Chicago Journal of International Law

Volume 7 | Number 2 Article 18

1-1-2007

Blackbeards of the Twenty-First Century: Holding Cybercriminals Liable under the Alien Tort Statute

Jennifer J. Rho

Blackbeards of the Twenty-First Century: Holding Cybercriminals Liable under the Alien Tort Statute

Jennifer J. Rho *

In 1997, an enemy state disrupted computer operations at key US military installations, including the Pentagon, the Joint Staff, and the Central Intelligence Agency ("CIA").[1] The attack caused large-scale blackouts and shut down emergency phone service in Washington, D.C. and other major cities.[2] Or at least it did hypothetically. The damage occurred in Eligible Receiver 97, "the first large-scale, no-warning military field exercise crafted to test the ability of the US to respond to an attack on both [US] military and civilian information infrastructure."[3] Conducted by the Joint Chiefs of Staff, Eligible Receiver 97 "inflict[ed] considerable simulated damage" and spotlighted US vulnerability to a new threat: cybercrime."[4]

Cybercrime is a worldwide phenomenon that involves computer-related attacks and computer network attacks in cyberspace—the "territory" commonly perceived as the Internet—and is unbound by geographical and physical constraints. Satellite phones and battery power make physical requirements, such as a telephone landline and electricity, superfluous. By the same token, the cybercriminal can target anyone in the world.

The scope and magnitude of cybercrime's consequences have garnered international attention. Foreign countries and multilateral organizations have

---

* BA 2004, University of California at Berkeley; JD Candidate 2007, The University of Chicago. I would like to thank Nicholas Degani, Eric Mack, Junlin Ho, Jared Marx, and Samuel Arieti for their invaluable advice and comments, as well as CJIL for its editing assistance. Special thanks to my family for their love and support.

1 Colin Robinson, *Military and Cyber-Defense: Reactions to the Threat* (Ctr for Def Info 2002), available online at <http://www.cdi.org/terrorism/cyberdefense-pr.cfm> (visited Jan 15, 2007).

2 Thomas C. Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace* 22 (Aegis Research Corp 2000).

3 Robinson, *Military and Cyber-Defense* (cited in note 1).

4 Id.

taken steps to identify and outlaw certain acts of cybercrime.[5] But the US may have taken it one step further. In *Sosa v Alvarez-Machain*,[6] the US Supreme Court recast the federal judiciary as the world's sheriff—at least for established violations of international law. It held that the Alien Tort Statute ("ATS") incorporates customary international norms into federal law.[7] It also held that citizenship, of either plaintiff or defendant, is irrelevant. Federal courts can hear all claims of international law violations regardless of where they arose. The US has already outlawed cybercrime domestically.[8] If cybercrime can be identified as a customary international norm, federal courts will have jurisdiction over all private cybercrime suits brought by plaintiffs of every country against defendants of every country.

This Comment explores whether cybercrime constitutes a violation of the law of nations under the ATS. It argues that certain acts of cybercrime may be actionable, but cybercrime as a whole has not yet reached the level of a customary international norm. Part I presents *Sosa*'s approach for recognizing a customary international norm as a private right of action under the ATS. Part II discusses the rising significance of cybercrime and international efforts to thwart it. Part III analogizes cybercrime to one of *Sosa*'s paradigm offenses against the law of nations—piracy—and argues that cyberspace should be viewed as the modern "high seas." This analogy demonstrates why cybercrime is suitable for international recognition, but it also indicates where cybercrime law lacks the requisite specificity. Finally, part IV concludes by presenting other methods of prohibiting violations of international law under federal domestic law and foreshadowing the future international status of cybercrime.

I. THE *SOSA* FRAMEWORK

The Alien Tort Statute ("ATS") states that "district courts shall have original jurisdiction of any civil action by an alien for a tort only, committed in violation of the law of nations or a treaty of the United States."[9] While the ATS had been dormant since its adoption in the Judiciary Act of 1789, it was recently

---

5 See, for example, Council of Europe, Convention on Cybercrime (2001), arts 2–13, ETS No 185, available online at <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm> (visited Jan 15, 2007).

6 542 US 692 (2004).

7 Id at 724–25; see Alien Tort Statute, 28 USC § 1350 (2000).

8 See, for example, Computer Abuse Amendments Act of 1994, 18 USC § 1030 (2000) (covering use of computers for fraud or extortion as well as unauthorized access to information protected for reasons of national defense or foreign relations, financial information, or a computer designated for exclusive government use).

9 28 USC § 1350 (2000).

invoked to combat violations of customary international norms.[10] In *Sosa v Alvarez-Machain*, the Supreme Court provided a framework for identifying actionable claims under the ATS.[11]

Sosa arose when a group of Mexican nationals abducted Humberto Alvarez-Machain ("Alvarez") from his home in Mexico and took him to the US, where he was arrested for the torture and murder of a US Drug Enforcement Agency agent.[12] Alvarez, also a Mexican national, sued his abductors in US federal court.[13] However, his suit failed. The Supreme Court held that actionable claims under the ATS were limited to a "narrow class of international norms."[14] These had to be "defined with a specificity comparable to the features of the 18th-century paradigms" of infringements of ambassadors' rights, violations of safe conduct, and piracy.[15]

The Supreme Court further held that the ATS preserves some of the inherent lawmaking authority possessed by federal courts in 1789, before the Court rejected the idea of federal common law.[16] The Court reached this conclusion by interpreting the statute with reference to the intent of the enacting Congress.[17] However, defining the lawmaking authority with respect to the eighteenth century did not confine that power to eighteenth century norms. The Court explained that federal courts could use their lawmaking powers to recognize causes of action arising under the law of nations as it exists today.[18]

---

10 Not one case during the nineteenth century invoked the ATS. See Genc Trnavci, *The Meaning and Scope of the Law of Nations in the Context of the Alien Tort Claims Act and International Law*, 26 U Pa J Intl Econ L 193, 196 (2005). Most cases brought under the ATS have occurred during the last forty years and have largely targeted international violations of human rights. See id at 196–97; see also *Filartiga v Pena-Irala*, 630 F2d 876, 880 (2d Cir 1980) (holding that the ATS allows foreign nationals to sue in federal courts based on "an act of torture committed by a state official against one held in detention" because it "violates established norms of the international law of human rights, and hence the law of nations."). Many commentators view this trend as very beneficial for international human rights law. See Harold Hongju Koh, *Transnational Public Law Litigation*, 100 Yale L J 2347 (1991); Anne-Marie Burley, *The Alien Tort Statute and the Judiciary Act of 1789: A Badge of Honor*, 83 Am J Intl L 461 (1989).

11 542 US 692.

