PROSECUTING CYBERTERRORISTS: APPLYING TRADITIONAL JURISDICTIONAL FRAMEWORKS TO A MODERN THREAT

Paul N. Stockton* & Michele Golabek-Goldman**

The United States faces a growing risk of cyberterrorism against its financial system, electric power grid, and other critical infrastructure sectors. Senior U.S. policymakers note that building U.S. capacity to prosecute cyberterrorists could play a key role in deterring and disrupting such attacks. To facilitate prosecution, the federal government is bolstering its technical expertise to attribute attacks to those who perpetrate them, even when, as is increasingly the case, the perpetrators exploit computers in dozens of nations to strike U.S. infrastructure. Relatively little attention has been paid, however, to another prerequisite for prosecuting cyberterrorists: that of building a legal framework that can bring those who attack from abroad to justice.

The best approach to prosecuting cyberterrorists striking from abroad is to add extraterritorial application to current domestic criminal laws bearing on cyberattack. Yet, scholars have barely begun to explore how the United States can best justify such extraterritorial extension under international law and assert a legitimate claim of prescriptive jurisdiction when a terrorist hijacks thousands of computers across the globe. Still less attention has been paid to the question of how to resolve the conflicting claims of national jurisdiction that such attacks would likely engender.

This Article argues that the protective principle—which predicates prescriptive jurisdiction on whether a nation suffered a fundamental security threat—should govern cyberterrorist prosecutions. To support this argument, the Article examines the full range of principles on which States could claim prescriptive jurisdiction and assesses their strengths and weaknesses for extending extraterritorial application of U.S. statutes to cyberterrorism. This Article also contends that if multiple nations asserted legitimate claims of jurisdiction based on the protective principle, sequential prosecutions would provide the best way to minimize

* Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs from June 2009 until January 2013, and President of Cloud Peak Analytics and Managing Director, Sonecon, LLC.

** J.D. Candidate 2014, Yale Law School, and M.P.P. Candidate 2014, Harvard Kennedy School of Government. The authors wish to thank Yale Law School Professors Lea Brilmayer and Oona Hathaway, whose invaluable comments and suggestions greatly contributed to this article. We also thank Julie Krishnaswami for her research assistance.

potential disagreements over which nation receives precedence. Both recommendations—to utilize the protective principle for prescriptive jurisdiction and to rely on sequential prosecutions to resolve multiple jurisdictional claims—could be important components of future international agreements to address cyberterrorism.

> We meet today at a transformational moment—a moment in history when our interconnected world presents us, at once, with great promise but also great peril . . . . [I]t's now clear that this cyber threat is one of the most serious economic and national security challenges we face as a nation.
>
> —President Obama[1]

INTRODUCTION

The United States faces a "rapidly growing threat from cyber-attacks," warned President Barack Obama in his 2013 State of the Union address. In particular, the President noted that U.S. adversaries are "seeking the ability to sab-

1. Remarks on Securing the Nation's Infrastructure and Communications Infrastructure, 1 PUB. PAPERS 731 (May 29, 2009).

otage our power grid, our financial institutions, and our air traffic control systems."[2] Leon Panetta, while serving as Secretary of Defense, singled out cyberterrorism as posing a dire threat to such targets. Stating that the United States is in a "pre-9/11 moment," Panetta noted that "attackers are plotting" to attack U.S. infrastructure with potentially devastating effects, and that "a destructive cyber-terrorist attack could virtually paralyze the nation."[3]

The Obama Administration is pursuing a wide array of initiatives to secure critical infrastructure from cyberattack.[4] Yet, one potentially vital opportunity for progress in cybersecurity has received relatively little attention: that of building an effective legal framework to prosecute cyberterrorists.[5] In October 2012, Lisa Monaco, U.S. Assistant Attorney General for National Security, noted the seriousness of the cyber threat posed by terrorists and other state and non-state actors, and emphasized that "prosecutions will be critical tools for deterrence and disruption" of such attacks.[6] We concur. If terrorists faced a substantial risk that they would be prosecuted for attacking U.S. critical infrastructure, they might be deterred from doing so. In the case of terrorists committed to attacking despite such risks, the ability to prosecute the plotters before they struck their targets would also be invaluable. Moreover, as part of a broader effort to build international norms and agreements in the cyber realm, creating a

2. Address Before a Joint Session of Congress on the State of the Union, 2013 DAILY COM. PRES. DOC. 90 (Feb. 12, 2013).

3. Leon Panetta, U.S. Sec'y of Def., Remarks on Cybersecurity to the Business Executives for National Security, New York City (Oct. 11, 2012) (transcript available at http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136).

4. This Article uses the definition of critical infrastructure as provided in Presidential Policy Directive/PPD-21 Subject: Critical Infrastructure Security and Resilience: "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Directive on Critical Infrastructure Security and Resilience, 2013 DAILY COM. PRES. DOC. 92 (Feb. 12, 2013).

5. This Article defines cyberterrorism as "premeditated, politically motivated cyberattacks perpetrated against civilian targets by subnational groups or clandestine agents intended to intimidate or coerce a government or its population in furtherance of political, religious, or ideological objectives by: a) inflicting, conspiring, or having the serious potential to inflict damage to a nation's critical infrastructure or extensive damage to its economy or b) inflicting, conspiring, or having the serious potential to inflict human deaths or injuries." This definition is modeled after 22 U.S.C. § 2656f(d) (2006). *See also* Jeffrey Thomas Biller, Cyber-Terrorism: Finding a Common Starting Point (May 20, 2012) (unpublished Master of Laws thesis) (on file with George Washington School of Law). Under this definition, a cyberattack perpetrated by an al-Qaeda agent, another self-proclaimed terrorist, or a politically motivated attacker that crippled a country's financial institutions, communications systems, or other critical infrastructure would be classified as cyberterrorism even if there were no resulting physical injuries or deaths. By inflicting widespread economic damage, the perpetrator aims to cause social and political turmoil and undermine civilians' faith in their government's ability to safeguard their way of life.

6. Lisa Monaco, Assistant Attorney Gen. for Nat'l Sec., Dep't of Justice, Speech at the 2012 Cybercrime Conference (Oct. 25, 2012) (transcript available at http://www.justice.gov/nsd/opa/pr/speeches/2012/nsd-speech-121025.html).

legal framework for prosecution with a strong foundation in international law would be a critical step forward in building a global approach to defeat cyberterrorism.

Building U.S. capacity to prosecute cyberterrorists will require progress in three especially important realms. First, the United States will need to improve its technical means to attribute attacks to those responsible for them, even when the attackers go to elaborate lengths to hide their identity. Attribution is especially difficult when attackers hijack thousands of computers across the globe without the owners' knowledge and commandeer these computers to conduct coordinated "botnet" operations. Such cross-jurisdictional botnet operations occurred when the Republic of Estonia suffered nationwide Distributed Denial of Service ("DDOS") attacks. The perpetrators used approximately one million "zombie" computers, located in countries ranging from Vietnam to the United States, to incapacitate Estonia's computer systems.[7] Large-scale botnet DDOS attacks are now occurring against U.S. banks and companies in other critical infrastructure sectors as well, with perpetrators reportedly employing tens of thousands of computers, half of which are overseas.[8] Accurately attributing massive, cross-jurisdictional botnet attacks to the perpetrator—and then marshaling the evidence to prove responsibility for the attack in a court of law—will require the resolution of major technical challenges.[9]

U.S. government and private sector organizations are intensively working to meet these attribution challenges. A revealing example of progress occurred in February 2013, when U.S. computer security company Mandiant detailed how it traced back cyberattacks to a specific group of perpetrators in a twelve-story office tower in Shanghai, China.[10] The Federal Bureau of Investigation ("FBI") and other federal agencies are also launching an intensive effort to strengthen U.S. attribution capabilities. They are creating new partnerships with private sector owners of critical infrastructure and state and local law enforcement to collect and share cyberattack data necessary for attribution efforts.[11]

---

7. Katharine C. Hinkle, *Countermeasures in the Cyber Context: One More Thing to Worry About*, 37 YALE J. INT'L L. ONLINE 11, 13-14 (2011).

8. *See* Siobhan Gorman & Danny Yadron, *Banks Seek U.S. Help on Iran Cyberattacks*, WALL ST. J. (Jan. 18, 2013), http://www.iranfocus.com/en/index.php?id=26837%3Abanks-seek-us-help-on-iran-cyberattacks&tmpl=component&layout=default&page=&option=com_content&Itemid=26; Ellen Nakashima, *Banks Seek NSA Help Amid Attacks on their Computer Systems*, WASH. POST (Jan. 11 2013), http://articles.washingtonpost.com/2013-01-11/world/36272281_1_banks-ddos-nsa.

9. For an overview of the technical problems associated with attribution, see David D. Clark & Susan Landau, *Untangling Attribution*, *in* NAT'L RES. COUNCIL, PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS 25-40 (2010).

10. *APT1: Exposing One of China's Cyber Espionage Units*, MANDIANT 11 (Feb. 2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

11. *See Cyber Security Responding to the Threat of Cyber Crime and Terrorism: Hearing before the Subcomm. On Crime and Terrorism of the Sen. Comm. On the Judiciary*, 112th Cong. 6 (2011) (statement of Gordon M. Snow, FBI Assistant Dir., Cyber Division); Robert S. Mueller, III, Dir., Fed. Bureau Investigation, Presentation to RSA Cyber Security

The FBI is also critically working with its law enforcement counterparts overseas to identify cyber criminals.[12]

In a second realm, the United States must develop the prosecutorial expertise and institutional framework necessary to address the specific problems posed by cyberterrorism. The National Security Division ("NSD") of the Department of Justice is devoting major resources to this effort. NSD has established a National Security Cyber Specialists' Network to serve as a "one-stop shop" to facilitate prosecution efforts, and is partnering with the Criminal Division's Computer Crime and Intellectual Property Section ("CCIPS") and U.S. Attorney's Offices around the nation to prosecute those who attack critical infrastructure and other assets vital to national security and the U.S. economy.[13]

In a third realm, however, progress has been notably absent. Scholars and policymakers have done little to build the legal framework needed to prosecute cyberterrorists who strike from abroad, and who launch cross-jurisdictional botnet attacks against U.S. critical infrastructure. Oona Hathaway et al. offer a comprehensive review of international and U.S. domestic legal tools currently available to help nations meet the challenges posed by cyberattacks from both state and non-state actors.[14] The authors find that major gaps exist in international law and agreements that apply to cyberattacks.[15] They also conclude that "existing domestic law largely fails to directly address the novel modern challenges posed by cyber-attacks, and is severely limited by its lack of extraterritorial reach."[16] They recommend, therefore, that the United States and other nations add extraterritorial applicability to their criminal laws bearing on cyberattack, as well as pursuing a longer-term effort to create an international treaty against cyber threats.[17]

We agree that extending the applicability of U.S. domestic laws to cover those who attack from abroad would provide a timely and much-needed basis to prosecute cyberterrorists. We argue, however, that two major issues must be

---

Conference: Combating Threats in the Cyber World: Outsmarting Terrorists, Hackers, and Spies (Mar. 1, 2012) (transcript available at http://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies); *National Cyber Investigative Joint Task Force*, FED. BUREAU INVESTIGATION, http://www.fbi.gov/about-us/investigate/cyber/ncijtf (last visited Jan. 11, 2014); *The NCFTA Combining Forces to Fight Cyber Crime*, FED. BUREAU INVESTIGATION (Sept. 16, 2011), http://www.fbi.gov/news/stories/2011/september/cyber_091611/cyber_091611.

12. *International Cooperation Disrupts Multi-Country Cyber Theft Ring*, FED. BUREAU INVESTIGATION (Oct. 1, 2010), http://www.fbi.gov/news/pressrel/press-releases/international-cooperation-disrupts-multi-country-cyber-theft-ring.

13. Monaco, *supra* note 6; *see also* Tracy Russo, *New Network Takes Aim at Cyber Threats to National Security*, DEP'T OF JUSTICE (Nov. 14, 2012), http://blogs.justice.gov/main/archives/2558.

14. Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 874-77 (2012).

15. *Id*. at 839-73.

16. *Id*. at 874 (footnotes omitted).

17. *Id*. at 877.

resolved before the United States can extend extraterritoriality in this manner. First, the United States would have to specify how such an extension of extraterritoriality could be justified under international law. For nations to apply their criminal statutes extraterritorially, they are required to first assert a legitimate basis of prescriptive jurisdiction. Prescriptive jurisdiction is defined as a sovereign state's authority to criminalize a given conduct or "apply its laws to certain persons or things."[18] If a nation that experienced a cyberterrorist attack lacked prescriptive jurisdiction over cyberterrorist activity, that nation would be precluded under international law from subjecting the perpetrator to its judicial process.[19] The five classical principles that justify prescriptive jurisdiction under international law are territoriality, nationality, passive personality, universality, and protection.

Nations claiming prescriptive jurisdiction most often invoke the principle of territoriality: the nation where a crime occurs has jurisdiction to prosecute the perpetrators. However, if a cyberterrorist launched a botnet attack from computers around the globe, it is unclear under international law whether jurisdiction should be predicated on where the cyberterrorist executed the attack, where the effects of the attack occurred, or the locations of the computers that were hijacked to perpetrate the attack.

Hathaway et al. do not address the issue of whether and how principles of prescriptive jurisdiction might justify the extraterritorial application of nations' domestic laws to cyberterrorists. The only article that examines that issue is authored by Kelly Gable. Gable proposes that nations prosecute cyberterrorists on the basis of universal jurisdiction, which allows states to claim criminal jurisdiction over a perpetrator regardless of whether they have any territorial connection to the crime.[20] Gable does not, however, adequately explore the effica-

---

18. Anthony J. Colangelo, *Constitutional Limits on Extraterritorial Jurisdiction: Terrorism and the Intersection of National and International Law*, 48 HARV. INT'L L.J. 121, 126 (2007).

19. Anthony J. Colangelo, *Double Jeopardy and Multiple Sovereigns: A Jurisdictional Theory*, 86 WASH. U. L. REV. 769, 781 (2009). The issue of prescriptive jurisdiction was recently front and center in the Alien Tort Statue (ATS) litigation before the Supreme Court. In *Kiobel v. Royal Dutch Petroleum Co.*, the extraterritorial reach of the ATS was challenged on numerous grounds, including its alleged lack of basis for prescriptive jurisdiction. *See* Brief of Chevron, et al. as Amici Curiae Supporting Respondents at 10-17, Kiobel v. Royal Dutch Petroleum, No. 10-1491 (Feb. 3, 2012). Since this article was submitted for publication, the Supreme Court has held that the "presumption against extraterritoriality applies to claims under the ATS, and that nothing in the statute rebuts that presumption." 133 S.Ct. 1659, 1669 (2013). Chief Justice Roberts' emphasis on practicing "judicial caution…in light of foreign policy concerns," together with Justice Breyer's concurring opinion invoking the Restatement's traditional bases for prescriptive jurisdiction, highlight the continued importance of these jurisdictional limits under international law. *Id.* at 1664-1673. It should be noted that the Court applied the presumption against extraterritoriality to the ATS, while acknowledging that the statute is "strictly jurisdictional." *Id.* at 1664.

20. *See* Kelly A. Gable, *Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, 43 VAND. J. TRANSNAT'L L. 57, 104-05 (2010).

cy of the many alternative principles of prescriptive jurisdiction that nations have applied to other violations of domestic law, or assess their relative strengths and weaknesses as a basis for extending extraterritoriality of U.S. laws to cover cyberterrorists attacking from abroad.

A second unresolved legal issue posed by cross-jurisdictional cyberterrorism is that of competing national claims of jurisdiction.[21] A single cyberterrorist group may simultaneously attack the critical infrastructure of a large number of nations. Indeed, if press accounts of the Stuxnet virus are true, there is substantial risk that attacks aimed at one nation may inadvertently spread to others.[22] At present, there is no agreed upon framework under international law that would determine which nation would have precedence to exercise jurisdiction over the accused. Without establishing a uniform approach, nations' assertions of jurisdiction would provoke unnecessary controversy and be vulnerable to charges of capricious abuse of power.[23] Relying on the principle of universal jurisdiction for such cases—which would enable all nations struck by an attack to simultaneously claim jurisdiction over the perpetrators—would magnify the likelihood of such conflict.

This Article argues that rather than rely on universal jurisdiction, the United States should justify the extension of extraterritoriality by using the protective principle of prescriptive jurisdiction for cyberterrorist attacks. The concept underlying the protective principle is simple and direct. This principle authorizes a nation to exercise jurisdiction over conduct outside its boundaries that directly threatens its security or critical government functions. Historically, nations have upheld jurisdiction based on the protective principle in cases involving terrorism, counterfeiting, drug trafficking, and immigration. If courts have held that these crimes sufficiently threaten national security to warrant jurisdiction, then a cyberterrorist attack that incapacitated a nation's power grid, jeopardizing public safety and the nation's economy, should also authorize jurisdiction under the protective principle. We also argue that if multiple states

---

21. The Lockerbie bombing, although a conventional terrorist attack, highlights the significant potential for states to wrangle over jurisdiction in cyberterrorist cases. On December 21, 1988, Pan Am Flight 103, flying from London to New York, exploded over Lockerbie, Scotland, killing 259 passengers and residents on the ground. Following the attack, Libya, the United States, and the United Kingdom quarreled over which nation should have jurisdiction over the suspects. The jurisdictional conflict deteriorated into a vehement dispute, made worse by the unfriendly relations and mutual distrust between the States involved. *See* MITSUE INAZUMI, UNIVERSAL JURISDICTION IN MODERN INTERNATIONAL LAW 163-66 (2005). Jurisdictional conflicts would be more frequent and of greater magnitude in cyberterrorist cases since attacks would emanate from and impact many more nations.

22. *See* James P. Farwell & Rafal Rohozinski, *Stuxnet and the Future of Cyber War*, 53 SURVIVAL 23 (Jan. 28, 2011), *available at* http://www.cyberdialogue.ca/wp-content/uploads/2011/03/James-Farwell-and-Rafal-Rohozinski-Stuxnet-and-the-Future-of-Cyber-War.pdf.

23. Stanley J. Marcuss & Eric L. Richard, *Extraterritorial Jurisdiction in United States Trade Law: The Need for a Consistent Theory*, 20 COLUM. J. TRANSNAT'L L. 439, 483 (1981).

have legitimate claims to protective jurisdiction over cyberterrorists, they should be entitled to conduct sequential prosecutions.

Part II of this Article summarizes the cyberterrorist threat and frames that threat in terms of broader U.S. efforts to secure critical infrastructure from cyberattack. A great deal of recent legal scholarship has examined how to apply the law of war to cyberattacks, and—in particular—to attacks by nation states or state-sponsored terrorists. Much less attention has been paid to examining the jurisdictional framework for prosecuting cyberterrorists when such attacks are not state-sponsored.[24] As Part II will argue, however, the threat posed by non-state sponsored terrorists to U.S. critical infrastructure is significant and of growing concern to senior U.S. policymakers. This Article focuses on such non-state sponsored actors and the development of a legal framework to bring them to justice.

It may often be challenging to differentiate between privately sponsored cyberterrorism and state-sponsored cyberterrorism. In contrast to state-sponsored conventional terrorism, nations can support cyberterrorist attacks without leaving behind a "large money, material, or communications 'trail,'" which verifies the nation's involvement.[25] The Internet is therefore a "perfect platform for plausible deniability."[26] Even if a cyberterrorist attack were traced back to a particular government, the government could deny responsibility, blaming the attack on terrorist organizations or "hacktivists." The prosecutorial framework that we propose would help ensure that cyberterrorists are brought to justice in cases where it would be impossible to corroborate state sponsorship.

