Approaches to Cybercrime Jurisdiction

By Susan W. Brenner[1] & Bert-Jaap Koops[2]

Cite as: 4 J. High Tech. L. 1 (2004)

1. NCR Distinguished Professor of Law & Technology, University of Dayton School of Law.
2. Associate Professor in Law & Technology at Tilburg University, the Netherlands.

 ISSN 1536-7983

CONTENTS

I. INTRODUCTION

A Web site in Germany caters to the adult market, and has done so happily for three years. Then, out of the blue, it finds itself indicted in Singapore because of spreading pornographic material in Singapore, even though the company has never done business with someone from Singapore. To make things worse, the Web site owners are ordered to appear in court in Belgium, because some of the adult pictures are considered to be of 17-year old minors, constituting the crime of child pornography (which, in Belgium, entails persons under 18 years of age; in Germany, the age limit is 14). The business is perfectly legal in Germany, but since it uses the Internet to conduct its business, it finds itself confronted with the criminal laws of all countries connected to the Internet—that is, all countries of the world.

A script kiddie concocts a new worm and, without really thinking of the potential consequences, launches it on the Internet. To his amazement (and somewhat to his fear), he finds that he has blocked large portions of the Internet, causing significant damage in numerous countries around the world. Many countries have laws criminalizing the spreading of worms, and so, in theory, he can be prosecuted by many countries, perhaps consecutively. In practice, however, perhaps no country will claim jurisdiction, thinking that surely other countries will have suffered more damage and hence will have priority in prosecuting.

These examples show that jurisdiction in cybercrimes is a tricky issue. Acts on the Internet that are legal in the state where they are initiated may be illegal in other states, even though the act is not particularly targeted at that single state. Jurisdiction conflicts abound, both negative (no state claims jurisdiction) and positive (several states claim jurisdiction at the same time). Above all, it is unclear just what constitutes jurisdiction: is it the place of the act, the country of residence of the perpetrator, the location of the effect, or the nationality of the owner of the computer that is under attack? Or all of these at once?

It appears that countries think differently on this issue. The cybercrime statutes that have been enacted over the past decades in numerous countries show varying and diverging jurisdiction clauses. In this article, we want to outline these varying approaches in cybercrime jurisdiction, by indicating when states claim jurisdiction and which factors influence that claim. This outline is aimed at answering the questions, what kinds of approaches do states have in claiming jurisdiction over cybercrime, and what are the potential consequences if these approaches significantly diverge globally?

In this article, we focus on jurisdiction in substantive criminal law by analyzing the cybercrime statutes of numerous countries and states. When the cybercrime statute at issue lacks a jurisdiction clause, we focus on the existing principles of jurisdiction in that country, which by implication also apply to the cybercrime laws. We have restricted ourselves mainly to statutory law, since so far there is little case law available on cross-border cybercrime jurisdiction.

It is not our intention to be comprehensive. Rather, we want to raise awareness that cybercrime jurisdiction clauses differ significantly, and, to do so, it is sufficient to analyze a sample of states and countries around the world. In North America, we analyze several U.S. states and the federal U.S. law; in Europe, we study the Netherlands,[3] Belgium,[4] and Germany;[5] in Australasia, we focus on Singapore,[6] Malaysia,[7] and the Australian state of Tasmania.[8] We also include the jurisdiction clause in the Council of Europe's Cybercrime Convention.[9] The selection of these states and countries is rather eclectic: we have simply chosen those states that have interesting jurisdiction clauses with respect to cybercrime. Other countries may have comparable clauses, but the present sample in any case serves the purpose of showing the diversity of approaches in cybercrime jurisdiction.

We start with a general description of jurisdiction (§ 2). Then, we

3. Dutch Computer Crime Act (*Wet computercriminaliteit*) of 1993, *Stb.* 1993, 33, adapting the Dutch Criminal Code (*Wetboek van Strafrecht*), *available in Dutch at* http://www.wetten.nl. A bill is pending to update the Act, Computer Crime Bill II (*Wetsvoorstel computercriminaliteit II*), Parliamentary Series (*Kamerstukken II*) 26 671, *available in Dutch at* http://www.overheid.nl/op/.

4. Belgian Computer-Science Crime Act of 2000 (*Wet van 28 november 2000 inzake informaticacriminaliteit*), *Belgisch Staatsblad* 3 February 2001, p. 2909, adapting the Belgian Criminal Code (*Strafwetboek*), *available in Dutch and French at* http://www.juridat.be/cgi_wet/wetgeving.pl. *See also* The Law Containing the Preceding Title to the Code of Criminal Procedure of 25 April 1878 (*Wet houdende de voorafgaande titel van het Wetboek van Strafvordering*), *available at* http://www.juridat.be/cgi_wet/wetgeving.pl [hereinafter: Belgian PTCCP].

5. The cybercrime provisions are to be found in the German Criminal Code (*Strafgesetzbuch*), *available in German at* http://bundesrecht.juris.de/bundesrecht/stgb/index.html and *available in English at* http://www.asianlaws.org/cyberlaw/library/legislations/cc/germany.htm.

6. Singapore Computer Misuse Act, Act 19 of 1993, 1994Ed. Cap. 50A, as amended in 1998, *available at* http://statutes.agc.gov.sg/.

7. Malaysia Computer Crimes Act 1997, *available at* http://www.ktkm.gov.my/template01.asp?Content_ID=379&Cat_ID=4&CatType_ID=85 (under 'Cyberlaws').

8. Tasmanian Criminal Code Act 1924, in particular Chapter XXVIIIA, *available through* http://www.thelaw.tas.gov.au/.

9. Convention on Cybercrime, Budapest 23 November 2001, ETS 185, *at* http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185.

survey jurisdiction clauses in cybercrime statues that establish jurisdiction, either based on territorial claims, e.g., because the act itself, an affected computer, or an affected person is located in the country (§ 3), based on personality claims (§ 4), or based on other claims, such as the protection principle and universality (§ 5). Jurisdiction does not only require a connection with the crime; it also demands that this connection be sufficiently close to warrant the exercise of jurisdiction—the reasonableness standard (§ 6). Particularly with cybercrimes that are connected with many countries, the various jurisdiction clauses described will clash, resulting in positive jurisdiction conflicts, or even in negative conflicts when no state claims jurisdiction on the presumption that some other state is more closely affected (§ 7). We end with summarizing the various approaches in cybercrime jurisdiction, the problems that this variation poses, and we indicate resulting issues that merit further study (§ 8).

II. JURISDICTION

"Jurisdiction" encompasses several discrete concepts, including jurisdiction to prescribe, jurisdiction to adjudicate, and jurisdiction to enforce.[10] Jurisdiction to prescribe is a sovereign entity's authority "to make its law applicable to the activities, relations, or status of persons, or the interests of persons in things . . . by legislation, by executive act or order, by administrative rule . . . or by determination of a court."[11] Jurisdiction to adjudicate is a sovereign entity's authority "to subject persons or entities to the process of its courts or administrative tribunals" for the purpose of determining whether prescriptive law has been violated.[12] Jurisdiction to enforce is a sovereign entity's authority "to induce or compel compliance or to punish noncompliance with its laws or regulations, whether through the courts or by use of executive, administrative, police, or other

10. *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 401 (1987). The Restatement (Third) of Foreign Relations Law of the United States is a "treatise or commentary" on jurisdictional and other principles of international law and, as such, is "not a *primary* source of authority upon which, standing alone, courts may rely for propositions of customary international law. *See* United States v. Yousef, 327 F.3d 56, 99 (2d Cir. 2003). "Such works at most provide evidence of the practice of States, and then only insofar as they rest on factual and accurate descriptions of the past practices of states, not on projections of future trends or the advocacy of the 'better rule.'" *Id.*

11. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 401(a) (1987).

12. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 401(b) (1987).

nonjudicial action."[13]

Traditionally, all three types of jurisdiction have been based primarily upon the concept of territory. A nation (or a state) had jurisdiction to prescribe what was and was not proper conduct within its physical territory and had jurisdiction to enforce those prescriptions against actors whose unlawful conduct had occurred within its territory. This concept of jurisdiction followed from the basic principle that a sovereign entity had the lawful authority to exert control within "its territory generally to the exclusion of other states, authority to govern in that territory, and authority to apply law there."[14] As the U.S. Supreme Court said in *American Banana Company v. United Fruit Company*, 213 U.S. 347, 356 (1909), "the character of an act as lawful or unlawful must be determined wholly by the law of the country where the act is done." From this, it followed that no nation could apply its criminal laws to conduct occurring within the physical territory of another nation.[15]

The twentieth and twenty-first centuries' increased geographical mobility and use of telecommunications technology undermined certain of the assumptions that gave rise to the traditional model of jurisdiction.[16] It became much easier for someone to commit a criminal act in one country and quickly flee the country, thereby frustrating its ability to apply its criminal laws to the perpetrator; it also became possible for someone in Nation A to commit a criminal act against a victim physically situated within the territory of Nation B without the perpetrator's ever leaving his own country.[17] This latter type of activity created new and unique challenges for criminal jurisdiction, as illustrated by the saga of the "Love Bug" virus.

In May of 2000, the "Love Bug" virus appeared on the Internet and spread around the world in two hours.[18] It is estimated to have

13. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 401(c) (1987).

14. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 206 cmt. b (1987).

15. *See, e.g.*, The Apollon, 22 U.S. (9 Wheat) 362, 371 (1824). *See also* United Nations Convention Against Transnational Organized Crime, Article 4 ("Protection of Sovereignty") (2000), *available at* http://www.uncjin.org/Documents/Conventions/dcatoc/final_documents_2/convention_eng.pdf. *See generally* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 206 cmt. b (1987).

16. *See, e.g.*, Marc D. Goodman & Susan W. Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace*, 2002 U.C.L.A. Journal of Law & Technology 3, 4-24, *available at* http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.php.

17. *See, e.g., id.* at 18-24.

18. *See, e.g., id.* at 4-7.

affected over forty-five million users in over twenty countries, and to have caused between two and ten billion dollars in damage.[19] Virus experts quickly traced the "Love Bug" virus to the Philippines, where agents from the Federal Bureau of Investigation and the Philippines Bureau of Investigation focused on Onel de Guzman, who had been identified as the likely creator of the virus.[20] The agents' investigation was, however, hampered by the fact that virus dissemination was not at the time a criminal offense in the Philippines; because virus dissemination was not an offense, they had difficulty obtaining a warrant to search de Guzman's apartment for evidence pertaining to the creation and dissemination of the virus.[21] And once they obtained and executed the warrant and arrested de Guzman they faced another problem: How could he be prosecuted when virus dissemination was not a crime in the Philippines? Philippine authorities charged him with fraud and credit card theft—on the premise that the virus was meant to harvest user passwords that would be used to obtain Internet service and other things of value—but the charges were dismissed as legally insufficient.[22] Ultimately, it was determined that the Philippines could not prosecute de Guzman, and because he could not be prosecuted there he could not be extradited for prosecution in the United States or in any of the other countries in which the "Love Bug" inflicted damage.[23] Reflecting the concern with national sovereignty noted above, extradition treaties require "double criminality," i.e., require that the conduct at issue have been a crime in both countries for extradition to be permissible.[24] Absent such a requirement, a citizen of Nation A could be prosecuted by Nation B for conduct that occurred entirely within the territory of Nation A, and that was quite legal under the laws of Nation A, but that violated the laws of Nation B. To allow such an eventuality would be to undermine Nation A's sovereign authority—its jurisdiction—over its citizens and others within its borders. In the example of the German adult Web site with which we started, Germany would not extradite the Web site owner to Singapore of Belgium because of its sovereign authority; hence, the Web site's lawfulness is protected by the requirement of double criminality.