12 Id at 697–98.

13 Id at 698.

14 Id at 729.

15 Id at 725.

16 See *Erie* RR *Co v Tompkins*, 304 US 64, 78 (1938).

17 See *Sosa*, 542 US at 720–25.

18 Id at 724–25.

A. REINVIGORATING FEDERAL COMMON LAW: THE ATS IS NOT JUST JURISDICTIONAL

In *Sosa*, the Supreme Court first asked whether federal courts could make common law, or whether they were restricted to those causes of action explicitly defined by the political branches of government. It found that congressional intent and historical evidence made the former a better position.[19] The ATS had been passed not as a "jurisdictional convenience to be placed on the shelf for use by a future Congress,"[20] but to allow US courts to recognize international substantive law. *Erie* did not require a different answer; it only indicated a need for caution.[21] Professor Jessup provides one possible reason for *Erie's* inapplicability: *Erie* simply did not terminate lawmaking authority with respect to international law.[22] International law and domestic law are distinct because US foreign relations can be brought within federal power.[23] Alternatively, *Erie* may not apply because lawmaking with respect to customary international law involves recognizing existing law, not creating new law.

The Court then chose not to limit its reinvigorated lawmaking authority to the few causes of action existing under the law of nations of 1789. It predicated this holding on the negative finding that no development over the last two centuries required otherwise.[24] There are additional reasons for reaching this conclusion. First, Professor Jessup's theory did not base the lawmaking authority on its origin in the eighteenth century. If the lawmaking authority is not defined with respect to the eighteenth century, then it would be unnecessary to confine the recognizable causes of action to that time period. Second, there is a congressional intent argument. It is plausible that the enacting Congress that did not want a "jurisdictional convenience" would also intend for the "law of nations" to be interpreted dynamically so the statute would remain consequential. This finds support in the legislative history of the Torture Victim Protection Act, which indicates Congress's belief that the ATS applies modern customary international law.[25]

---

19 Id at 714.

20 Id at 719.

21 Id at 726, 729.

22 Philip C. Jessup, *The Doctrine of* Erie Railroad v Tompkins *Applied to International Law*, 33 Am J Intl L 740, 743 (1939).

23 See id.

24 *Sosa*, 542 US at 724–25.

25 See Julian Ku and John Yoo, *Beyond Formalism in Foreign Affairs*, 2004 Sup Ct Rev 153, 161 (2004).

B. WHICH CAUSES OF ACTION WILL BE RECOGNIZED?

Nevertheless, any exercise of the court's lawmaking power should be restrained. The ATS recognizes only a "narrow class of international norms:"[26] those "defined with a specificity comparable to the features of the 18th century paradigms" of infringements of ambassadors' rights, violations of safe conduct, and piracy.[27] The use of the term "tort" demonstrates an interaction between domestic private law and the law of nations; the paradigms each constituted conduct producing both a "judicial remedy" and a threat of "serious consequences in international affairs."[28] For example, "[a]n assault against an ambassador . . . impinged upon the sovereignty of the foreign nation and if not adequately addressed could rise to an issue of war."[29] These international ramifications justified the exercise of jurisdiction by any nation. But the act of assault remained a standard tort actionable under the domestic common law of the ambassador's host country.

Sosa identified a three-factor test for establishing an international norm. First, the cause of action cannot have "less definite content and acceptance among civilized nations than the historical paradigms familiar when [the ATS] was enacted."[30] The claim in *Sosa* did not satisfy this test. That norm was "a general prohibition of 'arbitrary' detention defined as officially sanctioned action exceeding positive authorization to detain under the domestic law of some government, regardless of the circumstances."[31] The Court found it unlikely that nations would permit "an action in [US] federal court for arrests by state officers who simply exceed their authority; and for the violation of any limit that the law of any country might place on the authority of its own officers to arrest."[32]

Second, universal jurisdiction must exist over the cause of action. There must be international acceptance on "the substantive principle that [the conduct in question] [was] universally wrong" and "the jurisdictional principle that any nation that found [the perpetrator] could prosecute him."[33] Consensus on the latter requires a potential systemic effect "in international affairs."[34] In his *Sosa*

---

26 *Sosa*, 542 US at 729.

27 Id at 725.

28 Id at 715.

29 Id.

30 Id at 732.

31 Id at 736.

32 Id at 737.

33 Id at 762 (Breyer, J concurring).

34 Id at 715.

concurrence, Justice Breyer rationalized this requirement on the grounds of international comity. He argued that "ask[ing] whether the exercise of jurisdiction under the ATS is consistent with . . . notions of comity . . . help[s] ensure that 'the potentially conflicting laws of different nations [will] work together in harmony'"[35]

Third, a court must consider the "practical consequences of making [a] cause of action available to litigants in federal court."[36] The content of this prong is unclear, but it appears to require exhaustion of domestic legal remedies and "a policy of case-specific deference to the political branches."[37] Arguably, this is where the arbitrary detention norm failed in *Sosa*. The Court emphasized the norm's potential consequences by declaring the norm overbroad. It reached any unauthorized arrest in the world. Federal judicial resources would be overwhelmed if all of these actions could be litigated in US courts.[38] Further, diplomatic and institutional concerns would arise if US judges were required to evaluate the domestic criminal laws of other sovereign countries.

II. CYBERCRIME

The "Information Revolution" of the last two decades has witnessed the diffusion of computers and cyberspace into every aspect of society. Computers control telecommunications, electrical power systems, gas and oil storage, transportation, banking and finance, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government.[39] The Internet's information infrastructure is used to conduct business, transmit messages, and process information.

The term "cyberspace" refers to the environment that has been created by the interaction of networks of computers, information systems, and the Internet. Network effects have made the cyberspace more valuable with each additional computer or infrastructure that is connected.

However, the benefits of cyberspace are precisely what make it dangerous. Network effects enable the "dedicated and persistent threat . . . [of] access to almost any Internet-linked information infrastructure of any state in the world."[40] In the US, this has both civilian and military implications, because

---

35 Id at 761 (Breyer concurring) (quoting *F Hoffman-La Roche Ltd v Empagran SA*, 542 US 155, 164 (2004)).

36 Id at 732–33.

37 Id at 732, 733 n 21.

38 Id at 737.

39 Wingfield, *The Law of Information Conflict* at 25 (cited in note 2).

40 Id at 21–22.

"most military systems obtain and process information from civilian systems over which [the US] Department of Defense ("DoD") has a lesser—or no—degree of control."[41] Further, the absence of physical constraints makes "[i]nformation-age threats . . . more diffuse, dispersed, multidimensional nonlinear, and ambiguous than industrial-age threats."[42] Such threats could include corporate or government espionage, manipulation of data and the decisionmakers who use it, physical damage, and general chaos. [43] Alternatively, sabotage of an emergency services computer network could exponentially increase the collateral damage from a conventional attack.[44]

This type of attack has been given many names, including cyberterrorism, cyber attack, computer network attack (as opposed to computer network espionage and computer network exploitation), computer-related attack, cyberwar, net war, cybercrime, information operations, and information warfare. The seemingly incoherent terminology becomes sensible if computer attacks are organized in two dimensions: by perpetrator and by nature of conduct.

