gov/paymentsystems/files/fedfunds_coreprinciples.pdf.

139. CHIPS is "a privately operated, real-time multilateral payments system typically used for large dollar payments . . . The payments transferred over CHIPS are often related to international interbank transactions." FED. FIN. INST. EXAMINATION COUNCIL, WHOLESALE PAYMENT SYSTEMS IT EXAMINATION BOOKLET 5 (2004), *available at* http://www.ffiec.gov/ffiecinfobase/booklets/Wholesale/whole.pdf.

140. The Clearing House, About CHIPS, http://www.chips.org/about/pages/033738.php (last visited Jan. 4, 2010).

141. *CHIPS Private Network- Live!*, CHIPS NEWS BRIEFS (The Clearing House Payments Co., LLC, New York, NY), Nov. 2005, at 4, *available at* http://www.chips.org/reference/docs_newsBriefs/001338.pdf.

142. The National Institute of Standards and Technology defines EDI as "the computer-to-computer interchange of strictly formatted messages that represent documents other than monetary instruments." NAT'L INST. OF STANDARDS & TECH., FED. INFO. PROCESSING STANDARDS PUBL'N NO. 161-2, ANNOUNCING THE STANDARD FOR ELECTRONIC DATA INTERCHANGE (EDI) para. 3.1 (1996), *available at* http://www.itl.nist.gov/fipspubs/fip161-2.htm. EDI is supplemented by the Financial Electronic Data Interchange (FEDI), a similar network entirely devoted to financial

TCP/IP Protocol, is used extensively by companies to transfer business documents such as purchase orders and invoices, using separate dedicated networks. Web-based EDI (i.e., EDI that has been connected to the Internet) enables electronic commerce, typically using the Hyper Text Transfer Protocol Secure (HTTPS).[143] Each of these fundamental networks of the international financial system, due to their similar structure to the Internet, is inherently vulnerable to a "jumping" attack.

Although international banks do not often publicize cyberattacks, "banks send federal regulators some 600,000 alerts a year about potentially suspicious withdrawals, deposits, transfer, and money laundering."[144] Indeed, the Chief Security Officer of "a major New York-based financial house" admitted that his company had been attacked one million times in a single day.[145] President Obama recently used the example of the incident in 2008 in which "thieves used stolen credit card information to steal millions of dollars from 130 ATM machines in 49 cities around the world—and they did it in just 30 minutes."[146] This has been going on for decades.[147] As described above, it is easy to see how cyberterrorists can destabilize the international financial system and, therefore, the world economy.

A second major security threat is the potential for a direct attack on those aspects of the international financial system that are directly connected to the Internet, such as Web-based EDI. Information sent via the Internet is inherently insecure, and international banks cannot guarantee that their information is not being spied upon, stolen, tampered with, or replaced altogether. For example, if a cyberterrorist discovered a "back-door" to an on-line brokerage site, he or she could alter the data and set off a run on the market by dumping massive amounts of shares at the newly altered higher prices.[148] Given the current volatility of international

---

transactions and utilized not only by individual banks and corporations, but also by the U.S. and other governments.

143. When making a purchase via the Internet, you may notice that the address changes from "http://" to "https://"—this is indicating that the protocol on which you are viewing the webpage has changed from the Hyper-Text Transfer Protocol to the Hyper-Text Transfer Protocol Secure—a (theoretically) more secure protocol in order to protect consumer information that often uses the Secure Sockets Layer protocol. The Secure Sockets Layer is based on the TCP/IP Protocol, however, and therefore all of the insecurities described herein, including "island-hopping" (jumping from network to network), apply there as well. *See* SCHELL & MARTIN, *supra* note 1, at 281–82 (defining and describing "Secure Sockets Layer" and "Secure Transactions").

144. De Borchgrave, *supra* note 19 (noting that "Cyberheists have netted billions for cybercrooks.").

145. *Id.*

146. President Barack Obama, *supra* note 71.

147. *See supra* p. 80 for discussion of the 1994 attack on Citicorp.

148. A "back door," aka "trap door," is a software shortcoming that is either part of the software program or added to a software program by a hacker that allows access

financial markets, this could potentially trigger a domino-effect across the major financial markets and a devaluation of the entire global economy.

These possibilities have political ramifications as well. It is not necessary for the individual to have access to data for the entire international market; if he or she were able to tamper with the reports of a single influential country, like Japan or the United States, the economic impact could begin a ripple effect that would be felt throughout the international economy. This could have potentially destabilizing effects on foreign relations, especially concerning sensitive economic issues.

Furthermore, despite the unresolved security threats faced by the international financial system, an overall lack of awareness continues to render those institutions extremely vulnerable to attack. Many network administrators either do not understand the nature of the problem or do not believe that their particular systems are insecure.[149] Neither states nor individual members of the international financial system can afford to remain so unaware, however, of the serious threat to national and international security posed by the Internet. This consideration must be factored into the discussions that are beginning to take place.

Finally, entities must recognize that these problems are permanent. Though security measures are continually improved, so, too, is the arsenal deployed by those who would compromise that security. As described by Denning,

> 100% security is neither possible nor worth the price. Computer systems are tremendously complex, containing millions of lines of code. No single person can comprehend that much code well enough to confirm that it is free of security holes or hidden trapdoors. . . . The goal is risk management, not risk avoidance at all cost.[150]

Furthermore, increased security often means less flexibility, ease of use, and interoperability. Thus, difficult choices must be made regarding security—decisions that require consideration of many factors. It is no longer a question of whether to act, however, or even when to act, because time is of the essence. Accordingly, the remaining question is what actions can be taken to protect national and international security.

---

to a computer system. *See* SCHELL & MARTIN, *supra* note 1, at 27–28 (describing these software features).

149. *See* Robert Lemos, *DNS Hack Leaves Corporate Networks Wide Open*, SILICON.COM, Aug. 2, 2004, http://software.silicon.com/security/0,39024655,39122803,00.htm (describing one such example of a problem that network administrators are not aware of that leaves their networks vulnerable to attacks by hackers).

150. DENNING, *supra* note 93, at 12.

IV. ATTEMPTS AT PREVENTION: LAWS, POLICY AND TECHNOLOGY

In an effort to counter the seemingly endless array of available methods by which cyberterrorists can infiltrate computer networks, governments, international organizations, and private industry have taken a number of steps over the years in the areas of law, policy and technology to protect information and prevent cyberterrorism, including entering into a multilateral convention, passing domestic laws, and adopting international technological standards. These steps toward international cooperation are important and should be continued.[151] None of these steps, however, is capable of completely securing the Internet.

A. *Laws and Policy*

States and international organizations are increasingly recognizing that international cooperation is key to addressing cyberterrorism.[152] The United States has done much to address cyberterrorism, although the government admits that more is needed.[153] International organizations, including the European Union, NATO, the United Nations, and the OSCE, among others, have taken important legal and policy steps to address cybersecurity.[154] These are just the beginning steps, however, in attempting to protect national and international security.

1. U.S. Domestic Efforts

On the domestic side, the U.S. government recently has taken a number of steps to attempt to secure cyberspace. At a minimum, these actions recognize the threat to national and international security posed by the Internet and by cyberterrorism and are a starting point for resolving those insecurities.

First, even before the attacks on the U.S. and South Korean governments, the Obama administration brought new focus to the issues of cyber crime and cyberterrorism by promising to appoint a "cyber czar" and by issuing the Cyberspace Policy Review, a comprehensive report on the status of cybersecurity in the United

---

151. Perl, *supra* note 73, at 2–3.

152. *Id.*

153. *See* THE WHITE HOUSE, *supra* note 82, at iii–iv ("While efforts over the past two years started key programs and made great strides by bridging previously disparate agency missions, they provide an incomplete solution".).

154. *See infra* Part IV.A.2 (discussing the steps taken by such international organizations).

States from a national security perspective.[155] The Cyberspace Policy Review recognized up front that the United States still "needs a strategy for cybersecurity designed to shape the international environment and bring like-minded nations together on a host of issues, such as technical standards and acceptable legal norms regarding territorial jurisdiction, sovereign responsibility, and the use of force."[156] In the opening pages of that report, the U.S. government acknowledged that

> [t]he architecture of the Nation's digital infrastructure, based largely on the Internet, is not secure or resilient. Without major advances in the security of these systems or significant change in how they are constructed or operated, it is doubtful that the United States can protect itself from the growing threat of cybercrime and state-sponsored intrusions and operations.[157]

Although the Obama administration may be the first to state the problem in such categorical terms, it is by no means the first government or international organization to attempt to address the issue.[158]

Congress, too, has been active. Congress passed the well-known USA PATRIOT Act, the stated intent of which was to deter and punish terrorists.[159] Congress also passed the Cyber Security Enhancement Act of 2002 as part of the Homeland Security Act of 2002.[160] Senator John Rockefeller recently introduced Senate Bill 773, styled as "The Cybersecurity Act of 2009."[161] The Act would have potentially far-reaching effects, including directing the President to establish or designate a Cybersecurity Advisory Panel.[162] The Act also would require the Department of Commerce to "serve as the clearinghouse of cybersecurity threat and vulnerability information" and to "develop and implement a system to provide cybersecurity status and vulnerability information regarding all federal information systems and networks managed by the Department of Commerce," and would require "the Director of National Intelligence and the Secretary of Commerce to submit to Congress an annual report on cybersecurity threats to and

---

155. *See* THE WHITE HOUSE, *supra* note 82, at vi (outlining the Administration's policy goals).

156. *Id.* at iv.

157. *Id.* at i.

158. *See infra* Part IV.A.2 (discussing steps taken by various international organizations).

159. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified in scattered titles of U.S.C.).

160. 6 U.S.C. § 145 (2009).

161. Cybersecurity Act of 2009, S. 773, 111th Cong. (2009).

162. *Id.* § 3.

vulnerabilities of critical national information, communication, and data network infrastructure."[163]

The Department of Defense is in the process of setting up its own cybercommand in order to defend its military networks against the increasing number of cyberattacks and to develop cyber-weapons.[164] The cybercommand likely will be led by the National Security Agency as part of U.S. Strategic Command, and should be fully operational by October 2010.[165] The Joint Task Force for Global Network Operations, under the U.S. Strategic Command, has managed the Pentagon's computer networks since 2004.[166] The U.S. government also has been conducting cyberattack simulations since at least 1997, in an effort to identify weaknesses in U.S. computer networks.[167]

As a further effort at international cooperation, the Federal Bureau of Investigation (FBI) is permanently stationing a computer crime expert in Estonia, which is significant because it is the first time the FBI has stationed an agent focused purely on cybercrime outside the United States.[168]

Finally, the United States, although not a member of the Council of Europe, signed and ratified the CoE Cybercrime Convention. This

---

163. The Library of Congress, Summary of S. 773, http://thomas.loc.gov/cgi-bin/bdquery/z?d111:SN00773:@@@D&summ2=m& (last visited Jan. 4, 2010).