Part III analyzes U.S. legal constraints on extraterritorial jurisdiction. In particular, it describes the *Charming Betsy* presumption and why statutes applied extraterritorially to prosecute cyberterrorists must be grounded on an accepted basis of prescriptive jurisdiction. Part III also provides an overview of the Computer Fraud and Abuse Act and other federal criminal statutes that the United States could conceivably use to prosecute cyberterrorists.

Part IV analyzes the five classical theories of prescriptive jurisdiction under international law—territoriality, nationality, passive personality, universality, and protection. It demonstrates that, given the borderless and unconventional features of cyberterrorism, the theories of territoriality, nationality, passive

---

24. *See, e.g.*, Daniel B. Silver, *Computer Network Attack as a Use of Force Under Article 2(4) of the United Nations Charter*, *in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 73 (Michael N. Schmitt & Brian T. O'Donnell eds., 2002); David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SEC. L. & POL'Y 87 (2010); Hathaway, *supra* note 14; Marco Roscini, *World Wide Warfare* – Jus ad Bellum *and the Use of Cyber Force*, 14 MAX PLANCK Y.B. UNITED NATIONS L. 85 (2010).

25. Matthew J. Littleton, Information Age Terrorism: Toward Cyberterror 103 (Dec. 1995) (unpublished thesis, Naval Postgraduate School) (on file with author), *available at* http://www.fas.org/irp/threat/cyber/docs/npgs/terror.htm.

26. Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 192, 208 (2009).

personality, and universality are ill-suited for effectively bringing the perpetrators of cyberterrorism to justice. Among these theories, the protective principle has the greatest potential to minimize competing jurisdictional claims, foil cyberterrorist plans before they are consummated, and ensure that cyberterrorists do not escape with impunity. Judicial precedents provide ample support for extending the protective principle to cyberterrorism.

In particular, this Article argues that in determining which prescriptive basis of jurisdiction should apply to cyberterrorist prosecutions, two objectives should be considered paramount. First, jurisdictional conflicts that threaten interstate relations should be avoided. In the legal jurisprudence on conflicts of law, conflicts of jurisdiction are generally categorized as positive or negative. A negative conflict occurs when no nation is willing to, or capable of, asserting jurisdiction. A positive conflict transpires when multiple states claim jurisdiction over the same case. In the context of cyberterrorism, negative conflicts would rarely occur due to the grave nature of cyberterrorist attacks and nations' consequent motivations to apprehend the perpetrators. In contrast, since a devastating cyberterrorist attack would transcend multiple nations, positive conflicts would abound. Competing jurisdictional claims could provoke interstate tension and undermine respect for international law and comity. In order to mitigate this possibility, the basis for exercising prescriptive jurisdiction over cyberterrorism should not be too expansive as to give rise to overlapping claims.

The second overarching objective that should guide the determination of an appropriate jurisdictional basis is that cyberterrorists should not be permitted to escape with impunity. Effective and persistent prosecutions of cyberterrorists are vital in order to secure justice for the victims and potentially deter future cyberterrorist attacks.[27] Therefore, the basis of prescriptive jurisdiction should not be so narrow as to prevent nations from exercising jurisdiction and effectively prosecuting the perpetrator.

In the context of cyberterrorism, the protective principle would minimize the number of competing jurisdictional claims, reduce international tension, and enable nations to preventively apprehend and prosecute cyberterrorists. Since not every nation affected by a cyberterrorist attack would suffer a critical threat to its security, there would be less potential for nations to wrangle over jurisdiction. Furthermore, given that nations that suffered direct threats to their security interests would have the strongest motive to investigate and apprehend the perpetrator, application of the protective principle would reduce the potential for terrorists to escape prosecution. Finally, the protective principle is the only jurisdictional basis under international law that authorizes extraterritorial

27. Gable, *supra* note 20, at 105.

jurisdiction over crimes that pose a potential danger to a nation's security.[28] The protective principle would therefore enable nations to prosecute cyberterrorists before devastating attacks occurred. This Article concedes that the determination of what constitutes a threat to a nation's security is inherently subjective, and thus the principle is vulnerable to politicization and abuse. The international community should thus make a concerted effort to define and limit the types of cyberterrorist attacks covered under the protective doctrine. This would increase predictability and reduce the potential for conflict among states.

In many cases, a cyberterrorist attack would severely endanger only one nation's security, even if it inflicted collateral damage elsewhere. In those instances, the protective principle would therefore completely eliminate conflicting jurisdictional claims.[29] However, in the scenario in which more than one state had a legitimate claim to protective jurisdiction, Part V recommends that sequential prosecutions should be authorized. The principle of *ne bis in idem*, which is conceptually similar to double jeopardy, is not required at the interstate level under international law. Sequential prosecutions by states that had valid claims to protective jurisdiction would reduce interstate tension and serve as a strong deterrent to cyberterrorism. Cyberterrorists would be warned that by launching a catastrophic and unpredictable cyberattack, they could potentially be subject to multiple judicial proceedings. Such a policy would also accord with our sense of justice because any state that experienced a catastrophic attack that threatened its security should be entitled to prosecute the perpetrator. Part VI demonstrates why a policy of sequential prosecutions would be superior to alternatives such as a balancing test or conferring jurisdiction on the nation that first gained custody over the defendant.

Our proposed jurisdictional framework is not a panacea for mitigating the threat of cyberterrorism. If the United States faces the prospect of an especially crippling attack on its critical infrastructure, more immediate measures to blunt that attack may be preferable to relying on prosecution of the perpetrators. We do not propose, then, that prosecution be the only remedy to address the threat of cyberterrorism. Rather, as part of a broader effort to counter this threat, building a legal framework to prosecute cyberterrorists would fill a significant gap in current U.S. efforts to secure infrastructure from attack, and provide an important new basis to deter cyberterrorists and—if deterrence fails—either help foil their attacks or bring them to justice.

---

28. Monika B. Krizek, *The Protective Principle of Extraterritorial Jurisdiction: A Brief History and an Application of the Principle to Espionage as an Illustration of Current United States Practice*, 6 B.U. INT'L L. J. 337, 345 (1988).

29. For an illustration of how the protective principle would eliminate overlapping jurisdictional claims, *see infra* Part IV.E.1.

I. THE THREAT OF CYBERTERRORISM TO U.S. CRITICAL INFRASTRUCTURE AND U.S. PREPAREDNESS AGAINST IT

Before determining how to assert prescriptive jurisdiction over cyberterrorists and resolve potential jurisdictional conflicts, an appropriate first step is to examine how current U.S. efforts to secure critical infrastructure could be bolstered by creating a legal framework to prosecute those who attack that infrastructure from abroad.

President Obama, in issuing his February 2013 Executive Order *Improving Critical Infrastructure Cybersecurity*, noted that "the cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront."[30] The pace of this growth is astonishing. General Keith Alexander, Commander of U.S. Cyber Command, reported that there was a seventeen-fold increase in computer attacks on U.S. critical infrastructure between 2009 and 2011. He also warned in July 2012 that the United States is dangerously vulnerable to such attacks. On a scale of one to ten, Alexander rated American preparedness for a large-scale cyberattack at "around 3."[31]

The private companies that own the vast majority of U.S. critical infrastructure face sustained computer network exploitation ("CNE") attacks. In CNE attacks, perpetrators steal trade secrets and other intellectual property, seize passwords and other computer network access tools, map computer networks and operating systems, and conduct other forms of data theft and intelligence gathering. Of course, critical infrastructure owners are not alone in facing such attacks from both state and non-state actors. According to the February 2013 Mandiant report on China, a single Chinese military unit had stolen hundreds of terabytes of data from 141 organizations in 20 industries in the United States and around the world, including owners of the U.S. electrical power grid, gas lines, and water infrastructure.[32] Those reported CNE attacks are only part of the broader global threat from state and non-state actors.[33]

CNE attacks not only endanger U.S. economic competitiveness, but also—especially in terms of mapping system vulnerabilities and gaining illicit access to computer networks—can help enable terrorists and other actors to execute Computer Network Attacks ("CAN"). For financial institutions and global stock markets, the possibility that attackers will use their network access to de-

30. Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 12, 2013).

31. David E. Sanger & Eric Schmitt, *Rise Is Seen in Cyberattacks Targeting U.S. Infrastructure*, N.Y. TIMES (July 26, 2012), http://www.nytimes.com/2012/07/27/us/cyberattacks-are-up-national-security-chief-says.html.

32. MANDIANT, *supra* note 10, at 3.

33. OFF. OF THE NAT'L COUNTERINTELLIGENCE EXECUTIVE, FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE, 1 (Nov. 2011), *available at* http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

stroy or corrupt data poses a special risk.[34] Banks and other components of the financial sector also face increasingly sophisticated Distributed Denial of Service ("DDOS") attacks, in which botnets overwhelm computer networks with massive, disruptive message traffic. Indeed, following the attacks on the Bank of America and other financial institutions that occurred in 2012, then-Secretary of Defense Panetta warned that "the scale and speed" with which perpetrators launched those attacks "was unprecedented."[35] Panetta also cautioned the owners of critical infrastructure companies and other business leaders that computer networks were becoming vulnerable to much more destructive cyberattacks. As a prime example, he cited the August 2012 "Shamoon" attack on the computer network of the Saudi oil company ARAMCO, which "rendered useless" more than 30,000 computers.[36]

The electric power grid, oil and gas infrastructure, and water systems face an additional CNA threat: that of attacks against their industrial control systems ("ICS") and Supervisory Control and Data Analysis ("SCADA") systems. These systems constitute the digital devices that control and monitor the operation of motors, pumps, and other equipment central to the functioning of gas pipelines and other operations critical to the economy and public safety. The Department of Homeland Security ("DHS") reports that the number of cyberattacks on SCADA systems is rapidly growing, as is their technical prowess.[37] Of particular concern is the rise of CNA capabilities to functionally destroy com-

---

34. Jason Ryan, *NSA Director on Cyberattacks: 'Everybody's Getting Hit,'* ABC NEWS (Nov. 7, 2012 7:53 PM), http://abcnews.go.com/blogs/politics/2012/11/nsa-director-on-cyberattacks-everybodys-getting-hit.

35. Panetta, *supra* note 3.

36. *Id*. More recent reporting indicates that the Shamoon attack may have been conducted by a perpetrator who had direct access to an ARAMCO computer and inserted a USB stick ("i.e., thumb drive) to introduce the malware into the ARAMCO business network that was responsible for billing and other administrative functions. The attack reportedly failed to disrupt the ARAMCO computer network responsible for oil production and other facility operations. Michael Riley & Eric Engleman, *Code in Aramco Cyber Attack Indicates Lone Perpetrator*, BLOOMBERG (Oct. 25, 2012), http://www.bloomberg.com/news/2012-10-25/code-in-aramco-cyber-attack-indicates-lone-perpetrator.html.

37. *See DHS: Industrial Control Systems Subject to 200 Attacks in 2012*, HOMELAND SEC. NEWS WIRE (Jan. 14, 2013), http://www.homelandsecuritynewswire.com/dr20130114-dhs-industrial-control-systems-subject-to-200-attacks-in-2012. The best summary of reports of recent SCADA system attacks and trends in cyber threats is provided by the Department of Homeland Security. *See, e.g*., Dep't Homeland Sec., *Industrial Control Systems-Cyber Emergency Response Team Monitor*, ICS-CERT MONITOR (Dec. 2012), ics-cert.us-cert.gov/pdf/ICS-CERT_Monthly_Monitor_Oct-Dec2012.pdf. For additional recent threat data on attacks on critical infrastructure industrial control systems, see Kennedy Maize, *Cyber Threats to SCADA Systems Are Real*, MANAGING POWER (July 18, 2012), http://www.managingpowermag.com/it/Cyber-Threats-to-SCADA-Systems-Are-Real-_388.html; *Vulnerability Trends: SCADA Vulnerabilities*, SYMANTEC (Jan. 2013), http://www.symantec.com/threatreport/topic.jsp?id=vulnerability_trends&aid=scada_vulnerabilities.

puters and other critical infrastructure assets, as reportedly occurred in the August 2012 attacks on ARAMCO.[38]

Of course, terrorists have other potentially advantageous means to destroy U.S. critical infrastructure, including high explosive attacks on vital system nodes and "insider" computer attacks on SCADA systems by rogue employees.[39] Launching cyberattacks from abroad also involves significant technical challenges. Debates persist over the degree to which attacks on industrial control systems require massive, carefully tailored malware programs to strike particular targets (capabilities that only large nation states can easily marshal), or whether these attacks can utilize more generic malware that exploits vulnerabilities widely shared across ICS components in the United States.[40] The example of Stuxnet, the cyberattack that destroyed 1,000 centrifuges at Iran's Natanz uranium enrichment facility, exemplifies this scholarly disagreement.[41] Some reports indicate that Stuxnet was carefully tailored to exploit specific vulnerabilities in the control mechanisms of enrichment centrifuges in Iran.[42] Other reports, including a 2011 analysis by the Congressional Research Service, indicate that a broad range of adversaries could develop new variants of Stuxnet to attack U.S. critical infrastructure, putting at risk public safety and "the government's ability to safeguard national security interests."[43]

The current ability of al-Qaeda and other non-state sponsored terrorist groups to meet these technical challenges is also unclear. Al-Qaeda operatives are calling for "electronic jihad" against the U.S. electric grid and other infrastructure components, and are urging Jihadists to exploit vulnerabilities in U.S. infrastructure networks just as they did with U.S. airlines on 9/11.[44] Opinions differ, however, over al-Qaeda's ability to launch such attacks today. In May

---

38. *See* Riley & Engleman, *supra* note 36.

39. NAT'L RESEARCH COUNCIL, TERRORISM AND THE ELECTRIC POWER DELIVERY SYSTEM 48 (2012). This book provides an excellent overview of threats to the electric power grid and—by extension—many other critical infrastructure sectors.

40. Ludovic Piètre-Cambacédès et al., *Cybersecurity Myths on Power Control Systems: 21 Misconceptions and False Beliefs*, 26 IEE TRANS. ON POWER DELIVERY 161, 161-72 (2011).

41. David Albright et al., *Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report*, INST. FOR SCI. & INT'L SEC. 1 (Feb. 15, 2011), http://isis-online.org/uploads/isis-reports/documents/stuxnet_update_15Feb2011.pdf.

42. *See* Mark Clayton, *How Stuxnet Cyber Weapon Targeted Iran Nuclear Plant*, CHRISTIAN SCI. MONITOR (Nov. 16, 2010), http://www.csmonitor.com/USA/2010/1116/How-Stuxnet-cyber-weapon-targeted-Iran-nuclear-plant.

43. PAUL KERR, ET AL., CONG. RESEARCH SERV., 7-5700, THE STUXNET COMPUTER WORM: HARBINGER OF AN EMERGING WARFARE CAPABILITY (Dec. 9, 2010), *available at* http://www.fas.org/sgp/crs/natsec/R41524.pdf; see also Mark Clayton, *Son of Stuxnet? Variants of the Cyberweapon Likely, Senators Told*, CHRISTIAN SCI. MONITOR (Nov. 17, 2010), http://www.csmonitor.com/USA/2010/1117/Son-of-Stuxnet-Variants-of-the-cyberweapon-likely-senators-told.

44. Jack Cloherty, *Virtual Terrorism: Al Qaeda Video Calls for 'Electronic Jihad,'* ABC NEWS (May 22, 2012), http://abcnews.go.com/Politics/cyber-terrorism-al-qaeda-video-calls-electronic-jihad/story?id=16407875#.UORononjkoY.

2012, then-Senator Susan Collins warned that al-Qaeda is aggressively seeking the ability to attack U.S. infrastructure, and that given the "huge increase in the number of cyberattacks against our country in the last two years, it would be naive for us to think that al-Qaeda is not responsible for at least some of those attacks."[45] The senior intelligence official at the Department of Defense's ("DoD") Cyber Command, Rear Admiral Samuel Cox, offered a contrasting perspective. He testified in 2012 that al-Qaeda's current cyberattack capabilities are weak. Cox warned however, that the cyber threat from al-Qaeda could rapidly increase, and that to gain the necessary expertise the group could "hire it, or blackmail it, or find the right person who has that skill set and be able to use that and rapidly increase their capabilities."[46] Assistant Attorney General Lisa Monaco offers a still more severe assessment of the terrorist threat. Citing "cyber-enabled terrorism" as a "major national security threat in cyberspace," Monaco noted that while terrorist organizations have not yet launched a full-scale cyberattack on the United States, "it is a question of when, not if, they will attempt to do so."[47]

The United States government and the private sector are partnering in innovative ways to protect critical infrastructure from cyberattack. The Obama Administration's February 2013 Executive Order on cybersecurity provides for improved information sharing to identify and block cyberattacks, and establishes a Voluntary Critical Infrastructure Cybersecurity Program to help the private sector identify, assess, and manage cyber risks.[48] The Department of Energy's Electricity Subsector Cybersecurity Capability Maturity Model allows electric utilities and grid operators to assess their cybersecurity capabilities and prioritize their actions and investments to improve cybersecurity.[49] The DHS has a broad range of initiatives to protect infrastructure from cyberattack. Particularly ground-breaking is the joint DHS-DoD Enhanced Cybersecurity Services program. Under this voluntary program, the federal government provides private companies with classified and unclassified cyber threat information to help them protect critical infrastructure, initially within the defense industrial base

45. Catherine Herridge, *Al Qaeda Video Calling for Cyberattacks on Western Targets Raises Alarm in Congress*, FOXNEWS.COM (May 22, 2012), http://www.foxnews.com/politics/2012/05/22/al-qaeda-video-calling-for-cyberattacks-on-western-targets-raises-alarm-in/#ixzz2M7L4V2iG.

46. Tony Capaccio, *Al-Qaeda Seeks Cyber-Attack Skills, U.S. Official Says*, BLOOMBERG (Apr. 24, 2012), http://www.bloomberg.com/news/2012-04-25/al-qaeda-seeks-cyber-attack-skills-u-s-official-says.html.

47. Monaco, *supra* note 6.

48. Exec. Order No. 1363678, Fed. Reg. 11,739 (Feb. 12, 2013).

49. *Electricity Subsector Cybersecurity Capability Maturity Model*, U.S. DEP'T OF ENERGY, http://energy.gov/oe/services/cybersecurity/electricity-subsector-cybersecurity-capability-maturity-model (last visited Jan. 11, 2014).

and now for a growing range of infrastructure sectors.[50] The Department of Justice and Federal Bureau of Investigation are also ramping up industry partnership initiatives, many of them—such as the National Cyber Forensics and Training Alliance and the National Cyber Investigative Joint Task Force—explicitly designed to facilitate prosecution of cyberterrorists and other attackers.[51]

Yet, as Assistant Attorney General Monaco noted in 2012, significant legal and policy challenges must be resolved before such prosecutions can fulfill their potential to deter and disrupt attacks. Monaco urged scholars to help in "pushing forward with questions that need to be asked and answered by all of us as we navigate this legal space together."[52] This Article addresses one particularly important, unresolved question: how to establish an effective jurisdictional framework to prosecute cyberterrorists who attack our critical infrastructure from abroad.

