

**International Society for the Reform of Criminal Law
16th Annual Conference**

***Technology and Its Effects on Criminal Responsibility,
Security and Criminal Justice***

(December 6-10, 2002)

Cybercrime: The Need to Harmonize National Penal and Procedural Laws

A Paper to be Presented by

Susan W. Brenner and Marc D. Goodman

INTRODUCTION

Nations are concerned about cybercrime, a concern that is shared by many international organizations, including the United Nations, the G-8, the European Union and the Council of Europe. There are a number of reasons to be concerned, perhaps the most important of which is the problems law enforcement officers and prosecutors can encounter when they try to apply existing law to criminal activities in cyberspace.

Many of the legal challenges facing police and prosecutors in their pursuit of cybercriminals can be illustrated by the brief but destructive career of the “Love Bug” virus.¹ The virus, which destroyed files and stole passwords,² appeared in Hong Kong on May 11, 2000, and rapidly spread around the world.³

The virus, which also affected NASA and the CIA,⁴ raced around the world in two hours, three times faster than its Melissa predecessor.⁵ The virus was ultimately estimated to have affected at least forty-five million users in more than twenty countries.⁶ As to the damage it inflicted, estimates varied from \$2 billion to \$10 billion,⁷ since it is always difficult to assess estimate the harm inflicted by cybercrime.

Virus experts quickly traced the “Love Bug” to the Philippines.⁸ Using information supplied by an Internet Service Provider, agents from the Philippines’ National Bureau of Investigation and from the FBI identified individuals suspected of creating and disseminating the “Love Bug,”⁹ but then ran into problems with their investigation: The Philippines had no cybercrime laws, so creating and disseminating a virus was not a crime; since creating and disseminating a virus was not a crime, the officers had a hard

¹ Technically, the “Love Bug” was both a virus and a worm. See, e.g., Lev Grossman, *Attack of the Love Bug*, TIME EUROPE, May 15, 2000, <http://www.time.com/time/europe/magazine/2000/0515/cover.html>.

² See, e.g., *Students Named in Love Bug Probe*, APBNEWS.COM, May 20, 2000, http://www.apbnews.com/newscenter/internetcrime/2000/05/10/lovebug0510_01.html.

³ See, e.g., Lev Grossman, *Attack of the Love Bug*, TIME EUROPE, May 15, 2000, <http://www.time.com/time/europe/magazine/2000/0515/cover.html>.

⁴ See, e.g., *Experts Call for “Anti Love-Bug” Computer Czar*, APBNEWS.COM, May 11, 2000, http://www.apbnews.com/newscenter/internetcrime/2000/05/11/lovebug_congress0511_01.html.

⁵ See, e.g., Lev Grossman, *Attack of the Love Bug*, TIME EUROPE, May 15, 2000, <http://www.time.com/time/europe/magazine/2000/0515/cover.html>.

⁶ See, e.g., *Philippine Investigators Detain Man in Search for “Love Bug” Creator*, CNN.COM, May 8, 2000, <http://www.cnn.com/2000/TECH/computing/05/08/ilove.you.02/>.

⁷ See, e.g., Martin Clark, *Love Bytes*, PC REVIEW, May 13, 2000, <http://www.mg.co.za/pc/2000/05/13may-lovebug01.htm>.

⁸ *Id.*

⁹ See, e.g., *Philippine Investigators Detain Man in Search for “Love Bug” Creator*, CNN.COM, May 8, 2000, <http://www.cnn.com/2000/TECH/computing/05/08/ilove.you.02/>.

time convincing a magistrate to issue a warrant to search the suspects' apartment.¹⁰ Getting the warrant took days, allowing the suspect ample time to destroy essential evidence.¹¹ Authorities finally executed the warrant and seized evidence which indicated that Onel de Guzman, a former computer science student, was the person responsible for creating and disseminating the "Love Bug."¹² But because Philippine law did not criminalize hacking or the distribution of viruses, officials struggled with whether de Guzman could be prosecuted. They finally charged him with theft and credit card fraud,¹³ but the charges were dismissed, as inapplicable and unfounded.¹⁴ De Guzman could not be extradited for prosecution in other countries--such as the United States--that have cybercrime laws; extradition treaties require "double criminality," require, in other words, that the act for which the person is extradited be a crime in both the extraditing nation and the nation seeking extradition.¹⁵ The conduct attributed to de Guzman was a crime in the United States, but was not, of course, a crime in the Philippines. Despite millions of dollars in damage and thousands of victims in dozens of countries, the person responsible could not be brought to trial in the matter. So, no one was ever prosecuted for the damage the "Love Bug" caused.

Law enforcement officials cannot take action against cybercriminals unless countries have laws that criminalize the activities in which these offenders engage. As the "Love Bug" investigators learned, the existence of such laws is a fundamental prerequisite for investigation as well as for prosecution. This is an issue as to which there is neither doubt nor dispute. It would therefore seem obvious that all nations would have or at least desire to have cybercrime laws on the books.

The difficulty comes in defining the laws that need to be in place to allow the apprehension and prosecution of cybercriminals. While this might seem a straightforward task, it actually raises some difficult issues. One is the scope of cyber-offenses a country needs to define: Is it, for example, sufficient for a nation to adopt

¹⁰ See, e.g., *Philippines' Laws Complicate Virus Case*, USA TODAY, June 7, 2000, <http://www.usatoday.com/life/cyber/tech/cth879.htm>.

¹¹ See *id.*

¹² See, e.g., *Waiting for "Love" Suspect*, ABCNEWS.COM, May 8, 2000, http://204.202.137.113/sections/tech/DailyNews/virus_000508.html. See also *Suspect Charged in Love Bug Case*, WIRED NEWS, June 29, 2000, <http://www.wired.com/news/lovebug/0,1768,37322,00.html>.