164. William Jackson, *DOD Creates Cyber Command As U.S. Strategic Command Subunit*, FED. COMPUTER WK, June 24, 2009, http://www.fcw.com/Articles/2009/06/24/DOD-launches-cyber-command.aspx.

165. *Id.*

166. *See* U.S. Strategic Command—Home, http://www.stratcom.mil (last visited Jan. 4, 2010) (listing its "missions" as including "to ensure US freedom of action in space and cyberspace"); *see also* Bradley Graham, *Hackers Attack Via Chinese Web Sites*, WASH. POST, Aug. 25, 2001, at A1 (discussing how the Pentagon has responded to computer attacks from China).

167. In 1997, the U.S. government conducted Eligible Receiver, which identified serious vulnerabilities in military systems. *See* SCHELL & MARTIN, *supra* note 1, at 112. Next came Digital Pearl Harbor in 2002, a multi-day war game that simulated a multiple-industry cyberterrorism attack against critical infrastructure. *Id.* In 2003, the government again ran Eligible Receiver, which identified the need for better military-nonmilitary coordination. *Id.* In 2006, the government ran Cyber Storm I, which simulated a large-scale attack on critical infrastructures such as energy, transportation, and telecommunications. *See* BRENNER, *supra* note 12, at 49–54. Cyber Storm I, like the other simulations, identified a multitude of weaknesses and insecurities. *Id.* Most recently, in 2008 the government ran Cyber Storm II, which simulated a coordinated cyber-attack on multiple aspects of critical infrastructure. Press Release, Department of Homeland Security, DHS Holds Cyber Storm II Exercise to Further Cyber Security Preparedness and Response Capabilities (Mar. 10, 2008), *available at* http://www.dhs.gov/xnews/releases/pr_1205180340404.shtm; *see also* Ian Grant, *Cyber Storm 2 Exercise Reveals Security Preparedness*, COMPUTERWEEKLY.COM, Mar. 18, 2008, http://www.computerweekly.com/Articles/2008/03/18/229909/cyber-storm-2-exercise-reveals-security-preparedness.htm (providing details about the exercise).

168. *FBI to Station Cybercrime Expert in Estonia*, ASSOCIATED PRESS, May 11, 2009, http://www.msnbc.msn.com/id/30683801/.

is an extraordinary step, signaling the United States' willingness to work with other states on the issue of cybercrime.

2. Efforts by International Organizations

The Organization for Security and Cooperation in Europe (OSCE), a branch of the United Nations, has developed numerous counter-terrorism technical assistance programs, one of which is the Action against Terrorism Unit (ATU).[169] The ATU is "the focal point for co-ordinating and facilitating OSCE counter-terrorism activities," which include capacity-building assistance programs, training, and expert workshops on the subject of counter-terrorism.[170] Since 2004, cyberterrorism has been one of the ATU's main areas of emphasis.[171] Although Ambassador Eric Lebédel of France, Chairman of the OSCE Forum for Security Co-operation, described the OSCE as being "proactive" in responding to the threat of cyberterrorism, he admits that "much remains to be done to face this protean threat which affects all three OSCE dimensions of security."[172] The OSCE recently has held a number of cybersecurity workshops;[173] the most recent workshop, held on March 17–18, 2009, aimed to bring together key individuals to discuss a comprehensive approach to cyber security.[174]

NATO has recently taken a number of important steps—first and foremost, it agreed on a common policy on cyber defense in January 2008, which was adopted at the Bucharest Summit on April 3, 2008.[175] The policy contains, among other things, a commitment to

---

169. Organization for Security and Co-operation in Europe, Counter-Terrorism Technical Assistance Programs, http://www.un.org/sc/ctc/directory/doa/OSCE.html (last visited Jan. 4, 2010).

170. *Id.*

171. *Id.* ("Combating the use of the Internet for terrorist purposes.").

172. Press Release, Org. for Sec. & Co-operation in Eur., Co-operation, Comprehensive Strategies Vital to Facing Cyber Security Challenges, Says Estonian Defense Minister (Mar. 17, 2009), http://www.osce.org/item/36814.html.

173. *See* Perl, *supra* note 73, at 8 (describing workshops held in 2005, 2006, and 2007).

174. Organization for Security and Co-operation in Europe, Secretariat—Action against Terrorism Unit: Combating Terrorist Use of the Internet, http://www.osce.org/atu/17702.html (last visited Jan. 4, 2010).

175. *See* North Atlantic Treaty Organization, NATO Topics, Defending Against Cyber Attacks, What Does This Mean in Practice?, http://www.nato.int/issues/cyber_defence/practice.html (last visited Jan. 4, 2010) [hereinafter NATO Topics].

> The Alliance's relevant military and technical committees and bodies, as well as the Allies individually, are now engaged in implementing the policy. In line with this, a cyber defence Centre of Excellence has been set up in Estonia and NATO's Military Committee recently agreed on a Cyber Defence Concept which adds practical action programmes to fit within the overarching policy.

Id. North Atlantic Treaty Organization [NATO], *Bucharest Summit Declaration*, para. 47, NATO Doc. PR/CP(2008)049 (Apr. 3, 2008), *available at*

protecting critical information systems and strengthening national–international cooperation.[176] NATO also created a Cyber Defence Management Authority,[177] and established a Cooperative Cyber Defence Center of Excellence in Tallinn, Estonia, the establishment of which was preceded by the Bucharest Summit Declaration in April 2008.[178] Just a few months ago, the CCD COE held a three-day conference on cyber warfare, covering such topics as investigating cyber-espionage networks, "the use of the Internet by terrorist organizations and the possibilities of terrorist cyber attacks," and whether sovereignty can "adapt to the cyber security challenge."[179] Despite these steps, however, "[a]t present, NATO does not define cyber-attacks as a clear military action. This means that the provisions of Article V of the North Atlantic Treaty, or, in other words, collective self-defence, will not automatically be extended to the attacked country."[180]

The European Union recently launched the Critical Information Infrastructure Protection Initiative (CIIPI). The CIIPI recognizes the threat facing critical information infrastructures, "defines a plan of immediate actions to strengthen the security and resilience of [critical information infrastructures]," and calls for greater international cooperation on the subject of infrastructure protection.[181] The CIIPI

---

http://www.globalsecurity.org/military/library/news/2008/04/mil-080403-nato01.htm [hereinafter *Bucharest Summit Declaration*] ("We have recently adopted a Policy on Cyber Defence, and are developing the structures and authorities to carry it out.").

176. *Bucharest Summit Declaration*, *supra* note 175, para. 47.

177. *See* NATO Topics, *supra* note 175 (discussing the phases of development).

178. *See* Press Release, N. Atl. Treaty Org., NATO Opens New Centre of Excellence on Cyber Defence (May 14, 2008), http://www.nato.int/docu/update/2008/05-may/e0514a.html ("In April, the Bucharest Summit Declaration paved the way for the establishment of the Estonian COE, emphasizing the need for NATO members to protect key information systems and develop the ability to counter a cyber attack.").

179. Cooperative Cyber Defence Centre of Excellence, Agenda for June 17–19, 2009 CCD COE Conference on Cyber Warfare, http://www.ccdcoe.org/123.html (last visited Jan. 4, 2010).

180. Traynor, *supra* note 13 (quoting Estonian Defence Minister Jaak Aaviksoo). *See also* North Atlantic Treaty art. 5, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243.

> The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.

Id.

181. COM (2009) 149 final, *supra* note 33, at 2; *see also Commission Green Paper on a European Programme for Critical Infrastructure Protection*, COM (2005) 576 final (Nov. 17, 2005) (outlining the options to create an initiative for Europe called EPCIP).

is meant to work in tandem with the recent actions taken in this area by the OSCE, the G-8 principles on Critical Information Infrastructure Protection,[182] and the United Nations General Assembly Resolution 58/199, entitled "Creation of a global culture of cybersecurity and the protection of critical information infrastructures."[183]

The United Nations Security Council and General Assembly have also taken actions to address cyberterrorism. General Assembly Resolution 51/210 of January 16, 1997, calls upon UN member states to "note the risk of terrorists using electronic or wire communications systems and networks to carry out criminal acts and . . . to find means . . . to prevent such criminality and to promote cooperation where appropriate."[184] Security Council Resolution 1373 of September 28, 2001, calls upon UN member states to increase international cooperation by way of exchanging information regarding "use of communications technology by terrorist groups."[185] Security Council Resolution 1566 of October 8, 2004 calls upon UN member states to strengthen international cooperation against terrorism,[186] and Security Council Resolution 1624 of September 14, 2005 calls upon UN member states to prohibit "incitement to commit a terrorist act or acts."[187] These resolutions demonstrate UN member states' growing commitment to addressing terrorism.

Possibly the most significant step is the Council of Europe's enactment of the Convention on Cybercrime, which entered into force in 2004.[188] The Convention requires parties to enact substantive and procedural legislation to criminalize certain computer crimes and facilitates extradition of those charged with committing such crimes. The Convention is significant because it is the first multilateral treaty to address the issues of computer crime and electronic

---

182. See G8 Principles for Protecting Critical Information Infrastructures, http://www.usdoj.gov/criminal/cybercrime/g82004/G8_CIIP_Principles.pdf (last visited Jan. 4, 2010) for the G8 Principles adopted by the Department of Justice.

183. G.A. Res. 58/199, U.N. Doc. A/RES/59/199 (Jan. 30, 2004).

184. G.A. Res. 51/210, ¶ 3(c), U.N. Doc. A/RES/51/210 (Dec. 17, 1996).

185. S.C. Res. 1373, ¶ 3(a), U.N. Doc. S/RES/1373 (Sept. 28, 2001).

186. S.C. Res. 1566, ¶ 6, U.N. Doc. S/RES/1566 (Oct. 8, 2004).

187. S.C. Res. 1624, ¶ 1(a), U.N. Doc. S/RES/1624 (Sept. 14, 2005).

188. Council of Europe, Convention on Cybercrime, Chart of Signatures and Ratifications, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=2&DF=21/10/2009&CL=ENG (last visited Jan. 4, 2010). The United States signed the treaty on November 23, 2001, ratified it on September 29, 2006 and asserted a partial reservation with respect to Article 22, addressing Jurisdiction. Council of Europe, Convention on Cybercrime, List of Declarations, Reservations, and Other Communications, http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=185&CM=2&DF=21/10/2009&CL=ENG&VL=1 (last visited Jan. 4, 2010).

gathering of evidence related to such crimes.[189] As of July 17, 2009, twenty-six states had ratified the Convention, and an additional twenty had signed but not ratified it.[190] Numerous organizations, including the OSCE and Interpol, have recommended the Convention as "providing an important international legal and procedural standard for fighting cyber crime."[191]

More recently, the Council of Europe published the Project on Cybercrime Final Report, which was prepared by the Economic Crime Division of the Directorate General of Human Rights and Legal Affairs.[192] The purpose of the Final Report is to promote implementation of the Convention on Cybercrime; it describes a five-page list of activities relating to cybersecurity that were undertaken during the period from September 2006 to February 2009, including numerous regional conferences, meetings, and workshops.[193]

B. *Technology*

States, international organizations, and private industry also have been actively cooperating to develop international standards to help prevent cyberterrorism. The two main areas of focus have been standards for economic transactions and standards for encryption.