The concept of requiring double criminality for extradition and the proposition that nations have sovereign authority over those within

19. *See, e.g., id.*
20. *See, e.g., id.*
21. *See, e.g.*,Goodman & Brenner, *supra* note 16 at 4-7.
22. *See, e.g., id.*
23. *See, e.g., id.*
24. *See, e.g., id.*

their territorial boundaries still retain their validity, but the past few decades have seen an expansion in the premises that can support the exercise of criminal jurisdiction. Jurisdiction is no longer predicated solely upon one's having been physically present within a nation at the time the offense was committed. As one source explains, under the modern conception of jurisdiction, a nation has jurisdiction to prescribe law with regard to any of the following:

(a) conduct that, wholly or in substantial part, takes place within its territory;

(b) the status of persons, or interests in things, present within its territory;

(c) conduct outside its territory that has or is intended to have substantial effect within its territory;

(2) the activities, interests, status, or relations of its nationals outside as well as within its territory; and

(3) certain conduct outside its territory by persons not its nationals that is directed against the security of the state or against a limited class of other state interests.[25]

Even under this expanded view of jurisdiction, however, a nation cannot "exercise jurisdiction to prescribe law with respect to a person or activity having connections with another state when the exercise of such jurisdiction is unreasonable."[26] The test of the validity of a nation's attempt to prescribe law comes, of course, in the courts.[27] Whether the exercise of jurisdiction to prescribe is unreasonable is determined by considering various factors, including the following:

(a) the link of the activity to the territory of the regulating state, i.e., the extent to which the activity takes place within the territory, or

25. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 402 (1987). *See also* Ray August, *International Cyber-jurisdiction: A Comparative Analysis*, 39 AM. BUS. L. J. 531, 534 (2002). Courts have invoked four different bases, or "nexuses," to justify their exercise of jurisdiction in criminal cases: (1) the territorial nexus, i.e., where the offense was committed; (2) the nationality of the person committing the offense; (3) a protective nexus that allows the exercise of jurisdiction when a national interest of the forum state is at stake; and (4) the universality nexus which gives courts jurisdiction over "certain offenses that are recognized by the community of nations as being of universal concern." *Id.* Notwithstanding this expansion of the predicates for exercising jurisdiction, "[t]erritoriality is considered the normal, and nationality an exceptional, basis for the exercise of jurisdiction." RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 402 cmt. b (1987).

26. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 403(1) (1987).

27. *See, e.g.*, August, *supra* note 25, at 533 (2002). "Although prescriptive jurisdiction is exercised by legislatures and executive agencies (through the making of laws, rules, and regulations), it is most commonly challenged and tested in the courts." *Id.*

has substantial, direct, and foreseeable effect upon or in the territory;

(b) the connections, such as nationality, residence, or economic activity, between the regulating state and the person principally responsible for the activity to be regulated, or between that state and those whom the regulation is designed to protect;

(c) the character of the activity to be regulated, the importance of regulation to the regulating state, the extent to which other states regulate such activities, and the degree to which the desirability of such regulation is generally accepted.

(d) the existence of justified expectations that might be protected or hurt by the regulation;

(e) the importance of the regulation to the international political, legal, or economic system;

(f) the extent to which the regulation is consistent with the traditions of the international system;

(g) the extent to which another state may have an interest in regulating the activity; and

(h) the likelihood of conflict with regulation by another state.[28]

Reasonableness is also required for jurisdiction to adjudicate: nations have authority to exercise adjudicative authority through their courts if the relationship between that nation and the person or thing that is the object of the adjudicative effort is "such as to make the exercise of jurisdiction reasonable."[29] Such an exercise of jurisdiction will generally be deemed to be "reasonable" if any of the following exist:

(a) the person or thing is present in the territory of the state, other than transitorily;

(b) the person, if a natural person, is domiciled in the state;

(c) the person, if a natural person, is resident in the state;

(d) the person, if a natural person, is a national of the state;

(e) the person, if a corporation or comparable juridical person, is organized pursuant to the law of the state;

(f) a ship, aircraft or other vehicle to which the adjudication relates is registered under the laws of the state;

(g) the person, whether natural or juridical, has consented to the exercise of jurisdiction;

(h) the person, whether natural or juridical, regularly carries on business in the state;

28. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 403(2) (1987).

29. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 421(1) (1987).

(i) the person, whether natural or juridical, had carried ed on activity in the state, but only in respect of such activity;

(j) the person, whether natural or juridical, had carried on outside the state an activity having a substantial, direct, and foreseeable effect within the state, but only in respect of such activity; or

(k) the thing that is the subject of adjudication is owned, possessed, or used in the

state . . . in respect of a claim reasonably connected with that thing.[30]

Finally, a nation will have jurisdiction to "employ judicial or nonjudicial measures to induce or compel compliance or punish noncompliance with its laws" if "it has jurisdiction to prescribe" under the standard given above.[31]

The sections below examine the difficulties involved in applying these standards, i.e., both the substantive standards and the attendant "reasonableness" standards, to conduct that occurs in or via cyberspace.

III. TERRITORIAL CLAIMS

A. Location of acts

By far the most common factor found in jurisdiction provisions is the location of the act of the crime.[32] The Cybercrime Convention (CCC) uses this as the primary constituting factor of jurisdiction: "Each Party shall . . . establish jurisdiction over any offence established in accordance with Article 2 through 11 of this Convention, when the offence is committed . . . in its territory."[33] Deciding whether or not an offence has been "committed . . . in" a nation's territory is not, however, a simple undertaking when the commission of the offence involved the use of cyberspace. As a recent article explains,

[i]n one recent case, a French court assumed jurisdiction over Yahoo, an American online content provider, and ordered it to remove web pages showing Nazi memorabilia, material that is illegal to view in France but legal almost everywhere else. In another case, a British court held a British subject liable for posting photographs on

30. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 421(2) (1987).

31. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 411(1) (1987).

32. *See id.* at § II.

33. Art. 22(1)(a) Convention on Cybercrime.

an American web server considered obscene in Britain but not in the United States. Still another, an American court held the president of a gambling company organized and headquartered in Antigua liable for soliciting and accepting bets from Americans over the Internet.[34]

National and state statures take various approaches to defining when an offense is committed within a particular sovereignty's territory. In the United States, for example, several states take a very broad approach to this issue. The jurisdictional provision that was included in Arkansas' computer crime legislation, for example, states that "a person is subject to prosecution in this state for any conduct proscribed by this subchapter, if the transmission that constitutes the offense either originates in this state or is received in this state."[35] North Carolina's equivalent provision states that any offense defined by its computer crimes code is "committed by the use of electronic communication may be deemed to have been committed where the electronic communication was originally sent or where it was originally received in this State."[36]

The jurisdictional provision included in Connecticut's computer crimes code declares that if "any act performed in furtherance of the offenses" defined by the code "occurs in this state or if any computer system or part thereof accessed in violation of" the computer crimes code "is located in this state, the offense shall be deemed to have occurred in this state."[37] Other states such as Ohio and Utah rely on statutes defining general criminal jurisdiction to establish jurisdiction in cybercrime cases.[38] The Utah statute, for example, provides as follows:

(1) A person is subject to prosecution in this state for an offense

34. Ray August, *International Cyber-jurisdiction: A Comparative Analysis*, 39 American Business Law Journal 531, 531-532 (2002) (notes omitted) (citing Ligue Contre la Racisme et l'Antisemitisme v. Yahoo, Inc). *See* Yahoo Ordered to Bar French from Nazi Web Sites, at http://news.zdnet.co.uk/story/0,,t269-s2082683,00.html (Nov. 20, 2000). *See* Chris Nuttal, *Police Hail Net Porn Ruling*, BBC News *at* http://news.bbc.co.uk/hi/english/sci/tech/newsid_ 382000/382152.stm (July 1, 1999); United States v. Galaxy Sports. Press Release, U.S. Department of Justice, Jay Cohen Convicted Of Operating An Off-Shore Sports Betting Business That Accepted Bets From Americans Over The Internet, *at* http://www.usdoj.gov/criminal/cybercrime/cohen.htm (Feb. 28, 2000). *Cf.* Dow Jones & Company Inc. v. Gutnick [2002] HCA 56, *at* http://www.austlii.edu.au/au/cases/cth/high_ct/2002/56.html (December 10, 2002) (holding the U.S. publisher Dow Jones liable for defamation of the Australian citizen Gutnick, even though the material was published on a U.S. Web site).

35. Ark. Code Ann. § 5-27-606 (2003).

36. N.C. Gen. Stat. § 14-453.2 (2002).

37. Conn. Gen. Stat. Ann. § 53a-261 (2004).

38. *See* Oh. Rev. Code Ann. § 2901.11 & Utah Code Ann. § 76-1-201(2003).

which he commits, while either within or outside the state, by his own conduct or that of another for which he is legally accountable, if:

(a) the offense is committed either wholly or partly within the state;

(b) the conduct outside the state constitutes an attempt to commit an offense within the state;

(c) the conduct outside the state constitutes a conspiracy to commit an offense within the state and an act in furtherance of the conspiracy occurs in the state; or

(d) the conduct within the state constitutes an attempt, solicitation, or conspiracy to commit in another jurisdiction an offense under the laws of both this state and such other jurisdiction.

(2) An offense is committed partly within this state if either the conduct which is any element of the offense, or the result which is such an element, occurs within this state.[39]

39. Utah Code Ann. § 76-1-201 (2003). For an example of this approach, *see, e.g.*, State v. Cain, 360 Md. 205, 757 A.2d 142 (Md. 2000). *Cain* was a prosecution for theft by deception involving an individual who responded to an Internet ad offering "a 'mint' collection of ninety-five Barbie dolls." 757 A.2d, *at* 209. The Maryland victim mailed a check to the Georgia resident who placed the ad on the Internet from Georgia, but received a shipment of only thirty-six Barbie dolls, none of which was in "mint" condition. *See id.* The local Maryland prosecutor charged the Georgia seller with theft by deception and the defendant challenged the Maryland court's jurisdiction, arguing that the offense, if indeed it was committed, was committed entirely outside the state. The court rejected this argument, based on the following reasoning:

The essential element of the crime of theft by deception, at least for jurisdictional purposes, is the accused's obtaining control of the subject property. We conclude that if the check was mailed in the State of Maryland, the essential element occurred in Maryland, because Respondent obtained control of the property through the agency of the Postal Service when the complainant deposited it in the mail. Because obtaining control is the essential element of the theft by deception offense, the State will have established prima facie the necessary jurisdictional fact if it proves that the check was posted in Maryland.

The Model Penal Code's jurisdictional provisions have been very influential in shaping the general statute jurisdictional provisions of the type quoted in the text above. The relevant provisions of the Model Penal Code's jurisdictional provision are as follows:

(1) Except as otherwise provided in this Section, a person may be convicted under the law of this State of an offense committed by his own conduct or the conduct of another for which he is legally accountable if:

(a) either the conduct that is an element of the offense or the result that is such an element occurs within this State; or

(b) conduct occurring outside the State is sufficient under the law of this State to constitute an attempt to commit an offense within the State; or

(c) conduct occurring outside the State is sufficient under the law of this State to constitute a conspiracy to commit an offense within the State and an overt act in furtherance of such conspiracy occurs within the State; or

(d) conduct occurring within the State establishes complicity in the commission of,

The most expansive U.S. state provision is found in the provisions of the West Virginia Computer Crimes and Abuse Act, which added the following section to the West Virginia criminal code:

Any person who violates any provision of this [computer crimes code] and, in doing so, accesses, permits access to, causes access to or attempts to access a computer, computer network, computer data, computer resources, computer software or computer program which is located, in whole or in part, within this state, or passes through this state in transit, shall be subject to criminal prosecution and punishment in this state and to the civil jurisdiction of the courts of this state.[40]

Turning to other examples, we see that Tasmania claims jurisdiction if there is a real and substantial link with Tasmania, and this is the case if "a significant part of the conduct relating to, or constituting, the doing of the act or thing occurred in Tasmania."[41]

The European cybercrime statutes lack specific jurisdiction clauses; hence, the general jurisdiction provisions apply, and these are also primarily focused on the location of the act of the crime. Art. 2 of the Dutch Criminal Code provides that the Code "is applicable to anyone guilty of any offense in the Netherlands"; the Belgian and German criminal codes have similar provisions.[42] The German Criminal Code further details when an act is considered to have been

or an attempt, solicitation or conspiracy to commit, an offense in another jurisdiction that also is an offense under the law of this State; or
(e) the offense consists of the omission to perform a legal duty imposed by the law of the State with respect to domicile, residence or a relationship to a person, thing or transaction in the State; or
(f) the offense is based on a statute of this State that expressly prohibits conduct outside the State, when the conduct bears a reasonable relation to a legitimate interest of this State and the actor knows or should know that his conduct is likely to affect that interest.
(2) Subsection (1)(a) does not apply when either causing a specified result or a purpose to cause or danger of causing such a result is an element of an offense and the result occurs or is designed or likely to occur only in another jurisdiction where the conduct charged would not constitute an offense, unless a legislative purpose plainly appears to declare the conduct criminal regardless of the place of the result.
(3) Subsection (1)(a) does not apply when causing a particular result is an element of an offense and the result is caused by conduct occurring outside the State that would not constitute an offense if the result had occurred there, unless the actor purposely or knowingly caused the result within the State.
Model Penal Code § 1.03(1)-(3) (Official Draft 1962).