The first dimension turns on whether the perpetrator of the computer attack is a state or private entity, which in turn identifies which law to apply. When the perpetrator is a state or state-related entity, computer attacks are governed by public international law.[45] As a result, the public international legal regime would likely defer if a state claimed that it was acting in self-defense. This legitimizes all of a state's computer attacks. Specifically, it would authorize a state's "information operations," or "those activities that governments and military forces undertake to control and exploit the information environment via the use of the information component of national power."[46] Information operations include activity such as information warfare,[47] computer espionage,[48]

---

41 Arthur K. Cebrowski, *CNE and CNA in the Network-Centric Battlespace*, in Michael N. Schmitt and Brian T. O'Donnell, eds, *Computer Network Attack and International Law* 1, 4 (Naval War College 2002).

42 John Arquilla and David Ronfeldt, *The Advent of Netwar (Revisited)*, in John Arquilla and David Ronfeldt, eds, *Networks and Netwars: The Future of Terror, Crime, and Militancy* 1, 2 (RAND 2001).

43 Wingfield, *The Law of Information Conflict* at 22 (cited in note 2).

44 Fred Cohen, *Cyber-Risks and Critical Infrastructures*, in Alan O'Day, *Cyberterrorism* 1, 4 (Ashgate 2004).

45 Since *Sosa* deals with private causes of action, I will not discuss computer attacks committed by state entities and governed by public international law. I provide only an overview of the applicable legal regime.

46 Daniel T. Kuehl, *Information Operations, Information Warfare, and Computer Network Attack*, in Schmitt and O'Donnell, eds, *Computer Network Attack and International Law* 35, 37 (cited in note 41). According to definitions published by the DoD, information operations are "[a]ctions taken to affect adversary information and information systems while defending one's own information and information systems." Id at 36.

47 The DoD defines information warfare as "[i]information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or

and computer network attacks.[49] But a computer attack committed by a private entity would not be considered an information operation. It would instead be classified as an act of "cybercrime" and governed by the domestic law of the relevant state.

The second dimension distinguishes between two types of cybercrime: computer-related offenses and computer network attacks. Computer-related offenses include crimes where a computer is used to commit a crime outlawed under traditional criminal law. In the US, relevant statutes prohibit use of computers to steal, defraud, and destroy.[50] In contrast, computer network attacks are an entirely new species of crime. They identify cyberspace as the target of the offense.[51] The computer is the end, not the means, of the attack.

The difference between computer-related offenses and computer network attacks is one of degree, not kind. Offenses such as computer fraud or forgery are facilitated by a computer network, but that computer network is by no means critical to their commission. In contrast, the absence of a network would eliminate the computer network attack. There would be nothing to target. The importance of the computer and computer network directly correlates with the practical difficulties of committing the attack absent the computer. The spectrum thus depends on the significance of the computer or computer

---

adversaries." Id. The characterization of information warfare as information operations is the primary reason for characterizing information operations as exclusively state activity. Information warfare has a dual offensive-defensive nature that would be unlawful in the private arena.

48 Espionage is generally treated as lawful under public international law and unlawful under domestic law. See John Norton Moore, Robert F. Turner, and Frederick S. Tipson, eds, *National Security Law* 433 (Carolina Academic 1990) (explaining that espionage is viewed as part of a state's inherent right to self-defense); 18 USC § 794 (2000) (criminalizing espionage under the federal law). Since computer espionage refers to traditional espionage conducted in cyberspace, its legality should be no different.

49 See discussion of cybercrime (in following paragraphs) for a definition of computer network attack.

50 See 18 USC § 1030 (2000) (covering use of computers for fraud or extortion as well as unauthorized access to information protected for reasons of national defense or foreign relations, financial information, or a computer designated for exclusive government use). See also Abraham D. Sofaer and Seymour E. Goodman, *Cyber-Crime and Security: The Transnational Dimension*, in Abraham D. Sofaer and Seymour E. Goodman, eds, *The Transnational Dimension of Cyber Crime and Terrorism* 1, 25 (Hoover Inst 2001) (discussing § 1030); Eric J. Sinrod and William P. Reilly, *Cyber-crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 Santa Clara Computer & High Tech L J 177, 180–81 (2000) (discussing § 1030).

51 The US has also focused on criminalizing computer network attacks. Its initial attempt in dealing with use of the Internet for unlawful conduct (such as in situations where the computer is the target) is detailed in the report of a Presidential working group published in 2000. See President's Working Group on Unlawful Conduct on the Internet, *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet: A Report of the President's Working Group on Unlawful Conduct on the Internet* (Mar 2000), available online at <http://www.usdoj.gov/criminal/cybercrime/unlawful.htm> (visited Jan 15, 2007).

network. Computer-related attacks where the computer is easily replaced lie at one extreme; computer network attacks that would not occur absent a computer network lie at the other; and crimes where the computer substantially facilitates the crime lie in between.

III. APPLYING THE FRAMEWORK: PIRACY'S LESSONS FOR CYBERCRIME

Of the examples provided by the *Sosa* Court, piracy provides a remarkably good analogy to cybercrime. First, the offenses of piracy and cybercrime are both defined in relation to the location of the prohibited conduct.[52] The label "piracy" refers specifically to conduct on the high seas; "cybercrime" refers specifically to conduct in cyberspace.[53] Once the location requirement is met, the unlawful conduct could constitute any of a broad array of acts, from robbery to mutiny to traditional fraud to a computer network attack. The breadth of the piracy definition is demonstrated by Blackstone's inclusion of the term "depredation" in his definition of piracy as "those acts of robbery and depredation upon the high seas, which, if committed upon land, would have amounted to felony."[54] Similarly, cybercrime includes all acts committed by a private entity via computer, computer network, or the Internet, which otherwise done would amount to a felony.

Second, the close fit of the analogy is emphasized by the disparity between piracy and *Sosa*'s two other paradigm examples: offenses against ambassadors and violations of safe conduct. The latter two are defined with respect to the victim. They include all acts "[purposefully] committed by private nationals of the forum country against specially protected classes of foreigners."[55] In contrast, piracy is unlawful whether it targets an ambassador or a random merchant ship. The legality of an act of cybercrime also does not vary with the target; it is the act itself that is unlawful.