In order to begin to provide adequate security, states and international institutions must not only secure the information to be transmitted (i.e., maintain data integrity), but must also be able to ensure that the person with whom they are communicating is truly the person he claims to be (i.e., provide authentication).[194] The need for both data integrity and authentication significantly compounds the security structures to be implemented and maintained.

The first area of concern is provision for data integrity, which usually is resolved through encryption. Even strong encryption methods are not foolproof, however. Encryption is most effective in countering password-sniffing, snooping, and eavesdropping, but is

---

189. *Multilateral Enforcement Treaties: Hearing Before the S. Foreign Relations Comm.*, 108th Cong. (2004) (Statement of Bruce Swartz, Deputy Assistant Attorney General, Criminal Division).

190. *See* Council of Europe, Convention on Cybercrime, Chart of Signatures and Ratifications, *supra* note 188 (listing those states that have ratified and signed the Convention).

191. Perl, *supra* note 73, at 5.

192. COUNCIL OF EUR., PROJECT ON CYBERCRIME FINAL REPORT (SEPTEMBER 2006 – FEBRUARY 2009), COUNCIL OF EUR. DOC. ECD/567(2009)1 Provisional (2009), *available at* http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567-d-final%20report1h%20provisional%20_14%20may%2009_%20+footnote.pdf.

193. *Id.* at 3–10.

194. *See* DENNING, *supra* note 93, at 51.

absolutely useless in preventing the injection of malicious code, spoofing, and tampering, to name a few other types of attacks.

Encryption is only one way to protect data, however. Moreover, it only protects the data itself, not the network over which the data is being sent, the intranet or computer from which the data originated, or any other information on the Internet. Protecting these other aspects of the network is much more difficult, as a result of both the basic flaws in the infrastructure of the Internet and the transparency of information available via the Internet.

The second area of concern, authentication,[195] can be assuaged to some degree through the use of methods to validate both the source and content of information and the identity of users during login.[196] The two most common methods of authentication are passwords and digital signatures. The most effective type of password is the one-time password, which generally is not susceptible to password guessing or sniffing attacks due to the sheer effort that is involved—if a password is a six-digit number that changes randomly each minute, an attacker has one chance in a million of guessing the password, which would have to be done in under one minute.[197] Digital signatures also can be effective. A digital signature is a form of public-key cryptography that effectively adds an electronic "signature" to the end of a message or file, proving that the person who claims to have sent it actually did so.[198]

Yet these measures have not been enough—they have failed to prevent massive cyberattacks totaling billions of dollars in losses and inestimable damage to national security,[199] as shown in Estonia and more recently in attacks on U.S. government websites.[200] It is unclear whether the technological steps taken as a result of multi-sector international cooperation will be more effective at reducing

---

195. Authentication is an issue for both states and multinational corporations. Returning to the hypothetical case involving Russia and the United States, if the United States had implemented effective authentication measures, it could have confirmed that the attacker was not really the Russian government and thus could have avoided escalated tensions.

196. DENNING, *supra* note 93, at 38.

197. Peter J. Denning, *Passwords, in* INTERNET BESEIGED: COUNTERING CYBERSPACE SCOFFLAWS, *supra* note 101, at 159, 163.

198. *See* PC Magazine, Definition of Digital Signature, http://www.pcmag.com/encyclopedia_term/0,2542,t=digital+signature&i=41384,00.asp (last visited Jan. 4, 2010) (defining and illustrating digital signatures).

199. *See* Ellen Nakashima & Steven Mufson, *Hackers Have Attacked Foreign Utilities, CIA Analyst Says,* WASH. POST, Jan. 19, 2008, at A4, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/01/18/AR2008011803277.html ("[C]yber attackers have made increasingly sophisticated intrusions into corporate computer systems, costing companies worldwide more than $20 billion each year, according to some estimates.").

200. James D. Zirin, *Abdicating on a Cyber Czar?*, L.A. TIMES, Oct. 14, 2009, at A25, *available at* http://www.latimes.com/news/opinion/commentary/la-oe-zirin14-2009oct14,0,603775.story.

both the scope and the magnitude of the potential damage inflicted by cyberterrorist attacks.

1. International Standards for Economic Transactions

International standards for economic transactions are critical to protecting information and networks in the international financial system from cyberterrorism. Although states and private industry have played some role, international organizations have been the primary developers of the current standards.

A number of organizations have played important roles in the process, especially in coordinating policies among countries. Of these, the American National Standards Institute (ANSI), the International Organization for Standards, the International Electrotechnical Commission, and the International Telecommunication Union are some of the most important.[201] These organizations helped develop the first standard, known as ANSI X-12, which has been ubiquitous for the past thirty years.[202] ANSI also maintains the ANSI X9.9 standard, which is used to prevent the unauthorized manipulation or loss of Electronic Funds Transfer data.[203] The global standard, the United Nations Electronic Data Interchange for Administration, Commerce, and Trade (UN/EDIFACT), is also increasingly important. This international EDI standard was developed and is maintained by the United Nations Economic Commission for Europe Centre for Trade Facilitation and Electronic Business.[204] Both the European Union and the United States have endorsed UN/EDIFACT.[205] Indeed, some countries require the use of UN/EDIFACT as a matter of law.[206]

---

201. See INFORMATION INFRASTRUCTURE TASK FORCE, THE GLOBAL INFORMATION INFRASTRUCTURE: AGENDA FOR COOPERATION, *available at* http://www.ntia.doc.gov/reports/giiagend.html (last visited Jan. 4, 2010) ("Three principal international standards organizations involved in the development of information technology and telecommunications standards are the International Organization for Standards (ISO), the International Electrotechnical Commission (IEC), and the International Telecommunication Union (ITU).").

202. Howard Millman, *A Brief History of EDI*, INFOWORLD, Apr. 6, 1998, at 83 (1998).

203. Treas. Dep't Order 106-09 (Oct. 2, 1986), *available at* http://www.ustreas.gov/regs/to106-09.htm.

204. United Nations Economic Commission for Europe, United Nations Directories for Electronic Data Interchange for Administration, Commerce and Transport, UN/EDIFACT, http://www.unece.org/trade/untdid/welcome.htm (last visited Jan. 4, 2010).

205. *The Future of Money: Hearing Before the House Subcommittee on Domestic and International Monetary Policy*, 104th Cong. 193 (1996) (statement of Jeffrey B. Ritter, Program Director, ECLIPS, Ohio Supercomputer Center and Chair, American Bar Association Committee on the Law of Commerce in Cyberspace).

206. *Id.*

The U.S. government has also dedicated extensive resources to the issue, most notably via the National Telecommunications and Information Administration (NTIA), a branch of the Department of Commerce.[207] NTIA's Office of International Affairs is particularly active in the area of Internet regulations, as it plays a key role in advising the President on international telecommunications and information policy.[208] Private industry also has taken steps to address the issue, and industry leaders are currently investigating various regulation measures, often in collaboration with one or two sister companies. Visa and MasterCard, for example, consolidated their standards into the Secure Electronic Transactions payment system.[209] Key recovery systems are becoming another increasingly demanded component of international standards.

2. International Standards for Encryption

Another technological option to reduce network insecurity is encryption, which has been used in various increasingly complex forms for hundreds of years. Banking and financial institutions in the United States have used the Advanced Encryption Standard (AES) since 2001, when it was published by the National Institute of Standards and Technology.[210] AES uses a 128, 192, or 256 bit key to encrypt data in 128-bit blocks.[211]

Although better and stronger forms of encryption are constantly being developed, the search for stronger encryption appears to be never-ending, because each increase in encryption strength seems to be matched by an advance in decryption. It is a bit like trying to secure a house—one can add as many locks and deadbolts as possible to the front door, but no matter how many locks are installed or how complicated they are, given enough time and enough resources, even

---

207. *See generally* National Telecommunications and Information Administration, Office of International Affairs, http://www.ntia.doc.gov/oiahome/oiahome.html (last visited Nov. 16, 2009) (explaining the function of the Office of International Affairs).

208. *Id.*

209. Anish Bhimani, *Securing the Commercial Internet, in* INTERNET BESEIGED: COUNTERING CYBERSPACE SCOFFLAWS, *supra* note 101, at 407, 417.

210. *See* NAT'L INST. OF STANDARDS & TECH., FED. INFO. PROCESSING STANDARDS PUBL'N NO. 197, ANNOUNCING THE ADVANCED ENCRYPTION STANDARD (AES) (2001), *available at* http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf (outlining the specifications for the Advanced Encryption Standard).

211. *See* Press Release No. G 2001-111, Nat'l Inst. of Standards & Tech., Commerce Secretary Announces New Standard for Global Information Security (Dec. 4, 2001), *available at* http://www.nist.gov/public_affairs/releases/g01-111.htm ("Secretary of Commerce Don Evans today announced approval of a new information technology encryption standard for the federal government."); *see also* Zimmerman, *supra* note 52, at 110 (explaining how "[w]ell-designed cryptography systems can ensure the secrecy" of e-mail and other electronically sent information).

the most "unbreakable" of situations can be hacked. Furthermore, there is usually a back door or a window that is less secure. Essentially, encryption only allows a network to stay just one step ahead, and sometimes not even that.

C. *Attempts Are Insufficient to Prevent Cyberterrorism*

States, private industry, and international organizations are taking important legal, policy, and technological steps to combat cyberterrorism. The steps taken to date, however, are insufficient, and greater international cooperation is needed.[212]

On the legal and policy side, states and international organizations have generated the beginnings of what could be significant efforts to mitigate the damage done by cyberterrorism. More must be done, however, and at a faster pace, to catch up to cyberterrorists and to attempt to address the threats to national and international security that cyberterrorism poses. Such efforts could include a convention on cyberterrorism, a UN conference on cyberterrorism, or some other similar measure. On the technological side, much is riding on the few international standards presently in place. As technology progresses, these standards will become outdated. States, private industry, and international organizations should begin discussions of the next standards sooner rather than later.