II. U.S. DOMESTIC LEGAL CONSTRAINTS ON EXTRATERRITORIALITY AND FEDERAL STATUTES BEARING ON CYBERTERRORISM

Before examining which prescriptive basis of jurisdiction should govern cyberterrorism, it is necessary to understand the domestic legal constraints on extraterritorial application of U.S. law and the domestic statutes that could be used to prosecute cyberterrorists. Historically, the majority of U.S. penal laws did not provide for extraterritorial application.[53] U.S. law was predicated almost exclusively on the *locus delicti* territorial doctrine. This doctrine asserted that America's authority to prescribe its laws was circumscribed to crimes committed within its borders. In 1909, Justice Holmes famously promulgated this traditional principle in *American Banana Co. v. United Fruit Co.*: "the general and almost universal rule is that the character of an act as lawful or unlawful must be determined wholly by the law of the country where the act is done."[54] American courts and international legal scholars historically justified the presumption against extraterritoriality of U.S. laws as critical for preserving

50. Press Release, U.S. Dep't of Def., DOD Announces the Expansion of Defense Industrial Base ("DIB") Voluntary Cybersecurity Information Sharing Activities (May 11, 2012), *available at* http://www.defense.gov/releases/release.aspx?releaseid=15266.

51. *Cyber Security Responding to the Threat of Cyber Crime and Terrorism: Hearing before the Subcomm. On Crime and Terrorism of the Sen. Comm. On the Judiciary*, 112th Cong. (2011) (detailing statement of Gordon M. Snow, FBI Assistant Dir., Cyber Division); *National Cyber Investigative Joint Task Force*, FED. BUREAU INVESTIGATION, http://www.fbi.gov/about-us/investigate/cyber/ncijtf (last visited Jan. 11, 2014).

52. Monaco, *supra* note 6.

53. William S. Dodge, *Understanding the Presumption Against Extraterritoriality*, 16 BERKELEY J. INT'L L. 85, 85-86 (1998).

54. Applying this principle, the Supreme Court found that the Sherman Act did not govern monopolistic activity beyond America's territory. Am. Banana Co. v. United Fruit Co., 213 U.S. 347, 356 (1909) (citing Slater v. Mexican Nat. R. Co. 194 U.S. 120 (1904)).

international comity and avoiding discord among nations.[55] For example, the renowned jurist Oppenheim argued that non-interference in other nations' internal affairs "is a corollary of every state's right to sovereignty, territorial integrity and political independence."[56]

However, with the advent of globalization, U.S. courts gradually began to acknowledge that crimes perpetrated abroad could inflict significant domestic harm. The judiciary therefore authorized increasing numbers of exceptions to the presumption against extraterritoriality. As the Supreme Court reasoned in *U.S. v. Bowman*, for some criminal statutes, to "limit the[] locus to the strictly territorial jurisdiction would be greatly to curtail the scope and usefulness of the statute[s] and leave open a large immunity for frauds as easily committed by citizens on the high seas and in foreign countries as at home."[57]

At the present time, U.S. courts follow two canons of construction to determine whether a statute has extraterritorial application.[58] First, unless congressional intent indicates otherwise, it is presumed that statutes do not apply extraterritorially. To gauge congressional intent, courts conduct traditional methods of statutory interpretation.[59] They consider the explicit language of the statute as well as its structure, legislative history, and presumed "nature and purpose."[60]

The second significant canon of interpretation is referred to as the *Charming Betsy* doctrine. The Supreme Court first enunciated this presumption in the 1804 case of *Murray v. Schooner Charming Betsy*. The Court held that "an act of Congress ought never to be construed to violate the law of nations if any other possible construction remains."[61] The Restatement (Third) of Foreign Relations Law embraces this presumption, providing that "[w]here fairly possible, a United States statute is to be construed so as not to conflict with international law or with an international agreement of the United States."[62]

However, if Congress evinces a clear intent to contravene international law, courts are required to deviate from the *Charming Betsy* presumption and enforce congressional aims. As the Ninth Circuit held in *United States v. Yousef*,

---

55. International comity has been described as the "respect that sovereign nations . . . owe each other." Philips Med. Sys. Int'l. v. Bruetman, 8 F.3d 600, 604 (7th Cir. 1993).

56. Michael Wood, *Non-Intervention (Non-interference In Domestic Affairs)*, PRINCETON ENCYCLOPEDIA OF SELF-DETERMINATION, http://pesd.princeton.edu/?q=node/258 (last visited Nov. 4, 2013).

57. United States v. Bowman, 260 U.S. 94, 98 (1922).

58. Anthony J. Colangelo, *A Unified Approach to Extraterritoriality*, 97 VA. L. REV. 1019, 1031-32 (2011).

59. *See* Hathaway, *supra* note 14, at 874 n.275.

60. *See* United States v. Bowman, 260 U.S. at 97-98 (1922).

61. Murray v. Schooner Charming Betsy, 6 U.S. (2 Cranch) 64 (1804).

62. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 114 (1987) [hereinafter RESTATEMENT THIRD].

> [A]n act of Congress ought never to be construed to violate the law of nations if any other possible construction remains. Nonetheless, in fashioning the reach of our criminal law, Congress is not bound by international law. If it chooses to do so, it may legislate with respect to conduct outside the United States in excess of the limits posed by international law.[63]

Therefore, unless Congress demonstrates a clear intent to negate the *Charming Betsy* presumption, statutes that have extraterritorial application must be grounded on one of the five traditional bases of prescriptive jurisdiction under international law.

In both the United States and abroad, the majority of existing criminal statutes that could govern cyberterrorism lack extraterritorial reach.[64] In the event of a cyberterrorist attack, this would significantly constrain nations from prosecuting cyberterrorists who operate in other countries. In the United States, however, there are some "exceptions to that general rule."[65] For example, 18 U.S.C. § 2332b ("Acts of terrorism transcending national boundaries") has extraterritorial application. Although this statute does not explicitly recognize cyberterrorism, given that cyberterrorism is a type of terrorism, it could feasibly be applied to the perpetrators of this crime.[66] If a cyberterrorist targeted a U.S. energy facility or mass transportation system, prosecutors could also rely on two other domestic criminal statutes with extraterritorial provisions—18 U.S.C. § 1366 ("Destruction of an energy facility") and 18 U.S.C. § 1992 ("Terrorist attacks and other violence against railroad carriers and against mass transportation systems on land, on water, or through the air").[67]

The Computer Fraud and Abuse Act ("CFAA") could serve as another pivotal statute in cyberterrorist prosecutions. This federal statute, which was enacted in 1984, criminalizes a variety of conduct relating to abuse of computers and the Internet. The CFAA is the most significant computer crime statute in the United States because "almost every other statute that deals with computer crime modifies the CFAA."[68] The CFAA precludes hacking a government computer;[69] damaging a government computer, bank computer, or computer affecting interstate or foreign commerce;[70] and accessing a computer to commit espionage.[71] Attempts or conspiracies to perpetrate any of these offenses are

---

63. United States v. Yousef, 327 F.3d 56, 86 (2d Cir. 2003), *cert. denied*, 540 U.S. 933 (U.S. 2003) (citations omitted).

64. Hathaway, *supra* note 14, at 877-78.

65. *Id.* at 874-75.

66. 18 U.S.C. § 2332b (2006).

67. 18 U.S.C. § 1366 (2006); 18 U.S.C. § 1992 (2006).

68. Maxim May, *Federal Computer Crime Laws*, SANS INST. 2 (June 1, 2004), http://www.sans.org/reading_room/whitepapers/legal/federal-computer-crime-laws_1446; *see also* Reid Skibell, *Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act*, 18 BERKELEY TECH. L.J. 909, 912 (2003).

69. 18 U.S.C. § 1030(a)(3) (2006).

70. *Id.* (a)(5).

71. *Id.* (a)(1).

also prohibited under the statute.[72] Depending on the nature of the crime, the perpetrator may be charged with a felony or misdemeanor. An offender may receive a penalty of life imprisonment if he or she intentionally or recklessly causes death.[73]

Increased instances of cyberspace abuses in the 1980s spurred Congress to significantly revise the CFAA in 1986. Since 1986, Congress has amended the CFAA nine times to keep pace with technological advances and counter the evolving sophistication of computer crimes.[74] Most significantly, following the September 11th attacks and enactment of the 2001 USA PATRIOT Act, Congress explicitly conferred extraterritorial application on the CFAA. The USA PATRIOT Act expanded the CFAA's definition of "protected computers" to include computers that affect "interstate or foreign commerce or communication," regardless of whether they are located outside of the United States.[75] Since courts have expansively interpreted "protected computers" to include any computer connected to the Internet, the CFAA prohibits knowingly or recklessly damaging the vast majority of computers within the U.S.[76] Furthermore, the provisions of "exceeds authorized access" can be interpreted to preclude cyberterrorist botnet attacks.[77]

Since Congress conferred extraterritorial reach on the CFAA and the other aforementioned statutes, applying such statutes to cyberterrorists abroad would accord with the first canon of statutory construction. In order to comply with the second canon, the *Charming Betsy* doctrine, the United States must prosecute cyberterrorists abroad predicated on one of the five accepted bases of prescriptive jurisdiction under international law. Although Congress could have chosen to negate the *Charming Betsy* doctrine, the legislative history of these

---

72. *Id*. (b).

73. *Id*. (c).

74. EXEC. OFFICE FOR U.S. ATTORNEYS, PROSECUTING COMPUTER CRIMES 2 (2007), *available at* http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf.

75. *Id*. at 5. *See also* 18 U.S.C. § 1030(e)(2)(b) (2006); Charles Doyle, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*, CONG. RESEARCH SERV. (2010), http://www.fas.org/sgp/crs/misc/97-1025.pdf.

76. For example, in *United States v. Trotter,* the Eighth Circuit held that the defendant's damage to his former employer's computer network violated the CFAA. Since the computer network was connected to the Internet, it was used for "interstate communication" and therefore constituted a "protected computer" under the statute. 478 F.3d 918 (8th Cir. 2007). More recently, in *Freedom Banc Mortgage Services v. O'Harra*, the district court held that a computer fulfilled the definition of a "protected" computer under the CFAA by virtue of its merely being connected to the Internet. 2012 U.S. Dist. LEXIS 125734 (S.D. Ohio 2012); *see also* U.S. v. Ivanov, 175 F. Supp. 2d 367 (D. Conn. 2001) (holding that a Russian defendant's hacking into Connecticut corporation's computer connected to the Internet constituted an unauthorized access of a protected computer within the meaning of the CFAA).

77. Ed Felten, *Botnet Briefing,* FREEDOM TO TINKER (Apr. 26, 2007, 5:41 AM), http://freedom-to-tinker.com/blog/felten/botnet-briefing.

statutes and their subsequent amendments do not indicate any intent to contravene international law.[78]

III. INTERNATIONAL LAW GROUNDS FOR EXTRATERRITORIAL JURISDICTION APPLIED TO CYBERTERRORISM

International law circumscribes nations' authority to exercise jurisdiction in matters that implicate foreign interests or activities.[79] Each nation must avoid undue encroachment on other countries' jurisdictions or territories. As the international law scholar J.H. Currie contends, "a state is, as a general matter, prima facie free to legislate or regulate with respect to persons or events beyond its territory, as long as doing so does not interfere with the same right of states that may have a closer connection to those persons or events."[80]

Under international law, states are subject to limitations on their jurisdiction to prescribe, jurisdiction to adjudicate, and jurisdiction to enforce.[81] Prescriptive jurisdiction, which this Article is primarily concerned with, is the state's authority to apply its substantive laws to the "activities, relations, or status of persons," whether by the legislative, executive, or judicial branches.[82] Adjudicative jurisdiction is the state's power to subject individuals to its courts or administrative tribunals in civil or criminal proceedings. Enforcement jurisdiction is the authority to "induce or compel compliance" or punish violations of a nation's laws or regulations. These three categories of jurisdiction are interdependent. A nation's ability to adjudicate and enforce is predicated on whether it has jurisdictional authority to prescribe.[83] In criminal cases, nations will rarely exercise jurisdiction to adjudicate if they lack jurisdiction to prescribe. This is because courts typically refuse to apply other countries' criminal laws.[84] Similarly, a nation's power to exercise prescriptive or adjudicative jurisdiction is rendered meaningless without the power to enforce its judgment.[85]

This Article turns next to demonstrating that the traditional bases of prescriptive jurisdiction under international law are largely inadequate for govern-

78. *See, e.g.*, S. DOC. NO. 99-432 (1986); S. DOC. NO. 101-544 (1990).

79. RESTATEMENT THIRD, *supra* note 62, § 401 cmt. a.

80. JOHN CURRIE, PUBLIC INTERNATIONAL LAW 299 (2001).

81. RESTATEMENT THIRD, *supra* note 62, § 401.

82. *Id*.

83. RESTATEMENT (SECOND) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 7 (1965) [hereinafter cited as RESTATEMENT SECOND] ("A state having jurisdiction to prescribe a rule of law does not necessarily have jurisdiction to enforce it in all cases . . . . [A] state does not have jurisdiction to enforce a rule of law prescribed by it unless it had jurisdiction to prescribe that rule.").

84. Stephan Wilske & Teresa Schiller, *International Jurisdiction in Cyberspace: Which States May Regulate the Internet*, 50 FED. COMM. L.J. 117, 129-42 (1997).

85. Joel P. Trachtman, *Global Cyberterrorism, Jurisdiction, and International Organization*, SOC. SCI. RES. NETWORK 16 (July 20, 2004), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=566361.

ing the modern challenge of cyberterrorism. This is unsurprising given that these jurisdictional theories were formulated long before the advent of the Internet. The classical theories of prescriptive jurisdiction—territoriality, nationality, passive personality, protection, and universality—were codified in the 1935 Harvard Research Draft Convention on Jurisdiction with Respect to Crime ("Draft Convention"). The Draft Convention is regarded by many scholars as a monumental "contribution to the systemization of international law,"[86] and served as the intellectual underpinning of the American Law Institute's Second and Third Restatements of Foreign Relations Law of the United States, published in 1965 and 1987 respectively.[87] Although there is some controversy concerning whether the Draft Convention and Restatements are accurate reflections of customary international law, legal scholars and courts within and outside the United States consider these documents as authoritative sources on the classical principles of prescriptive jurisdiction.[88]

The Harvard Law School faculty and American Law Institute members who contributed to these jurisdictional theories in the 1930s, 1950s, and 1980s could not have foreseen the potential for terrorists to execute sophisticated computer network attacks against critical infrastructure. Since their prescriptive doctrines of jurisdiction predated the emergence of the borderless and transnational Internet, it is unsurprising that most of them are ill equipped to prosecute crimes that route through multiple jurisdictions and devastate multiple countries simultaneously. The following sections elucidate these principles' inadequacies in the context of cyberterrorism.

A. *Territoriality*

"Territoriality," which is the most pervasive and least controversial principle of prescriptive jurisdiction under international law, confers jurisdiction

86. R. P. DHOKALIA, THE CODIFICATION OF PUBLIC INTERNATIONAL LAW 71 (1970).

87. Harold G. Maier, *Jurisdictional Rules in Customary International Law, in* EXTRATERRITORIAL JURISDICTION IN THEORY AND PRACTICE 64, 67 (Karl M. Meessen ed., 1996) (arguing that the Draft Convention formed "the intellectual, if not the institutional, forerunner" of the American Law Institute's Restatements).

88. *See* David B. Massey, *How the American Law Institute Influences Customary Law: The Reasonableness Requirement of the Restatement on Foreign Relations Law*, 22 YALE J. INT'L L. 419, 423 (1997); *see also* Robert J. Currie & Stephen Coughlan, *Extraterritorial Criminal Jurisdiction: Bigger Picture or Smaller Frame?*, 11 CANADIAN CRIM. L. REV. 141, 145-48 (2007) (articulating the five bases for extraterritorial application of Canadian criminal law); Frank Tuerkheimer, *Globalization of U.S. Law Enforcement: Does the Constitution Come Along?*, 39 HOUS. L. REV. 307, 314 (2002) ("Perhaps the most definitive statement of jurisdiction over transnational crime was articulated in 1935 in the *Draft Convention on Jurisdiction with Respect to Crime* by Harvard Research in International Law."). *But see* Cecil J. Olmstead, *Jurisdiction*, 14 YALE J. INT'L L. 468, 472 (1989) (challenging the argument that the Restatement Third's jurisdictional principles constitute customary international law).

based on the "locus" of the crime.[89] The principle derives from the Westphalian model of state sovereignty and underscores each nation's "right to political self-determination," and dominion over activities within its borders.[90] As Chief Justice Marshall articulated in the famous 1812 *Schooner Exchange* case, "The jurisdiction of the nation within its own territory is necessarily exclusive and absolute. It is susceptible of no limitation not imposed by itself. Any restriction upon it, deriving validity from an external source, would imply a diminution of its sovereignty."[91] The territoriality doctrine comports with the traditional *lex loci delecti* approach to conflicts of laws, which was promulgated by Joseph Story and Professor Joseph Beale and codified in the First Restatement of Conflicts.[92]

When prosecuting many traditional crimes, applying the territoriality principle confers multiple advantages. By affording respect for each nation's sovereignty, the territoriality doctrine generally reduces the potential for international tension. The principle also fosters efficiency and predictability. As one international scholar has posited, "By establishing a priori that only the nation where an event occurs has power, [territoriality] limited states' lawmaking competence so that conflict was practically impossible."[93] Prudential considerations also underlie the territoriality principle. In many criminal prosecutions, the nation in which the crime occurred has the greatest capacity to investigate the crime, collect evidence, examine witnesses, and apprehend the perpetrators.[94]

However, the borderless nature of the Internet and unconventional techniques employed by cyberterrorists render it challenging, if not futile, to apply the traditional doctrine of territoriality to cyberterrorism. The inefficacy of applying the territoriality doctrine to cyberterrorism is evident among all four of the doctrine's subcategories that we examine next: subjective territoriality, objective territoriality, effects-based territoriality, and targeting.

1. Subjective Territoriality

The "subjective" territoriality doctrine confers prescriptive jurisdiction on the nation in which the perpetrator commenced the crime, regardless of whether its consequences occurred elsewhere. The justification for this principle is that a nation has a predominant interest in enforcing peace and security within its

89. RESTATEMENT (THIRD), *supra* note 62, § 402 cmt. c.

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

91. Schooner Exch. v. McFadden, 11 U.S. (7 Cranch) 116, 136–37 (1812).

92. RESTATEMENT (FIRST) OF CONFLICT OF LAWS § 55 (1934).

93. Larry Kramer, *Vestiges of Beale: Extraterritorial Application of American Law,* 1991 SUP. CT. REV. 179, 189 (1991).

94. INT'L BAR ASS'N, REPORT OF THE TASK FORCE ON EXTRATERRITORIAL JURISDICTION, 171 (2009), *available at* http://tinyurl.com/taskforce-etj-pdf.

borders. The majority of nations' criminal legislation is based on the subjective territoriality doctrine.[95] Since subjective territoriality does not infringe on other nations' sovereignty and territorial integrity, it is considered the least controversial form of prescriptive jurisdiction. In the United States, the American Law Institute's Model Penal Code, which has significantly influenced most states' criminal legislation, promulgates the subjective territoriality principle.[96]

However, applying "subjective territoriality" to prosecuting cyberterrorists is impractical for a number of reasons. First, the inherent concept of territorial borders appears inappropriate in the context of cyberspace. The Internet, unlike physical territory, is located in virtual or "intangible" space. It lacks borders and traverses all nations simultaneously. As Yaman Akdeniz contends, "The Internet is a complex, anarchic, and multi-national environment where old concepts of regulation, reliant as they are upon tangibility in time and space, may not be easily applicable or enforceable."[97] Similarly, David Johnson and David Post argue that the Internet "radically subverts the system of rule-making based on borders between physical spaces . . . [and] territorially defined rules."[98]

Although nations have been able to demarcate Internet activity to a certain extent by assigning Internet Protocol ("IP") and domain name addresses to computers that coincide with their physical addresses (such as a ".us" domain name extension), cyberterrorists can easily evade this identification system.[99] For example, even if a cyberterrorist's computer is assigned to an Internet Protocol address in a certain country, the terrorist could simply transport the computer to another state without altering its domain name.[100] Alternatively, cyberterrorists could connect to the Internet using virtual private networks and route through proxy servers in multiple countries to obscure their IP addresses.[101] This would obfuscate their physical location and make it appear that their attacks were emanating from other countries. Although attribution capabilities are improving, tracing the source of a cyberattack for the purpose of establishing subjective territoriality jurisdiction is still very time-consuming and resource intensive.