---

52 One article also analogizes piracy to cybercrime on the grounds that both involve situations where the citizens of state A engage in crimes of property, with economic motive, against citizens of other states "outside the territorial boundaries of any nation and therefore outside the scope of any laws." Marc D. Goodman and Susan W. Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace*, 2002 UCLA J L & Tech 3, 74–76 (2002).

53 The term "cyberspace" will be defined in Section III.A.1 below.

54 William Blackstone, 4 *Commentaries* 72.

55 Eugene Kontorovich, *Implementing* Sosa v. Alvarez-Machain: *What Piracy Reveals about the Limits of the Alien Tort Statute*, 80 Notre Dame L Rev 111, 155–56 (2004). The ambassador is given diplomatic immunity, a legal status granted by the host government; a person given safe conduct is given a governmental guarantee of passage through that territory.

A. PRONG ONE: DEFINED WITH SUFFICIENT SPECIFICITY?

The ATS requires a cause of action to be defined with specificity under the law of nations.[56] The plaintiff must identify the "civilized nations," or the group of nations that agreed on a definition, and prove that its definition is as specific as that of a historical paradigm, such as piracy.[57] In *Sosa*, the Court cited *United States v Smith*,[58] an 1820 Supreme Court case that affirmed a death sentence for piracy as defined under the law of nations, to demonstrate piracy's "definite content and acceptance among civilized nations."[59] The *Smith* court upheld the conviction on the grounds that the law of nations defined piracy with "reasonable certainty."[60] This was based on the general international consensus that piracy was "robbery, or forcible depredations upon the sea," though there was divergence on other elements of the offense.[61]

But the definition did not really have "definite content and acceptance among civilized nations." *Smith* explicitly noted the existence of "diversity of definitions" when it found convergence on only two elements: "robbery" and "upon the sea."[62] Blackstone's examples of piracy also demonstrate that piracy is not as simple as it seems. He placed a lot of content in the term "depredation." That term could embrace mutiny, trading or consorting with pirates, outfitting a pirate ship, or destroying the cargo of a forcibly-boarded merchant ship (without seizing it first).[63]

Twenty-four years later, Justice Story, the same Justice who wrote in *Smith*, confirmed that the all-inclusive term of "depredation" was an integral part of the piracy offense. He argued:

> A pirate is deemed, and properly deemed, *hostis humani generis*. But why is he so deemed? Because he commits hostilities upon the subjects and property of any or all nations, without any regard to right or duty, or any pretence of public authority. If he willfully sinks or destroys an innocent merchant ship, without any other object than to gratify his lawless appetite for mischief, it is just as much a piratical aggression, in the sense of the law of nations, and of the act of Congress, as if he did it solely and exclusively for the sake of plunder, *lucri causa*[.] The law looks to it as an act of hostility, and being

---

56 *Sosa*, 542 US at 724–25.

57 Id at 732.

58 18 US 153 (1820).

59 *Sosa*, 542 US at 732.

60 *Smith*, 18 US at 160.

61 Id at 161.

62 *Smith*, 18 US at 161–62.

63 Blackstone at 72 (cited in note 54).

> committed by a vessel not commissioned and engaged in lawful warfare, it treats as the act of a pirate[.][64]

This statement added several elements to what seemed a very simple offense. "Depredation" included the commission of hostilities or any action done with mischievous intent, without regard to duty or pretense of public authority, or while not commissioned and engaged in lawful warfare. Any offensive act could presumably be considered a "depredation." As a result, countries agreeing that piracy was bad in general could presumably disagree on the specific acts that constituted piracy by placing that disagreement within the confines of the "depredation" term. This could result in substantial inconsistency from country to country, depending on how the term "depredation" was read.

Nevertheless, the piracy definition is very precise. The key to its specificity is the location component. All unlawful conduct committed on the high seas constitutes piracy, but an act cannot be one of piracy unless it occurs on the high seas. Piracy is limited by its locale. Facially, this is promising for cybercrime, which is also restricted by location. However, two issues prevent cybercrime's definition from being equally simple. The first is the ambiguity of the term "cyberspace." The second is the international community's desire not to condemn cybercrime as a whole.

1. Is "Cyberspace" Sufficiently Definite?

Both piracy and cybercrime appear specific because they are location-based. An act is one of piracy if it occurs on the high seas; an act is one of cybercrime if it occurs in cyberspace. However, a definition that turns on the location of conduct loses specificity if the location itself cannot be defined with specificity.

Piracy, although it encompasses a wide range of activity, is limited because it is defined with respect to a term with concrete meaning. The "high seas" are defined as the physical bodies of water on Earth large enough to support multiple sailing ships. This is a clear definition accepted worldwide. Any confusion about the definition could be easily eliminated by photographs or a visit to such a body of water.

Cybercrime is defined as all unlawful activity committed by a private individual in cyberspace. But "cyberspace" is a term subject to debate. There are two interpretations of "environment:" the technical perspective and the community perspective. The technical perspective views "cyberspace" and the Internet as synonymous. Technically, cyberspace is thus "a global electronic network of computer networks (including the World Wide Web) that connects

---

64 *United States v Brig Malek Adhel*, 43 US 210, 232 (1844).

people and information."[65] From this perspective, cyberspace is easily visualized as the collection of physical equipment comprising the Internet: computers, wires, processing chips, and other pieces of manufactured technology. The technical definition of cyberspace retains specificity comparable to that of piracy.

The community perspective refers to the community created on and by the Internet. It defines "cyberspace" by virtue of the objects and identities existing within the computer networks themselves. Cyberspace is more than copper wires and computer parts; it is an intangible space or a parallel dimension existing in the conceptual space beyond the computer. It is similar to oxygen, which we cannot see, but we know surrounds us. A paradigmatic example appears in *The Matrix*, a popular science fiction movie that depicted a world where humans were harvested for energy by sentient machine overlords.[66] To keep humans unaware of their true purpose, the machines connected them to "the Matrix." There, these human batteries lived artificial lifetimes; "the Matrix" told their minds they were leading ordinary lives even as their bodies were kept in dark, fluid-filled pods. "The Matrix" is the epitome of a virtual reality, where a person's perceived identity exists entirely in a computer network. But even the Matrix is hard to explain. The community definition of cyberspace is likely to fail the specificity requirement when even its paradigm situation cannot be precisely described.

Failure on this prong may be avoided by assigning different definitions of "cyberspace" to the constituent categories of cybercrime. As explained, there are two types of cybercrime: computer-related offenses and computer network attacks. Computer-related offenses are those offenses where the use of a computer or computer network facilitates the commission of the offense. They are traditional offenses committed through new, technologically advanced means. The computer or network is nothing more than a tool used to commit a crime that could be committed outside of cyberspace. It is thus more appropriate to view cyberspace as a collection of physical equipment. Even in a situation where the cybercriminal is ostensibly taking advantage of the cyberspace community, such as using his online identity to defraud someone, that online identity only replicates existing society. The cybercriminal is not committing a new type of crime.