The problems posed by the inherent insecurity of the TCP/IP Protocol are extremely difficult, if not in some cases impossible, to solve, however. States and international organizations must question whether they are willing to accept such a fundamental threat to their national and international security. In the end, it is an issue of risk management and of deterrence.

Initially, the question arises of whether standards should be established at all. Indeed, regulation brings with it numerous problems, not the least of which is a false sense of security. Furthermore, if better standards and security measures are not continually developed, those working to break security mechanisms will quickly catch up to and surpass those trying to maintain security. The U.S. government acknowledged this deficiency in the early phase of the public Internet, stating in The Framework for Global Electronic Commerce that setting standards too soon can lock in outdated

---

212. James Jones, U.S. Nat'l Sec. Adviser, Remarks at 45th Munich Conference On Security Policy (Feb. 9, 2009), *available at* http://www.cfr.org/publication/18515/remarks_by_national_security_adviser_jones_at_45th_munich_conference_on_security_policy.htmlGable_camera_ready_final.doc ("If there is one overriding characteristic to the world we face, it is the truth that security is shared.").

technology.[213] Once in motion, however, the momentum behind standardization may be nearly impossible to reverse, even if the potential problems significantly outweighed the potential benefits.

V. DETERRENCE VIA PRESCRIPTIVE JURISDICTION

Cyberspace really is the final frontier—borderless, pervasive, and potentially very dangerous. In this new realm, territory is irrelevant, which means that a radical upheaval of the traditional territory-based model of sovereignty and jurisdiction that has existed for the past few hundred years is all but inevitable.[214] As cyberterrorism cannot be prevented, the next logical step is to attempt to deter cyberterrorists by means of effective and consistent prosecution.

International law provides several forms of jurisdiction to prescribe (i.e., to apply one's laws);[215] nationality jurisdiction, based on either the nationality of the victim (passive personality) or the aggressor (active personality); territorial jurisdiction, based on the crime occurring in or affecting a state's territory (objective) or commencing in a state's territory despite completion elsewhere (subjective); universal jurisdiction, based on the extreme gravity of the crime under international law; and protective jurisdiction, based on a threat to the security and integrity of the state.[216] Of those, territorial jurisdiction and universal jurisdiction are of particular interest to deterring cyberterrorism. It is extremely difficult to apply territorial jurisdiction to cyberterrorism, however, due to both the nature of the Internet and the realities of cyberterrorism. Universal jurisdiction is much easier to apply, in part because it shares with cyberterrorism a disregard of national borders. Thus, this increased facility makes universal jurisdiction a much more feasible option for deterrence.

---

213. THE WHITE HOUSE, THE FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE (1997), *available at* http://clinton4.nara.gov/textonly/WH/New/Commerce/read.html.

214. Thomas Schultz, *Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface*, 19 EUR. J. INT'L L. 799, 800–01 (2008).

215. *See* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 401 cmt. a (1987) ("Aspects of Jurisdiction").

216. *See* James D. Fry, *Terrorism as a Crime Against Humanity and Genocide: The Backdoor to Universal Jurisdiction*, 7 UCLA J. INT'L L. & FOREIGN AFF. 169, 173–74 (2002) (discussing jurisdiction over crimes committed outside the prosecuting state's territory); *see also* Kenneth C. Randall, *Universal Jurisdiction Under International Law*, 66 TEX. L. REV. 785, 786-87 (1988) [hereinafter Randall, *Universal Jurisdiction*] (explaining the international principles of jurisdiction).

A. *Territorial Jurisdiction—Too Unwieldy For Cyberterrorism*

The ability of a state to apply its laws under the international law concept of territorial jurisdiction is generally based on the location of the attack.[217] Territorial jurisdiction is important to international law and is one of the most fundamental and well-accepted methods of exercising jurisdiction to prescribe. Indeed, Professor Raustiala describes territoriality as providing "the bedrock principles for the development of modern international law."[218] Due to the nature of the Internet and the realities of cyberterrorism, however, the use of territorial jurisdiction is at best exceedingly complicated and at worst infeasible.

First, there is no territory in cyberspace where cyberterrorism is concerned.[219] Scholars such as Professors Goldsmith and Wu argue that characterizations of the Internet as borderless or lacking any territorial connection are invalid because the Internet increasingly is conforming to national laws and requirements, thus losing the characteristic of being beyond the state.[220] Similarly, Professor Raustiala describes the Internet as "increasingly bordered" and subject to the control of sovereign states.[221] Although these analyses may apply with respect to certain areas of law, it does not apply with respect to cyberterrorism for a number of reasons, not least of which is that there presently are no national laws that apply directly to cyberterrorism.[222] Furthermore, although cyberspace may be subject to state control in the sense that domain names can be assigned or content can be filtered, no state can control cyberterrorism from a

---

217. *See* Randall, *Universal Jurisdiction*, *supra* note 216, at 786–87 (The territoriality principle is invoked "when an offense occurs in the prosecuting state's territory."). This form of territorial jurisdiction is also known as "objective territorial jurisdiction." A situation where an attack begins on the territory of State A but completes on the territory of State B may give State A what is called "subjective territorial jurisdiction"; in that situation, State B would have objective territorial jurisdiction.

218. KAL RAUSTIALA, DOES THE CONSTITUTION FOLLOW THE FLAG? THE EVOLUTION OF TERRITORIALITY IN AMERICAN LAW 11 (2009).

219. *See, e.g.*, Sean P. Kanuck, *Information Warfare: New Challenges for Public International Law*, 37 HARV. INT'L L. J. 272, 288 (1996) ("Even in the most abstract sense, the notion of territory (and its corollary on possessory rights) can only imperfectly account for the information realm. Cyberspace and information alike transcend physical boundaries, thereby requiring a legal paradigm that looks beyond merely the locus of events.").

220. *See generally* GOLDSMITH & WU I, *supra* note 36 at 87–104 (explaining how national laws control internet activity).

221. RAUSTIALA, *supra* note 218, at 9.

222. Although some domestic and international laws have been enacted to address cybercrime, they do not specifically address cyberterrorism.

technological perspective.[223] Cyberterrorists operate without borders, explicitly refusing to obey any parameters a state may have erected for law-abiding citizens. As a result, these concepts of a "bordered" Internet are inapposite in the context of cyberterrorism.

Although states may attempt to assert jurisdiction based on the state where an individual views a website or the state of incorporation of a company whose website is involved in a dispute, such situations do not exist in cyberterrorism. Cyberterrorists attack not just particular data, such as stock prices, but entire computer systems, such as stock exchanges or power grids. Determining the origin of a cyberattack in the later scenario is even more difficult because it is unclear where the crime being committed occurs—in truth, the crime itself occurs in cyberspace.[224]

A second and related problem is determining the location of the computer the cyberterrorist is using to launch the attack. Due to the fact that cyberterrorists operate beyond the territory of any state, often use computers in multiple states to commit their crimes, and have extensive technological tools at their disposal to make it look like the attack came from elsewhere, it is exceedingly difficult to make the traditional determinations necessary to assert territorial jurisdiction. The identity and location of a cyberterrorist is nearly impossible to pinpoint, as cyberterrorists intentionally conceal their location by looping or leapfrogging several computer systems in several countries before attacking their target.[225] Recall that in the recent attack on the U.S. and South Korean governments, the South Korean government initially believed that the attack originated in North Korea.[226] Only later did they come to believe (and even then, not definitively) that the attack may have originated from within the United Kingdom.[227] The same thing happened with the 2007 attacks on Estonia.[228]

Although it may be possible to identify a computer's (and therefore cyberterrorist's) IP address by using tracing packets, which might provide the path that the cyberterrorist took to reach his destination and, therefore, his original location, this method is far from guaranteed to identify a particular computer,[229] especially given

---

223. *See* John B. Avlon, *The Growing Cyberthreat*, FORBES, Oct. 20, 2009, http://www.forbes.com/2009/10/20/digital-warfare-cyber-security-opinions-contributors-john-p-avlon.html (describing the United States' vulnerability towards cyberattacks).

224. Kanuck, *supra* note 218, at 288 ("From a legal perspective, even more problematic than information warfare against data is an attack against the medium itself.").

225. De Borchgrave, *supra* note 19.

226. Williams, *supra* note 10.

227. *Id.*

228. *See* BRENNER, *supra* note 12, at 5–6, 133.

229. Goldsmith & Wu II, *supra* note 36, at 43.

that IP addresses are not necessarily static.[230] Furthermore, a cyberterrorist can spoof this information or use an anonymous or masked IP address,[231] confounding attempts to determine with any accuracy the true location or identity of the attacker.[232] As Professor Brenner explained, this enables cyberterrorists to manipulate and obfuscate their true location ("point of attack origin"), leading to misidentification of the identity and location of the cyberterrorist and the nature of the attack (state-sponsored or not).[233] As a result, point of attack origin can be given only limited weight in attributing blame for cyberterrorist attacks.[234] Looking at this aspect of the attack for purposes of establishing jurisdiction is nearly impossible.

A third difficulty exists in determining whether other states may have an interest in asserting jurisdiction. As previously discussed, cyberterrorists often loop their attacks through multiple computers or servers, which may be in different states, in an effort to disguise their location. Determining whether any of those additional computers represent additional cyberterrorists that are actually involved or are merely decoys renders the necessary analyses even more complicated.

Although the territorial effects doctrine of jurisdiction theoretically could be applied,[235] the admissibility of the doctrine

---

230. IP addresses are assigned by Internet Service Providers like Comcast, Verizon, or RCN, which do not always have enough IP addresses to assign them permanently. *See* SCHELL & MARTIN, *supra* note 1, at 264.

231. *See id.* at 15 (noting ways that a hacker can visit websites without leaving a trace of his or her visit, such as proxy servers, Janus, and the Anonymizer).

232. Kanuck, *supra* note 219, at 287–88.

> A satellite can be owned, identified, and located. These traits make it possible to evaluate actions conducted by or against it. Satellite emissions, cellular telephone calls, and e-mail messages, on the other hand, may be 'owned' in some sense, but their identification or location can easily be prevented, thereby rendering attribution and regulation ineffective. . . . The uncertainties surrounding the actual ownership of information have led to the development of cryptographic techniques that protect the very ideas, or information itself, for which the law offers no aegis.

Id.

233. *See* BRENNER, *supra* note 12, at 133–34.