---

95. Darrel C. Menthe, *Jurisdiction In Cyberspace: A Theory of International Spaces*, 4 MICH. TELECOMM. & TECH. L. REV. 69, 72 (1998).

96. Christopher L. Blakesley, *United States Jurisdiction Over Extraterritorial Crime*, 73 J. CRIM. L. & CRIMINOLOGY 1109, 1119-1121 (1982).

97. Yaman Akdeniz, *Governance of Pornography and Child Pornography on the Global Internet: A Multi-Layered Approach, in* LAW AND THE INTERNET: REGULATING CYBERSPACE 223, 225 (Lilian Edwards & Charlotte Waelde eds., 1997).

98. David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1370 (1996).

99. *Id*. at 1371.

100. *Id*.

101. Larry Greenemeier, *Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers*, SCIENTIFIC AM. (June 11, 2011), http://www.scientificamerican.com/article.cfm?id=tracking-cyber-hackers.

The severe challenge of determining the origin of a cyberattack was demonstrated in the aftermath of the July 2009 distributed denial of service attacks against American and South Korean websites. The attacks caused the websites of the U.S. Departments of Transportation and Treasury, Secret Service, U.S. Federal Trade Commission, South Korean National Assembly, and U.S. Forces of Korea to be inoperable for a week. South Korea's National Intelligence Service ("NIS") initially accused the North Korean government of launching the attacks. Subsequently, a Vietnamese computer security analyst who studied the virus and the log files of the hijacked servers concluded that hackers residing in the United Kingdom were culpable.[102] As of today, authorities have still not verified the attacks' actual origin. Similarly, in the immediate aftermath of the 2007 distributed denial of service attacks against Estonia, the Estonian government confidently asserted that the Russian government had funded and led the attacks in retribution for Estonia's decision to relocate a Soviet-era World War II monument. Estonian officials alleged that the "mastermind" behind the cyberattacks was a member of the Russian security service.[103] However, analysts later discovered that at least some of the attacks emanated from Brazil and Vietnam.[104] In spite of careful technical analysis, Estonian government officials have still not been able to attribute the attacks to any state, organizational entity, or individuals.[105]

A second and related challenge with applying subjective territoriality to cyberterrorism is that the doctrine could authorize an infinite number of nations to assert jurisdiction. Although subjective territoriality confers jurisdiction on the state where the crime originated, a cyberterrorist attack may emanate from multiple nations simultaneously. Cyberterrorists may exploit unsuspecting Internet users across the globe by hijacking their computers and transforming these computers into "zombies" or "robot botnets," from which they can then launch attacks. Such computers are compromised when their owners inadvertently download malware or click on nefarious email message links or web-

102. Martyn Williams, *U.K., Not North Korea, Source of DDOS Attacks, Researcher Says,* PC WORLD (July 14, 2009, 3:02 PM), http://www.pcworld.idg.com.au/article/311070/uk_north_korea_source_ddos_attacks_researcher_says/; Noah Shachtman, *Kremlin Kids: We Launched the Estonian Cyber War*, WIRED (Mar. 11, 2009, 12:45 PM), http://www.wired.com/dangerroom/2009/03/pro-kremlin-gro/.

103. Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, THE GUARDIAN (May 16, 2007), http://www.theguardian.com/world/2007/may/17/topstories3.russia.

104. Anne Applebaum, *For Estonia and NATO, A New Kind of War*, WASH. POST (May 22, 2007), http://www.washingtonpost.com/wp-dyn/content/article/2007/05/21/AR2007052101436.html.

105. Rain Ottis, *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective, in* PROCEEDINGS OF THE 7TH EUROPEAN CONFERENCE ON INFORMATION WARFARE AND SECURITY, PLYMOUTH 168 (2008).

sites.[106] For example, in the 2009 distributed denial of service attacks against American and South Korean websites, the perpetrators commandeered a botnet of 50,000 to 166,000 PC computers located in seventy-four countries to inundate and incapacitate both government and commercial websites in South Korea and the United States.[107] Similarly, in the attacks against Estonia, the offenders harnessed approximately one million computers in countries ranging from Vietnam to the U.S. to launch attacks against the country's computer networks.

One method for resolving this jurisdictional quandary would be to confer jurisdiction on the nation where the cyberterrorist is located. The rationale would be that the attack actually commenced when the cyberterrorist hijacked the third party computers and programmed them to launch attacks. The owners of the zombie computers assumedly lacked the requisite intent to perpetrate the attacks and therefore should be appropriately characterized as third party victims or unknowing accomplices. As some scholars have contended, to hold zombie computer owners culpable for the attacks would be to effectively punish "ignorance and technophobia."[108] However, it would often be challenging if not impossible to determine whether any of these other computers were "decoys" and were owned and operated by additional terrorist co-conspirators. This would further confound the subjective territoriality jurisdictional analysis.[109]

A third limitation of applying the subjective territorial principle to cyberterrorism is that it would incentivize cyberterrorists to forum shop in order to evade prosecution. There is significant disparity in cybercrime laws across the international community and some nations have failed to enact any substantive cybercrime legislation. For example, in a recent Arab summit exploring cyberattacks, participants concluded that the absence of comprehensive cybercrime statutes in the Arab region has "allowed cybercrimes to proliferate everywhere."[110] Even among those Arab states that have recently enacted cybercrime statutes, their legislation frequently governs only narrow categories of cyber threats, such as e-commerce.[111] Such statutes are therefore inadequate for prosecuting cyberterrorism.

---

106. John Wallace, *Botnet Zombie Apocalypse: How to Protect Your Computer,* TOP TEN REVIEWS, http://mac-internet-security-software-review.toptenreviews.com/how-do-i-know-if-my-computer-is-a-botnet-zombie-.html (last visited Jan. 11, 2014).

107. Williams, *supra* note 102; *see also* Choe Sang-Hun & John Markoff, *Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea,* N.Y. TIMES (July 8, 2009), http://www.nytimes.com/2009/07/09/technology/09cyber.html?hp.

108. *See* Lilian Edwards, *Dawn of the Death of Distributed Denial of Service: How to Kill Zombies*, 24 CARDOZO ARTS & ENT. L.J. 23, 46 (2006).

109. Gable, *supra* note 20, at 102.

110. *Cybercrime Costs Top USD 1 Trillion*, ITU NEWS, https://itunews.itu.int/En/2341-Cooperate-%C2%95-Secure-%C2%95-Protect.note.aspx (last visited Jan. 11, 2014) (emphasis omitted).

111. *Id.*

If subjective territoriality were the primary basis for prescriptive jurisdiction over cyberterrorists, this would induce terrorists to execute their attacks from within states lacking cybercrime laws. Indeed, a large percentage of terrorists are already located in physical safe havens in Southeast Asia, the Middle East, and Africa. Many of these countries also serve as cybercrime "legal safe havens," lacking any cybercrime legislation. In contrast, the most probable targets of cyberterrorism are Western nations with comprehensive cybercrime laws. The international community cannot permit the perpetrators of devastating cyberterrorist attacks to escape prosecution by launching attacks from within "legal safe havens."

2. Objective Territoriality, Effects-Based, and Targeting Doctrines

The objective territoriality principle, which is the inverse of the subjective territoriality principle, confers jurisdiction over a crime that was initiated abroad yet consummated within a nation's borders. The classic example of this doctrine is a lethal shooting across a border.[112] According to the Permanent Court of International Justice's ("PCIJ") famous formulation of the principle in *S.S. Lotus*, "offences, the authors of which at the moment of commission are in the territory of another State, are nevertheless to be regarded as having been committed in the national territory, if one of the constituent elements of the offence, and more especially its effects, have taken place there."[113]

As originally understood, objective territoriality required that the conduct's effects were "localized" within the prescribing nation's territory.[114] In the early twentieth century, U.S. courts controversially extended and refined the objective territoriality principle, promulgating what became known as the effects-based doctrine. In 1911, Justice Oliver Wendell Holmes articulated in *Strassheim v. Daily* that "[a]cts done outside a jurisdiction, but . . . producing detrimental effects within it, justify a state in punishing the cause of the harm as if he had been present at the effect."[115] Subsequently, in the landmark *Alcoa* decision, Judge Hand held that the Sherman Antitrust Act applied to foreign cartel conduct that generated economic effects on the domestic market. The court found that "any state may impose liabilities, even upon persons not within its allegiance, for conduct outside its borders that has consequences within its borders which the state reprehends."[116] Since this decision, U.S. courts have up-

112. RESTATEMENT (THIRD), *supra* note 62, § 402 cmt. d.

113. The Case of the S.S. Lotus (Fr. v. Turk.), 1972 P.C.I.J. (ser. A) No. 10, at 23 (Sept. 7).

114. David J. Gerbert, *Beyond Balancing: International Law Restraints on the Reach of National Laws*, 10 YALE J. INT'L L. 185, 195 (1984).

115. Strassheim v. Daily, 221 U.S. 280, 285 (1911). Justice Oliver Wendell Holmes's exact wording was "[a]cts done outside a jurisdiction, but intended to produce and producing detrimental effects within it." *Id*. However, courts have broadly interpreted the effects principle to not require a showing of intent.

116. United States v. Aluminum Co. of Am., 148 F.2d 416, 443 (2d Cir. 1945).

held effects-based jurisdiction in cases involving importation of narcotics,[117] copyright infringement,[118] and importation of faulty products "introduced into the stream of commerce."[119]

Most courts and scholars conflate or fail to distinguish between the objective territoriality and effects-based principles. Often, court dicta will indicate that prescriptive jurisdiction is justified by objective territoriality when the facts of the case indicate that the effects principle should govern. Nevertheless, there is a clear and important difference between these doctrines. In contrast to objective territoriality, the effects-based principle does not require that a "constituent element of the offense" transpire within the prescribing nation.[120] The nation seeking jurisdiction must merely demonstrate that the crime's consequences were detrimental and occurred within its territory. These deleterious consequences may be intangible, such as economic harm, and may be far removed from the initial offense. For example, under the effects-based principle, any of the nations that suffered damaging economic consequences from a foreign cartel could assert jurisdiction. The effects-based doctrine therefore constitutes a significant expansion and dilution of the traditional territoriality theory. Accordingly, although the international community has gradually accepted the applicability of the effects-based principle to some offenses, U.S. assertion of the principle in the securities and antitrust fields remains highly controversial. Nations have responded to U.S. claims of jurisdiction in these fields by enacting blocking statutes and engaging in other forms of retaliation.[121] The Restatement (Third), although embracing the effects-based principle, concedes that the doctrine has been a "major source of controversy" when it has been applied to economic conduct abroad.[122]

Due to the unique features of cyberterrorism, applying the objective territoriality or effects-based principles would prove both cumbersome and destabiliz-

---

117. *See* United States v. Noriega, 746 F. Supp. 1506, 1512-13 (S.D. Fla. 1990) (finding that importation of narcotics from Panama into the U.S. produced "deleterious" effects within the U.S. and jurisdiction was therefore warranted under the effects-based principle), *aff'd,* 117 F.3d 1206 (11th Cir. 1997); *see also* Geoffrey R. Watson, *Offenders Abroad: The Case for Nationality-Based Criminal Jurisdiction*, 17 YALE J. INT'L L. 41, 83 (1992).

118. *See* Graduate Mgmt. Admission Council v. Raju, 241 F. Supp. 2d 589 (E.D. Va. 2003).

119. RESTATEMENT (THIRD), *supra* note 62, § 402 cmt. d.

120. Roger O'Keefe, *Universal Jurisdiction: Clarifying the Basic Concept*, 2 J. INT'L CRIM. JUST. 735, 739 (2004).

121. *See* Austen Parrish, *The Effects Test: Extraterritoriality's Fifth Business*, 61 VAND. L. REV. 1455, 1457-59 (2008); O'Keefe, *supra* note 120; RESTATEMENT (THIRD), *supra* note 62, § 402 reporters' n.2; *see also* Rio Tinto Zinc v. Westinghouse Elec. Corp., [1978] 1 All E.R. 434, 639. In *Rio Tinto*, the House of Lords admonished America's expansion of the jurisdictional effects principle to include prescribing its antitrust regulations abroad. For an additional antitrust case in which a U.S. court asserted prescriptive jurisdiction based on the "effects" principle, see United States v. Timken Roller Bearing Co., 83 F. Supp. 284 (N.D. Ohio 1949), *aff'd*, 341 U.S. 593 (1951).

122. *See* RESTATEMENT (THIRD), *supra* note 62, § 402.

ing to interstate relations. Since cyberterrorist attacks would probably impact multiple countries, these doctrines would engender infinite and competing jurisdictional claims. Terrorist organizations such as al-Qaeda have a demonstrated proclivity for orchestrating simultaneous attacks against numerous targets.[123] Perpetrating complex, simultaneous attacks against multiple targets maximizes the "newsworthiness" and lethality of terrorists' assaults.[124] This technique amplifies the psychological consequences of the attack, undermining civilians' morale and faith in their government's capacity to protect them.[125]

Terrorist organizations' attacks in cyberspace would probably bear this hallmark feature given that cyberweapons render it easier and less costly to inflict significant damage on multiple locations. For example, in order to execute a coordinated suicide attack, a terrorist organization needs to purchase explosives and other weaponry, recruit and train radicals willing to carry out simultaneous suicide missions, provide extensive physical and psychological training to these operatives, and evade multiple security detection systems or checkpoints. In contrast, cyberterrorists can cheaply deliver debilitating DDOS attacks and viruses from remote locations. Many countries use similar supervisory control and data acquisition ("SCADA") systems to control and monitor their critical infrastructure. Therefore, once a terrorist identifies a defect in one such system, he can exploit this vulnerability to penetrate critical infrastructure and cause significant damage in numerous nations.[126] Applying the effects-based or objective territoriality principles to cyberterrorism would therefore legitimize countless claims of prescriptive jurisdiction.

---

123. This hallmark feature was exhibited in the coordinated embassy bombings in Nairobi and Tanzania in 1998, the September 11th attacks against the World Trade Center and Pentagon in 2001, the simultaneous bombings of Bali and the U.S. consulate in Denpasar in 2002, and the recently foiled al-Qaeda terrorist plot against multiple civilian and government targets in Jordan. *See* A HANDBOOK OF TERRORISM AND INSURGENCY IN SOUTHEAST ASIA 439 (Andrew T. H. Tan ed., 2007); Joby Warrick & Taylor Luck, *Jordan Disrupts Major Al-Qaeda Terrorist Plot*, WASH. POST (Oct. 21, 2012), http://articles.washingtonpost.com/2012-10-21/world/35501513_1_terrorist-plot-jordanians-syrian-conflict.

124. Brian K. Houghton & Jonathan M. Schachter, *Coordinated Terrorist Attacks: Implications for Local Responders,* 74 FBI LAW ENFORCEMENT BULLETIN 11, 12-15 (May 2005), *available at* http://www.au.af.mil/au/awc/awcgate/fbi/coord_terr_attks.pdf.

125. *Id*.; *see also* Bill Braniff & Assaf Moghadam, *Towards Global Jihadism: Al-Qaeda's Strategic, Ideological and Structural Adaptations Since 9/11*, 5 PERSP. ON TERRORISM 36, 47 n.4 (2011) ("Al-Qaeda's trademark attack is the complex suicide terrorist attack in which multiple bombers strike multiple targets simultaneously, thereby magnifying the psychological effect of the attack.").

126. According to Symantec, a global computer security software corporation, the number of software security vulnerabilities burgeoned by eighty percent in 2002 alone. John Schwartz, *Decoding Computer Intruders*, N.Y. TIMES (Apr. 24, 2003), http://www.nytimes.com/2003/04/24/technology/decoding-computer-intruders.html?pagewanted=all&src=pm; *see also* Gabriel Weimann, *Cyberterrorism: How Real Is the Threat?*, U.S. INST. OF PEACE (Dec. 2004), http://dspace.cigilibrary.org/jspui/bit-stream/123456789/15033/1/Cyberterrorism%20How%20Real%20Is%20the%20Threat.pdf ("The sheer number and complexity of potential targets guarantee that terrorists can find weaknesses and vulnerabilities to exploit.").

The effects-based doctrine could also generate infinite claims of prescriptive jurisdiction even when cyberterrorists did not intend to target multiple nations. Cyberweapons are far less predictable than conventional weaponry and may produce collateral damage across the globe. A mistaken algorithm or an error in a code can cause even a precisely targeted cyberweapon to proliferate out of control. Many cybersecurity experts have cautioned about cyberweaponry's volatile and unpredictable nature.[127] According to Martin Libicki, a Senior Management Scientist at RAND Corporation, cyberweapons are far more capricious than conventional weaponry because:

> Physical attacks at least have the "advantage" of physics and chemistry to work with. Because, say, the blast radius of a thousand-pound bomb is fairly well understood, one can predict what definitely lies outside the blast radius and what definitely lies inside. Error bands in cyberattack are much wider.[128]

Due to their volatility, cyberweapons have frequently been compared to biological weapons.[129] Biological weapons, which consist of living organisms, are susceptible to changes in meteorological, physiological, epidemiological, and ecological conditions.[130] Fluctuations in winds and temperatures can suddenly alter a biological agent's path of propagation.[131]

The high potential for cyberattacks to generate peripheral effects on multiple countries was elucidated by the 2010 "Stuxnet" attack. Considered the most

---

127. *See* Amber Corrin, *Digital Collateral Damage Blurs Cyber Warfare Strategies*, BUS. FED. TECH. (Apr. 23, 2010), http://fcw.com/articles/2010/04/26/home-page-inside-dod-collateral-damage.aspx (citing James Lewis, the Director of the Center for Strategic and International Studies' Technology and Public Policy Program, who said that collateral damage is the "biggest constraint" on America's willingness to conduct offensive cyberattacks. According to Lewis, a cyberattack on North Korea could inflict peripheral effects on Japan or China because "we don't have a good map of how networks connect.").

128. Martin Libicki, *Pulling Punches in Cyberspace*, *in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS 123, 126 (National Research Council ed., 2010).

129. The use of biological weaponry is prohibited under international law, as codified in the Geneva Protocol of 1925. The 1972 Convention of Biological Weapons, ratified by the United States and 164 other state parties, extends the Geneva Protocol by further precluding the development, production, and stockpiling of biological weaponry. *See* Jozef Goldblat, *The Biological Weapons Convention - An Overview*, INT'L COMM. OF THE RED CROSS (June 30, 1997), http://www.icrc.org/eng/resources/documents/misc/57jnpa.htm.

130. F. Roberto, *Transport and Dispersion of Biological Agents/Toxins*, SCAPA BIOSAFETY WORKING GRP. 5 (Nov. 2009), http://orise.orau.gov/emi/scapa/files/Transportand Dispersion.pdf.