In contrast, computer network attacks inherently require cyberspace to be more than a collection of wires and chips. The attack targets the data or objects of the cyberspace community. The contents of cyberspace are themselves valuable. But the technical view of cyberspace does not view the information

---

65 President's Working Group on Unlawful Conduct on the Internet (cited in note 51).

66 *The Matrix* (Village Roadshow Pictures Entertainment 1999).

transferred over the Internet as part of the Internet. A technically-defined computer network attack could then only target the wires and chips. The computer network attack is thus inherently predicated on the community definition of cyberspace. A computer network attack then cannot be defined with sufficient specificity to be recognized as a customary international norm.

2. Do the "Civilized Nations" Agree?

Sosa requires the "civilized nations" to agree on the definition of a customary international norm.[67] With regard to piracy, it is relatively easy to identify the "civilized nations." *Sosa* explicitly points to Blackstone's understanding of international law, and Blackstone limited civilization to the countries of West Europe.[68]

Today, however, determining which nations are "civilized" is fraught with pitfalls. The context of cybercrime may provide an easy loophole; it may be impossible for a country to be civilized with respect to cybercrime unless it is computerized. Being civilized would turn on the direct relationship between the degree of computerization of a state's national economy and/or infrastructure and its vulnerability to computer crime. A state would be sufficiently "civilized" if its national government were computerized. However, the nature of cyberspace and portable computers places every "computerized" country in jeopardy of attack from another country that has an international telephone connection or satellite access. Since almost every country now possesses at least one computer, "civilized nations" would essentially include every country in the world.

The alternative is to use multilateral agreements as a proxy. There is a general global effort to criminalize acts of cybercrime. But multilateral efforts in the cybercrime arena undercut an argument that there is a consensus on the exact definition of cybercrime. Multinational organizations target only certain types of conduct for prohibition, such as unauthorized computer access or computer fraud. The Organisation for Economic Co-operation and Development ("OECD"), United Nations, and Council of Europe each maintain lists of particular unlawful acts. By adopting this approach, the international community has demonstrated its intention not to adopt the categorical prohibition seen in piracy.

Identifying cybercrime in a particularized manner, though potentially very specific, has led instead to definitional imprecision. This is evidenced by the Council of Europe's Convention on Cybercrime. The Convention's treaty model

---

67 542 US at 732.

68 Id at 724.

leaves each signatory state with considerable latitude in defining a computer offense and allows them to retain their disparity in definitions. For example, in the European Union, the offense of unauthorized access varies from: (1) protecting "'secure systems' for which some effort has been made to inhibit open access" to (2) requiring damage to the penetrated system to (3) constituting a "progression from a 'basic' hacking offense to more serious forms of conduct implicating 'ulterior' offenses."[69]

The desire to selectively criminalize cybercrime likely stems from a lack of consensus on the normative value of cybercrime. Countries are unwilling to condemn cybercrime as per se wrong. The acts comprising cybercrime range from mere access to deliberate destruction to fraud, and thus vary from completely new crimes to new ways of committing old crimes. States may simply lack the experience to determine how they feel about them, which makes experimentation and the lack of consensus unsurprising. In contrast, the pirate was perceived as "*hostis humani generis*," or an enemy of mankind.[70] All of his or her acts, stretching from robbery to murder, were viewed as normatively bad by the countries. Further, each country had extensive experience with such conduct.

A harm principle, predicated on the identity of the victim, could be used to save certain types of conduct. For example, a computer network attack designed to damage critical government infrastructure might be sufficiently definite and worrisome to be a candidate for general condemnation. In that case, the identity of the victim would inform the level of harm caused, similar to offenses against ambassadors and violations of safe conduct. For example, the Code Red worm, which targeted the US White House website, could constitute an act of cybercrime cognizable under the ATS.[71] Although Code Red was arguably a denial-of-service attack,[72] its harm was augmented because it disrupted technical services at a critical location.

---

69 Tanya L. Putnam and David D. Elliott, *International Responses to Cyber Crime*, in Sofaer and Goodman, eds, *The Transnational Dimension* 35, 46 (cited in note 50).

70 *Brig Malek Adhel*, 43 US at 232. See also Malvina Halberstam, *Terrorism on the High Seas: The Achille Lauro, Piracy and the IMO Convention on Maritime Safety*, 82 Am J Intl L 269, 275 (1988) (noting that, according to nineteenth century international law, "the pirate is a man who satisfies his personal greed or his personal vengeance by robbery or murder in places beyond the jurisdiction of a state.").

71 Eric Chien, *Security Response: CodeRed Worm*, available online at <http://www.symantec.com/avcenter/venc/data/codered.worm.html> (visited Jan 15, 2007) (describing how the Code Red Worm operated).

72 "A 'denial-of-service' attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include: attempts to 'flood' a network, thereby preventing legitimate network traffic; attempts to disrupt connections between two machines, thereby preventing access to a service; attempts to prevent a particular individual

However, the possibility of false positives makes use of the harm principle unsatisfactory. The results of a denial-of-service attack are identical to those in a situation where an innocent user attempts to access the White House website with a defective Internet browser. In the latter situation, the innocent user would also be repeatedly denied in his attempts to gain access. It is thus unclear whether the inherent ambiguities in defining cybercrime could defeat the prerequisite worldwide agreement for original jurisdiction under the ATS.

B. PRONG TWO: UNIVERSAL JURISDICTION?

Sosa requires that a cognizable international norm warrant universal jurisdiction.[73] Universal jurisdiction over piracy, which permits a state to prosecute any pirate it finds, had several justifications. The most common is the argument that the pirate is "*hostis humani generis*," or an enemy of all mankind.[74] Everyone is harmed by the pirate's indiscriminate acts of depredation. "Piratical attacks, particularly when viewed cumulatively, may disrupt commerce and navigation on the high seas. Such lawlessness was especially harmful to the world at a time when intercourse among states occurred primarily by way of the high seas . . . ."[75] Prosecution by any country was also justified by the difficulty in catching pirates. Pirates act "in places where the pirate can easily take advantage of a lack of law and order due to the lack of any valid organizational structure."[76] Jurisdiction was further predicated on the idea that engaging in piracy waives the protection of the flag under which the ship is sailing.[77] Countries did not have to worry about damaging their foreign diplomatic relations.