234. *Id.*

235. The territorial effects doctrine, essentially a form of the objective territoriality principle of jurisdiction, holds that if an action taken in another country has serious effects on a state, the affected state may find jurisdiction to apply its laws to prosecute the crime. The Permanent Court of International Justice recognized the territorial effects doctrine as a proper basis for prescriptive jurisdiction in *The Case of the S.S. Lotus*. *See* Sanjay S. Mody, *National Cyberspace Regulation: Unbundling the Concept of Jurisdiction*, 37 STAN. J. INT'L L. 365 (2001) (arguing that regulating transnational cyberspace activity is fully consistent with a state's rulemaking authority under international law).

under international law is controversial in many states.[236] As cyberterrorism must be widely condemned in order for that condemnation and prosecution to have any deterrent effect, a basis of jurisdiction not widely accepted in the international community is insufficient. Furthermore, although the territorial effects doctrine, or the "tighter" version thereof as described by Professor Thomas Schultz where the defendant is determined to have purposefully availed himself of the forum where the injury was caused,[237] may make sense for civil actions, it is not applicable to cyberterrorism. As discussed, cyberspace is nowhere and everywhere. Defacing or shutting down a website happens in cyberspace, not in the territory of a given state.[238] Although some cyberattacks, such as that on the government of Estonia, could be seen as being intended to harm the government of Estonia, the targets of cyberattacks are not always so easily identified.

Each of these difficulties makes it impractical to attempt to assert territorial jurisdiction, especially if the primary goal is deterrence. Cyberterrorists are not likely to be deterred if it takes years just to identify the attackers and where they are located. Further, once identification is accomplished, states may wrangle over extradition. Although the identity and location of the cyberterrorist must be determined prior to asserting any form of prescriptive jurisdiction (including universal jurisdiction), effective deterrence also requires an ease of prosecution that only universal jurisdiction can provide. It is difficult enough to identify and locate cyberterrorists; if they can only be prosecuted if they happen to visit the state they attacked, effective prosecution would be impossible.

---

236. Schultz, *supra* note 214, at 812. The territorial effects doctrine is not controversial in the United States, however, and may be increasingly accepted abroad. *See* RAUSTIALA, *supra* note 218, at 188–89.

237. Schultz, *supra* note 214, at 817. In many ways, this "tighter" version is akin to the analysis of *Asahi Metal Indus. v. Superior Court*, 480 U.S. 102 (1987), a case from U.S civil procedure law governing personal jurisdiction and holding that a potential defendant must purposefully avail itself of a forum before jurisdiction will be found in that forum.

238. Kanuck, *supra* note 219, at 287.

> Now add the further wrinkle that 'cyber-transactions' can occur anonymously, in perfect secrecy with the aid of encryption, and completely outside of all legal jurisdictions. It seems rather difficult, indeed, to identify exactly where the information in Citibank or AT&T's international databases exists, or to which jurisdiction's laws the electromagnetic quanta carrying an encrypted cellular telephone call are subject. Any comprehensive regulator structure based on physical location thus seems grossly inadequate.

Id.

Thus, territorial jurisdiction is too restrictive[239] and would provide only a limited deterrent, if any, to cyberterrorism. Due to the absence of these complicating factors with respect to universal jurisdiction, prosecution of cyberterrorism under universal jurisdiction would be a more effective deterrent.

B. *Universal Jurisdiction—Uniquely Suited To Cyberterrorism*

Cyberterrorism is not your garden variety crime. It is a particularly heinous act, a version of terrorism on par with more "traditional" acts carried out by Al Qaeda and other terrorist organizations, and it is even more difficult to defend against due to the borderless, state-less, and territory-less nature of cyberspace.[240]

Similarly, universal jurisdiction is not your garden variety basis for exercising prescriptive jurisdiction. Of the many ways to obtain jurisdiction under international law, universal jurisdiction is perhaps the most extreme, although probably not the most controversial.[241] Far from the more traditional sources of jurisdiction, where the connection to a state's nationals or territory confers authority to prosecute, universal jurisdiction "confers on any nation the authority to prosecute alleged international criminals, even when the prosecuting nation has no connection whatsoever with the offense."[242] Although universal prescriptive jurisdiction has existed for centuries, it only now seems to be "coming into its own as a systematic means for promoting legal accountability."[243]

---

239. Schultz, *supra* note 214, at 811 (explaining that territorial jurisdiction is "a too restrictive basis of jurisdiction in the face of information flows potentially having effects in every country of the world.").

240. Indeed, Al Qaeda and others have indicated their desire to attack the United States using cyberterrorism. *See* President Barack Obama, *supra* note 71 (discussing the challenges facing America's digital infrastructure). Furthermore, terrorist groups are growing increasingly nimble in their use of the Internet and are increasingly able to parry and evade cyberattacks themselves. *See* Report from International Institute for Strategic Studies and Young Professionals in Foreign Policy Panel Discussion on "NATO—Cyber-Crime and Cyber-Security" (July 19, 2007), *available at* http://www.iiss.org/EasysiteWeb/getresource.axd?AssetID=2695&type=full&servicetype=Attachment (exploring the role that NATO could play in combating cyber terrorism).

241. That dubious distinction arguably belongs to either the territorial effects doctrine or the protective principle.

242. Kenneth C. Randall, Book Review, 98 AM. J. INT'L L. 627, 627 (2004) (reviewing LUC REYDAMS, UNIVERSAL JURISDICTION: INTERNATIONAL AND MUNICIPAL LEGAL PERSPECTIVES (2003)) [hereinafter Randall, Book Review]; *see also* Eugene Kontorovich, *The Piracy Analogy: Modern Universal Jurisdiction's Hollow Foundation*, 45 HARV. INT'L L.J. 183, 183 n.3 (2004) (noting various iterations of definitions of universal jurisdiction).

243. Steven W. Becker, *Commentary on the Princeton Principles, in* BURNS H. WESTON ET AL., INTERNATIONAL LAW AND WORLD ORDER 1370, 1371 (4th ed. 2006).

As it is all but impossible to prevent cyberterrorism, the next best solution is to deter those who would commit acts of cyberterrorism. Like most crimes, deterrence is accomplished by way of effective and consistent prosecution. Unlike most crimes, however, cyberterrorists are often motivated by political, religious, or ideological causes, which make deterrence more challenging.[244] Due to both the broad reach of universal jurisdiction and the inherent practical difficulties caused by those terrorists operating in cyberspace, universal jurisdiction is the most efficient way to deter cyberterrorism, provide accountability, and promote international peace and justice.[245]

The arguments for extending universal jurisdiction to cyberterrorism are many and varied. First, a case can be made that there is a basis in either treaty law or customary international law for extending universal jurisdiction over cyberterrorism. Second, the heinousness of the crime is on par with traditional terrorism, genocide, and crimes against humanity. These crimes were subjected to universal jurisdiction not because they were analogous to piracy, as Professor Eugene Kontorovich argues,[246] but because of the heinous nature of the crimes. Furthermore, an analogy can be made to piracy, not based on whether piracy was or was not outlawed for its heinousness, but based on the definition of piracy as a "crime committed more or less indiscriminately against citizens of different nations . . . on the high seas."[247] Third, each of the rationales that have been provided for universal jurisdiction, as outlined by Jonathan Marks,[248] applies at least in some degree to cyberterrorism. Finally, various other concerns that have been raised in the context of traditional terrorism, such as the difficulty in defining terrorism and the possibility of universal jurisdiction getting out of control, are not causes for concern with respect to cyberterrorism.

---

244. BRENNER, *supra* note 12, at 7.

245. *See* M. Cherif Bassiouni, *Universal Jurisdiction for International Crimes: Historical Perspectives and Contemporary Practice*, 42 VA. J. INT'L L. 81, 153 (2001) ("Universal jurisdiction is the most effective method to deter and prevent international crimes by increasing the likelihood of prosecution and punishment of its perpetrators. This approach to international criminal accountability is also believed to be a factor in reducing impunity for the perpetrators of these crimes.").

246. *See generally* Kontorovich, *supra* note 242 (arguing that the piracy analogy is an insufficient method to support new universal jurisdiction).

247. Anne-Marie Slaughter, *Defining Limits: Universal Jurisdiction and National Courts, in* UNIVERSAL JURISDICTION: NATIONAL COURTS AND THE PROSECUTION OF SERIOUS CRIMES UNDER INTERNATIONAL LAW 168, 169 (Stephen Macedo ed., 2006).

248. Jonathan H. Marks, *Mending the Web: Universal Jurisdiction, Humanitarian Intervention and the Abrogation of Immunity by the Security Council*, 42 COLUM. J. TRANSNAT'L L. 445, 463–71 (2004) [hereinafter Marks, *Mending the Web*].

1. The Case for Universal Jurisdiction

As a general rule, universal jurisdiction can be based in either a treaty regime or customary international law.[249] In the case of terrorism and, by extension, cyberterrorism, both treaty law and customary international law provide legitimate bases for the exercise of universal jurisdiction.

First, numerous treaties recognize various forms of terrorism as international crimes, such as the Convention to Prevent and Punish Acts of Terrorism Taking the Form of Crimes Against Persons and Related Extortion that are of International Significance,[250] and the International Convention for the Suppression of Terrorist Bombings.[251] Although none of these recognizes cyberterrorism specifically, cyberterrorism is, in many ways, a form of terrorism generally. Indeed, by definition, cyberterrorism is traditional terrorism carried out via the Internet or against the Internet.[252] As a result, these treaties conceivably could apply to cyberterrorism.

Second, the general prohibition on terrorism (and, by extension, cyberterrorism) arguably has become subject to universal jurisdiction as a matter of customary international law. Although a complete treatment of this issue is beyond the scope of this Article, both the required elements of customary international law (*opinio juris* and state practice) are satisfied for terrorism.[253] States consider terrorism (putting aside the issue of definition) as a heinous crime on the order of a crime against humanity (*opinio juris*) and have acted to memorialize that consideration in a number of treaties (state practice) as described above.[254] In addition, the international community generally condemns terrorism as a crime against

---

249. Leila Nadya Sadat, *Redefining Universal Jurisdiction*, 35 NEW ENG. L. REV. 241, 244 (2001).

250. Convention to Prevent and Punish Acts of Terrorism Taking the Form of Crimes Against Persons and Related Extortion that are of International Significance, Feb. 2, 1971, 27 U.S.T. 3949 [hereinafter Convention to Prevent and Punish Acts of Terrorism].

251. International Convention for the Suppression of Terrorist Bombings, Jan. 9, 1998, 37 I.L.M. 249.

252. *See* BRENNER, *supra* note 12, at 37.

253. This is the generally-accepted expression of customary international law. Some may dispute the need to establish *opinio juris* and/or state practice. *See, e.g.*, Randall, *Universal Jurisdiction*, *supra* note 216, at 827–29 (describing various statements and actions by states and concluding that terrorism is an international crime).