¹³ The theory behind the charges was that the virus was designed to steal passwords which, in turn, would be fraudulently used to obtain Internet services and other things of value. See, e.g., *"Love Bug" Suspect Not Off Hook Yet*, USA TODAY, Sept. 5, 2000, <http://www.usatoday.com/life/cyber/tech/cti482.htm>.

¹⁴ See, e.g., *Charges Dropped Against Love Bug Suspect*, USA TODAY, August 21, 2000, <http://www.usatoday.com/life/cyber/tech/cti418.htm>.

¹⁵ See, e.g., Lynn Burke, *Love Bug Case Dead in Manila*, WIRED NEWS (Aug. 21, 2000), <http://www.wired.com/news/print/0,1294,38342,00.html>. See also *Washington (State of) v. Johnson*, [1988] 1 S.C.R. 327, http://www.lexum.umontreal.ca/csc-scc/en/pub/1988/vol1/html/1988scr1_0327.html.

laws that prohibit activities targeting computers—hacking and virus dissemination, say—or should it also outlaw crimes against individuals such as cyberstalking and cyberterrorism? Another issue is the extent to which these laws should be cybercrime-specific, i.e., should only target crimes which are committed by exploiting computer technology. Is it, for example, necessary for a country to add a “computer fraud” offense if it has already outlawed fraud?

Both these issues are national in scope, that is, they go only to the nature of the legislation a country should adopt. Other issues are international in scope—they pertain to how a country’s cybercrime laws, or lack of such laws, impact on other countries. The Philippines’ failure to have cybercrime laws meant that a Philippine national inflicted damage in twenty countries but suffered no consequences for his acts; the failure to have legislation was inadvertent, but it still impacted around the globe. The “Love Bug” episode illustrates how fragile our modern networked world is.¹⁶ As a study pointed out, cybercrimes differ from terrestrial crimes in four ways: “They are easy to learn how to commit; they require few resources relative to the potential damage caused; they can be committed in a jurisdiction without being physically present in it; and they are often not clearly illegal.”¹⁷ They also pose far greater challenges for law enforcement:

Effective law enforcement is complicated by the transnational nature of cyberspace. Mechanisms of cooperation across national borders to solve and prosecute crimes are complex and slow. Cyber criminals can defy the conventional jurisdictional realms of sovereign nations, originating an attack from almost any computer in the world, passing it across multiple national boundaries, or designing attacks that appear to be originating from foreign sources. Such techniques dramatically increase both the technical and legal complexities of investigating and prosecuting cyber crimes.¹⁸

Nations must modernize their procedural law as well as their substantive law, their law of crimes. While an adequate framework of cybercrime penal law is an absolute prerequisite for effective action against cybercriminals, such action can be frustrated by antiquated procedural law which, for example, only authorizes the issuance of warrants to search for and seize tangible evidence.¹⁹ Since the prosecution of

¹⁶

Anyone with a computer and an Internet connection . . . can use software easily available on the Web to spawn an electronic plague with global implications. ‘There are no borders on the Internet,’ said Roberto Villabona, the operations manager at Sky Internet, one of the Internet service providers used by the suspects to distribute the virus.

Filipino Arrested in “Love Bug” Case, ST. PETERSBURG TIMES ONLINE, May 9, 2000, http://www.sptimes.com/News/050900/Worldandnation/Filipino_arrested_in_.shtml.

¹⁷ *Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information*, MCCONNELL INTERNATIONAL, Dec, 2000, <http://www.mcconnellinternational.com/services/cybercrime.htm>.

¹⁸ *Id.*

¹⁹ See, e.g., D.C. SUPER. CT. RULES CRIM. PRO. 41(h) (“The term ‘property’ is used in this rule to include documents, books, papers and any other tangible objects”).

cybercrimes usually requires collecting and analyzing intangible evidence, this omission can be a serious problem for investigators.²⁰ Countries must, therefore, also evaluate their procedural law governing evidence-collecting and –analysis and amend it, as necessary, so it does not suffer from this and other limitations.²¹

To prevent the recurrence of another “Love Bug” scenario, the Philippines quickly adopted legislation outlawing certain types of cybercrimes, including the creation and dissemination of viruses.²² But since legislation is a product of a nation’s political and social philosophies, countries may not agree as to what should be defined as a cybercrime. Some countries, for example, make it a crime to publish “hate speech” or otherwise incite “racial hatred.”²³ In the United States, such activity is protected by the First Amendment, which creates a conflict of cybercrime law.²⁴

I. What Is Cybercrime and Why Is It a Source of Global Concern?

Technology gives cybercriminals the abilities to loot and inflict harm around the world with little chance of being apprehended;²⁵ it also lets them experiment with new varieties of criminal endeavors.²⁶ The sections below examine the distinct phenomenon of “cybercrime,” compare it with traditional crime and review the statistics that have been compiled on its incidence and the damage it inflicts.

²⁰ See, e.g., Council of Europe, Draft Explanatory Memorandum to the Draft Convention on Cyber-Crime ¶ 171 (February 14, 2001), <http://conventions.coe.int/treaty/EN/cadreprojets.htm>.

²¹ See, e.g., Model Code of Cybercrime Investigative Procedure, Article VII, <http://www.cybercrimes.net/MCCIP/art7.htm>.

²² See, e.g., “Love bug” Prompts New Philippine Law, USA Today (June 14, 2000), <http://www.usatoday.com/life/cyber/tech/cti095.htm> (under the new law, hackers and those who spread computer viruses can be fined a minimum of \$2,350 and a maximum “commensurate” with the damage caused, and can be imprisoned for up to three years). See also Republic of the Philippines, Eleventh Congress – Second Regular Session, Republic Act No. 8792, Part V § 33, <http://www.mcconnellinternational.com/services/country/philippines.pdf>.