Professor Kontorovich has identified six key characteristics that justify universal jurisdiction over piracy. Applying these factors to cybercrime will illuminate its candidacy for universal jurisdiction. The six factors are: (1) uniform condemnation; (2) a narrow and universally accepted definition; (3) uniform punishment; (4) the accused's refusal of home state protection; (5) the act's

---

from accessing a service; [and] attempts to disrupt service to a specific system or person." CERT Coordination Center, *Denial of Service Attacks* (June 4, 2001), available online at <http://www.cert.org/tech_tips/denial_of_ service.html> (visited Jan 15, 2007).

73 542 US at 715.

74 *Brig Malek Adhel*, 43 US at 232; Halberstam, 82 Am J Intl L at 275 (cited in note 70).

75 Kenneth C. Randall, *Universal Jurisdiction under International Law*, 66 Tex L Rev 785, 794–95 (1988).

76 Lorelle Londis, *The Corporate Face of the Alien Tort Claims Act: How an Old Statute Mandates a New Understanding of Global Interdependence*, 57 Me L Rev 141, 204 (2005).

77 Kontorovich, 80 Notre Dame L Rev at 148 (cited in note 55).

occurrence in a location where conventional domestic enforcement is difficult; and (6) international harms resulting from indiscriminate attacks.[78]

1. Uniform Condemnation

"[I]nternational law merely reflected an already ubiquitous condemnation of" piracy because it was "a crime in the municipal law of all nations . . . ."[79] Cybercrime has the same characteristic at a broad level. A 1999 study found that "nearly 70 percent of the countries for which data were readily found have promulgated, or are planning to promulgate, laws prohibiting a reasonably comprehensive slate of computer-related crimes."[80] In general, this group included "the most highly industrialized countries" and their trading partners.[81] Thirty-two countries publicly agreed to enact comprehensive cybercrime legislation when they signed the Council of Europe's Convention on Cybercrime.[82] "[C]rimes involving intrusion and damage" have been most frequently targeted, usually with similar language.[83] The level of international dialogue thus demonstrates a general condemnation of cybercrime. Nevertheless, the discussion in section III.A.2 above indicates an inability or unwillingness to adopt any true uniformity in condemning cybercrime.

2. A Narrow and Universally Accepted Definition

This requirement repeats the first prong of the *Sosa* approach. The outcome of my discussion from above was that cybercrime as a whole does not have a sufficiently specific definition. As I explained, however, particular constituent offenses of cybercrime, such as computer-related offenses, might qualify as sufficiently definite.

3. The Same Punishment across Nations

In the eighteenth century, all nations gave pirates the death penalty.[84] This prevented "forum shopping, weakened deterrence, and conflict between states that prescribe different penalties."[85] Today, differing penal systems, sentencing jurisprudences, and quality of prisons make it practically impossible to achieve

---

78 Id at 114–15.

79 Id at 114.

80 Putnam and Elliott, *International Responses* at 37 (cited in note 69).

81 Id at 51.

82 Convention on Cybercrime (cited in note 5).

83 Putnam and Elliott, *International Responses* at 40–41, 46 (cited in note 69).

84 Kontorovich, 80 Notre Dame L Rev at 142 (cited in note 55).

85 Id.

uniform punishment across countries. The death penalty, especially for a crime such as computer fraud, would be unthinkable for those countries that do not condone such a penalty for even murder. Further, monetary fines cannot remedy the problem. Financial standardization of punishment entails analysis of economic utility, cost of living, and other factors, all of which inject discretion into the sentencing process. Use of the harm principle also may not achieve uniformity in punishment. Predicating punishment on harm is a sentencing philosophy that may not be shared by all countries.

Much of the sentencing disparity may derive from non-uniform criminalization of the same acts. This is demonstrated by the different situations of creators of functionally identical computer viruses. David Smith created the Melissa virus, a computer worm that overwrote files on an infected computer, and then spread by infiltrating the Microsoft Outlook address book.[86] Onel de Guzman wrote the I Love You virus, a worm modeled on Melissa.[87] Smith, who lived in New Jersey and did not intend the resulting damage, was sentenced to 20 months in prison, 100 hours of community service, 3 years of supervised release, and a $5000 fine.[88] De Guzman, a resident of the Philippines who intended to cause the resulting damage, got nothing; all charges against him were dropped because the Philippines did not prohibit computer crime.[89]

Still, it is possible that countries cooperating to create common definitions of crimes could also work together to create a uniform sentencing regime—especially once uniform consensus on a narrow, precise definition of cybercrime is achieved.

4. Refusing the Protection of a Home State

A pirate in possession of a letter of marque and reprisal was a state-sponsored pirate—he was a privateer. His piratical activity was legitimized if he limited his targets to those specified by his sponsor country and gave that

---

86 See Raul K. Elnitiarta, *Security Update: W97M.Melissa.A*, available online at <http://securityresponse.symantec.com/avcenter/venc/data/w97m.melissa.a.html> (visited Jan 15, 2007) (providing a technical description of the Melissa virus).

87 See Eric Chien and Brian Ewell, *Security Response: VBS.Love Letter and Variants*, available online at <http://securityresponse.symantec.com/avcenter/venc/data/vbs.loveletter.a.html> (visited Jan 15, 2007) (providing a technical description of the I Love You virus).

88 See David Kocieniewski, *Man Is Charged in the Creation of E-Mail Virus*, NY Times A1 (Apr 3, 1999); Chris Taylor, *How They Caught Him: Tracking the Hacker Who Hatched the Melissa Virus*, Time 66 (Apr 12, 1999); Steven Levy, *Biting Back at the Wily Melissa*, Newsweek 62 (Apr 12, 1999).

89 See Mark Landler, *A Filipino Linked to "Love Bug" Talks About His License to Hack*, NY Times C1 (Oct 21, 2000).

country a share of his revenue.[90] The letter of marque essentially made piratical activity a matter of foreign diplomatic relations. Accordingly, the pirate who did not obtain a letter of marque deliberately forfeited his nationality and the benefits that citizenship entailed. This gave other countries assurance that the pirate's home country would not object to their exercise of jurisdiction.[91]

Arguably, the cybercriminal is the exact opposite of a pirate: the cybercriminal actively seeks the protection of the legal system in which he resides for forum shopping reasons or protection against extradition. De Guzman no doubt strongly proclaimed his Filipino citizenship during his prosecution; that factor kept him in the Philippines and free from jail or fines.

Nevertheless, one type of state label may legitimize otherwise unlawful cybercrime: "information operations," or acts of cybercrime committed by individuals working for the state. The difference in legality turns on the different legal regimes for state and private activity. Just as the letter of marque immunized privateers from piracy prosecution by making it a matter of international relations, working in information operations also removes the cybercrime issue to the state level. Both authorize volunteers to "help" their country by targeting others.