254. Convention to Prevent and Punish Acts of Terrorism, *supra* note 250; International Convention for the Suppression of Terrorist Bombings, *supra* note 251. *See* Fry, *supra* note 216, at 182–83 (describing efforts to define terrorism).

humanity.[255] The United Nations Security Council has been vocal in its condemnation of terrorism.[256] The international community as a whole voiced opposition to terrorism in United Nations General Assembly Resolution 51/210, which recognized the potential for cyberterrorism (though not using that term) and called upon states to promote international cooperation to prevent cyberterrorism.[257] States and international organizations are actively working to implement these resolutions, thus demonstrating both *opinio juris* and state practice.[258]

In recent decades, the international community has expanded the category of offenses subject to international law and has recognized a number of international crimes that are so serious that the *aut dedere aut judicare* (extradite or prosecute) principle applies.[259] As Professor Damrosch explained, the category of crimes subject to universal jurisdiction is "more or less congruent with those entailing prosecute-or-extradite obligations,"[260] and many forms of terrorism presently entail prosecute-or-extradite obligations.[261] Further, courts and lawmakers increasingly are applying or invoking universal jurisdiction for various terrorist actions.[262] As a result, one may conclude that terrorism, and by extension cyberterrorism, is subject to universal jurisdiction.[263]

---

255. *See* Fry, *supra* note 216 (providing the illustrative example of U.S. Secretary of State Colin Powell declaring the September 11, 2001 attacks on the World Trade Center in New York City and on the Pentagon in Washington D.C. as a crime against humanity, and arguing that this description is accurate).

256. *See* S.C. Res. 1566, *supra* note 186 (calling upon UN member-states to strengthen international cooperation against terrorism); S.C. Res. 1624, *supra* note 187, ¶ 1(a) (calls upon UN member-states to prohibit "incitement to commit a terrorist act or acts"); S.C. Res. 1373, *supra* note 185, ¶ 3(a) (calling upon UN member-states to increase international cooperation by way of exchanging information regarding "use of communications technology by terrorist groups").

257. G.A. Res. 51/210, *supra* note 184, 3(c).

258. *See, e.g., Bucharest Summit Declaration*, *supra* note 175, para. 15 (announcing a commitment to fully implement UNSCR 1373 and "related UNSCRs, in particular UNSCR 1540").

259. *See* Randall, *Universal Jurisdiction*, *supra* note 216, at 789 (arguing that in the postwar decades states have generally recognized that some crimes required prosecution or extradition regardless of the nationality of the accused or the location of the crime).

260. Lori F. Damrosch, *Comment: Connecting the Threads, in* UNIVERSAL JURISDICTION: NATIONAL COURTS AND THE PROSECUTION OF SERIOUS CRIMES UNDER INTERNATIONAL LAW, *supra* note 247, at 91, 93.

261. *Id.* at 93.

262. *See* Randall, *Universal Jurisdiction*, *supra* note 216, at 789–90 (noting the example of *United States v. Layton*, 509 F. Supp. 212 (N.D. Cal.), *appeal dismissed*, 645 F.2d 681 (9th Cir.), *cert. denied*, 452 U.S. 972 (1981), and citing remarks by Senator Specter, 131 CONG. REC. S8999 (daily ed. June 27, 1985) (statement of Sen. Specter), which argue that universal jurisdiction should be applied to terrorists by comparison to pirates and slave traders).

263. Also drawing this conclusion are, among others, Damrosch, *supra* note 260, at 93–94, and Randall, *Universal Jurisdiction*, *supra* note 216, at 789–90.

Thus, universal jurisdiction exists as a means of prosecuting and deterring cyberterrorists pursuant to a variety of rationales and analyses. Providing states with the ability to prosecute cyberterrorists would send "a strong message . . . to terrorists that they are never safe from prosecution."[264] Although such application is not without difficulty due to the nature of cyberspace, that difficulty would exist no matter what form of jurisdiction might be applied, and other prescriptive bases for jurisdiction, such as territorial jurisdiction, are fraught with even more difficulty. Effective deterrence would be impossible if an attacked state had to wait for a cyberterrorist either to voluntarily enter the country or be extradited by a country friendly to the attacked state. Applying the analyses and rationales provided by other international law scholars thus strengthens the case for universal jurisdiction over cyberterrorism.

2. The Non-Piracy Analogy

As noted above, the principle of universal jurisdiction to prosecute acts, under international law, is "the principle that certain crimes are so heinous and so universally recognized and abhorred, that a state is entitled or even obliged to undertake legal proceedings without regard to where the crime was committed or the nationality of the perpetrators or the victims."[265] Historically, universal jurisdiction applied only to pirates, who were considered enemies of all mankind.[266] Under universal jurisdiction, if pirates were caught, any state could prosecute them on behalf of the international community.[267] Although there does not seem to be a definitive definition of piracy, it generally is defined as an act committed by non-state actors aboard a vessel on the high seas or outside of any state's jurisdiction.[268]

In the past few decades, universal jurisdiction has become accepted with regard to a greater variety of violations of international law, such as war crimes,[269] crimes against humanity,[270] and

---

264. Fry, *supra* note 216, at 197–98 (arguing for deterrence but noting that the deterrence argument assumes that the terrorist is a rational actor, which may or may not be a valid assumption).

265. Stephen Macedo, *Introduction*, *in* UNIVERSAL JURISDICTION: NATIONAL COURTS AND THE PROSECUTION OF SERIOUS CRIMES UNDER INTERNATIONAL LAW, *supra* note 247, at 1, 4.

266. Randall, *Universal Jurisdiction*, note 216, at 791.

267. *Id.*

268. *See id.* at 791-98 (discussing the history and rationale behind universal jurisdiction over piracy).

269. Randall, *Universal Jurisdiction*, *supra* note 216, at 800; *see generally* Henry T. King, Jr., *Universal Jurisdiction: Myths, Realities, Prospects, War Crimes and Crimes Against Humanity: The Nuremberg Precedent*, 35 NEW ENG. L. REV. 281 (2001)

genocide.[271] In each of those instances, judges and scholars put forth the rationale that universal jurisdiction applies because of the heinousness of those crimes; they were seen as being so inherently wrong that they effectively were crimes against society.[272] Although piracy may have been used as an analogy, the specific circumstances of the crime were not at the heart of the analysis; instead, the heinousness of the crime in question, as well as, in some circumstances, the non-viability of territorial or national jurisdiction was the true rationale.[273] The Princeton Principles also recognize the heinousness of a crime as the basis for universal jurisdiction.[274]

Professor Kontorovich asserts that applications of universal jurisdiction based on the piracy analogy are meaningless because those analogies were wrongly based on the assumption that piracy was subject to universal jurisdiction due to its heinousness.[275] He explains that piracy actually was not considered especially heinous and therefore that could not have been the reason it was subject to universal jurisdiction.[276] His argument does not, however, entirely defeat the case for universal jurisdiction. Even if piracy was not considered especially heinous (and heinousness not the reason why piracy was undisputedly subject to universal jurisdiction),[277] that

---

(describing the expansion in application of universal jurisdiction after Nuremburg to include war crimes, and arguing for a continued expansion of universal jurisdiction).

270. Randall, *Universal Jurisdiction*, *supra* note 216, at 800.

271. *See* Randall, *Universal Jurisdiction*, *supra* note 216, at 834–37 (describing the legal development of genocide as a universal jurisdiction crime).

272. *See, e.g.*, Madeline H. Morris, *Universal Jurisdiction in a Divided World: Conference Remarks*, 35 NEW ENG. L. REV. 337, 337 (2001) ("The rationale for universal jurisdiction is that crimes such as genocide, war crimes, and crimes against humanity are an affront to humanity and, therefore, are of concern to all states.").

273. *See* Randall, Book Review, *supra* note 242, at 628 ("[M]oot today is an analysis of whether the current universal offenses are analogous to the original universal offense of piracy."); Leila Nadya Sadat, *Redefining Universal Jurisdiction*, 35 NEW ENG. L. REV. 241, 244 (2001) ("Application of the theory of universal jurisdiction in these case is predicated largely on the notion that some crimes are so heinous that they offend the interest of all humanity – indeed, they imperil civilization itself.").

274. *See* PRINCETON PROJECT ON UNIVERSAL JURISDICTION, THE PRINCETON PRINCIPLES ON JURISDICTION 23 (2001), *available at* http://lapa.princeton.edu/hosteddocs/unive_jur.pdf ("National courts can exercise universal jurisdiction to prosecute and punish, and thereby deter, heinous acts recognized as serious crimes under international law.").

275. Kontorovich, *supra* note 242, at 186.

276. *Id.*

277. Although Kontorovich is not able to explain what that reason was, it is unclear whether there is an explanation to be had. *See generally* Joshua Michael Goodwin, *Universal Jurisdiction and the Pirate: Time for an Old Couple to Part*, 39 VAND. J. TRANSNAT'L L. 973 (2006) (examining the history of piracy and submitting various rationales for subjecting piracy to universal jurisdiction, such as disruption of trade and other economic concerns, but not determining that any one explanation is correct).

does not necessarily render the last few decades of international criminal law meaningless.

In the last few decades, the international community has recognized a number of international crimes as subject to universal jurisdiction. Those international crimes, such as genocide, war crimes, and crimes against humanity, provide at a minimum the opportunity for a state to act on behalf of itself and the international community by addressing the heinous act(s) in question.[278] Merely because the Nuremberg Tribunal and the Israeli Supreme Court analogized the heinousness of war crimes to what they thought was the heinousness of piracy, their judgments did not rise and fall on whether war crimes were like piracy, but on whether war crimes were especially heinous acts.[279] The courts did not dwell, for instance, on whether the war crimes were committed on the high seas, outside of state control, by glorified robbers, or on a ship (to take it to its logical extreme).[280] Instead, they based their decisions on the gravity of the acts and the unlikelihood of the state to criminalize the acts, using piracy only as an analogy based on their (possibly misguided) understanding of why universal jurisdiction applied to piracy. One possible factual error cannot unmake decades of international criminal law. In fact, such a body of law has built up around the heinousness of a crime as the determining factor for extending universal jurisdiction that that is now understood as the litmus test, with piracy only an afterthought thrown in for good measure.[281]

Even treating piracy as simply a crime committed on the high seas by an individual or individuals without state permission,[282] as opposed to a particularly heinous crime, remarkable parallels can be drawn to cyberterrorism. First, each is committed beyond the control of any state, as the cyberspace easily can be analogized to the high

---

278. Professor Stephen P. Marks identifies some disagreement as to whether *aut dedere aut judicare* is an obligation (mandatory) or merely a right (permissive). *See* Stephen P. Marks, *The Hissène Habré Case, in* UNIVERSAL JURISDICTION: NATIONAL COURTS AND THE PROSECUTION OF SERIOUS CRIMES UNDER INTERNATIONAL LAW, *supra* note 247, at 131, 139 ("There is some disagreement as to whether this duty to extradite or punish under customary international law is permissive or mandatory."). *See also* Damrosch, *supra* note 260, at 94 ("[A]t a minimum all the prosecute-or-extradite crimes are ones as to which there is an *option* to exercise jurisdiction without any link to the crime other than custody of the offender.").