²³ See, e.g., Elizabeth G. Olson, *Nations Struggle with How to Control Hate on the Web*, N.Y. TIMES, Nov. 24, 1997, <http://www.nytimes.com/library/cyber/week/112497racism.html>.

²⁴ See, e.g., *Seminar on the Role of Internet with regard to the Provisions of the International Convention on the Elimination of All Forms of Racial Discrimination*, Item V (Prohibition of Racist Propaganda on the Internet), U.N. HIGH COMMISSIONER FOR HUMAN RIGHTS, Nov. 10-14, 1997, <http://www.unhchr.ch/html/menu2/10/c/racism/shahi.htm>.

²⁵ See, e.g., Conclusions of the Study on Effective Measures to Prevent and Control High-Technology and Computer-Related Crime: Report of the Secretary-General, U.N. Commission on Crime Prevention and Criminal Justice, 10th Sess., Item 4 at 12, U.N. Doc. E/CN.15/2201/4 (2001), http://www.odccp.org/adhoc/crime/10_commission/4e.pdf.

A What is cybercrime?

The terms "cybercrime," "computer crime", "Information Technology crime," and "high-tech crime" are often used inter-changeably to refer to two major categories of offenses: In one, the computer is the target of the offense; attacks on network confidentiality, integrity and/or availability -- i.e. unauthorized access to and illicit ampering with systems, programs or data -- all fall into this category.²⁷ The other category consists of traditional offenses -- such as theft, fraud, and forgery -- that are committed with the assistance of or by means of computers, computer networks and related information and communications technology; here, the computer is a tool used to commit a conventional crime.²⁸ This article uses the term "cybercrime" to refer to offenses falling into either of these categories.²⁹ Computers can also play an incidental role in the commission of a traditional offense, as when a blackmailer uses a computer to generate blackmail letters (or e-mails) or a drug dealer who uses Quicken to track his drug purchases and sales.³⁰ This article will not specifically address instances such as these; because the computer plays such a peripheral role in these scenarios, they are unlikely to require the adoption of new substantive cybercrime law to allow the apprehension and prosecution of the perpetrator. This is not to say that they pose no challenges for law enforcement; like the "true" cybercrime categories noted above, these offenses will contribute to the enormous mountain of cyber-forensic work that will routinely become part of all criminal investigations in the near future and for which law enforcement is wholly unprepared.³¹

Cybercrimes range from economic offenses -- such as computer fraud, theft, forgery, industrial espionage, sabotage and extortion, product piracy and other crimes against intellectual property -- to infringements of privacy, the propagation of illegal and harmful content, the facilitation of prostitution and other offenses against morality, and organized crime.³² The upper limits of severity of cybercrime border on terrorism, as they encompass attacks against life and electronic warfare directed against national security establishments, critical infrastructure, and other vital veins of society. Terrorism encompasses actions intended to provoke a state of terror in the general public, a group

²⁷ See Marc D. Goodman, *Why the Police Don't Care About Computer Crime*, 10 HARVARD J. LAW & TECH. 465, 468-469 (1997), <http://jolt.law.harvard.edu/articles/10hjolt465.html>. See also *Criminal Threats to E-Commerce* 17, INTERPOL, Jan. 2001.

²⁸ See Marc D. Goodman, *Why the Police Don't Care About Computer Crime*, 10 HARVARD J. LAW & TECH. 465, 468-469 (1997), <http://jolt.law.harvard.edu/articles/10hjolt465.html>. See also *Criminal Threats to E-Commerce* 17, INTERPOL, Jan. 2001.

²⁹ See, e.g., MINISTÈRE FRANÇAIS DE L'INTÉRIEUR - DIRECTION CENTRALE DE LA POLICE JUDICIAIRE, DONNÉES STATISTIQUES SUR LA CRIMINALITE LIEE AUX NTIC ET L'ACTION DES SERVICES REPRESSIFS (18 Avril 2000), <http://freebies.weburb.net/link/newsservice.php?messageId=311&id=1&url=http://lambda.eu.org/6xx/dcpj99.html>.

³⁰ See Marc D. Goodman, *Why the Police Don't Care About Computer Crime*, 10 HARVARD J. LAW & TECH. 465, 468-469 (1997), <http://jolt.law.harvard.edu/articles/10hjolt465.html>.

³¹ See *Criminal Threats to E-Commerce* 26, INTERPOL, Jan. 2001.

³² See, e.g., *Criminal Threats to E-Commerce* 17, INTERPOL, Jan. 2001:

of persons or particular persons.³³ Terrorist acts cause grave harm to society by disrupting civil order and/or causing mass terror, loss of life, physical destruction or economic hardship.³⁴ In cyberterrorism, as in cybercrime, the "cyber" component usually refers to perpetrating qualitatively new offenses enabled by information technology or integrating cyberspace into more traditional activities (such as planning, intelligence, logistical capabilities, finance, etc.).³⁵ The categories may also overlap, as they frequently do in the cases of capable, computer-savvy offenders.

Cybercrimes are complex and sometimes elusive phenomena; there is no comprehensive, globally accepted definition that separates the sensational from the sensible and scientific. The following scenarios—all of which are quite real and take place frequently--illustrate the range of activities that can be considered cybercrimes.

1. HACKING AND RELATED ACTIVITIES

Hacking, or gaining unauthorized access to a computer system, programs or data, opens a broad playing field for inflicting damage. A snooper might read the victim's personal information and even take over his computer,³⁶ or a vandal might alter the victim's webpage.³⁷ A saboteur could erase R&D data or paralyze a network, and an industrial spy might steal trade secrets.³⁸ A blackmailer might plant a digital time/logic bomb and threaten to trash a system unless the victim pays up.³⁹

2. VIRUSES AND OTHER MALICIOUS PROGRAMS

Section I describes the damage done by the "Love Bug," a virus that may have been unleashed unintentionally. Other viruses and other types of malicious code can be

³³ See, e.g., Louis J. Freeh, Director, Federal Bureau of Investigation, Threat of Terrorism in the United States, Statement before the Senate Committee on Appropriations, Armed Services and Select Committee on Intelligence, May 10, 2001, <http://www.fbi.gov/congress/congress01/freeh051001.htm>.