40. W. Va. Code Ann. § 61-3C-20 (2004).

41. Art. 257F(2)(a) Tasmanian Criminal Code Act 1924.

42. Art. 3 *Strafwetboek* (Belgian CC) ("The crime, committed on the territory of the Kingdom by Belgians or foreigners, is punished in accordance with the provisions of the Belgian laws"); § 3 *Strafgesetzbuch* (German CC) ("German criminal law shall apply to acts, which were committed domestically").

committed on the territory:

(1) An act is committed at every place the perpetrator acted or, in case of an omission, should have acted, or at which the result, which is an element of the

offense, occurs or should occur according to the understanding of the perpetrator.

(2) Incitement or accessoryship is committed not only at the place where the act was committed, but also at every place where the inciter or accessory acted or, in case of an omission, should have acted or where, according to his understanding, the act should have been committed. If the inciter or accessory in an act abroad acted domestically, then German criminal law shall apply to the incitement or accessoryship, even if the act is not punishable according to the law of the place of its commission.[43]

This latter provision is an interesting deviation from the requirement of double criminality that is often posed in cases of cross-border crime.[44] For cybercrime purposes, it means that someone who, for example, sends an email message in Germany with a virus-making program as an attachment, and if the recipient in Benin uses this to spread a virus in his own country, he is criminally liable in Germany for accessoryship of virus spreading, regardless of whether spreading viruses is criminal in Benin.

Equally interesting is the question of the location of an attempt. Activities can take place abroad that aim at committing a crime within the country but that fail to have an actual effect there, such as an attempt from a computer in New York to hack into a computer in Singapore that fails because of a power failure in New York. In that case, Singapore claims jurisdiction:

(1) Any person who abets the commission of or who attempts to commit or does any act preparatory to or in furtherance of the commission of any offence under this Act shall be guilty of that offence and shall be liable on conviction to the punishment provided for the offence.

(2) For an offence to be committed under this section, it is immaterial where the act in question took place.[45]

This would also imply that a virus that is spread on the Internet but that is stopped in time through a concerted effort of the countries where it first appears would confer jurisdiction on Singapore for

43. § 9(2) *Strafgesetzbuch* (German CC).
44. *See supra* § II.
45. Art. 10 Singapore Computer Misuse Act.

attempted unauthorized modification of computer material or attempted unauthorized obstruction of use of computer. Similar provisions appear in the jurisdictional statutes of several U.S. states.[46]

Of course, with cybercrime it is difficult to pinpoint "where" the act actually takes place. Publishing a Web site with a content-related offense, such as child pornography or hate speech, may be considered to take place at the computer where the material is uploaded, which constitutes the act of publishing the material. But the act of uploading can cover several countries, if the content provider is in Country A while the hosting provider is in Country B: in that case, the act of uploading is initiated in A and terminated in B, and it may even be considered to occur in the intermediate countries through which the data is transported.[47] But publishing the Web site may also be considered to take place at the location of the host computer where the material is actually located, since the publication is an ongoing act that takes place continuously from the moment of uploading onwards. In this reasoning, the criminal act only takes place in the country of the host computer.[48] Yet another argument might hold that the act of publication occurs in every place where the material can be received and viewed; although this is more likely the location of the effect[49] rather than of the act, a country that lacks jurisdiction over *effect* might claim that the *act* of disseminating child porn takes place in the recipient's country.

Particularly in the countries that lack specific cybercrime jurisdiction clauses, such difficulties of interpretation will inevitably rise. But also with the more specific jurisdiction clauses, there will be much room for interpreting the phrase "where the act takes place."

46. *See, e.g.*, Or. Rev. Stat. § 131.215 (2003):
[A] person is subject to prosecution under the laws of this state for an offense that the person commits by the conduct of the person or the conduct of another for which the person is criminally liable if:
(1) Either the conduct that is an element of the offense or the result that is an element occurs within this state; or
(2) Conduct occurring outside this state is sufficient under the law of this state to constitute an attempt to commit an offense within this state; or
(3) Conduct occurring outside this state is sufficient under the law of this state to constitute a conspiracy to commit an offense within this state and an overt act in furtherance of the conspiracy occurs within this state; or
(4) Conduct occurring within this state establishes complicity in the commission of, or an attempt, solicitation or conspiracy to commit an offense in another jurisdiction which also is an offense under the law of this state. . . .
See also Utah Code § 76-1-201(1)(b) (2003).

47. *Cf.* Section III(E).

48. *Cf. infra* Section III(B).

49. *See infra* Section III(D).

Courts will have to decide when they think a cybercrime occurred in the territory over which it has jurisdiction, and with the lack of guidance by the statutes on this point, they will likely use various approaches in determining the location of the act. One of the issues, therefore, that requires further study is to survey the factors courts will use to determine the location of the act of a cybercrime.

B. Location of computers

As noted in § III(A), *supra,* some American states, such as Connecticut, have statutes that confer jurisdiction in cybercrime cases upon the fact that some part of the conduct constituting a cybercrime offense impacts upon a computer located in that state.[50]

Likewise, Singapore claims jurisdiction over cybercrimes "if, for the offence in question . . . the computer, program or data was in Singapore at the material time."[51] Malaysia uses the same wording,[52] but extends this in a much broader way.[53]

A related issue is the location of satellites when they are used for crime-related communications. Since satellites orbit around the world, their territorial location can only be assumed to be their ground station, which would most likely count as a computer. Hence, the location of satellite ground stations might also, in some states, constitute a basis for establishing jurisdiction. More relevant than the location, it seems to us, will be the "nationality" of the satellite, i.e., the country in the name of which it is registered.[54]

C. Location of persons

Sometimes the location of a person is a constituting factor for jurisdiction.[55] This is specifically the case in a few special instances where the victim of the crime is located within the territory. For instance, Germany's penalization of the violation of corporate secrecy of a corporation (*Betrieb*) holds for corporations that are located in Germany or that are established (*seinen Sitz hat*) in

50. *See* Conn. Gen. Stat. Ann. § 53a-261 (quoted in § III(A) *supra). See also* Haw. Rev. Stat. Ann. § 708-895 ("For purposes of prosecution . . . a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction").

51. Art. 11(3) Singapore Computer Misuse Act (1993).

52. Art. 9(2) Malaysia Computer Crimes Act (1997).

53. *See infra* § III(E).

54. *See infra* § V(A).

55. *See supra* § II.

Germany, or that are dependent from such a corporation.[56] This is not specifically cybercrime-related, although such a crime will nowadays usually involve computers and networks.

More generally, however, the location of the victim has traditionally been regarded as one of the constituting factors of the location where the act takes place.[57] With physical crimes, the crime regularly occurs in the same place as that of the victim. With cybercrimes, however, perhaps it is no longer such a reasonable assumption to regard the location of the victim as the location of the act as such. Particularly with content-related crimes, one may wonder whether the location of the victim(s) should be constitutive of jurisdictional claims. For instance, hate speech targeted at Jews (which is punishable in a significant number of countries) supposedly victimizes all Jews, but should this mean that any country with a hate-speech provision and with resident Jews can claim jurisdiction?

Another interesting cybercrime in this respect is virtual child pornography, that is, child pornography that has been created or adapted electronically without real children having been abused. This has already been criminalized in a number of countries, including the U.S., Canada, and the Netherlands, and it is also included in the penalization of the Cybercrime Convention.[58] Who is the victim of

56. § 5(7) *Strafgesetzbuch* (German CC).

57. *See supra* §§ II & III(A).

58. Art. 9 para. 2 Convention on Cybercrime: "realistic images representing a minor engaged in sexually explicit conduct." Art. 240b *Wetboek van Strafrecht* (Dutch CC): "or seemingly is involved." Art. 163.1 Canadian Criminal Code: "who is or is being depicted as." As noted in the text below, the U.S. Supreme Court struck down the original ban on virtual child pornography in In Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002). In April of 2003, the PROTECT Act restored the ban to 18 U.S. Code § 2256(8). Section 2256(8) now defines "child pornography" as "any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct" if (i) "the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;" (ii) "such visual depiction is a digital image, computer image, or computer- generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct;" or (iii) "such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct." Many do not believe that option (ii), which was intended to restore the prohibition which the Supreme Court struck down in *Ashcroft*, will pass constitutional muster. *See, e.g.*, Jasmin J. Farhangian, *Problem Of "Virtual" Proportions: The Difficulties Inherent In Tailoring Virtual Child Pornography Laws To Meet Constitutional Standards*, 12 J.L. & Pol'y 241, 273-274 (2003). The language contained in the Convention on Cybercrime is "nearly identical" to that which the Court struck down in *Ashcroft. See* Dina I. Oddis, *Combating Child Pornography On The Internet: The Council Of Europe's*

such offenses? It cannot be children who have been abused in the making of the pornography. Since one of the reasons for criminalizing virtual child porn is its alleged lust-inducing effect on potential offenders, one might argue that all children are potential victims.[59] Should this mean that country A that has criminalized virtual child porn can claim jurisdiction over child porn produced and located in country B, with the argument that it fueled the lust of pedophiles who abused children in country A? The answer to this question will no doubt depend, in large part, upon whether scientific evidence establishes that virtual child pornography does in fact impel pedophiles to act on their unlawful fantasies about children.[60] If country A can show that the virtual child pornography produced in country B was a causal factor in crimes committed against its citizens and within its territory, that makes a much stronger case for allowing country A to claim jurisdiction against the individuals in country B who are responsible for the virtual child pornography. If, on the other hand, no causal nexus can be shown between the virtual child pornography and the crimes committed against children in country A, that undermines the argument for allowing the assertion of jurisdiction.

Convention On Cybercrime, 16 Temp. Int'l & Comp. L.J. 477, 514 (2002).

59. In Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002), the U.S. Supreme Court struck down the U.S.' original ban on virtual child pornography because it found (a) that virtual child pornography is "speech" protected by the First Amendment and (b) that it cannot be banned because, unlike "real" child pornography, its creation does not involve the infliction of harm on real children. As the note immediately above explains, the U.S. Congress quickly re-instituted a ban on virtual child pornography. At this writing, the constitutionality of that ban has not yet been challenged.

In the *Ashcroft* case, the U.S. Department of Justice sought to defend the prohibition on virtual child pornography by claiming that it "whets the appetites of pedophiles and encourages them to engage in illegal conduct." 535 U.S. at 253. The Court rejected this argument because it found that the "mere tendency of speech to encourage unlawful conduct is not a sufficient reason for banning it." 535 U.S. at 253. The Canadian Supreme Court reached a similar conclusion in R. v. Sharpe, 2001 Can. Sup. Ct. LEXIS 8 (2001), which dealt with whether the personal possession of textual or visual child pornography could be criminalized without violating the Canadian Charter of Rights and Freedoms. The Convention on Cybercrime's prohibition on virtual child pornography is based on the premise that even artificially created child pornography should be outlawed because it "might be used to encourage or seduce children" into participating in sexual acts. Council of Europe – Convention on Cybercrime: Explanatory Report at ¶ 202. The Department of Justice raised this issue in *Ashcroft*, but the Court did not find it compelling. *See* 535 U.S. at 250.

60. Those who support banning virtual child pornography argue that it incites sexual abuse of children; those who oppose such a ban argue that it provides "substitute satisfaction" and "reduce[s] offences." *See* R. v. Sharpe, 2001 Can. Sup. Ct. LEXIS 8 (2001).