279. *See* Kontorovich, *supra* note 242, at 194–97 (discussing the use and necessity of the piracy analogy in the Nazi War Crimes Tribunals and the Eichmann trial).

280. *See id.* at 196 (addressing the Israeli Supreme Court's contention that if a broader principal (such as "heinousness") could not be drawn from the example of piracy, then Universal Jurisdiction might only be relevant to piracy).

281. *Id.* at 185.

282. *See id.* at 186 (arguing that piracy was not subject to universal jurisdiction because of its heinousness); Morris, *supra* note 272, at 339–40 (arguing that definitions of piracy as private activity were specifically intended to prevent universal jurisdiction over piracy from causing international conflict).

seas.[283] Although states have attempted to prosecute for actions involving the Internet,[284] no one state controls cyberspace. Second, each crime is committed by individuals or groups of individuals acting without state consent. Indeed, should either piracy or cyberterrorism be conducted by state actors, such actions would be considered acts of aggression and, possibly, acts of war.[285] Third, each threatens international trade and the global economy.[286] Finally, each is a form of crime meant to further the actor's agenda—for pirates, the motive is financial; for cyberterrorists, the motive is primarily religious or political, although it may also be financial in order to finance the religious or political agenda.[287]

3. A Six-Fold Rationale

The question of whether to extend universal jurisdiction to cyberterrorism also can be analyzed under the multiple rationales outlined by Professor Jonathan Marks,[288] most of which support universal jurisdiction for cyberterrorism. The rationales variously draw from philosophy, political science, democratic theory, international relations, and international law, in order to explain universal jurisdiction.[289]

First, the Manichean rationale "considers the perpetrators of serious international crimes to be enemies of all mankind by reason of the 'heinous' crimes that they have committed."[290] This early

283. As recognized above in *supra* Part V.A, there may be circumstances where the Internet may not be considered borderless or territory-less, but those analyses do not apply in the context of cyberterrorism.

284. *See, e.g.*, Yahoo! Inc. v. L.I.C.R.A., 169 F. Supp. 2d 1181, 1194 (N.D. Cal. 2001) (granting a declaratory judgment that a French Court could not enforce its court order that Yahoo! remove Nazi content from its auction site due to First Amendment concerns).

285. *See* JAMES A. LEWIS, ASSESSING THE RISKS OF CYBER TERRORISM, CYBER WAR AND OTHER CYBER THREATS 3–4 (2002) (stating that cyberattacks by nation states would almost certainly be seen as acts of war), *available at* http://www.steptoe.com/publications/231a.pdf.

286. *See* Traynor, *supra* note 13 (describing an instance in which an attack seriously affected Estonia's banking system).

287. *See* BRENNER, *supra* note 12, at 7, 41 (describing the motivations of such individuals).

288. *See generally* Marks, *Mending the Web*, *supra* note 248 (describing the Manichean rationale, the common interest rationale, the agency rationale, the jus cogens rationale, the harm rationale and the pragmatic rationale). *Id.* Indeed, after describing these rationales, Marks (briefly) applies them to terrorism himself and concludes that "many states would now consider acts of international terrorism to pose the greatest threat to international peace and security as well as to their national interests, and it may only be a matter of time before serious acts of international terrorism are recognized as attracting universal jurisdiction in their own right." *Id.* at 471.

289. *Id.* at 463–71.

290. *Id.* at 463.

rationale is based largely on piracy. The Manichean rationale for universal jurisdiction applies to cyberterrorism because, as described above, cyberterrorists also are perpetrators of serious international crimes that are considered especially heinous. Furthermore, as discussed above, one can easily draw analogies between cyberterrorism and piracy, regardless of whether piracy originally was considered especially heinous.

Second, the common interest rationale, based on Kant's Perpetual Peace,[291] considers universal jurisdiction to be an extension of the protective principle of prescriptive jurisdiction.[292] The protective principle enables a state to exercise jurisdiction over crimes that are considered to threaten the state's national interests.[293] All states have an interest in prosecuting cyberterrorists, as cyberterrorists threaten to undermine the global financial infrastructure and are a threat to national and international security. Thus, each state may consider cyberterrorism as a threat to its national interests and, therefore, exercise protective jurisdiction.

Third, the agency rationale sees the prosecuting state as acting as the agent for the international community: "[T]he universality of the norms violated becomes the premise for the universal nature of the criminal jurisdiction that is being exercised."[294] There may be a certain aspect of rationalization to this common definition of universal jurisdiction, however. The traditional Realist school of international relations would argue that this is merely the common interest rationale dressed up for international acceptance, as the state will act to protect its interests before it will be concerned with maintaining order in international society.[295] To the extent that the Realist school is wrong or that a state simply sees it in its interest to maintain order in international society by prosecuting cyberterrorists, the agency rationale would support the exercise of universal jurisdiction over cyberterrorists.[296]

---

291. *Id.* at 465 ("'The peoples of the earth have . . . entered in varying degrees into a universal community, and it has developed to the point where a violation of rights in *one* part of the world is felt *everywhere*.'") (quoting Immanuel Kant, *Perpetual Peace: A Philosophical Sketch*, *in* KANT'S POLITICAL WRITINGS 107–08 (H.B. Nisbet trans., Hans Reiss ed., 1970)).

292. *Id.*

293. *Id.*; *see also* Fry, *supra* note 216, at 173 (listing the protective principal as a source of international jurisdiction); Randall, *Universal Jurisdiction*, *supra* note 216, at 787–88 (listing the protective principal as a source of international jurisdiction).

294. Marks, *Mending the Web*, *supra* note 248, at 467.

295. *See generally* HANS MORGENTHAU, KENNETH THOMPSON, & DAVID CLINTON, POLITICS AMONG NATIONS (7th ed. 2005) (discussing different understandings of international relations).

296. *See* Marks, *Mending the Web*, *supra* note 248, at 467 ("On this view, the universality of the norms violated becomes the premise for the universal nature of the criminal jurisdiction that is being exercised.").

Fourth, the *jus cogens* rationale Marks articulated seems to hold simply that if an international crime violates a *jus cogens* norm, universal jurisdiction exists for any state to prosecute that violation.[297] This analysis makes the incorrect assumption that universal jurisdiction is available only for *jus cogens* violations, however.[298] Numerous violations of international law are subject to universal jurisdiction and are not recognized as *jus cogens* norms; for example, many consider terrorism to be subject to universal jurisdiction even though it not considered a *jus cogens* norm.[299]

The fifth rationale, the harm rationale, provides even stronger justification for universal jurisdiction. The harm rationale states that "[w]hat should be of most concern is . . . the enormity of [the] acts," including the destruction of societal structures, physical and psychological damage to victims, and the concern "that the perpetrators of such serious international crimes may carry out such acts again."[300] This is essentially a version of the heinousness analysis; as discussed above, these concerns certainly apply to cyberterrorism, both because of the potential for serious disruption of entire governments and world commerce, and because, as a result of the technological methods available for covering one's tracks, apprehension of the cyberterrorist is extremely difficult. Thus, not only is the enormity of the acts arguably unparalleled but there is a significant likelihood of repeat attacks.

Finally, the pragmatic rationale "asserts that universal jurisdiction is justified when the perpetrator of the crimes would otherwise go unpunished."[301] This rationale is concerned with policy considerations such as deterrence and the promotion of peace and justice. For the reasons described below, it is doubtful that cyberterrorists would be prosecuted in the absence of universal jurisdiction, as significant practical difficulties exist that essentially bar the application of territorial jurisdiction. Although it is conceivable that territorial or other forms of prescriptive jurisdiction,

---

297. *See id.* at 468 ("International Law provides that offences jus cogens may be punished by any state because the offenders are 'common enemies of all mankind and all nations have an equal interest in their apprehension and prosecution.'") (quoting *Ex Parte* Pinochet Ugarte (No. 3), [2002] 1 A.C. 198 (H.L. 2002)).

298. *See, e.g.*, Randall, *Universal Jurisdiction, supra* note 216, at 789 (observing that states have recognized universal jurisdiction over some terrorist acts).

299. *See* Damrosch, *supra* note 260, at 93 (arguing that international law has "moved fairly far down a trajectory under which many (perhaps most or even all) forms of terrorism now entail prosecute-or-extradite obligations" and that "many commentators understand the category of universal jurisdiction crimes as more or less congruent with those entailing prosecute-or-extradite obligations"); Randall, *Universal Jurisdiction, supra* note 216, at 789 ("In the postwar decades, states at least impliedly have recognized that universal jurisdiction also extends to certain terrorist acts.").

300. Marks, *Mending the Web, supra* note 248, at 469.

301. *Id.* at 470.

such as protective jurisdiction, could apply, universal jurisdiction certainly would provide the most efficient basis for prosecution.

4. Dispelling Other Potential Concerns

Various scholars have raised a number of other concerns and potential problems with the application or extension of universal jurisdiction to terrorism generally or to cyberterrorism specifically. When examined closely, however, it is apparent that there is no cause for concern.

First is the concern that terrorism is difficult to define, and that "one man's terrorist is another man's freedom fighter."[302] This concern is no longer valid. Rephrasing the same concept in terms of genocide, for example—"one man's genocide is another man's ethnic cleansing"—the absurdity of the concept is readily apparent. It is undisputed that genocide is an international crime;[303] the similar classification of terrorism (and, by extension, cyberterrorism) also should not be disputed. Furthermore, as the United Nations Security Council stated in Resolution 1566, terrorism is "under no circumstances justifiable by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature."[304] Thus, the old adage has outlived its usefulness; there is no justification for terrorism or, by extension, cyberterrorism.

A second concern is that universal jurisdiction will become "a wildfire, uncontrolled in its application and destructive of the international legal processes."[305] There is little chance of this, however, primarily because determining the identity of a cyberterrorist is exceedingly difficult. As described above, it is extremely difficult to determine with any degree of certainty the location from which a cyberterrorist is attacking. Add to that the presumption that a cyberterrorist likely would execute evasive maneuvers such as spoofing or using anonymous or masked IP addresses, and the likelihood of identifying a cyberterrorist with any reasonable degree of certainty drops off dramatically.