The strength of this analogy may turn on an empirical comparison of the difficulty of obtaining a letter of marque versus the difficulty of obtaining an information operations job. Conceivably, the former is easier than the latter. It was in a state's interest to grant a letter of marque. It allowed states to reduce their vulnerability to pirates while profiting from the privateers' plunder. Further, there were presumably few volunteers. Though it is possible that a state would outfit privateers with ships and crew, it is more likely that a privateer had to provide his own. The combination of these factors made "[o]btaining a writ of marque . . . notoriously easy; one did not have to demonstrate nautical prowess or moral probity."[92]

Working for the government today is hopefully more difficult, though it depends on the government. Information operations is theoretically a matter of national security and should require security clearance for its operatives. Further, there is a much larger pool of potential applicants. Cybercrime does not require a large investment; a person can be a cybercriminal as soon as he or she possesses a computer—which are now relatively cheap. A potential information operative would thus face much lower odds of being hired as an information operative. Additionally, the state has less incentive to control the direction of

---

90 Eugene Kontorovich, *The Piracy Analogy: Modern Universal Jurisdiction's Hollow Foundation*, 45 Harv Intl L J 183, 212–13 (Winter 2004).

91 Kontorovich, 80 Notre Dame L Rev at 148 (cited in note 55).

92 Id.

cybercrime by hiring as many information operatives as possible. A state conducts information operations in order to sustain the integrity of its systems. The benefit is being stronger and more protected than everyone else, not in gaining something tangible.[93] Consequently, the difficulty in obtaining a position in information operations suggests that cybercrime does not have an operative moment, as symbolized by the letter of marque, in which the cybercriminal turns his back on his country's protection.

5. Difficulty of Conventional Domestic Enforcement

Universal jurisdiction over piracy was largely justified because there is "almost no governmental control" or "on the spot" enforcement on the high seas.[94] "[T]he vastness of seas [allowed] pirates [to] easily commit their crimes undetected."[95]

Cyberspace is equally vast, and it is equally difficult to detect an act of cybercrime. First, the cybercriminal effectively operates outside of governmental control. Technically, the cybercriminal is physically located in a sovereign state's territory—but he is not committing his crimes in the physical dimension. Even if a police officer saw the cybercriminal in the process of conducting his attack, they would see only a person sitting in front of his computer, which is perfectly legitimate. Unless the police officer could quickly read and understand computer code, there would be no real way for him, a conventional law enforcement officer, to patrol cybercrime until the damage is already done.

Second, cyberspace is more vast than the high seas. An attack of cybercrime may be committed from any place that provides a telephone connection. Cellular and satellite phones allow cyberspace to encompass the entire globe. No physical limitations constrain the cybercriminal's location; he could be literally anywhere in the world.

Third, cybercrime requires two types of investigation, one of which is new and incredibly complex. To catch a cybercriminal, the cyber attack must first be traced through cyberspace. Once the cyberspace origin has been identified, it must be matched to the actual perpetrator. Neither search will be easy. Electronic investigation is incredibly complicated; it requires a technical aptitude of a completely different kind from that needed in conventional law enforcement. (The ideal degree for the first would be a doctorate from MIT in computer science and electrical engineering, whereas the second would be a

---

93 Offensive information operations of this nature would likely prove to be counter-effective because weakening another state's computer systems would simply provide more locations from which cybercriminals could launch their attacks.

94 Kontorovich, 80 Notre Dame L Rev at 152 (cited in note 55).

95 Id.

doctorate in criminal forensics or psychology.) Conventional investigation is no easier because of the scope of cyberspace; it could require considerable cooperation and procedural uniformity (regarding search, seizure, etc.) between countries, which do not currently exist. These difficulties indicate cybercrime is an equally good candidate for universal jurisdiction on the grounds of insufficiency of conventional domestic law enforcement.

6. Indiscriminate Attacks that Harm the International Community

"Piracy imperiled international commerce and navigation, which many and perhaps all states had an interest in protecting. . . . [M]ost pirates were ready to attack any targets of opportunity."[96] Accordingly, Blackstone predicated the international norm against piracy on self-defense.[97]

Cybercrime also poses a threat to the international community. This is the "Information Age," an era in which everything has become computerized and everyone has become connected. The benefit, and the curse, of the Internet is that it allows a person sitting in Chicago to instantaneously access data stored on servers in Northern Ireland, Japan, or anywhere in the world. Critical infrastructure, such as water, transportation, and the military, are controlled by computers and connected by computer networks. Moreover, cyberspace does not recognize the physical boundaries seen in the real world. Nothing tangible blocks a computer network attack—just lines of code creating firewalls and virus protection programs. This immunity to geography is perhaps best shown by the reach of internet mail servers such as Gmail. Google provides free e-mail accounts—Gmail—to anyone who receives an invitation to join or signs up through their mobile phone.[98] Victimizing all people with a Gmail account could infiltrate computers in every computerized region of Earth. The argument for self-defense is as strong here as it was against a threat to international commerce that attacked one cargo load at a time.

C. PRONG THREE: PRACTICAL CONSEQUENCES?

Sosa requires a practical component in the analysis of a potential ATS-based cause of action. The Court did not want the federal judiciary to adjudicate all of the world's issues. The arbitrary detention norm was too broad if it

---

96 Id at 152–53.

97 Blackstone at 71 (cited in note 54).

98 Google, *About Gmail*, available online at <http://mail.google.com/mail/help/about.html> (visited Jan 15, 2007).

allowed suit for "any arrest, anywhere in the world, unauthorized by the law of the jurisdiction where it took place."[99]

At first glance, a cause of action for cybercrime fails under this prong. The nature of a cybercrime attack, especially a computer network attack, permits one act to victimize hundreds, maybe even millions, of people. Technology allows a cybercriminal to program his attack to continuously replicate itself. The I Love You and Melissa viruses each corrupted hundreds of computers.[100] Allowing these hundreds of affected computer owners to bring suit in US court would overwhelm federal judicial resources. A class action suit might solve this problem, but class action suits are complex and unwieldy. Piracy, in contrast, was inherently limited in scope. It affected international commerce, but a pirate was physically unable to attack more than one ship at a time. This constraint, combined with the amount of time it took to sail to a new target, placed a practical ceiling on the number of pirate victims.

Nevertheless, the range of cybercrime victims is limited by the practical difficulties of enforcement.[101] Provided that courts require specific identification of a cybercriminal, the amount of litigation will be considerably narrowed. However, this concern will lessen as law enforcement personnel gain experience and countries develop better protocol for cooperation.