³⁴ See, e.g., REPORT OF THE NATIONAL COMMISSION ON TERRORISM, COUNTERING THE CHANGING THREAT OF INTERNATIONAL TERRORISM § 1 (June 7, 2000), <http://www.terrorism.com/documents/bremercommission/index.shtml>.

³⁵ See, e.g., Dorothy E. Denning, *Cyberterrorism: Testimony Before the Special Oversight Panel on Terrorism*, House Committee on Armed Services, May 23, 2000, <http://www.terrorism.com/documents/denning-testimony.shtml>.

³⁶ See, e.g., Nicky Blackburn, *Forget Viruses, The Trojans Are Coming*, THE JERUSALEM POST, June 4, 2000, <http://www.jpost.com/Editions/2000/05/28/Digital/Digital.7384.html>.

³⁷ See, e.g., *Hackers Deface Army's Web Site*, APBNEWS.COM, June 28, 1999, http://www.apbnews.com/newscenter/breakingnews/1999/06/28/hack0628_01.html.

³⁸ See, e.g., Melvin F. Jager & William J. Cook, *Trade Secrets & Industrial Espionage – Online Piracy*, BHG&L RESOURCES, <http://www.brinkshofer.com/resources/tradesecrets.cfm>.

³⁹ See, e.g., Steven Lohr, *A New Battlefield: Rethinking Warfare in the Computer Age*, N.Y. TIMES, Sept, 30, 1996, <http://is.gseis.ucla.edu/impact/f96/Projects/smistry/nytwar.html>.

even more destructive: A calamitous virus could delete files or permanently damage systems; there has, for example, been speculation about “flash worms,” which could spread around the world in thirty seconds.⁴⁰ A Trojan horse, masquerading as a utility (e.g. anti-virus software) or animation may copy user-IDs and passwords, erase files, or release viruses. The program could be used for extortion, with activation of a virus or ‘detonation’ of a digital bomb threatened unless demands are met.⁴¹ A virus might cause a minor annoyance, or tremendous losses in money and productivity, or human lives, if it changes or destroys such crucial data as medical records at a hospital.⁴²

3. FRAUD AND THEFT

Fraud represents probably the largest category of cybercrime:

The Internet has . . . created what so far appears to be the perfect cybercrime—borderless fraud. So many different types of fraud are committed over computer networks that they have become almost impossible to police effectively. . . .

Those who engage in fraud operate globally on ‘Internet time,’ 24 hours a day, 7 days a week. . . . [T]he efficiency and speed of the network create new opportunities for criminals while simultaneously posing serious criminal threats to e-commerce.⁴³

One of the most common types of cyberfraud is online auction fraud:⁴⁴ You are buying something you saw advertised on, say, eBay. Is the person you are dealing with trustworthy? Often not: The vendor may be describing the products or services in a false or misleading manner, or may take orders and money, but fail to deliver the goods.⁴⁵ Or the seller may supply counterfeit goods instead of legitimate ones.⁴⁶

⁴⁰ See, e.g., Stuart Staniford, Gary Grim & Roelof Jonkman, *Flash Worms: Thirty Seconds to Infect the Internet*, Silicon Defense (August 16, 2001), <http://www.silicondefense.com/flash/>. See also Nicholas C. Weaver, *Warhol Worms: The Potential for Very Fast Internet Plagues*, <http://www.cs.berkeley.edu/~nweaver/warhol.html>.

⁴¹ See, e.g., *Email Virus Hoaxes*, Norton Antivirus IC, <http://norton-anti-virus-ic.com/virus.htm> (describing attempt at blackmail using emails that instruct recipients to wire money to a bank in the Ukraine to receive a program that will remove a virus which will otherwise cause damage).

⁴² Louis J. Free, Director, Federal Bureau of Investigation, *Statement Before the Senate Committee for the Judiciary – Subcommittee on Technology, Terrorism and Government Information*, March 28, 2000, <http://www.usdoj.gov/criminal/cybercrime/freeh328.htm>.

⁴³ *Criminal Threats to E-Commerce* 26, INTERPOL, Jan. 2001.

⁴⁴ *Criminal Threats to E-Commerce* 54, INTERPOL, Jan. 2001.

⁴⁵ *Criminal Threats to E-Commerce* 54-56, INTERPOL, Jan. 2001.

⁴⁶ *Id.*

Another common type of cyberfraud is investment fraud; the Internet can be used to fraudulently manipulate stock prices or to facilitate illegal insider trading.⁴⁷

As to simple theft, a thief can steal credit card details,⁴⁸ or siphon funds from a bank.⁴⁹ A twenty-five year old Moscow hacker stole credit card information that was put onto blank cards and used at ATMs all over Europe; fifty people were involved in the scam, and they managed to steal several million dollars before they were caught.⁵⁰

Cyberspace can easily be used to commit theft-by-threat or extortion, as one online retailer learned when a hacker who claimed to be a nineteen-year old Russian student named

‘Maxim’ stole 300,000 credit card numbers from the computer server of CD Universe. Maxim extorted CD Universe by agreeing to destroy the customer data he had stolen in exchange for \$100,000 cash. CD Universe did not pay the thief quickly enough for his liking, and Maxim published the credit card and customer data of 25,000 victims online. The event was widely reported in the media and was quite damaging to CD Universe’s reputation. . . .Maxim still remains at large.⁵¹

And in the fall of 2001, the FBI arrested two Russian hackers who had been breaking into the computers of U.S. businesses and attempting to extort money from them.⁵²

⁴⁷ See, e.g., Louis J. Free, Director, Federal Bureau of Investigation, Statement Before the Senate Committee for the Judiciary – Subcommittee on Technology, Terrorism and Government Information, March 28, 2000, <http://www.usdoj.gov/criminal/cybercrime/freeh328.htm>.