---

302. United States v. Yousef, 327 F.3d 56, 107 (2d Cir. 2003); *see* Parvez Ahmed, *Terror In the Name of Islam—Unholy War, Not Jihad*, 39 CASE W. RES. J. INT'L L. 759, 764–65 (2007–2008) (arguing that even a just cause does not excuse a terrorist act, and analyzing the common characteristics of several definitions of terrorism).

303. *See* Randall, *Universal Jurisdiction*, *supra* note 216, at 834–37 (discussing the jurisdictional justifications for prosecution of genocide, and concluding that while the Genocide Convention only creates a territorial *obligation* to prosecute genocide, customary international law creates a *right* to exercise universal jurisdiction over genocide); Convention on the Prevention and Punishment of the Crime of Genocide, Dec. 9, 1948, 78 U.N.T.S. 277, 278 ("[G]enocide is a crime under international law.").

304. S.C. Res. 1566, *supra* note 186.

305. Bassiouni, *supra* note 245, at 154.

Furthermore, when an attack occurs, it is unclear whether it is actually cyberterrorism or just the proverbial teenage hacker.[306] In the Estonian cyberattack, experts were unsure whether they could ascertain the identity (or identities) of the hacker(s) at all, much less discover individual names.[307] Some Estonian officials claimed that the Russian government was responsible for the attack, but Russia vehemently denied the allegations.[308] One individual, Dmitri Galushkevich, was convicted and fined for an attack that blocked the website of the Reform Party of Estonian Prime Minister Andrus Ansip.[309] Members of the Kremlin-backed youth movement Nashe subsequently claimed responsibility for the attacks, although they claimed that the attacks were not illegal in any way.[310] Similarly, in the Titan Rain incident, it was unclear whether the attacks were initiated by the Chinese government or simply hackers using notoriously permeable Chinese networks to disguise the origins of their attacks.[311]

This hopping around networks is common precisely because it helps evade detection. Cyberterrorists often use China as a jumping off point due to its relatively lax security.[312] This complicates efforts to pinpoint the identity and location of attackers, as the fact that the apparent source of an attack was a Chinese computer does not necessarily mean that the attack actually came from China.[313]

---

306. De Borchgrave, *supra* note 19 (quoting a Pentagon employee).

307. *See* Traynor, *supra* note 13 ("Expert opinion is divided on whether the identity of the cyber-warriors can be ascertained properly.").

308. *See* Halpin, *supra* note 12 (reporting accusations from Estonian officials); *Estonia Fines Man for "Cyberwar,"* BBC NEWS, Jan. 25, 2008, http://news.bbc.co.uk/2/hi/technology/7208511.stm ("Moscow denied any involvement.").

309. *Estonia Fines Man for "Cyberwar," supra* note 308.

310. Charles Clover, *Kremlin-Backed Group Behind Estonia Cyber Blitz*, FIN. TIMES, Mar. 11, 2009, http://www.ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html?nclick_check=1.

311. *See* Graham, *supra* note 166 (describing Tin Rain, and explaining that Pentagon officials were split as to whether the attacks were originated by the Chinese government or simply the result of the large number of vulnerable computers in China). Such was also the case with respect to foreign utilities that were hacked in 2008. *See* Ellen Nakashima & Steven Mufson, *Hackers Have Attacked Foreign Utilities, CIA Analyst Says*, WASH. POST, Jan. 19, 2008, at A4, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/01/18/AR2008011803277.html (noting that "cyber attackers have hacked into the computer systems of utility companies outside the United States and made demands, in at least one case causing a power outage that affected multiple cities" and, quoting a top CIA cybersecurity official, "'We do not know who executed these attacks or why, but all involved intrusions through the Internet'").

312. *See* Graham, *supra* note 166 (noting that hackers might employ the large number of vulnerable computers in China to launch attacks).

313. *See id.*

> Pentagon figures show that more attempts to scan Defense Department systems come from China, which has 119 million Internet users, than from any other country. [Lieutenant Colonel Mike VanPutte, Vice Director of Operations

Although this presents a practical difficulty to exercising universal jurisdiction,[314] the difficulty of determining the identity (or identities) of the cyberterrorist(s) must be overcome before any prescriptive jurisdiction can be claimed, including territorial jurisdiction. This simple reality of criminal prosecution is inherently complicated due to the technical realities of cyberspace.

Others dispute that universal jurisdiction should be applied to a greater variety of violations of international law, citing concerns that prosecution may be arbitrary and that there is no consideration of sovereign immunity.[315] The trend of recognizing universal jurisdiction over terrorism continues despite those critiques, however, and with good reason: there are clear analogies between the (once) ancient crime of piracy and the more recently recognized crimes of genocide, crimes against humanity, and terrorism and, most importantly, there are clear analogies to be drawn between each of the aforementioned crimes and the twenty-first century crime of cyberterrorism.

The application of universal jurisdiction to cyberterrorism fits within the natural evolution of international criminal law and is a logical and measured response to the threat to international peace and security posed by cyberterrorism. Although the authors of the 2001 Princeton Principles considered adding terrorism to the list of crimes subject to universal jurisdiction but ultimately did not, they nonetheless explicitly recognized that the list is neither exhaustive nor static.[316] Furthermore, the world has changed since then. In the

---

for the U.S. Strategic Command Joint Task Force for Global Network Operations] said this does not mean that China is where all the probes start, only that it is 'the last hop' before they reach their targets. He noted that China is a convenient 'steppingstone' for hackers because of the large number of computers there that can be compromised. Also, tracing hackers who use Chinese networks is complicated by the lack of cyber investigation agreements between China and the United States, another task force official said.

314. Professor Kenneth C. Randall suggests that "[p]erhaps the most serious obstacle to exercising universal jurisdiction comes in the form of international politics." Kenneth C. Randall, Book Review, 99 AM. J. INT'L L. 293, 297 (2005) (reviewing UNIVERSAL JURISDICTION: NATIONAL COURTS AND THE PROSECUTION OF SERIOUS CRIMES UNDER INTERNATIONAL LAW, *supra* note 247). Although international politics can complicate the exercise of universal jurisdiction, and may in other circumstances pose the largest difficulty, the territory-less nature of cyberspace poses the largest obstacle for exercising universal jurisdiction over cyberterrorists.

315. *See, e.g.*, Henry Kissinger, *The Pitfalls of Universal Jurisdiction*, FOR. AFF., July-Aug. 2001, at 86, 86 (expressing fears of "substituting the tyranny of judges for that of governments"); *see also* Marks, *Mending the Web*, *supra* note 248, at 471–75 (describing various objections to universal jurisdiction). *But see* Kenneth Roth, *The Case for Universal Jurisdiction*, FOR. AFF., Sept.-Oct. 2001, at 150, 153 (recognizing that Kissinger's concerns are legitimate but stating that in certain respects they may be "overblown").

316. The list is described as "explicitly illustrative, not exhaustive. Principle 2(1) leaves open the possibility that, in the future, other crimes may be deemed of such a

intervening eight years, the world has seen an exponential increase in terrorist activity and a parallel exponential increase in dependence on the Internet.[317] Modern states should recognize these realities and their attendant implications.

Some contest this conclusion and argue against looking to universal jurisdiction so quickly. Professor Abu-Odeh argues that universal jurisdiction should not be recognized as a binding principle of international law because it would be disproportionately enforced and therefore have disproportionate effects both on those prosecuted under a theory of universal jurisdiction and on the balance of power in the world.[318] Professor Abu-Odeh presents this argument by assessing three questions: (1) "[T]he judges of which countries are more likely to exercise jurisdiction over such cases?" (2) "[W]hat kind of crimes are more likely to be deemed 'heinous' by those judges?" and (3) "[W]hat would be the effect of those judges' decisions on the overall balance of power in the world?"[319] Although his is a cogent argument, a fair question he does not present is, "What would happen if international crimes were not prosecuted?"

Indeed, Professor Abu-Odeh's critique of universal jurisdiction arguably applies to all international law. Regardless of the theory of jurisdiction, states ultimately choose whether or not to prosecute. The potential biases that Professor Abu-Odeh identifies in states' determination of whether to prosecute and what crimes to prosecute, to the extent that they exist, apply equally to all forms of jurisdiction under international law.

Returning to the unasked question, the answer is that if international crimes are not prosecuted, international criminals like cyberterrorists will flourish undeterred, secure in the knowledge that they can commit the most heinous act imaginable without even the possibility of being held accountable. Although prosecution of cyberterrorism is imperfect, a complete lack of prosecution is not a tenable option.

---

heinous nature as to warrant the application of universal jurisdiction." Becker, *supra* note 243, at 1375.

317. *See Internet Growth Cooling, but Dependence Increasing—Survey,* AFX NEWS LIMITED, Mar. 29, 2006, http://www.forbes.com/feeds/afx/2006/03/29/afx2632297.html (reporting an international study which found an increase in dependence on the Internet); *see, e.g.*, Timothy Williams, *Iraq Bombings, Deadliest Since 2007, Raise Security Issue,* N.Y. TIMES, Oct. 25, 2009, at A1, *available at* http://www.nytimes.com/2009/10/26/world/middleeast/26iraq.html?_r=1&hp (describing a violent contemporary bombing in Baghdad, as well as past terrorist attacks in Iraq).

318. Lama Abu-Odeh, *A Radical Rejection of Universal Jurisdiction,* 116 YALE L.J. (POCKET PART) 393 (2007).

319. *Id.*

VI. CONCLUSION

Cyberterrorism poses perhaps the greatest threat to national and international security since the creation of weapons of mass destruction. As states and their economies become increasingly intertwined, largely due to the Internet and the international financial system of global trade, the effects of a cyberterrorist attack will be greater. Similarly, as cyberterrorists gain experience in disrupting national governments and shutting down critical infrastructure, their attacks likely will become increasingly successful. Although states, private industry, and international organizations have made significant efforts to increase international cooperation, much more needs to be done. In taking action, however, it must be understood that, due to the fundamental weakness of the structure of the Internet, those additional efforts will not completely prevent cyberterrorism. As a result, further efforts at international cooperation and international standards must be part of a layered approach to cyberterrorism that also includes deterrence.

As a result of the realities inherent to cyberspace, the most feasible way to deter cyberterrorism is through the international law principle of universal jurisdiction. This is not to say that territorial jurisdiction (or nationality, passive personality, or protective jurisdiction) could not be used to prosecute cyberterrorists, should there be sufficient information and state willingness to exercise other forms of jurisdiction. It is merely to say that universal jurisdiction is likely to be the most feasible manner of prosecution and, therefore, deterrence. A layered approach of mitigation and deterrence can reduce the threat of cyberterrorism substantially. Unless and until states are willing to exercise universal jurisdiction over cyberterrorist acts as part of that layered approach, however, it is only a matter of time before cyberterrorists are able to unleash a cyber-apocalypse.