As to location of the perpetrator, there is a particular case in which it is customary for a country to claim jurisdiction. It is when the alleged offender of a crime committed in country B is located in the territory of country A, where the person is not a national of A, and where country A for some reason does not extradite the person to country B (e.g., because A opposes the death penalty the person might get in B). That is one of the additional factors of jurisdiction in the Cybercrime Convention,[61] and a general jurisdiction basis in Germany.[62] In child pornography cases, countries also claim jurisdiction over foreigners who have committed the crime abroad if they reside in the country; even if the person starts to reside in the country after the crime was committed:

Prosecution can also take place, if the suspect has acquired a fixed residence [*vaste woon- of verblijfplaats*] in the Netherlands only after the committing of the crime.[63]

This is not the only form of jurisdiction based on the location of the perpetrator, however. Singapore claims jurisdiction over cybercrimes "if, for the offence in question, the accused was in Singapore at the material time," the "material time" presumably indicating the time when the offense was committed.[64]

D. Location of effect

It is common for jurisdictions to predicate their exercise of criminal jurisdiction upon conduct that occurred outside the territory of the sovereign seeking to exercise jurisdiction but that had a harmful effect within its territory.[65] Michigan's general criminal jurisdiction statute, for example, declares that the state can prosecute someone who, "while physically located within this state or outside

61. "Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph (1) of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him/her to another Party, solely on the basis of his/her nationality, after a request for extradition" (art. 22(3) Convention on Cybercrime).

62. When the act is committed abroad by a foreigner encountered in Germany if he is not extradited (but is extraditable), if the act is punishable in the country it was committed or is not subject to criminal jurisdiction where committed, § 7(2)(2) *Strafgesetzbuch* (German CC).

63. Art. 5a(2) *Wetboek van Strafrecht* (Dutch CC). A similar provision exists in Belgium: art. 7(1) *Wet houdende de voorafgaande titel van het Wetboek van Strafvordering* (Belgian PTCCP).

64. Art. 11(3) Singapore Computer Misuse Act.

65. *See supra* § II. *See also supra* § III(A). *See, e.g.*, United States v. Nippon Paper Industries Co., Ltd., 109 F.3d 1, 7 (1st Cir. 1997) (subject only to a general requirement of reasonableness, a state has jurisdiction to proscribe conduct outside its territory that has or is intended to have substantial effect within its territory).

of this state," commits a criminal offense that "produces substantial and detrimental effects within this state."[66] As § V(A), *infra*, explains in detail, the United States' basic federal computer crimes provision – 18 U.S. Code § 1030 – allows the U.S. government to exercise jurisdiction over criminal activity that "affects interstate or foreign commerce or communication of the United States."[67]

Likewise, Tasmania claims jurisdiction over cybercrimes if they have a substantial harmful effect in Tasmania: There is a real and substantial link with Tasmania "where the act or thing was done wholly outside Tasmania or partly within Tasmania, if substantial harmful effects arose in Tasmania."[68]

E. Location of anything

As noted *supra*, § III(A), the U.S. state of West Virginia has a particularly expansive jurisdictional provision in its computer crimes code. Under the West Virginia provision, the state can exercise criminal jurisdiction over anyone who violates any provision of the state's computer crimes code "and, in doing so, accesses, permits access to, causes access to or attempts to access a computer, computer network, computer data, computer resources, computer software or computer program which is located, in whole or in part, within this state, or passes through this state in transit."[69]

Like West Virginia, Singapore and Malaysia have wide-reaching jurisdiction clauses in their computer crime statutes. The Singapore provision reads as follows:

Territorial scope of offences under this Act

11. (1) Subject to subsection (2), the provisions of this Act shall have effect, in relation to any person, whatever his nationality or citizenship, outside as well as within Singapore.

(2) Where an offence under this Act is committed by any person in any place outside Singapore, he may be dealt with as if the offence had been committed within Singapore.

(3) For the purposes of this section, this Act shall apply if, for the offence in question

(a) the accused was in Singapore at the material time; or

(b) the computer, program or data was in Singapore at the material

66. State v. Dudley, 354 S.C. 514, 581 S.E.2d 171 (2003); People v. Blume, 443 Mich. 476, 505 N.W.2d 843 (Mich. 1993).

67. 18 U.S. Code § 1030(e)(2)(B) (2004).

68. Art. 257F(2)(b) Tasmanian Criminal Code Act 1924.

69. W. Va. Code Ann. § 61-3C-20 (2004).

time.[70]

Sections 1 and 2 give the Act unlimited extraterritorial effect; section 3, however, may be read as to limit the scope of sections 1 and 2. Only if the perpetrator, the computer, program or data related to the crime was in Singapore at the time of the offence will the act apply. That is, however, still a very broad application. The requirement of the data being in Singapore at the material time is comparable to West Virginia's data passing through the state in transit.

Malaysia's Computer Crime Act is even less limited than Singapore's:

(1) The provisions of this Act shall, in relation to any person, whatever his nationality or citizenship, have effect outside as well as within Malaysia, and where an offence under this Act is committed by any person in any place outside Malaysia, he may be dealt with in respect of such offence as if it was committed at any place within Malaysia.

(2) For the purposes of subsection (1), this Act shall apply if, for the offence in question, the computer, program or data was in Malaysia or capable of being connected to or sent to or used by or with a computer in Malaysia at the material time.[71]

Section 2, like the Singapore provision, limits the extraterritorial scope, but the addition of the clause "or capable of being connected to or sent to or used by or with a computer in Malaysia" gives *carte blanche* for jurisdiction claims. Any computer program or computer data related to the crime will be capable of being used by a computer in Malaysia, and in the networked world, most of the cybercrime-related computers are actually connected, if only indirectly, through the Internet to Malaysia. This effectively gives Malaysia's cybercrime statute the widest possible jurisdiction scope, to the effect of establishing universal jurisdiction.

F. Note on jurisdiction to enforce

An event that occurred in 2000 has raised controversy about a nation's jurisdiction to enforce its law with regard to investigating cybercrime cases. The FBI identified Russians Vasiliy Gorshkov and Alexey Ivanov as the hackers who had been breaking into the computer systems of U.S. businesses.[72] The FBI created a bogus

70. Art. 11 Singapore Computer Misuse Act.
71. Art. 9 Malaysia Computer Crimes Act.
72. U.S. v. Gorshkov, 2001 WL 1024026 at *1 (W.D.W.A. May 23,2001).

company called "Invita" located in Washington, and brought the hackers to Seattle to "interview" with Invita. As part of the "interview" they were asked to hack into a network set up by the FBI, to demonstrate their computer skills.[73] In doing so, they used laptops provided by the FBI to access Russian computers where they kept hacking tools.[74] The FBI had installed a keystroke logger program on each of the laptops and the program recorded the usernames and passwords Gorshkov and Ivanov used to access their Russian computers.[75] As soon as the "interview" was over, agents arrested Gorshkov and Ivanov. They used the information retrieved by the keystroke logger to access the Russian computers and download files they contained.[76] They did all this without obtaining a warrant.[77]

After being indicted for computer crime, Gorshkov moved to suppress the evidence obtained from the Russian computers, arguing that it was the product of a search and seizure that (a) violated the Fourth Amendment and/or (b) violated Russian law.[78] The district court denied the motion. It held (a) that the Fourth Amendment did not apply because it does not encompass extraterritorial searches directed at non-US citizens; and (b) even if it did apply, the agents' action was justified under the exigent circumstances exception to the Fourth Amendment's warrant requirement.[79] The court also held that (a) the agents' actions did not violate Russian law and (b) if they did, it was no basis for suppressing evidence in a U.S. proceeding.[80] Upset about what they regarded as the FBI's violation of Russian sovereignty, Russian authorities subsequently charged the FBI agent primarily responsible for the intrusion with hacking and asked that he be turned over for trial. U.S. authorities have not complied.[81]

The FBI agents' actions in the Gorshkov-Ivanov case have generated controversy and disagreement as to whether their actions were justified as an exercise of enforcement jurisdiction.[82] Some

73. *Id.*
74. *Id.*
75. *Id.*
76. *Id.*
77. Gorshkov, 2001 WL 1024026, *at* *1.
78. *Id.*
79. *Id.* The agents said they needed to act quickly for fear that individuals in Russia, who had learned of the arrests of Gorshkov and Ivanov, would delete files from the computer. *Id.*
80. *Id.*
81. *See, e.g.*, Nicolai Seitz, *Transborder Search: A New Perspective in Law Enforcement*, Yale Law School, *available at* http://islandia.law.yale.edu/isp/digital%20cops/papers/Seitz_Nicolai.pdf.
82. No one disputes that the United States had prescriptive jurisdiction to apply its criminal law to conduct that caused injury in the U.S. even though the conduct

claim that the agents' use of computer technology to search for and "seize" evidence located on the Russian computers violated Russian territorial sovereignty.[83] Others argue that it was a permissible exercise of enforcement jurisdiction, analogous to the use of a grand jury subpoena to obtain documents located in another country.[84] Still another view suggests that transborder searches and seizures such as those at issue in the Gorshkov-Ivanov case (a) are permissible exercises of enforcement jurisdiction when data is generally accessible[85] but (b) are impermissible violations of the principle of territoriality when data is protected, unless the affected state consents to the intrusion.[86] This approach is also chosen in Article 32 of the Convention on Cybercrime: transborder searches are allowed if data are publicly available or if an authorized person in the target state has given consent.

Unfortunately, these issues have yet to be resolved. Cybercrime has a pronounced tendency to cross national borders and digital evidence is by nature evanescent. As a result, law enforcement officers often find it necessary to obtain evidence quickly, without relying upon such traditional mechanisms as Mutual Legal Assistance Treaties or letters rogatory.[87] It is essential, therefore, to establish the circumstances and conditions under which transborder searches and seizures are permissible.[88]

was initiated from outside the U.S. *See, e.g.*, Jack Goldsmith, *The Internet and the Legitimacy of Cross-Border Searches*, (Chicago Public Law and Legal Theory Working Paper No. 16), *available at* http://www.law.uchicago.edu/academics/publiclaw/resources/16.JG.Internet.pdf.

83. *See, e.g.*, Seitz, *supra* note 81. "The principle of territoriality prohibits any form of sovereign activity by prosecuting authorities in foreign Territory." *Id.*

84. *See, e.g.*, Goldsmith, *supra*, note 82.

85. Seitz, *supra*, note 81 (noting that this result is consistent with international customary law).

86. *See, e.g.*, Seitz, *supra* note 81.. This author concludes that, based on the FBI agents' conduct in the Gorshkov-Ivanov case, the United States has consented to transborder searches within its territory if an emergency situation, such as the imminent destruction of evidence, requires such action. *Id*.

87. *See, e.g.*, Susan W. Brenner & Joseph J. Schwerha IV, *Transnational Evidence Gathering And Local Prosecution Of International Cybercrime*, 20 J. MARSHALL J. COMPUTER & INFO. L. 347 (2002).

88. *But see*, Goldsmith, *supra*, note 82. Goldsmith argues that transborder searches are, as a matter of practice, unlikely to be problematic because "nations that are subject to cross-border searches will have incentives to provide meaningful and hurried assistance in redressing crimes that originate from their borders." *Id.* In our opinion, this argument will not convince all governments that are sensitive to their sovereignty, and in any case, it holds only in case of double criminality.

IV. PERSONALITY CLAIMS

A. Nationality of the perpetrator

After territoriality, the nationality of the perpetrator is the second major constituting factor of jurisdiction in cybercrime.[89] The Cybercrime Convention requires parties to establish jurisdiction "when the offence is committed (. . .) by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State."[90] Germany has a comparable general jurisdiction clause: it has jurisdiction over a crime committed abroad by a German national if the act is punishable where it was committed or is not subject to criminal jurisdiction where it was committed.[91] The Netherlands has a comparable clause with a double criminality requirement, applied only to felonies, however, and not to misdemeanors.[92] Belgium's similar provision on nationality jurisdiction, however, even allows for the prosecution of foreigners who have aided and abetted a crime committed by a Belgian national outside of Belgium.[93]

The Netherlands, moreover, has a number of specific cybercrime-related personality jurisdiction provisions. Forgery, including computer forgery, committed abroad by Dutch government employees or employees of international organizations located in the Netherlands is punishable in the Netherlands, if the act is punishable in the country where it was committed.[94] There is jurisdiction over the crime of publishing corporate secrets acquired by accessing a computer by a Dutch national.[95] Finally, child pornography is punishable in the Netherlands if committed by a Dutch national.[96] Interestingly, jurisdiction on the basis of nationality exists also if the person becomes a Dutch national only after the crime was committed.[97]

89. *See supra* § II. *See, e.g.*, Australian Criminal Code Act 1995 § 476.3. Jurisdiction exists, under the incorporated § 15.1(a)(c), if the conduct occurred "wholly outside Australia" but the perpetrator is an Australian citizen, either an individual or a corporation. *Id.*

90. Art. 22(1)(d) Convention on Cybercrime, note 9.

91. § 7 Nr. (2)(1) StGB.*Strafgesetzbuch* (German CC).