D. OUTCOME OF APPLYING *SOSA*'S FRAMEWORK

The lessons from piracy are two-fold, and somewhat in opposition. First, the piracy analogy demonstrates the inadequacy of the cybercrime definition. The cybercrime definition lacks the specificity of the piracy definition. While both categorically prohibit all actions that occur in a certain location, the location component of cybercrime is too abstract and ambiguous. Cybercrime is defined as unlawful conduct in cyberspace—but there is no coherent definition of "cyberspace." Further, the categorical format of the definition is improper. Categorical prohibition of piracy was legitimate because all countries outlawed a pirate's specific acts under their domestic laws. In contrast, many instances of cybercrime have never been seen before. Even if they have, normative consensus has not been reached on their value. Thus, cybercrime's definition will not be sufficiently definite until the conception of "cyberspace" is clarified and an understanding reached about cybercrime's normative value.

---

99 *Sosa*, 542 US at 736.

100 See Taylor, *How They Caught Him*, Time at 66 (cited in note 88).

101 See part II.B.5 (discussing difficulty of conventional domestic enforcement of cybercrime prohibitions).

Second, the piracy analogy demonstrates that, once defined, cybercrime is suitable for universal jurisdiction. The international consequences of cybercrime and piracy are very similar. Universal jurisdiction over pirates was predicated on the idea that indiscriminate pirate attacks harm international commerce as a whole. Cybercrime is no less, and is probably much more, destructive to the international community. Cybercrime operates in an environment that knows no true physical boundaries; any such limits would be artificial and could be circumvented by a creative computer program. Further, technology has increased the speed at which people can interact with each other, regardless of the distance separating them. These speeds make more people susceptible to a computer attack in much less time. It also foretells a crushing amount of litigation. Virtually everyone in the world who owns a computer could sue for the same computer virus—in one court. Practically, that is incredibly burdensome for any single judicial system. However, a grant of universal jurisdiction could diffuse the amount of litigation across the "civilized nations" and reduce that load.

IV. CONCLUSION: ALTERNATIVE METHODS FOR US INCORPORATION OF INTERNATIONAL LAW

If not as a customary international norm, federal courts still have ways to reach violations of international law. The *Sosa* court identified these alternatives when demonstrating the limitations of the phrase "law of nations" as the basis of private causes of action under federal law.[102] There are two, one of which also invokes the ATS: (1) treaties signed between the US and another sovereign state and (2) federal statutes enacted by Congress. Both explicitly outlaw a particular offense and presumably grant the prescriptive jurisdiction needed to hear such matters.

The ATS denotes two bases for federal jurisdiction over a tort: the "law of nations" and "a treaty of the United States."[103] The analysis for both bases is substantially the same; both require the relevant law to authorize a private cause of action.[104] The only difference is the relevant law. With respect to a treaty, the court determines whether a private cause of action exists by making three findings.[105] First, the rights in the treaty must have been implemented, either because the treaty was self-executing or through subsequent domestic legislation. Second, the treaty must give rise to an individually-enforceable right that

---

102 *Sosa*, 542 US at 732.

103 28 USC § 1350.

104 See *Jogi v Voges*, 425 F3d 367 (7th Cir 2005).

105 Id.

provides a private, not just public, right of action. Third, the cause of action must provide for damages, not just an equitable remedy.

Normatively, institutional concerns make the ATS's "treaty" branch preferable. It involves judicial recognition of a right selected by the political branches of government, while the "law of nations" branch requires the judiciary to "create" the right themselves. The latter may implicate the political question doctrine and comprise activity prohibited by separation of powers.[106] The treaty basis thus presents a constitutionally safer method of acknowledging international law in the post-*Erie* world.

Alternatively, a federal statute "establishes an unambiguous and modern basis for federal claims."[107] Since Congress unquestionably possesses the authority to prescribe jurisdiction over extraterritorial violations,[108] this method provides the most direct way of incorporating international norms into domestic law. It is also viable, as seen in the case of torture. The Torture Victim Protection Act of 1991 was enacted to make torture and extrajudicial killing a federal cause of action when the torture was committed by those acting under the authority of foreign states.[109] It has been actively used by plaintiffs, many of whom were awarded very large damages.[110]

Although diplomatically controversial because it allows one state to interfere with another's affairs, this provides a method of preserving sovereignty. The Council of Europe chose exactly this path to create an international policing regime for cybercrime. Its Cybercrime Convention asks signatories to enact domestic legislation criminalizing Convention-specified categories of cybercrime.[111] The Convention provides states with latitude to match the particular elements of a cybercrime offense to its domestic perception.

The Cybercrime Convention's approach may be the best path to take. It balances the international need for rules with the disparity in state thinking about cybercrime. The Convention's approach creates a network of domestic prohibitions on cybercrime and allows states to tailor international norms to

---

106 See generally *Sosa*, 542 US at 739–51 (Scalia concurring); *Tel-Oren v Libyan Arab Republic*, 726 F.2d 774, 798–823 (DC Cir 1984) (Bork concurring).

107 *Sosa*, 542 US at 728.

108 See generally *Hartford Fire Insurance Co v California*, 509 US 764 (1993) (holding that federal courts can exercise jurisdiction over foreign anticompetitive conduct); see also *F Hoffman-LaRoche Ltd v Empagran SA*, 542 US 155 (2004).

109 See Torture Victim Protection Act of 1991, Pub L No 102–256, 106 Stat 73 (1992), codified as amended 28 USC § 1350 (2000).

110 See, for example, *Anderson v Islamic Republic of Iran*, 90 F Supp 2d 107, 114 (DDC 2000) (awarding $340 million in compensatory and punitive damages); *Cicippio v Islamic Republic of Iran*, 18 F Supp 2d 62, 69–70 (DDC 1998) (awarding $65 million in compensatory damages).

111 Convention on Cybercrime, arts 2–22 (cited in note 5).

their individual needs. Since cybercrime provides a categorical label for a number of offenses, some of which are less offensive in certain states, an international regime that allows states this flexibility is better than one that compelled all states to enact perfectly consistent prohibitions. Further, once states have developed the relevant domestic laws for cybercrime in its constituent offenses, it will be easier to identify those offenses with sufficient specificity and uniformity to qualify for universal jurisdiction. The international community, in other words, can overcome its confusion about cybercrime as a whole in the course of picking and choosing those parts of cybercrime they consider to be heinous.

The Convention's domestic approach may also alleviate the practical problems caused by the size of the potential victim pool. If each state has slightly different rules regarding cybercrime, there is increased likelihood of forum-shopping. While forum-shopping is usually considered undesirable, in this situation it would be beneficial because it would spread cybercrime prosecution over many countries. This would prevent active cybercrime enforcers, such as the US, from becoming the repository of all cybercrime prosecutions, and the US would not face the prospect of the entire world suing in its courts.