131. *Id.*; *see also* ERIC A. CRODDY, WEAPONS OF MASS DESTRUCTION 162 (2004). Biological weaponry's unpredictable nature persuaded policymakers from 164 nations to ratify the 1972 Convention on the Prohibition of the Development, Production, and Stockpiling of Bacteriological (Biological) and Toxin Weapons. In spite of their similar features, cyberweapons have yet to be outlawed by the international community. *See* Goldblat, *supra* note 129; *see also* Stefan Riedel, *Biological Warfare and Bioterrorism: A Historical Review*, BAYLOR UNIV. MED. CTR. (Oct. 17, 2004), http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1200679.

"sophisticated cyberweapon ever deployed,"[132] Stuxnet was purportedly designed by the United States and Israel to set back Iran's nuclear program. The malicious code caused the engines in Iran's centrifuges to intermittently accelerate and then decrease in speed, inducing excessive vibrations that overwhelmed and damaged the centrifuges. As the worm operated, it recorded routine operations at Natanz and played those images back to plant operators, thereby evading detection for nearly a year.

According to computer scientists who analyzed the code, Stuxnet's designers undertook elaborate precautions to avoid incidental damage. The malware's "fail-safe" features included an USB-spreading code that was programmed to ensure that each infected machine would only be able to infect a maximum of three additional devices.[133] Stuxnet's creators also programmed the malware to self-destroy on June 24, 2012, thereby eradicating itself from every Iranian machine that was infected.[134] According to reports, in order to further enhance the malware's precision, Israel and the United States allegedly tested the worm on nuclear centrifuges in Israel's Dimona complex.[135]

However, in spite of such careful precautions, an error in the code soon caused it to escape from the Natanz facility, "br[eaking] free, like a zoo animal that found the keys to the cage."[136] Stuxnet rapidly spread and infected civilian computer networks across the globe, including in China, India, Indonesia, Azerbaijan, Malaysia, South Korea, the United Kingdom, Australia, Finland, Germany, and the United States.[137] Over six hundred thousand computers were infected by the virus, of which more than half were located in Iran.[138] Chinese news agencies reported that the malware infected approximately six million personal computers and one thousand corporate computer systems.[139] In the United States, the Department of Homeland Security had to deploy its Industrial Control Systems Computer Emergency Readiness Team ("ICS-CERT") to a

132. William J. Broad et al., *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, N.Y. TIMES (Jan. 15, 2011), http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

133. Michael Joseph Gross, *A Declaration of Cyber-War*, VANITY FAIR (Apr. 2011), http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104.

134. *Id*.

135. Broad, *supra* note 132.

136. David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES (June 1, 2012), http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

137. Farwell, *supra* note 22, at 23.

138. *Id*.

139. Arthur Bright, *Clues Emerge About Genesis of Stuxnet Worm*, CHRISTIAN SCI. MONITOR (Oct. 1, 2010), http://www.csmonitor.com/World/terrorism-security/2010/1001/Clues-emerge-about-genesis-of-Stuxnet-worm.

critical manufacturing facility that had been infected with the Stuxnet malware.[140]

Cyberterrorism would likely generate far worse collateral effects than Stuxnet and other cyberattacks launched by states. Nations are bound by the laws of war, including the *jus in bello* principles of "proportionality" and "distinction." The principle of "distinction," codified in Articles 48 and 51 of the 1977 Additional Protocol I to the Geneva Conventions, precludes nations from targeting civilians in "indiscriminate attacks."[141] Similarly, "proportionality," which is codified in Article 51(5)(b) of Additional Protocol I, forbids attacks that "may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."[142] The principles of proportionality and distinction have evolved into customary international law. Therefore, even nations that are not party to the Additional Protocols to the Geneva Conventions must abide by these *jus cogens* doctrines. As applied to cyberwarfare, whenever nations conduct cyberattacks, they must invest in precautionary measures to prevent, or at least minimize, collateral damage to civilian populations and objects.

Terrorists, on the other hand, are not parties to the Geneva Conventions and the Additional Protocols, and do not perceive themselves as bound by customary international humanitarian law. To the contrary, terrorists' radical jihadist ideology and strategic objectives are anathema to the concepts of distinction and proportionality.[143] Seeking to inflict as much civilian carnage as feasible, they have no incentive to invest in developing precise technology and "fail safe" features to minimize their cyberattacks' peripheral consequences. This disincentive is further magnified because terrorists, unlike states, are unconcerned with the potential for cyber "blowback" or political backlash. Terrorists and their recruits take shelter in under-developed states that are far less reliant on computer networks and information technology. Even if terrorists' cyberattacks generated ripple effects on computer network systems across the globe, state sponsors of terrorism and potential recruits would be minimally impacted by such collateral damage. Given the high probability of collateral damage, applying the effects-based principle to cyberterrorism would legiti-

140. *ICS-CERT Incident Response Summary Report: 2009–2011*, DEP'T HOMELAND SEC. 9 (2011), http://ics-cert.us-cert.gov/sites/default/files/documents/ICS-CERT%20Incident%20Response%20Summary%20Report%20(2009-2011).pdf.

141. Protocol Additional to the Geneva Conventions of 12 August, 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 48, June 8, 1977, 1125 U.N.T.S. 3. *See also id*. art. 51(2).

142. Protocol Additional to the Geneva Conventions of 12 August, 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 51(5)(b), June 8, 1977, 1125 U.N.T.S. 3.

143. Ted Lapkin, *Does Human Rights Law Apply to Terrorists?*, 14 MID. EAST. Q. 3, 3 (2004).

mize countless claims of prescriptive jurisdiction. The sheer amount and complexity of the claims would increase the potential for international tension.

A third version of the territoriality doctrine, promulgated by Professor Thomas Schultz, is the "targeting" based principle. This theory posits that the perpetrator of the act must have "intended to have effects" within the territory of the state asserting jurisdiction.[144] Schultz depicts this principle as a "tighter version" of the objective territorial doctrine.[145] A potential advantage of this principle is that it could decrease the number of conflicting jurisdictional claims. Given cyberweaponry's volatile nature, it is likely that the perpetrator targeted a lower number of territories than the number of territories that actually experienced the attack's effects.[146] However, given the current state of technology and difficulty of deciphering the intended victim of a cyberterrorist attack, jurisdiction based on the targeting principle would be unfeasible. A cyberterrorist may believe that he would be afforded more honor, glory, and respect among fellow jihadists if he took credit for having deliberately targeted multiple nations rather than conceding that much of his damage was collateral. Therefore, he may bask in media coverage and boast that he had intended to target all of these nations. Cyberterrorists would not be deterred if it required years for computer scientists to determine the genuine target of the attack and thus resolve which nation is entitled to jurisdiction.

B. *Nationality Principle*

The "nationality theory," often referred to as "active personality," grants jurisdiction based on the nationality of the offender, regardless of where the crime took place. This theory derives from the recognition that a nation, by virtue of its sovereignty, exerts unlimited control over its citizens. Nations should therefore be entitled to exercise jurisdiction over their citizens regardless of their citizens' locations when they perpetrate a crime. Similarly, as long as nationals retain their citizenship, they should be expected to adhere to their countries' laws when they are abroad. As the U.S. Supreme Court articulated in *United States v. Bowman,* a case concerning a crime perpetrated by U.S. nationals in Brazil: "Clearly it is no offense to the dignity or right of sovereignty of Brazil to hold [the U.S. defendants] for this crime against the government to which they owe allegiance."[147] A decade later, in the widely cited case of *Blackmer v. United States*, the Supreme Court similarly reasoned,

> While it appears that the petitioner removed his residence to France in the year 1924, it is undisputed that he was, and continued to be, a citizen of the United States. He continued to owe allegiance to the United States. By virtue of the

144. Schultz, *supra* note 90, at 817.

145. *Id.*

146. *See id.*

147. United States v. Bowman, 260 U.S. 94, 102 (1922).

> obligations of citizenship, the United States retained its authority over him, and he was bound by its laws made applicable to him in a foreign country.[148]

In addition to the rationales of sovereignty and allegiance, the nationality theory of jurisdiction is also grounded on due process concerns. A citizen is expected to be most knowledgeable about his own country's laws. Therefore, the nationality principle would provide the perpetrator with sufficient notice about the criminality of his future actions. In contrast, applying another nation's criminal statute would limit the opportunity for fair warning.

However, the due process justification underlying the nationality doctrine is obsolete in the context of cyberterrorism. The Internet and other communications technology provide terrorists with unparalleled access to information regarding which nations have criminalized cybercrimes and cyberterrorism. The Internet is replete with newspaper articles, scholarly papers, and blogs addressing the criminal consequences for engaging in such activity. A terrorist who executed a technologically sophisticated cyberterrorist attack would be hard pressed to argue that he lacked fair notice concerning the unlawfulness of his actions.

The nationality principle of jurisdiction is also impractical for prosecuting cyberterrorists due to the aforementioned attribution dilemma in cyberspace. As discussed previously, cyberterrorists can hijack botnets in multiple countries, route through proxy servers, and leave behind a "false flag," therefore "implicating an otherwise innocent individual, group, or government."[149] Following the 2009 cyberattacks against Google, Yahoo, Morgan Stanley, and other corporations, dubbed "Operation Aurora," Google accused China of designing the attacks to steal intellectual property and other company data. However, approximately a year later, an Atlanta-based security firm that carefully analyzed the malware posited that "new and amateur botnet operators" had designed the attacks.[150] Attribution efforts proved similarly inconclusive following the Estonian attacks and 2009 distributed denial of service attacks against United States and South Korean websites.

Therefore, if prescriptive jurisdiction over a cyberterrorist were to be based on the nationality doctrine, the international community would have to reallocate jurisdiction as new information on the true source and nationality of the perpetrator was discovered. Such reallocation would generate high transaction costs and prosecutorial inefficiencies. Furthermore, nations would have less motivation to invest significant resources in prosecuting a cyberterrorist if they believed that other countries could usurp their jurisdiction once new revelations

---

148. Blackmer v. United States, 284 U.S. 421, 436 (1932); *see also* Blakesley, *supra* note 96, at 1118.

149. Duncan B. Hollis, *An e-SOS for Cyberspace*, 52 HARV. INT'L L.J. 373, 397 (2011).

150. Jaikumar Vijayan, *Update: Attacks on Google May Have Been Work of Amateurs*, COMPUTERWORLD (Mar. 3, 2010), http://www.computerworld.com/s/article/print/9165518/Update_Attacks_on_Google_may_have_been_work_of_amateurs_?taxonomyId=17&taxonomyName=Security.

about the perpetrator's nationality emerged. Although U.S. attribution capabilities are improving, they are still not sufficiently robust to avoid the pitfalls associated with applying the nationality principle to cyberterrorism.

C. *Passive Nationality Principle*

The "passive nationality" doctrine, often labeled "passive personality," confers jurisdiction based on the nationality of the victim. It is premised on the principle that nations have a responsibility to protect their citizens, even when they are abroad. In a few instances, nations have extended the doctrine to exercise jurisdiction over crimes perpetrated against their domiciliaries or residents. However, such an extension has been rare and controversial.[151]

Many nations and legal scholars consider the "passive personality" doctrine to be one of the most controversial bases of prescriptive jurisdiction under international law.[152] U.S. courts traditionally rejected the principle, reasoning that it would infringe on state sovereignty and territorial jurisdiction. Under this doctrine, criminals perpetrating crimes in their own countries would be subject to endless litigation under the criminal laws of every visitor's home state. Furthermore, the accused would be deprived of fair notice when the substantive laws of his country and that of the victim's nation differed.[153] Judge Moore's dissenting opinion in the *S.S. Lotus* case exhibited America's historical skepticism of the passive personality doctrine. Moore reasoned that "passive personality" is:

> [A]t variance not only with the principle of the exclusive jurisdiction of a State over its own territory, but also with the equally well-settled principle that a person visiting a foreign country, far from radiating for his protection the jurisdiction of his own country, falls under the dominion of the local law and, except so far as his government may diplomatically intervene in case of a denial of justice, must look to that law for his protection.[154]

Given the international community's widespread rejection of the passive personality principle, the Harvard Research Project's "Draft Convention" did not even recognize the principle as an independent basis of jurisdiction.[155] Although the Draft Convention did discuss this principle, it only acknowledged its potential application when jurisdiction would already be warranted under the universality doctrine. According to the drafters, when a universally recognized

---

151. *See Report of the Task Force on Extraterritorial Jurisdiction*, *supra* note 94, at 146-47.

152. John G. McCarthy, *The Passive Personality Principle and Its Use in Combatting International Terrorism*, 13 FORDHAM INT'L L.J. 298, 301 (1989).

153. Joshua Robinson, *United States Practice Penalizing International Terrorists Needlessly Undercuts Its Opposition to the Passive Personality Principle*, 16 B.U. INT'L L.J. 487, 489 (1998).

154. The Case of the S.S. Lotus (Fr. v.Turk.), 1972 P.C.I.J. (ser. A) No. 10, at 23 (Sept. 7) (Moore, J., dissenting).

155. McCarthy, *supra* note 152, at 306-07.

crime was perpetrated beyond the territory of any state, the state whose nationals were victims could receive jurisdictional preference.[156] The drafters believed that the nation whose citizens were victims would have the strongest motivation to prosecute the perpetrators.[157] When discussing the passive personality principle, the drafters repeatedly emphasized its controversial nature. They contended that passive personality "has been vigorously opposed in Anglo-American countries . . . has been more strongly contested than any other type of competence," and "is the most difficult to justify in theory."[158]

The passive personality doctrine continues to have the least support in customary international law among the other theories of prescriptive jurisdiction.[159] However, in recent decades, the international community has increasingly accepted the legitimacy of the passive personality principle when applied to international terrorism.[160] Numerous U.S. statutes, including the Hostage Taking Act of 1984 and the Omnibus Diplomatic Security and Antiterrorism Act of 1986, grant passive personality jurisdiction over crimes committed by foreigners against U.S. nationals abroad. The principle is also codified in international agreements, including Article 9 of the International Convention Against the Taking of Hostages[161] and Article 3(1)(c) of the Convention on the Prevention and Punishment of Crimes Against International Protected Personnel Including Diplomatic Agents.[162]

Asserting passive personality jurisdiction over cyberterrorists is impractical for similar reasons to those elucidated above for why the effects based principle is inappropriate. Since cyberattacks would inflict damage across the globe, citizens of multiple countries would fall victim. Applying the passive personality doctrine to cyberterrorism would therefore engender infinite and competing claims for prescriptive jurisdiction.

The fact that the passive personality doctrine, in comparison to other jurisdictional principles, constitutes such a significant encroachment on other nations' sovereignty also militates against extending this doctrine to cyberterrorism. International cooperation is critical for successfully investigating and prosecuting cyberterrorism. Other states would be less amenable to requests for

---

156. *See* The Am. Soc'y of Int'l L., *Draft Convention on Jurisdiction with Respect to Crime,* 29 AM. J. INT'L L. 435, 589 (Supp. 1935) [hereinafter *Draft Convention*].

157. *Id*. at 589-90.

158. *Id*. at 579; *see also* Christopher W. Robbins, *Finding Terrorists' Intent: Aligning Civil Antiterrorism Law with National Security*, 83 ST. JOHN'S L. REV. 1201, 1217 (2009).

159. *Id*.

160. The Restatement (Third) recognizes that nations have increasingly applied the passive personality principle "to terrorist and other organized attacks on a state's nationals by reason of their nationality, or to assassination of a state's diplomatic representatives or other officials." RESTATEMENT (THIRD), *supra* note 62, § 402 cmt. g.

161. International Convention Against the Taking of Hostages, Dec. 27, 1979, 1316 U.N.T.S. 206.

162. Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons Including Diplomatic Agents, Dec. 14, 1973, 1035 U.N.T.S. 167.

investigative assistance and extradition if they believed that the United States encroached on their sovereign authority even though there was no direct threat to American national security.[163]

D. *Universal Jurisdiction Doctrine*

According to the principle of universal jurisdiction, any nation may assert prescriptive jurisdiction over certain crimes regardless of the locations of the crimes or the nationalities of the perpetrators and victims. States may therefore receive jurisdiction even when they lack any connection to the offense.[164] Historically, courts and legal scholars provided two rationales for exercising universal jurisdiction. The first rationale focuses on the sheer atrocity of the crime. Certain crimes are so nefarious that they constitute an "affront to humanity" and endanger the international community as a whole.[165] The perpetrators of such crimes are considered *hostis humani generis*—the enemy of all mankind. Therefore any nation, serving as humanity's representative, should be empowered to prosecute the individuals who are responsible.[166]

The second historical rationale for universal jurisdiction focuses on the *locus delicti*, or the location of the act.[167] Crimes subject to universal jurisdiction often transpire in territories beyond any nation's sovereign authority, such as on the *terra nullius*, or high seas.[168] Alternatively, these crimes may occur in failed states that have suffered absolute breakdowns in their governance systems. Such countries are incapable of enforcing law and order within their borders and thus lack the resources to effectively prosecute criminals. Crimes subject to universal jurisdiction may also occur in states whose governments seek to shield the accused from prosecution. These states may merely attempt to appease international critics by conducting sham trials.[169] In such cases, universal jurisdiction would be warranted to prevent the perpetrators of heinous crimes from escaping with impunity.

---

163. *See* Robbins, *supra* note 158, at 1227.

164. 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)).

165. Madeline H. Morris, *Universal Jurisdiction in a Divided World: Conference Remarks,* 35 NEW ENG. L. REV. 337, 337 (2001).

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

167. *See* Lee A. Steven, Note, *Genocide and the Duty to Extradite or Prosecute: Why the United States is in Breach of Its International Obligations*, 39 VA. J. INT'L L. 425, 435 (1999).

168. Andrew J. Batog, *The Piracy Analogy and Modern Universal Jurisdiction*, RESPONDEAT (Apr. 10, 2010), http://respondeat.wordpress.com/2010/04/10/the-piracy-analogy-and-modern-universal-jurisdiction/.

169. *See Report of the Task Force on Extraterritorial Jurisdiction*, *supra* note 94, at 152-53.

In the recent literature on cyberterrorism, Kelly Gable has argued that universal jurisdiction is the most appropriate principle for prosecuting cyberterrorists. Gable contends, "[d]ue 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."[170] However, there are numerous legal and policy rationales against extending universal jurisdiction to cyberterrorism. We turn next to demonstrating that universal jurisdiction is legally unavailable to prosecutors in the cyberterrorism context, and use of this principle would magnify interstate conflict while proving ineffectual at preventing cyberterrorist attacks or prosecuting their perpetrators.

There is insufficient legal basis for extending universal jurisdiction to cyberterrorism. Under international law, crimes of universal jurisdiction must be created by international custom or treaty regime.[171] Customary international law and current treaty regimes have limited the category of universal crimes to cover offenses recognized as "heinous" in nature. This narrow set of crimes, including piracy, genocide, torture, war crimes, and crimes against humanity, must be considered so egregious that they "shock the conscience of humanity." Courts have not articulated the precise extent of depravity required to invoke universal jurisdiction. However, they have described the required threshold as crimes "viewed with universal abhorrence,"[172] "monstrous,"[173] and limited to a "handful of heinous actions."[174] The opinion of the District Court of Jerusalem in the trial of the Nazi leader Adolf Eichmann reiterated the "heinous" prerequisite for asserting universal jurisdiction. It stated that Eichmann's crimes "struck at the whole of mankind and shocked the conscience of nations."[175]

Many cyberterrorist attacks would produce effects that would not reach this required threshold of "heinousness." For example, although the 2007 cyberattacks against Estonia incapacitated the country's banking systems, media outlets, and Parliamentary websites, it would be difficult to contend that such attacks "shocked the conscience of mankind." Similarly, a major cyberterrorist attack against a nation's banking system that resulted in extensive economic damage might not rise to the required level of "heinousness." Such conse-

170. Gable, *supra* note 20, at 105.

171. *See* Steven, *supra* note 67, at 436.