92. Art. 5(1)(2) *Wetboek van Strafrecht* (Dutch CC).

93. Art. 11 *Wet houdende de voorafgaande titel van het Wetboek van Strafvordering* (Belgian PTCCP).

94. Art. 4(11) *jo*. 225 *Wetboek van Strafrecht* (Dutch CC).

95. Art. 5(1)(1) *jo*. 273 *Wetboek van Strafrecht* (Dutch CC).

96. Art. 5(1)(3) *jo*. 240b *Wetboek van Strafrecht* (Dutch CC).

97. Art. 5(2) *Wetboek van Strafrecht* (Dutch CC).

B. Nationality of the victim

Besides nationality of the perpetrator, the nationality of the victim may also be constituting factor.[98] Germany has a very general jurisdiction claim based on the nationality of the victim. There is jurisdiction over a crime committed against a German national if the crime is punishable in the country where it was committed or is not subject to a criminal jurisdiction where it was committed.[99] In Belgium, a crime against a Belgian national falls under Belgian jurisdiction if the act is punishable in the country where it was committed, with a penalty of at least 5 years' imprisonment.[100]

Specific to cybercrime, the Netherlands claims jurisdiction over computer sabotage or data damage committed against a Dutch national if the act is covered by article 2 of the International Convention for the Suppression of Terrorist Bombings,[101] or if it is covered by article 2 of the International Convention for the Suppression of the Financing of Terrorism.[102]

In the United States, the basic federal cybercrime provision – 18 U.S. Code § 1030 – confers jurisdiction to prosecute when the conduct at issue impacts upon the federal government, i.e., where the United States is itself the victim. Section 1030(a)(3) of title 18 of the U.S. Code, for example, makes it a federal offense for anyone "intentionally, without authorization to access any nonpublic computer of a department or agency of the United States." And section 1030(a)(6)(B) makes it a federal crime to "knowingly and with intent to defraud," traffic in any password that can be used to access a computer that is used "by or for the Government of the United States." Many U.S. states have similar provisions. Michigan, for example, has a statute which confers criminal jurisdiction, i.e., jurisdiction to adjudicate, whenever a "victim of the offence or an employee or agent of a governmental unit posing as a victim resides in this state or is located in this state at the time the criminal offense is committed."[103]

In cybercrimes, nationality of the victim may create a few

98. *See supra* § II.
99. §7 Nr. (2)(1) StGB.
100. Art. 10(5) *Wet houdende de voorafgaande titel van het Wetboek van Strafvordering* (Belgian PTCCP).
101. Art. 4(13) *Wetboek van Strafrecht* (Dutch CC). International Convention for the Suppression of Terrorist Bombings, New York, 15 December 1997.
102. Art. 4(14) *jo*. 161sexies and 350a *Wetboek van Strafrecht* (Dutch CC). International Convention for the Suppression of the Financing of Terrorism, New York, 9 December 1999.
103. Mich. Comp. Laws § 762.2(1)(d) (2004).

interesting results, in the same way that the location of the victim does.[104] Countries might claim jurisdiction over content-related offenses with the argument that one of their citizens is a member of the class that the offense targets. With viruses, countries could perhaps claim jurisdiction if the computer of one of their nationals residing abroad has been infected. Such examples show the wide range of potential jurisdiction that is possible with cross-border cybercrimes and the varying bases of establishing jurisdiction.

V. OTHER CLAIMS

A. Protection

The protective principle "allows a country to exercise jurisdiction when an act that occurs outside of its borders threatens its security or basic functions. Examples of such acts include counterfeiting and espionage."[105] At one time, the United States made little use of the protective principle as a predicate for exercising criminal jurisdiction, but that has changed in recent years.[106] The United States has come to rely on the principle more expansively,[107] as is illustrated by its approach to exercising jurisdiction in computer-crime cases. The United States' basic federal computer crimes provision – 18 U.S. Code § 1030 – allows the U.S. government to exercise jurisdiction over criminal activity impacting upon a "protected computer" which is, *inter alia,* defined as a computer that is "used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States."[108] This provision was added by the USA Patriot Act, enacted in October, 2001, specifically to confer extraterritorial jurisdiction in cybercrime cases:

> *Previous law:* Before the amendments . . . section 1030 of title 18. . . did not explicitly include computers outside the United States.
>
> Because of the interdependency and availability of global computer networks, hackers from within the United States are increasingly targeting systems located entirely outside of this

104. *See supra* § III(C).
105. Philip M. Nichols, *Outlawing Transnational Bribery Through the World Trade Organization,* 28 LAW AND POLICY IN INTERNATIONAL BUSINESS 305, 369 (1997) (reference omitted).
106. *See* Wayne R. LaFave, SUBSTANTIVE CRIMINAL LAW § 4.3(c) (2003).
107. *See* Wayne R. LaFave, SUBSTANTIVE CRIMINAL LAW § 4.3(c) (2003).
108. 18 U.S.C. § 1030(e)(2)(B).

country. The statute did not explicitly allow for prosecution of such hackers. In addition, individuals in foreign countries frequently route communications through the United States, even as they hack from one foreign country to another. In such cases, their hope may be that the lack of any U.S. victim would either prevent or discourage U.S. law enforcement agencies from assisting in any foreign investigation or prosecution.

Amendment: . . . . [T]he Act amends the definition of 'protected computer' to make clear that this term includes computers outside of the United States so long as they affect 'interstate or foreign commerce or communication of the United States.' . . . [T]he United States can now use speedier domestic procedures to join in international hacker investigations. As these crimes often involve investigators and victims in more than one country, fostering international law enforcement cooperation is essential.

In addition, the amendment creates the option, where appropriate, of prosecuting such criminals in the United States. Since the U.S. is urging other countries to ensure that they can vindicate the interests of U.S. victims for computer crimes that originate in their nations, this provision will allow the U.S. to provide reciprocal coverage.[109]

According to one author, it seems that the protective principle – as distinguished from the "effects" principle discussed in § III(D) – is not a viable basis for the exercise of jurisdiction by U.S. states.[110]

The protective principle might also be relevant for satellites.[111] Countries that put satellites in orbit for global communications, after all, may want to protect their technology and property from being abused for criminal reasons. In the Cybercrime Convention, however, it was decided not to create a specific jurisdictional basis on that ground:

Consideration was given to including a provision requiring each Party to establish jurisdiction over offenses involving satellites registered in its name. The drafters decided that such a provision was unnecessary since unlawful communications involving satellites will invariably originate from and/or be received on earth. As such, one of the bases for a Party's jurisdiction set forth in paragraph 1(a) – (c) will be available if the transmission originates or terminates in one of the locations specified therein. Further, to the extent the offense

109. U.S. Department of Justice, Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001, *at* http://www.cybercrime.gov/PatriotAct.htm (last visited July 22, 2004).
110. *See* Wayne R. LaFave, SUBSTANTIVE CRIMINAL LAW § 4.4(c)(1) (2003).
111. *See supra* § III(B).

involving a satellite communication is committed by a Party's national outside the territorial jurisdiction of any State, there will be a jurisdictional basis under paragraph 1(d). Finally, the drafters questioned whether registration was an appropriate basis for asserting criminal jurisdiction since in many cases there would be no meaningful nexus between the offense committed and the State of registry because a satellite serves as a mere conduit for a transmission.[112]

The last argument indeed seems to us a strong argument against establishing jurisdiction based on the protective principle. The same argument, of course, pleads against establishing jurisdiction based on very broad territorial claims, such as West Virginia's "in transit" clause or Malaysia's "capable of being connected to."[113]

B. Universality

For a restricted number of crimes, countries may claim universal jurisdiction. That is, a claim of jurisdiction, regardless of the location of the act, the nationality of the perpetrator or victim, or any protected interested of the country.[114] The Netherlands, for instance, claims jurisdiction over a number of crimes, such as attacks on the King and counterfeiting;[115] however, cybercrimes do not fall under the universal jurisdiction clause.

Belgium and Germany do claim universal jurisdiction for a particular cybercrime: child pornography. In these countries, the disseminating of child pornography can be prosecuted with universal jurisdiction.[116]

According to one author, "[n]o American state has purported to exercise" any type of universal criminal jurisdiction.[117] The author

112. Explanatory Report, *available at* http://conventions.coe.int/Treaty/en/Reports/Html/185.htm, § 234 (last visited July 22, 2004).

113. See *supra* § III(E).

114. *See supra* § II. *See also* Restatement (Third) of Foreign Relations Law of the United States § 404 (1987) ("A state has jurisdiction to define and prescribe punishment for certain offenses recognized by the community of nations as of universal concern, such as piracy, slave trade, attacks on or hijacking of aircraft, genocide, war crimes, and perhaps certain acts of terrorism, even where none of the bases of jurisdiction indicated in § 402 is present"). *Cf.* United States v. Yousef, 327 F.3d 56, 99-100 (2d Cir. 2003) (district court improperly found it could exercise universal jurisdiction over terrorist activities).

115. Art. 4 *Wetboek van Strafrecht* (Dutch CC).

116. Art. 10ter(1) *Wet houdende de voorafgaande titel van het Wetboek van Strafvordering* (Belgian PTCCP) *jo*. 383(1) *Strafwetboek* (Belgian CC); § 6(6) *jo*. 184(3) *Strafgesetzbuch* (German CC).

117. Wayne R. LaFave, SUBSTANTIVE CRIMINAL LAW § 4.4(c)(3) (2003).

also notes that "it is to be doubted that the theory would support jurisdiction by a state."[118] The federal government of the United States relies on the notion of universal jurisdiction with regard to only a few crimes, including piracy, hostage-taking, aircraft hijacking, aircraft sabotage and torture.[119]

VI. REASONABLENESS STANDARD

As the sections above explain, nations have used various theories – essentially, territoriality, nationality, protection and universality – to justify their exercising jurisdiction to proscribe and adjudicate the application of prescriptive law to particular types of criminal activity.[120] As § II explained, a nation's exercise of jurisdiction – either to prescribe or to adjudicate – must also be "reasonable." This section examines the extent to which the exercise of jurisdiction (a) to prescribe (§ 6.1) and (b) adjudicate (§ 6.2) based upon the several factors outlined above is "reasonable" under applicable standards.

A. Jurisdiction to prescribe

The determination as to whether an exercise of jurisdiction to prescribe is "reasonable" is made by considering the following factors:

(a) the link of the activity to the territory of the regulating state, i.e., the extent to which the activity takes place within the territory, or has substantial, direct, and foreseeable effect upon or in the territory;

(b) the connections, such as nationality, residence, or economic activity, between the regulating state and the person principally responsible for the activity to be regulated, or between that state and those whom the regulation is designed to protect;

(c) the character of the activity to be regulated, the importance of regulation to the regulating state, the extent to which other states regulate such activities, and the degree to which the desirability of such regulation is generally accepted.

(d) the existence of justified expectations that might be protected or hurt by the regulation;

(e) the importance of the regulation to the international political, legal, or economic system;

(f) the extent to which the regulation is consistent with the

118. *Id.* (citing Restatement (Third) of Foreign Relations Law of the United States of the United States § 402 cmt. k (1987)).
119. *See* Wayne R. LaFave, SUBSTANTIVE CRIMINAL LAW § 4.3(e) (2003).
120. *See supra* §§ III-V.

traditions of the international system;

(g) the extent to which another state may have an interest in regulating the activity; and

(h) the likelihood of conflict with regulation by another state.[121]

The two most common bases for exercising jurisdiction to prescribe are territory (i.e., the location of the acts, the location of computers when cybercrime is involved, the location of persons, the location of an effect of criminal acts and/or the location of anything else relevant to the commission of the crime) and the nationality of the perpetrator and/or the victim.[122] Indeed, these two predicates are the first factors set out in the "reasonableness" standards quoted above.

The commentary to this provision of the *Restatement (Third) of the Foreign Relations Law of the United States* notes, however, that "[t]here is wide international consensus that the links of territoriality or nationality, . . . while generally necessary, are not in all instances sufficient conditions for the exercise of such jurisdiction."[123] In each instance, the reasonableness of a particular exercise of jurisdiction to prescribe is determined by employing the factors set out above in a flexible balancing process, one in which no one factor is dispositive.[124] The essential touchstone of reasonableness is the extent to which there is a link, a connection, between the proscribing state and the person or activity at issue.