⁴⁸ See *id.*

⁴⁹ In 1994, Russian hacker Vladimir Levin and his accomplices transferred \$12 million out of Citibank accounts and into foreign accounts under their control. See, e.g., *Hacker Goes to Jail After Foiled Citibank Fraud Attempt*, INFOWAR.COM, Feb. 26, 1998, http://www.infowar.com/HACKER/hack_030198s_e.html-ssi. In one of the more unusual cases, a paralegal stole a trial plan which he hoped to sell to opposing counsel. See U.S. Department of Justice – Computer Crime and Intellectual Property Section, Press Release: New York City Law Firm Paralegal Pleads Guilty to Stealing Trial Plan, Oct. 4, 2001, <http://www.cybercrime.gov/farrajPlea.htm>.

⁵⁰ Arnaud de Borchgrave, *et al.*, *Cyber Threats And Information Security: Meeting The 21st Century Challenge*, v, CSIS (2000), http://www.csis.org/pubs/2001_cyberthreatsandis.htm.

⁵¹ *Criminal Threats to E-Commerce* 57, INTERPOL, Jan. 2001.

⁵² See, e.g., U.S. Department of Justice – Computer Crime and Intellectual Property Section, Press Release: Russian Computer Hacker Convicted by Jury, Oct. 10, 2001, <http://www.usdoj.gov/criminal/cybercrime/gorshkovconvict.htm>:

The operation arose out of a nationwide FBI investigation into Russian computer intrusions that were directed at Internet Service Providers, e-commerce sites, and online banks in the United States. The hackers used their unauthorized access to the victims’ computers to steal credit card information and other personal financial information, and then often tried to extort money from the victims with threats to expose the sensitive data to the public or damage the victims’ computers. The hackers also defrauded PayPal through a scheme in

4. GAMBLING, PORNOGRAPHY AND OTHER OFFENSES AGAINST MORALITY

Online casinos have proliferated widely,⁵³ despite that fact that gambling is illegal in many jurisdictions.⁵⁴ The Internet is also being used to distribute drugs, tobacco and liquor, again regardless of jurisdictional prohibitions.⁵⁵

5. CHILD PORNOGRAPHY AND OTHER OFFENSES AGAINST MINORS

Many types of pedophile activity—viewing images, discussing activities, arranging tourism, enticing a child to a meeting—can be carried out over the Internet.⁵⁶ As one report explained,

[c]hild sexual abusers are rapidly turning the Internet and commercial online services into red-light districts, where they can distribute vast quantities of pornography . . . and organize with like-minded individuals. The Internet. . . allows sexual predators to stalk juvenile victims anonymously from the comfort of their homes.⁵⁷

The Internet gives the pedophile the advantages of a wider scope of communications and the likelihood of eluding the law, given the transborder nature of the Internet and the jurisdictional problems that arise in prosecuting cases that transcend borders.⁵⁸

6. STALKING, HARASSMENT, HATE SPEECH

Stalking and harassment are malicious activities directed at a particular person, as two notorious California cases illustrate:

which stolen credit cards were used to generate cash and to pay for computer parts purchased from vendors in the United States.

⁵³ According to one estimate, there are “approximately 200+ casinos, sportsbooks, and full service venues operating on the Internet.” *A Personal Message*, ONLINE CASINO GAMBLING, http://www.adult-fun.net/Online/virtual_list.html.

⁵⁴ See, e.g., Tom W. Bell, *Policy Analysis*, ANTEUP GAMBLING LINKS, <http://gamblinglinks.com/legal.html> (legality of online gambling in several jurisdictions).

⁵⁵ See, e.g., Liquor Online, <http://www.abalonline.com/stores/Liquor&Spirits/liquoronline.html>; Cigars.com, <http://www.cigars.com/>; Mexico Pharmacy Online, <http://www.mexico-pharmacy-online.com/mex-phar/mex-phar.htm>.

⁵⁶ See, e.g., INTERNET WATCH FOUNDATION, <http://www.internetwatch.org.uk/>; MAPI, <http://www.info.fundp.ac.be/~mapi/mapi-eng.html>.

⁵⁷ NEW JERSEY ATTORNEY GENERAL & COMMISSION OF INVESTIGATION, COMPUTER CRIME: A JOINT REPORT 6 (June 2000).

⁵⁸ See, e.g., Opening Address by Ron O'Grady, Interpol: Child Pornography on the Internet Experts Meeting, Lyon, France, May 28-29, 1998, <http://www.ecpat.net/Childporn/Ron's.html>.

[A] 50-year-old former security guard . . . used the Internet to solicit the rape of a woman who rejected his romantic advances. . . . [He] terrorized his 28-year-old victim by impersonating her in various Internet chat rooms and online bulletin boards, where he posted, along with her telephone number and address, messages that she fantasized of being raped. On at least six occasions, sometimes in the middle of the night, men knocked on the woman's door saying they wanted to rape her. . . .⁵⁹

The dissemination of hate and racist speech has a more general focus,⁶⁰ but can be equally traumatic for those who are its targets. The dissemination of such speech is becoming more widespread, thanks to the Internet.⁶¹

The e-mail address of a group of Jewish students in Germany was bombarded with more than 17,000 messages from adolf@hitler.com containing a threat to repeat the Holocaust. The murder of six million more Jews, the sender threatened, would start Nov. 9 - the anniversary of Kristallnacht, the Nov. 9, 1938 'Night of Broken Glass' when the Nazi regime orchestrated attacks on Jews and Jewish businesses across Germany in a harbinger of the Holocaust. German cyber police conceded they were powerless to investigate because the e-mails were sent via a server in the U.S., material that falls outside German laws that make neo-Nazi propaganda a crime.⁶²

Stalking, harassment, hate and racist speech perpetrated over computer networks may or may not be criminal activities, depending on the jurisdiction.⁶³

7. OTHER OFFENSES AGAINST PERSONS

Cyberhomicide--using computer technology to kill someone--has not yet been reported, but it no doubt will. An aspiring mass murderer could, for example, hack into a hospital's computer system, learn about the medication prescribed for patients and alter

⁵⁹ U.S. Department of Justice, *Cyberstalking: A New Challenge for Law Enforcement and Industry*, August 1999, <http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm>.