172. Filartiga v. Pena-Irala, 577 F. Supp. 860, 863 (E.D.N.Y. 1984); *see also* Filartiga v. Pena-Irala, 630 F.2d 876, 884 (2d Cir. 1980).

173. Filartiga, 577 F. Supp. at 863.

174. Tel-Oren v. Libyan Arab Republic, 726 F.2d 774, 781 (D.C. Cir. 1984).

175. Attorney-General v. Eichmann, 36 I.L.R. 18, 26 (Dist. Jerusalem 1961) (Isr.), *aff'd,* 36 I.L.R. 277 (S. Ct. 1962).

quences would pale in comparison to the human atrocities resulting from the *jus cogens* violations of genocide or torture.[176]

Even if a cyberterrorist attack exhibited the requisite threshold of "heinousness," there would still be scant support under customary international law and treaty regimes for invoking universal jurisdiction.[177] Customary international law emerges from the general and consistent conduct of states, which states follow due to *opinio juris* or a "sense of legal obligation." Legal scholars have described *opinio juris* as the "psychological component of customary international law"[178] or the "external acceptance by states that a practice is recognized as being obligatory."[179] Contrary to Gable's assertions, there is no evidence of widespread belief among nations that preventing cyberterrorism and other forms of cyberattack amounts to a legal obligation under international law. The fact that government officials and legal scholars across the globe have conceded that there is a fundamental gap or "mismatch" between current law and cyber capabilities belies the argument that *opinio juris* is present.[180] The recent proliferation of state-sponsored cyberattacks and cyber-espionage also indicates that nations believe that they can perpetrate and sanction such conduct with impunity. Similarly, in terms of treaty regimes, while numerous international conventions recognize terrorism as a universal crime, most of them do not apply to cyberterrorism.[181] Although the European Convention on Cybercrime does preclude cyberterrorist attacks, it has only been ratified by one non-European nation: the United States. Therefore, it cannot be considered indicative of "global opinion" that cyberterrorism constitutes a universal crime.[182]

---

176. A *jus cogens* or peremptory norm is defined as a norm "accepted and recognized by the international community of States as a whole as a norm from which no derogation is permitted." Sévrine Knuchel, *State Immunity and the Promise of Jus Cogens*, 9 NW. U. J. INT'L HUM. RTS. 149, 150 (2011).

177. BENEDETTA UBERTAZZI, EXCLUSIVE JURISDICTION IN INTELLECTUAL PROPERTY 153 (2012).

178. JACK L. GOLDSMITH & ERIC A. POSNER, THE LIMITS OF INTERNATIONAL LAW 24 (2005).

179. M. Cherif Bassiouni, *Universal Jurisdiction for International Crimes: Historical Perspectives and Contemporary Practice, in* 2 INTERNATIONAL CRIMINAL LAW 153, 186 (M. Cherif Bassiouni ed., 3d ed. 2008).

180. *See, e.g.*, Thom Shanker, *Cyberwar Nominee Sees Gaps in Law*, N.Y. TIMES (Apr. 14, 2010), http://www.nytimes.com/2010/04/15/world/15military.html (quoting Lieutenant General Keith B. Alexander, Commander of U.S. Cyber Command, regarding the gap between cyber warfare capabilities and "governing laws and policies").

181. For example, the International Convention for the Suppression of Terrorist Bombings outlaws the deliberate use of explosives against a "place of public use" or "governmental facility." International Convention for the Suppression of Terrorist Bombings, Jan. 9, 1998, 37 I.L.M. 249, 253. Given that cyberterrorists exploit different "weaponry" to inflict destruction, such conventions are clearly inapplicable. *But see* Gable, *supra* note 20, at 106 (arguing that the International Convention for the Suppression of Terrorist Bombings "conceivably could apply to cyberterrorism").

182. Brian Harley, *A Global Convention on Cybercrime?*, COLUM. SCI. & TECH. L. REV. ONLINE (Mar. 23, 2010), http://www.stlr.org/2010/03/a-global-convention-on-cybercrime.

Universal jurisdiction therefore remains legally unavailable under both customary international law and treaties for asserting prescriptive jurisdiction over cyberterrorists.

In addition to legal concerns, policy considerations also militate against using universal jurisdiction as the primary jurisdictional principle for prosecuting cyberterrorists. Under universal jurisdiction, all nations in the world would be entitled to assert prescriptive jurisdiction over a cyberterrorist, regardless of whether they had any nexus to the offense at hand. Therefore, rather than helping to minimize competing prosecutorial claims, universal jurisdiction would exacerbate jurisdictional "tug-of-war" among nations' courts.[183] The ensuing diplomatic tension could cause the pursuit of justice to "become[] trapped within the labyrinth of an inter-State dispute."[184] For similar reasons, universal jurisdiction over cyberterrorism is unwarranted on efficiency grounds. By expanding the number of nations that are authorized to prosecute a cyberterrorist, universal jurisdiction would raise the transaction costs involved in negotiating over which state should receive prosecutorial preference. As legal scholar Eugene Kontorovich contends, universal jurisdiction "makes the class of [prosecutorial] rights holders sufficiently large that it may entirely preclude a negotiated allocation of the rights."[185]

Scholars might counter that such critiques of universal jurisdiction are exaggerated because nations that are unaffected by a cyberterrorist attack might not seek to prosecute the accused.[186] However, even if this were the case—and universal jurisdiction did not increase jurisdictional claims—it would still aggravate jurisdictional conflicts among the states that were impacted by an attack. Applying universal jurisdiction to cyberterrorism, a nation that only experienced minor and collateral effects from a cyberterrorist attack would have equal standing to prosecute the perpetrator as a nation that experienced a severe security threat. Such an approach would generate diplomatic hostility, alienating those nations that were severely impacted by an attack. A better approach to allocating jurisdiction over cyberterrorists would be to give priority to nations that suffered a fundamental threat to their security as a result of the attack. Indeed, the international community and legal scholars have long recognized that

183. BRANDEIS INST. FOR INT'L JUDGES, THE INTERNATIONAL RULE OF LAW: COORDINATION AND COLLABORATION IN GLOBAL JUSTICE 11 (2012), *available at* http://www.brandeis.edu/ethics/pdfs/internationaljustice/biij/BIIJ2012.pdf (last visited May 27, 2014).

184. INAZUMI, *supra* note 21, at 168.

185. Eugene Kontorovich, *The Inefficiency of Universal Jurisdiction*, 2008 U. ILL. L. REV. 389, 398 (2008).

186. *See* Jonathan H. Marks, *Mending the Web: Universal Jurisdiction, Humanitarian Intervention, and the Abrogation of Immunity by the Security Council*, 42 COLUM. J. TRANSNT'L L. 445, 474 (2004).

universal jurisdiction should only be pursued as a method of "last resort"[187] or "safety net for grave international crimes"[188] when nations that have stronger connection to these crimes are resistant or unable to prosecute the accused. For example, in the deliberations of the UN General Assembly Sixth Committee (Legal), delegates from across the international community insisted that universal jurisdiction remain a "complementary mechanism of last resort and States with primary jurisdictional links should have priority in carrying out investigations and prosecutions."[189] Given the importance of international cooperation in cyberterrorist prosecutions and universal jurisdiction's potential to cause unnecessary friction among states, using universal jurisdiction to prosecute cyberterroists would not be prudent.

Finally, another significant limitation of universal jurisdiction in the cyberterrorism context is that it would not authorize nations to prosecute cyberterrorists preventively. According to the doctrine, the community of nations must wait for heinous crimes that "shock the conscience of humanity" to occur before universal jurisdiction is warranted. Therefore, even if authorities discovered a cyberterrorist's imminent plan to incapacitate a nation's power grid, they would be restrained from exercising prescriptive jurisdiction until the plan was consummated. Since the protective principle of jurisdiction does not suffer from similar legal restraints, prosecuting cyberterrorists based on this principle would be more effective at preventing attacks.

E. *The Protective Principle of Jurisdiction: The Efficacious Method for Prosecuting Cyberterrorists*

Out of all the prescriptive bases for exercising jurisdiction under international law, the protective principle offers the greatest potential to reduce the number of conflicting jurisdictional claims and mitigate international discord. Applying the protective principle would also provide nations with stronger capacity to prosecute cyberterrorists and thwart debilitating attacks before they occurred. Judicial precedents provide strong support for extending the protective principle to cyberterrorism.

187. Press Release, General Assembly, As Debate Concludes, Delegates Stress Universal Jurisdiction Should Be Last Resort in Combat Against Impunity, U.N. Press Release GA/L/3442 (Oct. 18, 2012), *available at* http://www.un.org/News/Press/docs/2012/gal3442.doc.htm (last visited Oct. 26, 2013).

188. Ali Dayan Hasan, *The Shrinking World of George W Bush*, GLOBAL POLICY FORUM (Aug. 11, 2011), http://www.globalpolicy.org/international-justice/universal-jurisdiction-6-31/50627-the-shrinking-world-of-george-w-bush.html.

189. Press Release, General Assembly, *supra* note 187.

1. The Case for Protective Jurisdiction

During the nineteenth century, states began asserting extraterritorial jurisdiction over foreign conduct that posed a threat to their security interests, sovereignty, or critical government functions based on the "protective" principle.[190] In Articles 7 and 8 of the 1935 Harvard Draft Convention, the Harvard faculty described the principle as conferring jurisdiction on a nation "with respect to any crime committed outside [the nation's] territory by an alien against the security, territorial integrity or political independence of that State."[191] The protective principle is grounded on the axiom that every nation is entitled to defend itself. The principle is also rooted in the traditional notion of sovereignty. As legal scholar Iain Cameron notes, "both the right of self defense and right to exercise [protective] jurisdiction are aspects of (and, historically, preconditions of) the concept of sovereignty."[192] Finally, the doctrine may also derive from the rationale behind criminal law itself, the objective of which is to safeguard the nation and which should therefore "be extended as far as is necessary for such protection."[193]

Although the protective doctrine initially provoked opposition, it gained increasing acceptance in the United States and in the international community during the twentieth century.[194] The majority of countries' jurisprudence and penal codes, including the criminal codes of France, Ethiopia, and Venezuela, have acknowledged the protective principle. Judiciaries in France, Israel, and numerous Latin American countries have frequently invoked the protective doctrine to exercise extraterritorial jurisdiction over terrorists.[195]

Compared to principles such as effects-based territoriality that are far too expansive in addressing cyberterrorism, the protective principle of jurisdiction would vastly reduce conflicting claims of jurisdiction. Due to cyberweaponry's unpredictable nature, a cyberterrorist attack targeted against one nation could inadvertently infect computer systems in multiple nations. However, in many of these countries, such collateral damage would not be so severe as to endanger these nations' security, sovereignty, or important governmental functions. For example, in the recent Stuxnet attack against Iran's nuclear facility, although the virus affected computer systems in at least eleven other countries besides

190. ADEMOLA ABASS, COMPLETE INTERNATIONAL LAW: TEXT, CASES, AND MATERIALS 537 (2012).

191. *Draft Convention*, *supra* note 156, at 543.

192. IAIN CAMERON, THE PROTECTIVE PRINCIPLE OF INTERNATIONAL CRIMINAL JURISDICTION 46 (1994).

193. Lotika Sarkar, *The Proper Law of Crime in International Law,* 11 INT'L & COMP. L.Q. 446, 463 (1962); *see also* Marcuss & Richard, *supra* note 23, at 445.

194. *See* Susan Brenner & Bert-Jaap Koops, *Approaches to Cybercrime Jurisdiction***,** 4 J. HIGH TECH. L. 1, 26 (2004).

195. *See* Christopher C. Joyner & Wayne P. Rothbaum, *Libya and the Aerial Incident at Lockerbie: What Lessons for International Extradition Law?*, 14 MICH. J. INT'L L. 222, 236-37 (1992).

Iran, this collateral damage was minor and reversible. Corporate and civilian owners of the one hundred thousand computers that were infected across the globe had to hire anti-virus specialists to cleanse their workstations and servers from the malware.[196] Nevertheless, such relatively minor economic costs and inconvenience did not rise to the level of threatening these nations' vital security interests. If the Stuxnet attack had been launched by terrorists, only Iran could have asserted jurisdiction based on the protective principle since solely its sovereign interests were threatened. The Stuxnet attack therefore elucidates the capacity of the protective principle to circumscribe the potential for competing jurisdictional claims.

Compared to the territoriality principles, application of the protective doctrine would also reduce impunity for the perpetrators of cyberterrorism. The country that suffered a cyberterrorist attack that threatened its security and vital government functions would have the strongest incentive to vigorously prosecute the suspected perpetrator. Cyberforensic investigations cost millions of dollars, are time-consuming, require extensive cooperation with intelligence and law enforcement personnel in other countries, and often lead to false trails. Nevertheless, a nation whose security interest was at stake would not hesitate to undertake such an investigation, especially given the potential for it to serve as a repeat target of future cyberterrorist attacks. In contrast, a nation that experienced relatively minor effects or inconvenience from a cyberterrorist attack would be less inclined to invest such significant resources into prosecuting the case. Such efforts would divert the resources of its law enforcement and intelligence agencies from more dire security threats.

Most critically, application of the protective principle would provide nations with the authority to preventively prosecute and apprehend cyberterrorists before devastating cyberterrorist attacks occurred. The protective doctrine is the only jurisdictional basis under international law that authorizes extraterritorial jurisdiction over crimes that pose a potential danger to the security of a state. Although some U.S. courts and the Restatement (Third) have controversially asserted that both the objective territoriality and effects-based doctrines authorize jurisdiction over "intended but unrealized" crimes, judicial precedent and international legal opinions indicate the contrary.[197] It is evident from Justice Holmes' holding in *Strassheim*—"[a]cts done outside a jurisdiction, but intended to produce *and* producing effects within it"—that actual effects have to tran-

196. *See* Mikko Hypponen, *The Failure of Anti-Virus Companies to Catch Military Malware*, SCHNEIER ON SEC. (June 19, 2012), http://www.schneier.com/blog/archives/2012/06/the_failure_of_3.html (last visited Jan. 12, 2014).

197. A few U.S. court decisions have found that the mere intent to perpetrate a crime that would be consummated within a nation's territory is sufficient for upholding prescriptive jurisdiction based on objective territoriality. *See* United States v. Ricardo, 619 F.2d 1124, 1129 (5th Cir. 1980); *see* BOLESLAW A. BOCZEK, INTERNATIONAL LAW: A DICTIONARY 80 (2005); *see also* RESTATEMENT (THIRD), *supra* note 62, § 402 cmt. D.

spire within the nation seeking jurisdiction.[198] Similarly, foreign judicial decisions and scholarship have argued that in order for a state to have a legitimate claim to jurisdiction based on objective territoriality, an element of the crime must occur within its territory.[199] Therefore, thwarted conspiracies to perpetrate cyberterrorism against a nation would not entitle that nation to jurisdiction. Under the protective principle, however, mere discovery of terrorists' plans to execute an attack against a nation's power grid would warrant jurisdiction even if authorities managed to foil the attack.[200]

Unfortunately, given the unique vulnerabilities of the Internet and computer systems, many cyberterrorist attacks might not be preventable. Cyberterrorists are capable of launching attacks in milliseconds using zero-day exploits. By definition, zero-day exploits occur when attackers take advantage of a software vulnerability that is unknown to the software developers who could address and patch the vulnerability.[201] However, in spite of such technical challenges, it is possible for terrorists' plans to be discovered in advance through strong intelligence efforts. In recent years, the Pentagon, FBI, National Security Agency, CIA, and the rest of the U.S. intelligence community have prioritized collecting and sharing intelligence information about cyber threats with international partners.[202] In 2007, the FBI established the National Cyber Investigative Joint Task Force ("NCIJTF"), which currently consists of eighteen intelligence and law enforcement agencies collaborating to "predict and prevent" attacks and "identify and address cyber threats and vulnerabilities before adversaries are able to exploit weaknesses."[203] The task force works through "Threat Focus Cells" or "specialized groups of agents, officers, and analysts that are focused on particular threats, such as botnets."[204] The NCIJTF also collaborates extensively with the Department of Defense Cyber Crime Center to discover cyber threats emanating from both domestic and international sources.[205]

It is very possible that such intelligence efforts could prove fruitful in thwarting a cyberterrorist attack. For example, given that terrorist organizations

198. Strassheim v. Daily, 221 U.S. 280, 285 (1911) (emphasis added).

199. *See* Christopher L. Blakesley, *Jurisdiction as Legal Protection Against Terrorism,* 19 CONN. L. REV. 895, 923-926 (1986); *see also* R. MERLE & A. VITU, TRAITE DE DROIT PENAL 367 n.2 (2d ed. 1978).

200. *See* Robbins, *supra* note 158, at 1223-24.

201. *See* SANS INST., *Zero-Day Vulnerability Trends*, *in* TOP CYBER SECURITY RISKS 21, (Sept. 2009), *available at* http://www.cs.vu.nl/~crispo/teaching/seceng2012/Assignment1/toprisk.pdf.

202. *See* Panetta, *supra* note 3.

203. *See National Cyber Investigative Joint Task Force*, FED. BUREAU INVESTIGATION, http://www.fbi.gov/about-us/investigate/cyber/ncijtf (last visited Jan. 11, 2014).

204. *See* Robert S. Mueller, *Speech at the RSA Cyber Security Conference*, FED. BUREAU INVESTIGATION (Mar. 1, 2012), http://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies (last visited Jan. 12, 2014).

205. *Id*.

may hire sophisticated computer specialists or hackers to assist them in executing cyberattacks, they may leave behind email trails that could be monitored by intelligence agencies.[206] Given that the protective principle is the only jurisdictional basis that would empower nations to act on such intelligence findings, it affords nations the greatest potential to prosecute cyberterrorists preventively.[207]

Similarly, application of the protective principle could incentivize more nations that are vulnerable to cyberterrorism to enact statutes criminalizing such acts. If cyberterrorist attacks were to be governed by subjective territoriality, nations that suffered devastating cyberterorrist attacks would be barred from prescribing their laws extraterritorially to prosecute the perpetrators. Since cyberterrorists could easily escape punishment by launching attacks from within legal safe havens, nations likely to fall victim to cyberterrorism would have less motive to criminalize this conduct. In contrast, if the protective principle governed, states would have stronger reasons to criminalize such activity. If they suffered a devastating cyberterrorist attack, they would be legally authorized to prosecute the offender.

Prioritizing the protective doctrine over subjective territoriality would therefore undermine terrorists' capacity to shop for legal "safe havens" to avoid prosecution. As evinced by their fatwas and attacks, terrorist organizations such as al-Qaeda are committed to destroying nations belonging to the "Zionist-Anglo-Saxon-Protestant coalition," which they blame for "a litany of social and political" evils in the Islamic world.[208] Such terrorist organizations would continue to attack the same targets regardless of whether the international community adopted the "protective principle" to prosecute cyberterrorism. If the subjective territoriality principle no longer governed, terrorists would therefore be precluded from launching their attacks with impunity from lenient jurisdictions while still targeting the same nations.