It follows, therefore, that it will likely be reasonable for a nation to exercise jurisdiction to proscribe criminal conduct – including cybercriminal conduct – that takes place wholly or substantially within its territorial boundaries. This is consistent with the traditional

121. Restatement (Third) of Foreign Relations Law of the United States § 403(2). *See, e.g., id.* at cmt. a ("The principle that an exercise of jurisdiction on one of the bases indicated in § 402 is nonetheless unlawful if it is unreasonable is established in United States law, and has emerged as a principle of international law as well"). *See also supra* § II. For a general discussion of the application of these "reasonableness" standards to conduct occurring in cyberspace, *see, e.g.,* Brief of Amicus Curiae at 29-32, Yahoo!, Inc. v. La Ligue Contre le Racisme et L'Antisemisime, U.S. District Court – Northern District of California (Case No. C 00 – 21275 JF), *at* http://www.cdt.org/jurisdiction/010813yahoo.pdf (last visited July 22, 2004).

122. *See supra* §§ III & V.

123. Restatement (Third) of Foreign Relations Law of the United States § 403 at cmt. a (1987).

124. The factors listed in § 403 of the *Restatement (Third) of Foreign Relations Law of the United States* are "not exhaustive" and no "priority or other significance is implied in the order in which the factors are listed. 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." Restatement (Third) of Foreign Relations Law of the United States § 403 cmt. b (1987).

premise that nations have jurisdiction to proscribe conduct that is likely to threaten their ability to maintain internal order.[125] This principle is explicitly articulated in the second factor listed above, i.e., the connections between the regulating state and those principally responsible for the conduct being regulated.

The difficulty, of course, with cybercrime is that, unlike real-world crime, the sequence of conduct involved in the commission of an offense and its consequences may not occur within the territory of the nation within which the perpetrator is situated at the time he/she consummated the criminal act. Assume, for example, that Perpetrator Pete, who is located in Country A, uses a computer system also located in Country A to commit an act of fraud against Victim Vince, who is located in Country B. In this scenario, the commission of the cybercrime involves a person, a computer system and conduct that all occur within the territorial boundaries of Country A. Therefore, under the principles noted above, it would no doubt be reasonable for Country A to proscribe the commission of cyberfraud by anyone who is physically located in its territory, since Country A has a reasonable interest in both (a) protecting its citizens from internal cyberfraud and (b) preventing its citizens from preying upon citizens of other countries who are vulnerable to cyberfraud.[126] Such a proscription is consistent with the traditions of the international system,[127] since nations have historically exercised jurisdiction to proscribe conduct occurring within their borders.

Country B could challenge the reasonableness of this exercise of jurisdiction to proscribe by arguing that it has an extraterritorial effect when, as is the case in the example given above, the victim is located outside Country A and that this extraterritorial effect presents the likelihood that Country A's exercise of prescriptive jurisdiction will conflict with regulations enacted by another state (such as Country B).[128] In this scenario, which is typical of cybercrime cases, the perpetrator was located in and his actions occurred in Country A but the effects of his actions impacted upon a victim in Country B which, it is reasonable to assume, has also proscribed the conduct at issue.[129]

125. *See, e.g.*, Goodman & Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace*, *supra*, 2002 U.C.L.A. J. OF L. & TECH. 3, 54-65.

126. One can derive the latter obligation from the concept of comity, which implies "a sense of obligation among states." Restatement (Third) of Foreign Relations Law of the United States § 403 at cmt. a (1987).

127. *See* Restatement (Third) of Foreign Relations Law of the United States § 403(2)(f) (1987).

128. *See* Restatement (Third) of Foreign Relations Law of the United States § 403(2)(g) & 403(2)(h) (1987).

129. *See, e.g.*, United States v. Evans, 667 F. Supp. 975, 981 (S.D.N.Y. 1987)

Each nation's exercise of proscriptive jurisdiction is reasonable – Country A's for the reasons given earlier and Country B's because the victim is located within its territory and it has an obligation to protect its citizens from such victimization.[130]

When it "would not be unreasonable for . . . two states to exercise jurisdiction over a person or activity, but the prescriptions by the two states are in conflict, each state has an obligation to evaluate its own . . . interest in exercising jurisdiction, in light of all the relevant factors."[131] A state should defer to another state if "that state's interest

(exercise of extraterritorial jurisdiction was reasonable under the effects test). In the context of cyberspace, many courts have required "deliberate targeting" of a jurisdiction or of a victim known to be in a specific jurisdiction. *See, e.g.*, Horatia Muir Watt, *Yahoo! Cyber-Collision of Cultures: Who Regulates?*, 24 Mich. J. Int'l L. 673, 685 (2003) ("Using targeting as a yardstick has enabled courts of various countries to exercise jurisdiction sufficient to incriminate hate speech, indecency, libel, invasions of privacy, and copyright violations").

130. *See* Restatement (Third) of Foreign Relations Law of the United States § 403(2)(a) & 403(2)(b) (1987).

131. Restatement (Third) of Foreign Relations Law of the United States § 403(3) (1987). The United States Supreme Court has enunciated a slightly different approach for dealing with situations in which one country has outlawed the conduct at issue and the other has not. Using the scenario given above, this analysis would apply if Country A, which hosts the perpetrator and the conduct involved in the commission of the offense, has not outlawed the conduct at issue but Country B, home of the victim (and the "effects" of the conduct at issue), has outlawed it. In *Hartford Fire Insurance Company v. California*, 509 U.S. 764 (1993), the U.S. Supreme Court was faced with an argument that U.S. antitrust law could not be applied to conduct which occurred in Britain and which was "perfectly consistent with British law and policy." 509 U.S. at 799. The Supreme Court rejected this contention, finding that the

'fact that conduct is lawful in the state in which it took place will not, of itself, bar application of the United States antitrust laws,' even where the foreign state has a strong policy to permit or encourage such conduct. . . . No conflict exists, for these purposes, 'where a person subject to regulation by two states can comply with the laws of both.' Since the London reinsurers do not argue that British law requires them to act in some fashion prohibited by the law of the United States, . . . or claim that their compliance with the laws of both countries is otherwise impossible, we see no conflict with British law.

Id. (citing Restatement (Third) of the Foreign Relations Law of the United States § 403 at cmt. e (1987)). *See also* United States v. Kaczowski, 114 F. Supp.2d 143, 153 (W.D.N.Y. 2000) (Fact that bets were accepted offshore in a country in which gambling was legal did not preclude indictment for conspiracy to violate and violations of Wire Act where gambling was illegal in New York where the bets were placed). Under this standard, therefore, the assertion of jurisdiction to proscribe is "valid if the effects test is met and there is no genuine contradiction between United States law and the law or policy of another nation." International Jurisdiction, World Online Gambling, http://www.worldonlinegambling.com/laws/onlinegamblingjurisdiction.htm (last visited July 22, 2004). An online gaming Web site explains how this standard may be applied to exercises of jurisdiction to proscribe Internet gambling:

Online gambling sites would most likely satisfy the two-pronged effects test.

is clearly greater."[132] Here, Country B's interest is clearly greater

Internet sites make their service available to U.S. customers by knowingly accepting memberships to individuals from the U.S., making payments to the U.S. through checks or credit card transactions, or simply by making the site available in the states. Any of these connections could be seen as an intentional foreign act affecting U.S. commerce or, at the very least, as leading to a demonstrated effect in the United States.

Satisfying the true conflicts test is more challenging because some countries are beginning to recognize legalized online casinos and bookmakers. In Australia's Northern Territory resides Lasseters Online, the world's first government-licensed, fully regulated online casino. United States Justice Department officials claim that the operation of this casino is a violation of U.S. law if Americans use the site. However, according to the true conflicts theory, a court would have to determine (through a balancing test) that United States interests outweigh the incentive for maintaining harmonious foreign relations before American jurisdiction could be exercised. The exercise of such jurisdiction over a foreign defendant operating an online gambling operation has not yet been tested.

International Jurisdiction, World Online Gambling, *supra*. *But see* United States v. Kaczowski, 114 F. Supp.2d 143, 153 (W.D.N.Y. 2000) (fact that bets were accepted offshore in a country in which gambling was legal did not preclude indictment for conspiracy to violate and violations of Wire Act where gambling was illegal in New York where the bets were placed). *See also* People ex rel. Vacco v. World Interactive Gaming, 185 Misc.2d 852, 714 N.Y.S.2d 844 (N.Y.Sup. 1999). For more on this issue, *see, e.g.*, R. Scott Girdwood, *Place Your Bets . . . on the Keyboard: Are Internet Casinos Legal?*, 25 Campbell L. Rev. 135, 140-41 (2002).

In the *World Interactive Gaming* case cited above, the defendants argued that a New York state court could not exercise jurisdiction to proscribe over a foreign online gaming operation. *See World Interactive Gaming*, 185 Misc.2d at 859, 714 N.Y.S.2d at 850. The New York Supreme Court disagreed:

[U]nder New York Penal Law, if the person engaged in gambling is located in New York, then New York is the location where the gambling occurred. . . . Here, some or all of those funds in an Antiguan bank account are staked every time the New York user enters betting information into the computer. It is irrelevant that Internet gambling is legal in Antigua. The act of entering the bet and transmitting the information from New York via the Internet is adequate to constitute gambling activity within the New York state.

Wide range implications would arise if this Court adopted respondents' argument that activities or transactions which may be targeted at New York residents are beyond the state's jurisdiction. Not only would such an approach severely undermine this state's deep-rooted policy against unauthorized gambling, it also would immunize from liability anyone who engages in any activity over the Internet which is otherwise illegal in this state. A computer server cannot be permitted to function as a shield against liability, particularly in this case where respondents actively targeted New York as the location where they conducted many of their allegedly illegal activities. Even though gambling is legal where the bet was accepted, the activity was transmitted from New York. Contrary to respondents' unsupported allegation of an Antiguan management company managing GCC, the evidence also indicates that the individuals who gave the computer commands operated from WIGC's New York office. The respondents enticed Internet users, including New York residents, to play in their casino.

World Interactive Gaming,185 Misc.2d at 859-860, 714 N.Y.S.2d at 850-851.

132. Restatement (Third) of Foreign Relations Law of the United States § 403(3)

because it is Country B's citizen who was victimized by the conduct at issue: Country A's interest lies in enforcing and thereby ensuring the efficacy of its internal regulation; this, however, is subordinate to Country B's interest, which consists of demonstrating that it can enforce its own regulations and thereby protect its citizens from victimization either by internal or external perpetrators.[133]

The alternative examined in the previous paragraph assumes that both countries have proscribed the conduct at issue. What if the conduct is lawful in Country A, which hosts the perpetrator and his conduct, but is unlawful in Country B, as in the example of the German adult Web site, *supra*? Here, the conflict arises from the fact that one country has proscribed the conduct but the other has not. How should the test presented above be applied in this situation? One author has analyzed this scenario, using the conflict between German hate speech laws and the United States' First Amendment:[134]

Under widely-held views of international law, . . . Germany . . . has jurisdiction to prescribe with respect to conduct that has effects in its territory. . . . But this 'effects test' is not always enough by itself to justify the exercise of jurisdiction. Section 403 of the *Restatement (Third) of the Foreign Relations Law of the United States* includes a requirement that the exercise of jurisdiction be reasonable, taking into account the respective interests of other jurisdictions as well as the one in which the effects are felt.

The combination of these two tests means that both the proponent and the opponent of applying German hate speech law to Internet conduct originating in Montana would have respectable arguments. The proponent would argue that the effects of the hate speech are felt in Germany just as much as if the web server containing the offensive

(1987).

133. *See* Restatement (Third) of Foreign Relations Law of the United States § 403(2)(c) (1987) (importance of the regulation to the regulating state), § 403(2)(d) (the existence of justified expectations that are protected by the regulation) and (f) the extent to which regulation is consistent with the traditions of the international system). As to the latter, the international system has always given great deference to a state's desire to protect its own citizens. *See, e.g.*, United Nations Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, Article 5(1)(c) (1987), *at* http://www.unhchr.ch/html/menu3/b/h_cat39.htm (parties to the convention must take "such measures" as are necessary to establish their jurisdiction over the offenses defined by the convention when "the victim is a national of that State") (last visited July 22, 2004).