⁶⁰ See, e.g., Rights for Whites Web Ring, <http://nav.webring.yahoo.com/hub?ring=whitering&list>; The Vlaams Blok, <http://www.vlaams-blok.be/>; Holocaust Denial, <http://www.okneoac.com/dtsantijew.html>.

⁶¹ See, e.g., NEW JERSEY ATTORNEY GENERAL & COMMISSION OF INVESTIGATION, *COMPUTER CRIME: A JOINT REPORT* 32, 34 (June 2000).

⁶² Arnaud de Borchgrave, *et al.*, *Cyber Threats And Information Security: Meeting The 21st Century Challenge*, i, CSIS (2000), http://www.csis.org/pubs/2001_cyberthreatsandis.htm.

⁶³ See, e.g., NEW JERSEY ATTORNEY GENERAL & COMMISSION OF INVESTIGATION, *COMPUTER CRIME: A JOINT REPORT* 32, 34 (June 2000).

the dosages, causing them to die.⁶⁴ Cyberspace can be used to commit extortion, as illustrated by the exploits of the Russian hacker “Maxim,” discussed above.⁶⁵

8. CYBERTERRORISM

Cyberterrorism has been defined as a “premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by subnational groups or clandestine agents.”⁶⁶ Such an attack can take many forms:⁶⁷ A cyberterrorist might hack into computer systems and disrupt domestic banking, the stock exchanges and international financial transactions, leading to a loss of confidence in the economy. Or he or she might break into an air traffic control system and manipulate it, causing planes to crash or collide. A terrorist could hack into a pharmaceutical company’s computers, changing the formula of some essential medication and causing thousands to die. Or a terrorist could break into a utility company’s computers, changing pressure in gas lines, tinkering with valves and causing a suburb to detonate and burn.⁶⁸

B. “TERRESTRIAL CRIME” VERSUS “CYBERCRIME”

Historically, “crime” was addressed at the local, community level of government.⁶⁹ Until the last century, crime was small-scale, consisting of unlawful acts committed by one person or a few loosely-associated persons that were directed against a single victim. Some offenders, of course, made crime their profession, but their activities remained small-scale, limited to the repetitive commission of certain single-victim

⁶⁴ See, e.g., Louis J. Free, Director, Federal Bureau of Investigation, Statement Before the Senate Committee for the Judiciary – Subcommittee on Technology, Terrorism and Government Information, March 28, 2000, <http://www.usdoj.gov/criminal/cybercrime/freeh328.htm>. See also 1999 Revision of the Model State Computer Crimes Code, Commentary to § 2.01.1, <http://www.cybercrimes.net/99MSCCC/MSCCC/Article2/2.01.1.html> (committing mass murder by hacking into an industry computer and altering a product, such as an automobile, so that the product ultimately fails and kills its users).

⁶⁵ *Criminal Threats to E-Commerce* 57, INTERPOL, Jan. 2001.

⁶⁶ Mark M. Pollitt, “Cyberterrorism--Fact or Fancy?”, Proceedings of the 20th National Information Systems Security Conference, 285, October 1997 (quoted in Dorothy E. Denning, *Activism, Hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, <http://www.nautilus.org/info-policy/workshop/papers/denning.html>).

⁶⁷ See, e.g., John Arquilla, *The Great Cyberwar of 2002*, WIRED, Feb. 1998, http://www.wired.com/wired/archive/6.02/cyberwar_pr.html.

⁶⁸ See, e.g., *CyberWar*, RESEARCH-PAPERS.COM, <http://www.research-papers.com/papers/tech2.shtml>.

⁶⁹ See, e.g. *The History of Policing*, ENCYCLOPAEDIA BRITANNICA, <http://208.154.71.60/bcom/eb/article/2/0,5716,115162+1+108569,00.html>; *A Brief History of Law Enforcement*, http://hometown.aol.com/mre2all/A_Little_Historyindex.html.

offenses. The “crimes,” which were generally consistent across societies, fell into routinized, clearly-defined categories that reflected the basic categories of anti-social motivations: Crime was murder, crime was robbery, crime was rape.⁷⁰ Crime also tended to be personal; if the offender(s) and victim did not actually know each other, they were likely to share community ties that put offenses into a manageable, knowable context. This not only facilitated the process of apprehending offenders—who stood a good chance of being identified by the victim or by reputation—it also gave citizens at least the illusion of security, the conceit that they could avoid being victimized if they avoided certain activities or certain associations. Local law enforcement dealt effectively with this type of crime because its parochial character meant investigations were limited in scope and because the incidence of crime stood in relatively modest proportion to the size of the local populace. Law enforcement’s effectiveness in this regard contributed to a popular perception that social order was being maintained and that crime did not go unsolved or unpunished.