The protective principle also addresses the practical challenge of deciphering the precise intent of a cyberterrorist. Since cyberterrorism may impact multiple nations, principles such as the "targeting based" doctrine suffer from the impracticability of determining which nation was the intended object of an attack. The protective principle of jurisdiction eliminates this evidentiary problem. As the Eleventh Circuit reasoned in *United States v. Marino-Garcia*, the protective principle confers prescriptive jurisdiction on a nation even if there is

206. Eileen Sullivan, *New Intelligence Report Looks at Terrorism Threats Over the Next Five Years*, U.S. NEWS (Dec. 26, 2008), http://www.usnews.com/news/national/articles/2008/12/26/new-intelligence-report-looks-at-terrorism-threats-over-the-next-five-years.

207. *See* Krizek, *supra* note 28, at 345.

208. *See* CHRISTOPHER M. BLANCHARD, CONG. RESEARCH SERV., RL32759, AL QAEDA: STATEMENTS AND EVOLVING IDEOLOGY 5 (2007); s*ee also Al-Qaeda: Declarations & Acts of War*, THE HERITAGE FOUND., http://www.heritage.org/research/projects/enemy-detention/al-qaeda-declarations (last visited Jan. 12, 2014).

no "proof of an . . . intended effect."[209] Rather, the doctrine's focus is on whether the nation suffered a potentially dire threat to its fundamental security interests.[210] In altering this emphasis, the protective principle accords with our traditional sense of justice. Given the volatile and unpredictable nature of cyberweaponry, it is possible that even if a terrorist targeted one nation, another state may be the one to suffer a severe affront to its security interests. Although such consequences may be inadvertent, the second nation should still be entitled to assert jurisdiction over the perpetrator.

Applying the protective principle to prosecute cyberterrorists for their unintentional consequences would not bring up due process and "fairness" concerns that are typically raised when a defendant is prosecuted for unintentional acts. For many crimes, it would be unjust for a nation to prosecute a criminal when he did not act with "some degree of intent to cause an impact in the forum."[211] However, cyberterrorists are acutely aware of the volatility and unreliability of cyberweapons. Given the interconnectivity of the Internet and computer networks, a computer virus or worm can easily propagate from one computer system to another. Since cyberterrorists are knowledgeable about these weapons' unpredictable nature, they should be held responsible when they inadvertently cause a third-party nation to suffer a catastrophic security threat.

Finally, compared to doctrines such as passive personality, the protective principle would be less likely to provoke international tension. Many consider jurisdiction predicated on passive personality to be especially intrusive of other nations' sovereignty because it is designed to protect citizens who traveled abroad and purposely availed themselves of foreign nations' benefits and protections. Nations have a legitimate interest in safeguarding their citizens abroad. However, the justification for interfering in another state's sovereign domain is stronger if the crime in question directly endangers the asserting nation's vital security interests.[212]

2. Judicial Basis for Extending the Protective Principle to Cyberterrorism

Judicial precedents provide strong support for extending the protective principle to prosecute cyberterrorists. *U.S. v. Yousef* is one of the seminal cases involving terrorism in which a U.S. court upheld prescriptive jurisdiction based

209. United States v. Marino-Garcia, 679 F.2d 1373, 1381 n.14 (11th Cir. 1982).

210. United States v. Pizzarusso, 388 F.2d 8, 10-11 (2d Cir. 1968), *cert. denied,* 392 U.S. 936 (1968); *see also* Marino-Garcia, 679 F.2d at 1381 n.14; United States v. James-Robinson, 515 F. Supp. 1340, 1344 (S.D. Fla. 1981). Although these court decisions and most legal scholarship have not articulated an "intent" requirement for asserting jurisdiction based on the protective principle, some uncertainty remains.

211. Lea Brilmayer & Charles Norchi, *Federal Extraterritoriality and Fifth Amendment Due Process*, 105 HARV. L. REV. 1217, 1261 (1992).

212. *See* Robbins, *supra* note 158, at 1227.

on the protective principle. In *Yousef,* the two defendants were convicted of conspiring to bomb American commercial airplanes in Southeast Asia.[213] Although the defendants' plans for the attack occurred wholly outside of the United States, the Second Circuit upheld jurisdiction based on the protective principle because the attacks threatened U.S. security and "governmental functions" and were designed to "alter its foreign policy."[214]

More recently, in *United States v. Reumayr*, the United States District Court of New Mexico upheld extraterritorial jurisdiction based on the protective principle over Canadian defendants who conspired to detonate the Trans-Alaska Oil Pipeline. The defendants had planned the attack exclusively in Canada. In holding that extraterritorial jurisdiction was proper, the court reasoned that an "attempt to destroy a domestic energy facility, with the purpose of disrupting oil supply and as a corollary U.S. financial markets, is a crime that implicates a security interest of the United States and is thus cognizable within the protective principle of international jurisdiction."[215]

According to the outcomes in *Yousef* and *Reumayr*, a cyberterrorist attack would fall under the purview of protective jurisdiction. Acts of cyberterrorism, like conventional terrorism, are designed to intimidate a nation's civilian population. In the words of the *Yousef* court, the perpetrators seek to "alter [a nation's] foreign policy." These precedents establish that attacks against a nation's critical infrastructure or transportation systems constitute a sufficiently grave threat to the continual functioning of a nation's government to warrant protective jurisdiction.

The *Reumayr* decision is particularly relevant to assertions of protective jurisdiction over cyberterrorists because of the defendant's target in that case. The defendant challenged U.S. jurisdiction based on the protective principle because he had planned to detonate the Trans-Alaska Oil Pipeline, which is "privately owned property."[216] According to the defendant, attacks against private property could not implicate U.S. security interests or threaten the country's essential governmental functions. The court unequivocally rejected this contention. It reasoned that damaging any domestic energy facility, regardless of whether it was publicly or privately owned, endangered the nation's energy supplies and financial markets. Since cyberterrorists would likely attack America's critical infrastructure, the majority of which is privately owned, the *Reumayr* holding directly substantiates extending the protective principle to such conduct.

213. United States v. Yousef, 327 F.3d 56 (2d Cir. 2003), *cert. denied*, 540 U.S. 933 (U.S. 2003).

214. *Id.* at 96-97.

215. United States v. Reumayr, 530 F. Supp. 2d 1210, 1222 (D.N.M. 2008).

216. *Id.* at 1216.

It is noteworthy that, in addition to terrorism cases, U.S. courts have applied the protective doctrine to cases involving drug trafficking,[217] falsification of visa papers,[218] perjury before consular officials,[219] and immigration.[220] U.S. courts even upheld protective jurisdiction over crewmembers of foreign vessels transporting narcotics on the high seas when they were intercepted hundreds of miles away from the U.S. coast. For example, in *U.S. v. Peterson,* the Ninth Circuit held that "[d]rug trafficking presents the sort of threat to our nation's ability to function that merits application of the protective principle of jurisdiction."[221] Similarly, in one of the most famous cases involving immigration and the protection principle, *United States v. Pizzarusso,* the Second Circuit found: "The utterance by an alien of a 'false statement with respect to a material fact' in a visa application constitutes an affront to the very sovereignty of the United States. These false statements must be said to have a deleterious influence on valid governmental interests."[222]

Although such cases do not address terrorism, they provide strong justification for extending the protective principle to cover cyberterrorist offenses. If mere perjury in an immigration proceeding is sufficiently dangerous to warrant protective jurisdiction, then an attack that incapacitates the nation's power grid, leaving millions of Americans in the dark for weeks, should also warrant jurisdiction under this doctrine. Similarly, courts would be hard-pressed to argue that a vessel transporting a small shipment of narcotics hundreds of miles away from the U.S. shore constitutes a graver threat to U.S. security than a cyberterrorist attack that disrupts the nation's banking and financial systems.

3. Preempting Potential Counterarguments

Legal scholars might raise a number of concerns about extending the protective principle to cyberterrorism. However, careful scrutiny reveals that many of these concerns do not undermine the case for applying the protective doctrine to cyberterrorist attacks.

First is the potential counterargument that, according to the protective principle, the conduct in question must not only endanger the nation's security interests but also be "recognized as a crime under the law of states that have rea-

---

217. United States v. Peterson, 812 F.2d 486 (9th Cir. 1987); *see also* United States v. Normandin, 378 F. Supp. 2d 4, 7 (D.P.R. 2005) (holding that applying the Maritime Drug Law Enforcement Act ("MDLEA") extraterritorially to Canadian defendants caught transporting 750 kilograms of cocaine in international waters accorded with the protective principle of jurisdiction under international law).

218. United States v. Pizzarusso, 388 F.2d 8, 9-10 (2d Cir. 1968), *cert. denied,* 392 U.S. 936 (1968).

219. RESTATEMENT (THIRD), *supra* note 62, § 402.

220. Rocha v. United States, 288 F.2d 545, 549 (9th Cir. 1961) *cert. denied*, 366 U.S. 948 (1961).

221. *Peterson*, 812 F.2d at 494.

222. *Pizzarusso*, 388 F.2d at 9-10.

sonably developed legal systems."[223] The requirement of "general state practice" is articulated in both the Restatement (Third) and in other authoritative international legal sources.[224] Therefore, a counterargument could be that since many nations with "reasonably developed" legal systems lack legislation criminalizing cyberterrorism, the protective principle is inapposite in this context.

However, recent developments have rendered this argument invalid. Although some states have failed to criminalize such acts, there has been an emerging international recognition that cyberattacks such as cyberterrorism pose dire risks to nations' security interests. This consensus is reflected in the growing number of nations that have criminalized such acts. A survey of the legal codes of fifty countries conducted in 1999 demonstrated that approximately seventy percent of the countries had enacted, or were planning to enact, legislation that prohibited a wide variety of cyber offenses.[225] Similarly, forty-five states are currently signatories of the Council of Europe's Draft Convention on Cybercrime. This Convention mandates signatory states to enact statutes criminalizing a list of cyber offenses, which includes unauthorized access to computer systems, damage to functioning computer systems, and interception of non-public transmissions of electronic data.[226] Given that cyberterrorism would entail at least one of these offenses, the Draft Convention prohibits cyberterrorist attacks.[227] Since a large percentage of nations that lack cybercrime legislation are currently in the process of enacting such statutes, the requirement of "general state practice" no longer precludes extending the protective doctrine to cyberterrorism.[228]

Second, some scholars might invoke two judicial precedents in order to dispute the possibility of extending the protective principle to cyberterrorism. For example, they might counter that the International Court of Justice's ("ICJ") *Barcelona Traction* decision precludes invoking the protective principle to conduct that generates mere economic damage. In *Barcelona Traction*, the ICJ rebuffed Belgium's assertion of jurisdiction based on the protective doctrine over a foreign company that was primarily owned by Belgian shareholders. Belgium contended that the illegal use of the corporation's assets, owned by Belgian nationals, injured its economy.[229] Although the ICJ conced-

223. *Id*. at 10.

224. CAMERON, *supra* note 192, at 330; RESTATEMENT (THIRD) *supra* note 62, § 402.

225. Mark D. Goodman & Susan W. Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace*, 10 INT'L J.L. & INFO. TECH. 139, 202–05 (2002).

226. Council of Europe, *Convention on Cybercrime*, § 2 E.T.S. (2001) 185 [hereinafter *Convention on Cybercrime*].

227. Aviv Cohen, *Cyberterrorism: Are We Legally Ready?*, 9 J. INT'L BUS. & L. 1, 33 (2010).

228. Although there is indication of general state practice, the current absence of *opinio juris* undermines the case for extending universal jurisdiction to cyberterrorism under customary international law. *See supra* Part IV.D.

229. Barcelona Traction, Light and Power Co., Ltd. (Belg. v. Spain), 1970 I.C.J. 3, 46 (Feb. 5, 1964).

ed that individual Belgians suffered severe financial losses, the court argued that the protective principle could not be used to transform one state into the insurer of the wealth of another.[230] As a consequence, some scholars have erroneously inferred that nations may not invoke the protective principle to assert extraterritorial jurisdiction over conduct that causes mere economic harm. However, according to international legal scholars such as Michael Barton Akehurst and J.H.W. Verzijl, the protective principle would be appropriate if such conduct "threaten[ed] the whole economic structure of the State."[231] A cyberterrorist attack against a nation's banking and financial systems would therefore justify jurisdiction predicated on the protective doctrine.

Similarly, scholars might invoke the holding in *U.S. v. Yunis* as evidence that the protective principle should not be extended to terrorism generally or cyberterrorism specifically. In *Yunis,* the U.S. government asserted jurisdiction over a terrorist that had hijacked a commercial airliner.[232] Although the court rejected application of the protective principle, the facts of that case differed tremendously from that of a likely cyberterrorist attack. In *Yunis*, the defendant hijacked a Jordanian airliner in the Middle East, therefore posing no direct threat to U.S. national security. The hijackers did not threaten or attempt to coerce the U.S. government. Furthermore, the evidence indicated that the hijackers were unaware that three American nationals would be on board. Such circumstances vary significantly from a cyberterrorist attack that would directly target critical infrastructure on U.S. soil. Such an attack would fulfill the requirements for invoking the protective principle. In the words of the court's decision in *Yunis*, such an attack would pose "a direct, specific threat to national security."[233] Therefore, these counterarguments do not undermine the case for extending the protective principle to cyberterrorism.

4. The Major Limitations of the Protective Principle in the Cyberterrorism Context

Although the protective principle is far superior for prosecuting cyberterrorists to the other traditional principles of jurisdiction, it is not a panacea. The foremost limitation of applying the protective principle to cyberterrorism is the potential for nations to abuse the principle for nefarious purposes. The determination of what constitutes a threat to a nation's security is inherently subjective. As one prominent legal scholar contends, the "lack of external objective criteria leads to an infinitely expansive jurisdictional base covering virtually any con-

230. *Id*. at 46 ¶ 87; *see also* Marcuss & Richard *supra* note 23, at 446.

231. Michael Akehurst, *Jurisdiction in International Law*, 46 BRIT. Y. B. INT'L L. 145, 207 (1973).

232. United States v. Yunis, 681 F. Supp. 896, 903 (D.D.C. 1988*) aff'd*, 924 F.2d 1086 (D.C. Cir. 1991).

233. *Id*. at 903 n.14.

duct whatsoever."[234] Historically, there have been multiple instances where nations exploited the protective principle to enforce their ideological objectives. For example, a German court asserted extraterritorial jurisdiction based on this doctrine over a Jewish foreigner who engaged in sexual intercourse in Czechoslovakia with a German woman. The court reasoned that the man's conduct endangered the "racial purity of the German nation."[235] Similarly, many nations' statutes based on the protective principle are extremely vague and thus subject to broad interpretations. For example, at one time, the Hungarian Penal Code criminalized conduct against "a fundamental interest relating to the democratic, political, and economic order of the Hungarian People's Republic."[236] Such sweeping language is open to widespread politicization and abuse.

In order to limit the potential for abuse, the international community must establish safeguards for applying this principle to cyberterrorism. First, nations should promulgate a definition of what constitutes cyberterrorism and devise a list of what types of cyberattacks would warrant jurisdiction under the protective principle. Realistically, if such a list were formulated, it would only serve as guidance. Given the international community's failure to achieve a consensus on the definition of terrorism, attempts to achieve universal agreement on a cyberterrorism definition may prove similarly futile. Nevertheless, a concerted international effort to define and limit the types of cyberterrorist attacks covered under the protective principle would increase predictability, mitigate future accusations of abuse, and reduce the potential for conflict among states.

An additional limitation is that in some cyberterrorist attacks, the protective principle may not completely eliminate positive jurisdictional conflicts. Although, compared to the territoriality principles, the protective doctrine would significantly reduce conflicting jurisdictional claims, there is a potential for more than one country to suffer significant threats to their security. For example, although it may be challenging to accomplish, a cyberterrorist could successfully attack two countries' power grids simultaneously. The international community must therefore establish a methodology for assigning jurisdiction when multiple nations assert jurisdiction over a cyberterrorist based on the protective principle.

IV. SEQUENTIAL PROSECUTIONS: THE SUPERIOR APPROACH FOR ESTABLISHING JURISDICTION WHEN MULTIPLE NATIONS ASSERT JURISDICTION PREDICATED ON THE PROTECTIVE PRINCIPLE

In the case where more than one nation suffers dire threats to their security interests, the international community should authorize those countries to con-

234. *See* Anthony J. Colangelo, *The New Universal Jurisdiction: In Absentia Signaling over Clearly Defined Crimes*, 36 GEO. J. INTL L. 537, 540 n.15 (2005).

235. *See* Akehurst, *supra* note 231, at 158.

236. *Id*.

duct sequential prosecutions. The principle of *ne bis in idem*, which is conceptually synonymous with "double jeopardy," precludes prosecuting an individual more than once for the same crime. The majority of nations have codified the principle of *ne bis in idem* in their constitutions or statutes.[237] However, as the district court holding in *United States v. Benitez* and other judicial decisions indicate, there is no *jus cogens* rule of international law that requires nations to adhere to *ne bis in idem* at the interstate level.[238] International treaties that guarantee *ne bis in idem*, such as the International Covenant on Civil and Political Rights ("ICCPR"), only bar sequential prosecutions by the same government. For example, Article 14.7 of the ICCPR describes the *ne bis in idem* principle as: "No one shall be liable to be tried or punished again for an offence for which he has already been finally convicted or acquitted in accordance with the law and penal procedures of *each* country."[239] According to judicial interpretations, the word usage of "each country" elucidates that the *ne bis in idem* requirement only governs internal proceedings within a state.[240] Similarly, the *travaux préparatoires* of UN conventions on terrorism, including that of the International Convention for the Suppression of Unlawful Seizure of Aircraft, indicate that the treaties' negotiators "considered and rejected the possibility of expressly barring sequential prosecutions through a *ne bis in idem* provision."[241] The Third Restatement also does not espouse a doctrine of international *ne bis in idem*. According to Section 483, nations are not required to enforce the penal judgments of other states, unless required to do so by treaty. Section 483 elaborates that this is "a principle that has long been accepted both in international and in United States practice."[242] Nations' general opposition to an "international" *ne bis in idem* principle stems from their concern that such a doctrine would undermine national sovereignty.[243]

Even nations that support the concept of international *ne bis in idem* have generally recognized a "national security" exception. For example, the 1987 Convention on Double Jeopardy, an initiative of the European Political Coop-

---

237. *See* Reynaud N. Daniels, Non Bis in Idem *and the Roman Statute of the International Criminal Court*, BEPRESS LEGAL SERIES 2 (May 11, 2006), http://law.bepress.com/cgi/viewcontent.cgi?article=6282&context=expresso.

238. *See* United States v. Duarte-Acero, 208 F.3d 1282, 1282 (11th Cir. 2000); United States v. Benitez, 28 F. Supp. 2d 1361, 1363-64 (S.D. Fla. 1998); Gerard Conway, Ne Bis in Idem *in International Law*, 3 INT'L CRIM. L. REV. 217, 217-218 (2003); John A.E. Vervaele, *The Transnational* Ne Bis in Idem *Principle in the EU: Mutual Recognition and Equivalent Protection of Human Rights*, 1 UTRECHT L. REV. 100, 102 (2005).

239. International Covenant on Civil and Political Rights art. 14.7 (Mar. 23, 1976) (emphasis added), *available at* http://www.ohrcr.org/en/professionalinterest/pages/ccpr.aspx.

240. *See* Benitez, 28 F. Supp. 2d at 1363-64.

241. UNITED NATIONS OFFICE ON DRUGS AND CRIME, DIGEST OF TERRORIST CASES 16 (2010), *available at* https://www.unodc.org/documents/terrorism/09-86635_Ebook_English.pdf (citing Int'l Civil Aviation Org., Legal Comm., 17th Sess., Doc. 8877-LC/161, at 8 (1970)).