134. For a case in which such a conflict arose, *see, e.g.*, Kevin O'Hanlon, *Charges Dropped Against Neo-Nazi in Gun Case*, The Independent (December 4, 2001), *available at* http://www.theindependent.com/stories/120401/new_lauck04.html.

speech were located in Hamburg. German interests are involved because the purpose of prohibiting hate speech is to limit inflaming ethnic and racial hatreds, the very threat posed by the Montana web server. The opponents would argue that the First Amendment is a legitimate exercise of U.S. jurisdiction to prescribe, and supports the interest in uninhibited speech uttered in the United States. That is exactly what transpires through the web server, and thus mandates application of U.S. law. Acceptance of either argument would no doubt engender much controversy in the jurisdiction whose law was not applied.[135]

What if, expanding the scenario set out above, Country C wants to prosecute perpetrator Pete either because (a) he used a computer in Country C in the course of victimizing Vince of Country B;[136] or (b) Pete is a citizen of Country C?[137] If Country C relied on the first alternative, its exercise of jurisdiction to prescribe would clearly be unreasonable because (1) the link between the activity at issue and Country C's territory is much more attenuated than it is as to either Country A or Country B;[138] and (2) there are no significant connections between Country C and the perpetrator and/or between Country C and those whom its regulation is designed to protect.[139] If Country C relied on the second alternative, i.e., on the fact that Pete is its citizen, then the analysis becomes somewhat more problematic. One of the factors militating in favor of the reasonableness of an exercise of jurisdiction to proscribe is the nationality of the person "principally responsible for the activity to be regulated."[140] In this scenario, however, that is the only connection Country C has with the activity at issue, with the conduct at issue (and its physical locus) or with the harm inflicted by the criminal conduct at issue. Clearly, therefore, Country C's effort to exercise jurisdiction based only upon the nationality of the cybercrime perpetrator would be deemed unreasonable and therefore unallowable.[141]

The same conclusion is likely to apply when the premise for exercising jurisdiction to proscribe is the protective principle noted in

135. Henry H. Perritt, Jr., *Will the Judgment-Proof Own Cyberspace?*, 32 Int'l Law. 1121, 1126 (1998).
136. *See supra* § III(E).
137. *See supra* § IV(A)
138. *See* Restatement (Third) of Foreign Relations Law of the United States § 403(a) (1987).
139. *See* Restatement (Third) of Foreign Relations Law of the United States § 403(b) (1987).
140. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 403(b) (1987).
141. *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 403(a) (1987).

§ 5.1.[142] That section uses the jurisdictional provision of 18 U.S. Code § 1030(e)(2)(B) as an example of a cybercrime jurisdictional provision that relies upon the protective principle.[143] Section 1030(e)(2)(B) exercises proscriptive jurisdiction over extraterritorial criminal activity that impacts upon a computer which is located outside the United States but is "used in a manner that affects interstate or foreign commerce or communication of the United States."[144] While this statute would clearly constitute an authorized exercise of jurisdiction to prescribe,[145] the exercise of such jurisdiction could be found unreasonable if it were challenged using the principles set out at the beginning of this section[146] and if it relied upon nothing more than the use of a computer which affects United States commerce or communication.[147] As the above analyses demonstrate, for an exercise of jurisdiction to proscribe to be reasonable, it must be based upon some notable connection between the proscribing state and the activity or perpetrator.

It seems unlikely that basing jurisdiction to proscribe upon the universality principle would be upheld as reasonable, except, perhaps, if the proscription targeted child pornography. The creation, possession and distribution of child pornography is already an almost-universally outlawed activity,[148] and the universality principle can expand to encompass new offenses.[149]

Regardless of universality, it is clear that – particularly with cybercrimes – the ability of states to proscribe based upon various connections with the crime, the perpetrator, or the victim, may easily

142. *See, e.g.*, United States v. Evans, 667 F. Supp. 974, 981 (S.D.N.Y. 1987) (exercise of extraterritorial jurisdiction was reasonable under the protective principle).

143. *See supra* Part V(A).

144. 18 U.S.C. § 1030(e)(2)(B) (2002).

145. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 402(1)(c) (1987) (nation has "jurisdiction to prescribe law" with regard to extraterritorial conduct "that has or is intended to have substantial effects within its territory").

146. *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 403(2) (1987).

147. This would be particularly true if the conduct at issue had not been criminalized by the nation within whose physical territory it occurred. *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 403 cmt d (1987). *See also* United States v. Vasquez-Velasco, 15 F.3d 833, 839 (9th Cir. 1994) (state can reasonably exercise extraterritorial jurisdiction to proscribe acts that impinge upon the state's territorial integrity, security or political independence).

148. *See, e.g.*, Marc D. Goodman & Susan W. Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace*, 2002 UCLA J.L. & TECH. 3 (2002), *at* http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf pg.78-80 (last visited July 10, 2004).

149. *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 404 cmt. a (1987).

result in multiple states potentially claiming jurisdiction. Therefore, it is all the more vital to look at the reasonableness of states' jurisdiction to adjudicate, since there the main problems will emerge.

B. Jurisdiction to adjudicate

The determination as to whether an exercise of jurisdiction to adjudicate is "reasonable" is made by considering these factors:

(a) the person or thing is present in the territory of the state, other than transitorily;

(b) the person, if a natural person, is domiciled in the state;

(c) the person, if a natural person, is resident in the state;

(d) the person, if a natural person, is a national of the state;

(e) the person, if a corporation or comparable juridical person, is organized pursuant to the law of the state;

(f) a ship, aircraft or other vehicle to which the adjudication relates is registered under the laws of the state;

(g) the person, whether natural or juridical, has consented to the exercise of jurisdiction;

(h) the person, whether natural or juridical, regularly carries on business in the state;

(i) the person, whether natural or juridical, had carried on activity in the state, but only in respect of such activity;

(j) the person, whether natural or juridical, had carried on outside the state an activity having a substantial, direct, and foreseeable effect within the state, but only in respect of such activity; or

(k) the thing that is the subject of adjudication is owned, possessed, or used in the state . . . in respect of a claim reasonably connected with that thing.[150]

Once again, territoriality is an important element in the reasonableness calculus; the first three factors set out above go to territoriality, as do factors (h), (i) and (k).[151]

Some courts – notably in the United States – apply an expansive analysis of when one is "present" in a nation for the purposes of exercising jurisdiction to adjudicate. In *United States v. Kaczowski*,[152] for example, Kaczowski was one of two defendants charged with violating 18 U.S. Code §§ 2, 371, 1084, 1952, and 1955.[153]

150. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 421(2) (1987). *See supra* Part II.

151. *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 421(2) (1987). *See also supra* Part VI(A).

152. 114 F. Supp.2d 143 (W.D.N.Y. 2000),

153. *Id.* at 148.

Specifically, Defendants are charged with aiding and abetting and conspiring to conduct, finance and own an illegal gambling business which used facilities in interstate and foreign commerce to distribute the proceeds of unlawful bookmaking and using interstate and foreign wire communication facilities between this district and the West Indies and Central America to place bets on sporting events.[154]

Kaczowski moved to dismiss the charges, arguing that the court did not have jurisdiction to adjudicate because the "bets and wagers" at issue in the indictment "were accepted offshore in a country in which gambling is legal."[155] The U.S. district court rejected his argument, relying upon a New York state court decision in doing so:

[The] New York Supreme Court . . . held that . . . if a gambler physically is located in New York when the bet is placed, then New York is the location where the gambling occurred. . . . At issue in that case was whether bets placed over the internet by gamblers . . . who were physically within New York to a gambling enterprise located in Antigua where gambling is legal constituted gambling as defined under New York Penal Law Article 225. The court . . . held the act of placing the bet and transmitting the betting information from New York, even to an off-shore gambling facility located in a foreign jurisdiction where gambling is legal, constitutes gambling activity within New York state. Specifically, the court stated, '[i]t is irrelevant that gambling is legal in Antigua. The act of entering the bet and transmitting the information from New York . . . is adequate to constitute gambling activity within the New York state.' . . . Thus, even if . . . acceptance of bets and providing 'line' information is legal in the Dominican Republic, where it is alleged Defendants directed their customers' bets to be accepted, the Indictment nevertheless states an offense. . . .[156]

An Australian court reached a similar conclusion in a stalking

154. *Id.* at 148.

155. *Id.* at 153.

156. *Kaczowski*, 114 F. Supp. 2d at 154 (citing and quoting People *ex rel.* Vacco v. World Interactive Gaming, 714 N.Y.S.2d 844 (N.Y. Sup. 1999)). *World Interactive Gaming* is discussed *supra* Part VI(A). Jurisdiction in such a case could also reasonably be based upon the nationality of the defendant. *See, e.g.*, Antonia Z. Cowan, *The Global Gambling Village: Interstate and Transnational Gambling*, 7 GAMING L. REV. 251, 262 (2003) ("the nationality of the offender could . . . support extraterritorial jurisdiction because the federal government can exert personal jurisdiction over American citizens and American corporations anywhere in the world. Under international law, a nation may generally assert jurisdiction over its citizens" (citing United States v. Juda, 46 F.3d 961, 967 (9th Cir. 1995)). *See also* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 421(2)(d)-(e) (1987).

case.[157] Australian Brian Sutcliffewas accused of stalking an actress who lived in Toronto.[158] The charges were based on his having telephoned the victim and written her repeatedly over several years.[159] An Australian prosecutor charged Sutcliffe with stalking, but the Magistrate dismissed the charges, finding that she lacked jurisdiction to adjudicate the matter because the crime of stalking, if it occurred, occurred in Canada, where the victim was located.[160] The Supreme Court of Victoria reversed.[161] After concluding that the stalking occurred entirely in Canada and noting that there is a presumption against extraterritorial jurisdiction to adjudicate, the court found that "in the past 100 years crimes have ceased to be confined to single locations."[162] It noted that since the Internet has allowed almost instantaneous communication with anyone anywhere in the world, territorial boundaries can no longer define jurisdiction.[163] The Victoria court found that Sutcliffe was a resident of Australia and had committed all the ingredients of the crime "save for the . . . harmful effect" in Australia; it held that his conduct and presence in Australia established a sufficient connection to allow the court to exercise jurisdiction over the proceeding.[164]

In both the *Kaczowski* and *Sutcliffe* cases, the courts based their finding of jurisdiction to adjudicate on the fact that the criminal activity at issue – a substantial part of which occurred extraterritorially in both cases – involved some "local" conduct. In the *Kaczowski* case, the "local" conduct was carried out by the bettors, the ostensible "victims" of the criminal activity; in the *Sutcliffe* case, the "local" conduct was carried out by the perpetrator, whose victim was located halfway around the world. As to the latter, had Canada chosen to prosecute Sutcliffe for stalking under Canadian law, it is likely that the exercise of jurisdiction to adjudicate would be found reasonable based upon (a) his having engaged in activity

157. *See* Director of Public Prosecution v Sutcliffe, [2001] VSC 43 (Victoria, Australia), *available at* http://www.austlii.edu.au/au/cases/vic/VSC/2001/43.html (last visited July 10, 2004).
158. *See, e.g.*, William Birnbauer & John Mangan, *In Your Footsteps*, THE AGE, April 24, 2003,A3 at 4 available at http://www.theage.com.au/articles/2003/04/23/1050777301604.html (last visited July 10, 2004).
159. *Sutcliffe*, [2001] VSC 43 (Sutcliffe also created and operated a Web site dedicated to the television show in which the actress appeared).
160. *Id.*
161. *Id.*
162. *Id.*
163. *Id.*
164. *Sutcliffe*, [2001] VSC 43.

outside Canada that had "a substantial, direct, and foreseeable effect" within that country and (b) the fact that the prosecution was specifically directed at that activity.[165]

Thus, we see that jurisdiction to adjudicate in cross-border crimes may fulfill the reasonableness standard in various ways. The result is that jurisdiction conflicts may easily occur, especially with cybercrimes in which the effects often take place in one or more other countries than the country from which the perpetrator acts. The opposite can also take place, however: the situation that all relevant countries abstain from adjudicating because they all believe that their exercise of jurisdiction would not fulfill the reasonableness standard. What are the consequences of such positive and negative jurisdiction conflicts?