Twentieth century increases in the use of technologies, in urbanization and in geographical mobility undermined this model to some extent, but it persisted and still functioned effectively for the most part. Legal systems quickly adapted to the fact that telephones could be used to commit fraud and to harass others; that motor vehicles introduced a dimension of mobility into robbery, kidnapping and other crimes,⁷¹ and that radio and television could be used to perpetrate crimes. Because legal systems modified their substantive criminal law to encompass these activities, the old model still functions effectively for traditional, “real world” crime. Cybercrime is a different story:

What differentiates the criminal threats posed by the Internet is that it is based on a vastly more complex technology than the automobile. It spans the globe and moves information and potential criminal activity with a speed and efficiency heretofore unknown in human history. Not only does this give the police less time to react to any potential criminal threat, but it raises issues of jurisdiction, privacy, and anonymity.⁷²

Some cybercrimes—stalking, say—tend, so far, at least, to be small-scale, single-offender/single-victim crimes, but the world’s experience with cybercrime is still in its infancy and yet large-scale offenses targeting multiple, geographically dispersed victims are already being committed. A notorious example of this is the February, 2000 denial of service attacks⁷³ that targeted eBay, Yahoo and CNN, among others, that effectively shut down their web sites for hours and that were estimated to have caused \$1.2 billion in damage.⁷⁴

⁷⁰ See, e.g., SIR WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND, BOOK IV: OF PUBLIC WRONGS (1769).

⁷¹ See, e.g., Kathleen F. Brickey, *Criminal Mischief: The Federalization of American Criminal Law*, 46 HASTINGS L.J. 1135, 1142-1144 (1995).

⁷² *Criminal Threats to E-Commerce*, 3 INTERPOL, Jan. 2001.

⁷³ See, e.g., *Denial of Service Attacks*, Center for Democracy & Technology, <http://www.cdt.org/security/dos/>.

⁷⁴ See, e.g., Rivka Tadger, *Detect, Deflect, Destroy*, INTERNET WEEK (Nov. 13, 2000), <http://www.internetweek.com/indepth/indepth111300.htm> (“Roughly \$100 million was in lost

To understand the sea change computer technology introduces into criminal activity it is useful to consider a hypothetical: One can analogize a denial of service attack to using the telephone to shut down a pizza delivery business by calling the business' telephone number repeatedly, persistently and without remorse, thereby preventing any other callers from getting through to place their orders. Now, while it may be possible for someone to execute such a scheme, it would be very onerous to do so because it would require a great deal of physical effort and concentration on the perpetrator's part; he would have to be constantly dialing, maintaining the connection until it was broken and then redialing quickly to prevent any other calls from coming in. It would also involve a significant risk of apprehension because the victim could contact the authorities, who would presumably have no difficulty tracing the calls to the perpetrator, since he would presumably be using his personal or business telephone. (Aside from the increased risk of apprehension, the mechanics involved would make using a public telephone to conduct such a maneuver a daunting, if not impossible endeavor.) So, while this hypothetical assault is possible, the risks and rigors involved make it exceeding unlikely that anyone would ever undertake such an assault. But the vector of cyberspace lets someone carry out an attack such as this easily and with very little risk of apprehension, so easy, in fact, that a thirteen-year old boy recently used a denial of service attack to shut down a sophisticated computer company.⁷⁵

Like the distribution of the "Love Bug" virus, the February, 2000 denial of service attacks illustrate the tremendous reach a cybercriminal can have, in terms of the number of victims targeted, the amount of property destroyed or stolen,⁷⁶ and the territorial area involved in the attacks. And while these episodes may have been the work of a single perpetrator, organized cybercrime activity targeting multiple, geographically-dispersed victims has already emerged.⁷⁷

In addition to the increased scale of criminal activity it offers, cybercrime also has a tendency to evade traditional offense categories. While some cybercrime consists of using computer technology to commit traditional crimes such as fraud and theft, it also manifests itself as new varieties of anti-social activity that cannot be prosecuted using traditional offense categories.⁷⁸ The dissemination of the "Love Bug" virus illustrates this: As § I explained, the suspected author of the virus could not be prosecuted under the

revenue, \$100 million was the cost of additional security the victims had to add on following the attacks and a whopping \$1 billion was the combined market capitalization loss").

⁷⁵ See *The Strange Tale of the Denial of Service Attacks Against GRC.COM*, <http://grc.com/dos/grcdos.htm>.

⁷⁶ See *Criminal Threats to E-Commerce*, INTERPOL, Jan. 2001.

⁷⁷ See, e.g., Dennis Blank, *Hacker Hit Men For Hire*, BUSINESSWEEK ONLINE (May 4, 2001), http://biz.yahoo.com/bizwk/010504/dlnjckbcbkvg1r6ahnv_ua.html; D. Ian Hopper, *Large-Scale Phone Invasion Goes Unnoticed by All But FBI*, CNN.com (December 14, 1999), <http://www.signaltonoise.net/library/phonemasters.htm>.

⁷⁸ See, e.g., Craig Bicknell, *Sex.Com Ruling: It Wasn't Stolen*, WIRED NEWS, Aug. 25, 2000, <http://www.wired.com/news/print/0,1294,38398,00.html>.

repertoire of offenses defined by the Philippines penal code because none of them encompassed the distribution of a computer virus, even one which destroyed property (e.g., computer files) and stole passwords. An even better example is a denial of service attack,⁷⁹ which cannot be prosecuted as vandalism,⁸⁰ trespass,⁸¹ burglary,⁸² theft,⁸³ arson,⁸⁴ or extortion⁸⁵ even though it is malicious activity that damages—perhaps even destroys--the victim's ability to conduct business.⁸⁶ No "property" is damaged; there is no intrusion into a protected area (with or without the intent to commit an offense therein); nothing is stolen (at least not in the sense that the perpetrator "takes" property from the victim and thereby enriches himself at the victim's expense); no fires or explosives are used to damage property; and, typically, at least, no thing of value is extorted in exchange for ceasing the attack.⁸⁷

Cybercrime's ability to morph into new and different forms of antisocial activity that evade the reach of existing penal law creates challenges for law enforcement around the world. Cybercriminals can exploit gaps in their own country's criminal law to victimize their fellow citizens with impunity. They can also exploit gaps in the criminal laws of other countries to victimize the citizens of those, and other, nations; as the "Love Bug" episode demonstrated, cybercrime is global crime. The damage wreaked by the "Love Bug" may have been to some extent inadvertent,⁸⁸ if that is true, imagine what a cybercriminal dedicated to wreaking global havoc could achieve.