242. RESTATEMENT (THIRD), *supra* note 62, § 483 cmt. a.

243. Conway, *supra* note 238, at 218.

eration ("EPC") to promote *ne bis in idem* between states in the European Community, included an exception for "acts to which the foreign judgment relates constitute an offence against national security or other equally essential interests of the Contracting Party."[244] Similar exceptions can be found in the Convention Implementing the Schengen Agreement ("CISA").[245] When ratifying both of these conventions, the majority of nations submitted reservations for crimes that constitute an offense against national security.[246] Such exceptions led a German legislator to declare that the requirements in the Conventions minimally encroached on nations' sovereignty.[247] Since even nations that support "international" *ne bis in idem* recognize a national security exception, they would probably support a policy of authorizing multiple states that suffered critical security threats from cyberterrorism to prosecute the perpetrators.

Sequential prosecutions of cyberterrorists would help achieve the dual objectives of reducing international tension and ensuring that cyberterrorists do not escape with impunity. Under a strict international *ne bis in idem* approach, the determination of which nation would receive jurisdiction over a cyberterrorist would be both arbitrary and capricious. Even if two states suffered dire threats to their security, jurisdictional preference would be afforded to those nations on a "first come first served" basis.[248] Such an approach would severely strain diplomatic relations between the nations that seek jurisdiction and would be wholly inequitable. Rather, it accords with our sense of justice to enable any state that experienced a catastrophic cyberterrorist attack that threatened its security to prosecute the perpetrator.

In addition to minimizing diplomatic tension among states, this approach would help deter future acts of cyberterrorism. An effective deterrence posture must consist of increasing a cyberterrorist's perceived costs of executing such an attack. Deterrence of cyberterrorism is more challenging to achieve than almost any other crime, including conventional terrorism. This is because cyber-

---

244. Convention Implementing the Schengen Agreement of 14 June 1985 Between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic, on the Gradual Abolition of Checks at the Common Borders, Art. 55 (1)(b), June 14, 1985, 30 I.L.M. 68, 73 [hereinafter Schengen Convention], *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922%2802%29:en:HTML; *see also* Convention between the Member States of the European Communities on Double Jeopardy of May 25, 1987, Art. 2(1)(b), *available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52003IG0426(01):EN:HTML*; Vervaele, *supra* note 238, at 108.

245. Lars Hein, *The National State Security Exception Clause of Article 55 of the Schengen II Convention and Article 2 of the EC Convention on Double Jeopardy*, *in* NATIONAL SECURITY AND INTERNATIONAL CRIMINAL JUSTICE 209, 212 (Herwig Roggemann & Petar Šarčević, eds., 2002).

246. *Id*. at 212.

247. *Id*.

248. COMM'N EUROPEAN COMMUNITIES, ANNEX TO THE GREEN PAPER ON CONFLICTS OF JURISDICTION AND THE PRINCIPLE OF *NE BIS IN IDEM* IN CRIMINAL PROCEEDINGS 5 (2005), *available at* http://www.statewatch.org/news/2006/jan/com-696-crim-juris-annex.pdf.

terrorists can execute their attacks remotely and anonymously by routing through proxy servers. Since nations will frequently fail to verify the origin of the attack, cyberterrorists may believe that they have a high chance of escaping prosecution. By increasing the legal risks associated with getting caught, a policy of consecutive prosecutions would thus serve as a much-needed deterrent.

This Article concedes that the prospect of subjecting a cyberterrorist to sequential prosecutions by multiple governments is troublesome from the perspective of the individual rights of the accused. At the domestic level, the protection against double jeopardy provides defendants with "legal certainty" by preserving the integrity and finality of judicial judgments.[249] Subsequent prosecutions could impose burdensome attorney costs on the defendant as well as the "psychological burdens associated with the extended procedures."[250] However, certain policies could ameliorate these worrisome results. For example, nations could adopt a policy of "mandatory consideration of the former sanction," which would reduce the defendant's second sentence.[251] Both the Convention on Double Jeopardy and the Schengen Agreement require this policy when nations invoke a "national security" exception to *ne bis in idem*.[252]

Furthermore, under this Article's proposed jurisdictional framework, cyberterrorists would experience these additional legal burdens infrequently. In many cyberterrorist attacks, although many nations would be impacted by an attack, only one nation would suffer a threat to its vital security interests and thus have a legitimate claim to jurisdiction based on the protective principle. Therefore, there would often be no need for additional judicial proceedings. If the international community instead authorized all nations *affected* by a cyberterrorist attack to conduct consecutive prosecutions, the defendant would be subject to infinite litigation and punishment. Countless nations would be authorized to conduct consecutive prosecutions based on the effects-based, objective territoriality, or subjective territoriality principles. This Article's proposed requirement to first assert protective jurisdiction over the defendant therefore limits the potential for abuse.

V. SEQUENTIAL PROSECUTIONS ARE PREFERABLE TO OTHER POLICIES FOR BREAKING THE JURISDICTIONAL TIE

Legal scholars might propose a number of alternative policies to break the jurisdictional tie between two states that assert jurisdiction based on the protective principle. However, close examination of these alternatives demonstrates

249. Bas Van Bockel, *Two Perspectives on the Realization of the European* Ne Bis In Idem *Principle*, EUROPEAN UNIV. INST. 2 (May 2012), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2071312.

250. *Id*.

251. Hein, *supra* note 245, at 212.

252. *Id*.

that they would produce inferior outcomes compared to a policy of consecutive prosecutions.

The first alternative consists of applying a balancing test. In essence, such a test would seek to determine which nation's security was more threatened by a cyberterrorist attack and therefore which nation has a stronger interest in prosecuting the alleged perpetrator.[253] The Restatement (Third) promulgates a similar balancing approach in § 403. According to § 403, even if a nation seeks to prosecute a criminal in accordance with one of the five accepted bases of prescriptive jurisdiction, jurisdiction should be prohibited if it would be "unreasonable." The Restatement states that in evaluating "reasonableness," courts should balance such factors as the relationship between the forum state and the perpetrator or crime; the nature of the crime and the extent to which the prescribing nation has an interest in jurisdiction; the extent to which another state has an interest in jurisdiction; whether extraterritorial jurisdiction complies with international customs and law; and the potential for conflict with another nation's laws.[254] The Reporter's Note to § 403 elaborates further on the "reasonableness" requirement by noting that extraterritorial application of criminal statutes, as compared to civil statutes, may "be perceived as particularly intrusive" to foreign nations' sovereignty. Therefore, "criminal jurisdiction over activity with substantial foreign elements should be exercised more sparingly than civil jurisdiction over the same activity, and only upon strong justification."[255]

However, applying a balancing approach like the one articulated in the Restatement would fail to resolve jurisdictional conflicts. Scholars and courts have disparaged the Restatement's "reasonableness" test for being subjective and aspirational, rather than practical.[256] Instead of articulating guidelines for weighing competing factors, the Restatement merely stipulates: "Not all considerations have the same importance in all situations; the weight to be given to any particular factor or group of factors depends on the circumstances."[257] Given such ambiguity, a state that asserts jurisdiction over a cyberterrorist based on the protective principle would have broad discretion to interpret the test in its favor. This would pose severe consequences for both diplomatic relations and international law. Judicial decisions that elevate parochial interests while purporting to follow international law undermine international comity and encourage other nations to act in kind.[258] As the renowned jurist Arthur

253. *See Report of the Task Force on Extraterritorial Jurisdiction*, *supra* note 94, at 24.

254. RESTATEMENT (THIRD), *supra* note 62, § 403.

255. *Id*. § 403 reporters' n.8.

256. Hannah L. Buxbaum, *Territory, Territoriality, and the Resolution of Jurisdictional Conflict*, 57 AM. J. COMP. L. 631, 649 (2009).

257. RESTATEMENT (THIRD), *supra* note 62, §483 cmt. b. *See also* Arthur Nussbaum, *Rise and Decline of the Law-of-Nations Doctrine in the Conflict of Laws*, 42 COLUM. L. REV. 189, 200 (1942).

258. Harold G. Maier, *Interest Balancing and Extraterritorial Jurisdiction*, 31 AM. J. COMP. L. 579, 594-95 (1983).

Nussbaum once argued, "Nothing is more inconsistent with harmonious international cooperation than insistence upon national viewpoints under the pretense of their being international."[259] Rather than resolving jurisdictional conflicts, the reasonableness approach would therefore produce inconsistencies and exacerbate interstate tension.

Furthermore, the judiciary is institutionally incompetent to determine whether another nation's interest in prosecuting a cyberterrorist exceeds its own country's interest. Judges would have to delve into complex questions concerning foreign affairs, which are beyond the purview of the judicial branch. Given that such a balancing test requires extensive national security and foreign policy expertise, many U.S. courts have resisted applying the Restatement's multilateral balancing inquiry altogether. They have instead focused on whether prescribing their own nation's laws would be considered reasonable.[260] By instead implementing a policy of sequential prosecutions, judges would not have to make such challenging and highly subjective determinations.

A second alternative for resolving multiple jurisdictional claims based on the protective principle would be to encourage affected nations to consult each other to determine the most appropriate forum. Treaties such as the Financing Terrorism Convention and Council of Europe Convention on Cybercrime promulgate this approach.[261] For example, Article 22(5) of the European Convention on Cybercrime states, "When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution."[262]

Given that such treaties' "consultation" clauses are often toothless, this approach would probably fail to resolve jurisdictional conflicts. For example, the European Convention on Cybercrime's "Explanatory Report" explains:

> [T]he obligation to consult is not absolute, but is to take place "where appropriate." Thus, for example, if one of the Parties knows that consultation is not necessary (e.g., it has received confirmation that the other Party is not plan-

259. *Id*.

260. *See, e.g*., Laker Airways, Ltd. v. Sabena, 731 F.2d 909, 945-52 (D.C. Cir. 1984); In re Uranium Antitrust Litig., 480 F. Supp. 1138, 1148 (N.D. Ill. 1979); RESTATEMENT (THIRD), *supra* note 62, §403 reporters' n.6. Other courts have remanded to lower courts for the purpose of preparing records that would provide stronger substantiation for making "reasoned decision[s] on these highly complex issues." Mannington Mills, Inc. v. Congoleum Corp., 595 F.2d 1287, 1298 (3d Cir. 1979); *see also* Timberlane Lumber Co. v. Bank of America, 549 F.2d 597, 614 (9th Cir. 1976).

261. *See* International Convention for the Suppression of the Financing of Terrorism art. 7, S. Treaty Doc. 106-49 (opened for signature Dec. 9, 1999); Convention on Cybercrime, *supra* note 226, art. 22(5).

262. *See* Convention on Cybercrime, *supra* note 226, art. 22(5).

> ning to take action), or if a Party is of the view that consultation may impair its investigation or proceeding, it may delay or decline consultation.[263]

In the absence of a mandate to coordinate, nations vying for jurisdiction based on the protective principle would often refuse to compromise. They would likely invoke the Convention's "escape clause" and contend that consultation would impede their capacity to effectively and expeditiously prosecute the accused.[264] Moreover, even if nations demonstrated willingness to consult with each other, these Conventions typically fail to explicate criteria for prioritizing jurisdictional claims.[265] It is therefore expected that nations would often fail to achieve consensus on the appropriate jurisdictional forum. A policy of sequential prosecutions, in contrast, would eliminate the immense challenge of compelling a nation that experienced a catastrophic attack to voluntarily relinquish its claim to jurisdiction.

Another alternative would be to authorize each country that had a legitimate claim based on the protective principle to conduct parallel proceedings until the indictment stage. According to the Commission of the European Communities' Green Paper on Conflicts of Jurisdiction, discovery of additional facts during an investigation could alter nations' evaluation of the most suitable forum.[266] This could especially occur during a cyberterrorist investigation given that cyberterrorists can exploit proxy servers to implicate an innocent state or non-state party. By postponing determination of the appropriate forum until the indictment stage, nations would have more time to investigate the attack and prevent situations in which unfolding developments "jeopardize a prior decision on the choice of jurisdiction."[267] However, parallel proceedings would probably also fail to resolve jurisdictional conflicts over cyberterrorism. Investigations of cyberterrorist attacks would entail significant costs and would potentially take many years. If multiple nations that suffered damaging cyberterrorist attacks led independent investigations, they would become heavily invested in the case and less inclined to cede jurisdiction.

A fourth alternative for breaking the jurisdictional tie would be to confer jurisdiction on the nation that succeeded in acquiring possession of the defendant. However, such a "first come, first serve" policy would incentivize nations to gain custody over the alleged perpetrator as quickly as possible through controversial methods such as abduction or "extraordinary rendition." The formal legal method for gaining custody over a criminal located in another nation is

---

263. Council of Europe, Explanatory Report to the Convention on Cybercrime, § 3 ¶ 239 Nov. 8, 2001, E.T.S. 185.

264. *See* ANDREW T. GUZMAN, HOW INTERNATIONAL LAW WORKS: A RATIONAL CHOICE THEORY 152-153 (2008); Laurence R. Helfer, *Flexibility in International Agreements*, *in* INTERDISCIPLINARY PERSPECTIVES ON INTERNATIONAL LAW AND INTERNATIONAL RELATIONS 175, 186 (Jeffrey Dunoff & Mark A. Pollack, eds., 2013).

265. *See, e.g.*, Convention on Cybercrime, *supra* note 226, art. 22(5).

266. COMM'N EUROPEAN COMMUNITIES, *supra* note 247, at 7.

267. Colin Warbrick & Kate Brookson-Morris, *Conflicts of Criminal Jurisdiction*, 56 INT'L & COMP. L.Q. 659, 664 (2007).

extradition. However, the extradition process is extremely time-consuming. For example, in the United States, a request for extradition requires extensive evidentiary documents, the issuance of a warrant, and independent authorization by the State and Justice Departments.[268] Once U.S. authorities provide authorization, the request must travel through diplomatic channels in the other country, which poses additional bureaucratic hurdles.

If conferral of jurisdiction were predicated on which country first obtained possession of the defendant, nations would be more inclined to employ quicker methods such as "extraordinary rendition" or luring in order to capture the defendant first. "Extraordinary rendition" involves "kidnapping" a suspect without the permission of the host state.[269] "Luring," which is frequently used by U.S. prosecutors, consists of ruses designed to entice the defendant to travel to another country, from which he is then extradited to the forum nation.[270] According to U.S. precedent, the fact that the United States circumvents lawful extradition channels and abducts or lures a defendant "constitutes no jurisdictional impediment to trial or punishment."[271] For example, in the famous case of *United States v. Yunis*, the FBI and CIA lured the terrorist Fawaz Yunis into international waters close to Cyprus by pretending that he would profit from a drug transaction there. In spite of the luring operation, the D.C. Circuit rejected Yunis' jurisdictional challenge.[272]

As the European Court of Human Rights held in its recent decision of *El-Masri v. The Former Yugoslav Republic of Macedonia,* compelling or abducting a person from his home state violates fundamental principles of sovereignty and international law.[273] Many states consider other nations' use of extraordinary rendition or luring of their nationals to constitute a severe affront to their sovereignty.[274] By instead authorizing multiple states that experienced threats

268. ERIC ROSENBACH & AKI J. PERITZ, TRIALS BY FIRE: COUNTERTERRORISM AND THE LAW 60 (2010).

269. Michael John Garcia & Charles Doyle, *Extradition To and From the United States: Overview of the Law and Recent Treaties*, CONG. RES. SERV. 33 (Mar. 2010), http://www.fas.org/sgp/crs/misc/98-958.pdf.

270. *Id*.

271. *Id*.; *see also* United States v. Alvarez-Machain, 504 U.S. 655 (1992); United States v. Mejia, 448 F.3d 436, 442-43 (D.C. Cir. 2006); United States v. Torres Gonzalez, 240 F.3d 14, 16 (1st Cir. 2001).

272. United States v. Yunis, 859 F. 2d 953, 955 (D.C. Cir. 1988).

273. *See* Kirsty Sutherland, *ECtHR Rules Unanimously that CIA Implicated in Macedonia-Afghanistan Rendition of German National*, INT'L CRIMINAL LAW BUREAU (Dec. 14, 2012), http://www.internationallawbureau.com/index.php/macedonia.

274. For example, in one recent operation, the United States enticed Vladimir Zdorovenin, a Russian national accused of financial cybercrimes against U.S. citizens, to Switzerland. From there, he was extradited to the United States. This operation further strained U.S.-Russian relations, with the Russian Minister of Justice declaring, "Such practices are absolutely unacceptable to us . . . . [P]eople should not be abducted on the territory of third states, they should not be extradited illegally. Legal instruments and mechanisms should be used." Alexander Utkin, *Russia Proposes Bilateral Extradition Treaty with U.S.*, RIA NOVOSTI (Feb. 10, 2012, 6:42 AM), http://en.rian.ru/russia/20120210/171243300.html.

to their vital security to prosecute the perpetrator, nations' motivations to circumvent international law would be reduced. Such a policy would therefore avoid causing interstate conflict.

Of course, if tactics such as extraordinary rendition are to be avoided, the United States and the rest of the international community will have to strengthen their extradition relationships and harmonize domestic criminal statutes pertaining to cyberterrorism.[275] These critical reforms would enable nations that asserted jurisdiction over cyberterrorists based on the protective principle to gain custody over the accused, as well as facilitate consecutive prosecutions by multiple impacted nations.

CONCLUSION

Senior U.S. policymakers highlight cyberterrorism as a major national security threat. The emerging threat to U.S. critical infrastructure is especially significant because the U.S. economy and national security are so utterly dependent on this infrastructure and because adversaries are increasingly able to assemble thousands of computers around the globe to launch their attacks. Building an effective system to prosecute cyberterrorists would be a vital contribution to the broader U.S. effort to secure infrastructure from attack. Yet, policymakers and scholars have made minimal progress in establishing the legal framework necessary to prosecute cyberterrorists who strike from abroad.

The most immediate and effective legal approach to prosecute such attackers would be to add extraterritorial reach to domestic criminal statutes pertaining to cyberterrorism.[276] This would empower nations that suffered threats from such an attack to apply their laws to cyberterrorists acting in other countries. However, as this Article has shown, it is critical that such efforts be accompanied by an international consensus regarding which basis of prescriptive jurisdiction should govern such prosecutions and a prioritization scheme for reconciling competing jurisdictional claims. Since the protective principle of jurisdiction would abate jurisdictional conflicts, help authorities foil imminent attacks, and ensure that cyberterrorists are vigorously and efficiently prosecuted, this principle should be designated as the dominant basis for asserting jurisdiction over cyberterrorists. If multiple nations suffer debilitating security threats and seek to prosecute the accused under the protective principle, sequential prosecutions should be conducted. Sequential prosecutions would provide a strongly needed deterrent to cyberterrorism by warning potential offenders that they could be subject to multiple judicial proceedings.

---

275. Hathaway, *supra* note 14, at 878. Harmonizing domestic criminal statutes bearing on cyberterrorism is essential because most extradition treaties require "dual criminality," meaning that a nation would only agree to extradite the accused to the requesting nation if the crime for which he was charged constituted a crime in both nations. *See also* Doyle, *supra* note 268, at 9-10.

276. *See* Hathaway, *supra* note 14.

The United States is indeed in a pre-9/11 moment where cyberterrorism is concerned. Time is of the essence for the United States and the international community to agree on how best to apply traditional jurisdictional frameworks so that cyberterrorists can be prosecuted. Determining the proper jurisdictional basis now would help alleviate choice of law uncertainty and interstate conflict in the immediate aftermath of a cyberterrorist attack when international cooperation would be of utmost importance. Most importantly, this prosecutorial framework would help enable the international community to deter and foil attacks, as well as ensure that cyberterrorists hiding abroad are brought to justice.