VII. JURISDICTION CONFLICTS

A. Negative conflicts

Even though the cybercrime jurisdiction provisions are quite broad, at least in a number of states and countries, a negative jurisdiction conflict may still occur, that is, a situation in which not any country claims jurisdiction over a cybercrime. For most cybercrimes, most countries will have jurisdiction to proscribe: most crimes, such as hacking and denial-of-service attacks, are targeted at specific computers, and in those cases, countries can claim jurisdiction based on the location of the computer or of the effects of the crime, or on the nationality of the victim. Still, whether they will claim jurisdiction to adjudicate will depend on a number of factors, such as the visibility of the crime, the amount of damage, and the specific connection with the country.

With viruses and certain content-related offenses, the situation is even more diffuse. The nature of these crimes is that they do not essentially occur at a specific place but rather at numerous places at the same time (or "in Cyberspace"), nor are they usually targeted at specific computers, persons, or countries. In such cases, if the perpetrator acts from a country that is a cybercrime freehaven, and if she is a national of that country, a negative jurisdiction conflict may occur. Not necessarily, since there will usually be some factor to base jurisdiction on, such as the effect within a territory, or the passing through of data for states or countries with the widest jurisdiction claims, such as West Virginia or Singapore. But the issue is rather

165. *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 421(2)(j) (1987).

whether a state will always have sufficient interest in claiming jurisdiction: with viruses or Web sites showing hate speech, single countries may feel they are insufficiently harmed for them to claim jurisdiction, perhaps also because they may think that some other country will surely claim jurisdiction. It merits further research to analyze such situations and to survey possible solutions for countries to consult with each other in case a negative jurisdiction conflict threatens.[166]

B. Positive conflicts

More important than the negative conflicts are the positive jurisdiction conflicts, that is, when more than one country claims jurisdiction over the same cybercrime. This is a very realistic situation: cybercrimes usually cross borders, and given the broad jurisdiction provisions of many countries, with most crimes, at least theoretically there will be numerous countries that have the jurisdiction to prosecute. For instance, if a Dutch national uses a computer in Belgium to hack into a computer in Utah, at least the Netherlands, Belgium, and Utah will be able to claim jurisdiction, and possibly states like West Virginia or Singapore might claim jurisdiction as well if the hacker happened to transfer data through their territory while hacking. With viruses like the "love bug" or the Blast worm, many countries could claim jurisdiction based on the effect taking place on their territory. And with a Web site hosted in Wyoming that hyperlinks to child pornography on a Web site in Texas, there may be jurisdiction claims from the federal U.S. government (because the conduct would involve interstate commerce), the states of Wyoming and Texas, Belgium, Germany, and a number of other countries that claim that the Web site is aiding and abetting the offering of child pornography in their territory.

Such multiple jurisdiction claims should be mitigated by the reasonableness standard.[167] For certain countries in the above examples, the circumstances will be too weak to claim jurisdiction, if they have, e.g., suffered much less damage than another country, or if

166. Of course, jurisdiction is only part of the problem, and a minor part at that. The real issue in cross-border cybercrime is usually not whether a single state intends to prosecute and has the jurisdiction to do so, but whether it has the practical ability to prosecute. Free havens are not a particularly serious problem from the perspective of jurisdiction, but they are from the perspective of international co-operation and enforcement. Absent double criminality, a country may have the jurisdiction to prosecute but it will lack the tools to do so since requests for extradition and for evidence-gathering will usually fail.

167. *See supra* Part VI.

the data merely passed through the territory without causing damage. However, the reasonableness standard is flexible, and so, national courts may interpret it as they see fit, allowing jurisdiction claims despite weak links to the country. More often, though, the reasonableness standard will simply provide no solution, since in many cases of positive conflicts, it will be unclear which country evidently has the closest link to the crime or has clearly suffered the most damage.

Unfortunately, the Cybercrime Convention does not provide good guidance here. Instead of giving guidelines or setting up a mechanism for prioritizing jurisdiction claims, the convention merely says the following: "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."[168] According to the Explanatory Report, consultation is not obligatory: "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 planning 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."[169] The Explanatory Report says little, however, on the necessity or the outcome of the consultation, restricting itself to noting:

In some cases, it will be most effective for the States concerned to choose a single venue for prosecution; in others, it may be best for one State to prosecute some participants, while one or more other States pursue others. Either result is permitted under this paragraph.[170]

Here, then, is a clear need for further thought and elaboration. What factors influence the most appropriate jurisdiction for prosecution? Clearly, the location of the perpetrator will be a factor, as will be her nationality, and the question where significant damage occurred. But other factors may be relevant as well, such as the location of the computer from which the crime was initiated or through which the crime was committed. There is no clear hierarchy between all of these factors, and it is therefore important to develop ideas on how to resolve positive jurisdiction conflicts, besides the

168. Convention on Cybercrime, Nov. 23, 2001, Art. 22(5), Europ. T.S. No. 185, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (last visited July 10, 2004).

169. Explanatory Report to the Convention on Cybercrime, ¶ 239, 2001 WL 34368783, *available at* http://conventions.coe.int/Treaty/en/Reports/Html/185.htm (last visited July 10, 2004).

170. *Id.*

obvious need of countries consulting each other in particular cases.

There is another issue that is relevant with respect to multiple jurisdictions claiming jurisdiction. Could someone be prosecuted sequentially by different countries, all of which have jurisdiction? That is, suppose that someone who spread a virus has been prosecuted and convicted to a fine in country A, can countries B and C subsequently start proceedings and request extradition? The Cybercrime Convention has left this issue open, arguing that it is more a matter to be regulated by extradition treaties than by the convention itself.[171]

Sequential prosecution need not necessarily constitute double jeopardy. In the United States, it is often possible to prosecute both at the federal and the state level, since these are different sovereigns and with different sovereigns, a single act may be thought of as constituting different crimes.[172] One can easily imagine a virus spreader being prosecuted by different states on the basis of different indictments: for virus spreading in one country, for data damage in another, and for computer sabotage in yet another. But the indicted crime need not even be different: she can be prosecuted by country A for spreading a virus in computers in country A, as well as by B for spreading the virus in country B. These might be considered different acts, so that double jeopardy would not arise.

The issue does not seem to be merely theoretical: the spreader of the Kournikova virus was sentenced in the Netherlands to 150 hours of public service (*taakstraf*).[173] For countries in which the virus caused major damage, this might seem insufficient punishment, leading to a wish to prosecute as well. It will then be up to the Dutch courts to decide whether to extradite the convict or not, in other words, to decide whether the prosecution abroad would constitute double jeopardy or not. It may well turn out that national courts have different opinions on this matter. We have a feeling that the Netherlands, for instance, would sooner decide that sequential prosecution constitutes double jeopardy than would the United States.

171. Rik Kaspersen, Het Cybercrime-verdrag van de Raad van Europa [Cybercrime-Treaty Report of the Eurpean Council], in J.E.J. Prins et al. (eds.), RECHT & INFORMATIETECHNOLOGIE, The Hague: Sdu 2002, § 9.5.6.2.

172. For example, Terry Nichols was prosecuted federally for his part in the Oklahoma City bombing, and in the spring of 2004 was prosecuted by the state of Oklahoma for killing 168 residents of the state. *See, e.g.*, Ralph Blumenthal, *Defense Tries to Sow Doubts That Nichols Was an Accomplice in Oklahoma City Bombing*, N.Y. Times, May 7, 2004, at A20.

173. *Rechtbank* (district court) Leeuwarden, 27-09-2001, rechtspraak.nl, LJN-number AD3861, *at* http://www.rechtspraak.nl/uitspraak/frameset.asp?ui_id=28069 (last visited July 10, 2004).

This, therefore, is an issue that should be taken into account when studying ways to resolve positive jurisdiction conflicts.

VIII. CONCLUSIONS

Our survey of several jurisdictional provisions related to cybercrimes indicates that the traditional bases for jurisdiction, such as those listed in the *Restatement (Third) of the Foreign Relations Law of the United States*, can well be and in fact are applied to cybercrime. Perhaps surprisingly, territoriality is still a prime factor, despite the non-physical nature of the bits and bytes that usually constitute a cybercrime, and despite the alleged a-territorial nature of the Internet.[174] The location of the act itself or of its effect, as well as the location of computers or persons can establish a sufficient connection to a country or state to claim jurisdiction; some states even use the location of anything remotely connected to the crime to claim jurisdiction. Even so, the interpretation of particularly the location of the act will create problems in cybercrime, where the origin and the destination of the crime are usually in different locations, and where the means –computer networks and IP packets – usually cross numerous territories.

Therefore, other than with traditional, physical crime, cybercrime may sooner look at the location of the effect or the location of the perpetrator or victim. Significantly enough, few countries so far have created specific cybercrime jurisdiction based on effect, although the effect will likely often be used in determining the location of the *act*. Perhaps equally important will be the basis of the nationality of offender and victim, which is more easily determined than location and which is not affected by digitization and dematerialization.

But perhaps the jurisdictional bases can be applied *too* well to cybercrimes. After all, the survey also shows that for the average cybercrime, the jurisdictional bases that countries use will result in

174. The a-territorial nature of the Internet has been asserted by, *e.g.*, John Perry Barlow, *A Declaration of the Independence of Cyberspace*, Feb. 8, 1996, *at* http://www.eff.org/~barlow/Declaration-Final.html; David R. Johnson & David. G. Post, *Law And Borders – The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996); CRYPTO ANARCHY, CYBERSTATES, & PIRATE UTOPIAS, (Peter Ludlow ed., MIT Press 2001). However, more recently the territorial nature of the Internet has been stressed. *See, e.g.*, Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 IND. J. GLOBAL LEGAL STUD. 475 (1998); Mark A. Lemley, *Place and Cyberspace*, 91 CAL. L. REV. 521 (2003) *available at* http://papers.ssrn.com/abstract_id=349760; Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, CAL. L. REV., Forthcoming *at* http://ssrn.com/abstract=306662. Thus, 'de-territorialization' seems to have given way to 're-territorialization.'

numerous potential claims for jurisdiction, both prescriptive and adjudicative.

This need not be a problem, provided that there are clear and effective mechanisms to decide which country had the closest connection to the crime and thus has the priority to prosecute. However, this application of the reasonableness standard is all but clear when it comes to cybercrimes. For certain uniquely targeted crimes, such as hacking into a specific computer, the problem will not be that big, since usually only two or three countries will be involved and they can probably decide among themselves which has the priority to prosecute: the country of the perpetrator, or the country of the victim. With other cybercrimes, however, notably with viruses and Web sites with potentially illegal material, but also with offenses like distributed denial-of-service attacks, there are simply too many factors and countries involved, and it will be difficult in practice to decide upon precedence of jurisdictional claims. The reverse should also be taken into account: with offenses like a virus that has wreaked havoc around the world, it is quite possible that no particular country will claim jurisdiction, since it has only suffered a fraction of the harm caused by the virus, and since the country of residence of the perpetrator may not have the means or the will to prosecute – the "Love Bug" virus being a notable example.[175]

A complicating factor, moreover, is that countries and states turn out to have quite varying scopes and bases in their cybercrime jurisdictional provisions. Our survey of "Approaches in Cybercrime Jurisdiction" perhaps shows in fact rather "Distances in Cybercrime Jurisdiction." Particularly the interpretation of territorial connections and the use of the protective principle yield diverging outcomes. This is undesirable, since it will lead to problems when jurisdiction conflicts emerge whenever a serious cross-border cybercrime occurs that multiple states have an interest in prosecuting.

It is therefore vital that more effort be put into fine-tuning and possibly approximating countries' and states' creation and exercise of prescriptive and adjudicative jurisdiction in relation to cybercrime. This should preferably be undertaken at a global level, or at least at the level of the Council of Europe's Cybercrime Convention, which has also been signed by the U.S., Canada, South Africa, and Japan.

In order to facilitate such an effort, we propose to make a more systematic and in-depth survey of views and practices of cybercrime jurisdiction in various countries across the world.[176] This will

175. *See supra* Part II.
176. We intend to edit a book with country reports on this issue, and to publish

hopefully contribute to a more concerted international effort at effectively fighting the 21st-century bane of cybercrime.

all national cybercrime jurisdiction provisions in the Computer Crime Law Survey that is being coordinated by Tilburg University and the Free University of Brussels with assistance of the University of Dayton School of Law. Contributions to these activities are most welcome at <Susan.Brenner@notes.udayton.edu> and <e.j.koops@uvt.nl>.