⁷⁹ See, e.g., Eric J. Sinrod & William P. Reilly, *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 177, 194 (2000).

⁸⁰ See, e.g., MODEL PENAL CODE § 220.3 (Proposed Official Draft 1962).

⁸¹ See, e.g., MODEL PENAL CODE § 221.2 (Proposed Official Draft 1962).

⁸² See, e.g., MODEL PENAL CODE § 221.1 (Proposed Official Draft 1962).

⁸³ See, e.g., MODEL PENAL CODE § 223.2 (Proposed Official Draft 1962).

⁸⁴ See, e.g., MODEL PENAL CODE § 220.1 (Proposed Official Draft 1962).

⁸⁵ See, e.g., MODEL PENAL CODE § 223.4 (Proposed Official Draft 1962).

⁸⁶ See generally Mary M. Calkins, *They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-Hacking Regulatory Models*, 89 Geo. L.J., 171, 180 n. 46 (2000); Eric J. Sinrod & William P. Reilly, *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 177, 199-200 (2000).

⁸⁷ It is possible to analogize a denial of service attack to vandalism. See, e.g., Susan W. Brenner, *Is There Such a Thing as Virtual Crime?*, 4 California Criminal Law Review 1 (2001), <http://boalt.org/CCLR/v4/v4brenner.htm>. It seems more reasonable, however, to create a new offense category targeting denial of service attacks and similar activity.

⁸⁸ See, e.g., Dirk Beveridge, *Filipino Student Says Love Bug An Accident*, THE TIMES OF INDIA, May 12, 2000, <http://www.timesofindia.com/120500/12home7.htm>.

C. CONSENSUS CRIMES: FOUNDATION OF A GLOBAL STRATEGY

Inconsistent national criminal laws were acceptable so long as crime was parochial. A nation's decision to criminalize or not to criminalize activities was a matter solely of national discretion because the consequences of that decision would impact only upon those living within its borders, who tended to be its own citizens. Three hundred years ago, for example, a French citizen's chances of ever finding himself in China were remote, to say the least. But as earthbound technology—ocean-going vessels, trains, automobiles and then planes—evolved, citizens of one nation were increasingly likely to find themselves in another country's jurisdiction.

This trend accelerated and took new forms with the proliferation of computer technology, which makes geographical borders irrelevant; with the Internet people can now cross borders digitally without a passport, getting on a plane, or ever leaving their bedroom. In fact, through the looping and weaving nature of computer routers and the WWW, someone can intend to visit a Web site in France (only) but never realize that his or her communication is being routed through Japan and Brazil to get there. This is a major departure from the previous state of affairs.

While the world has slowly begun to deal with previous forms of border crossings, the nature of cyberspace is highly inconsistent with terrestrial based jurisprudence. Cybercriminals can hopscotch around the world, exploiting gaps in criminal laws and committing depredations with essential impunity . . . and citizens abiding by the laws of their own country can find themselves subject to prosecution in another country, where the laws are different.⁸⁹ The conflict in laws can also lead to peculiar results: If, for example, CompuServe were to take down a Nazi web site because of its content (not because of any violation of CompuServe's terms of service), CompuServe could find itself being sued in the United States for violating the site operators' First Amendment rights, whereas if it did not take down the web site legal action could be brought against it in France and/or Germany, for keeping the site up.

The emergence of cybercrime and its networked and interconnected nature make it imperative to achieve transnational consistency in criminal prohibitions. One way to accomplish this would be to create a single code of law governing the commission of cybercrime (which would have to be an agreed-upon term) anywhere in the world; this takes the articulation of a subset of criminal policy out of the hands of individual nations and thereby eliminates the possibility of inconsistencies.⁹⁰ That is not a viable solution; countries are disinclined to surrender their own law in favor of global cybercrime laws.

⁸⁹ See, e.g., *League Against Racism and Antisemitism v. Yahoo!, Inc.*, No. RG: 00/05308 (County Ct. of Paris, Nov. 2000), <http://www.kentlaw.edu/perritt/conflicts/yahooparis.html>.

⁹⁰ See, e.g., *Conclusions of the Study on Effective Measures to Prevent and Control High-Technology and Computer-Related Crime: Report of the Secretary-General*, U.N. Commission on Crime Prevention and Criminal Justice, 10th Sess., Item 4 at 15, U.N. Doc. E/CN.15/2201/4 (2001), http://www.odccp.org/adhoc/crime/10_commission/4e.pdf (possibility of creating a legally binding international instrument addressing cybercrime).

The alternative is to create a template, a set of principles countries can utilize in adopting cybercrime-specific law or in amending existing laws to ensure they adequately encompass the use of computer technology to commit traditional offenses. The Council of Europe took an important step in this direction with its Convention on Cybercrime, which was opened for signature in November of 2001.⁹¹ The section below analyzes the principles that might be used to create such a template or, in the more commonly used phrase, a set of “consensus crimes.”

1. CONSENSUS CRIMES: WHAT ARE THEY?

The notion of consensus crimes is oxymoronic insofar as it implies there are fundamental differences in the way nations go about defining the conduct that will result in the imposition of a society’s harshest sanctions.⁹² In fact, there is a great deal of consistency, across geography and across time, in how countries delineate the behaviors that are outlawed.⁹³

This consistency derives from the function of the criminal law, which is to maintain an acceptable level of social order within a society.⁹⁴ To do that, countries must establish prohibitions that are designed to maintain the integrity of certain vital interests: the safety of persons; the security of property; the stability of the government; and the sanctity of particular moral principles.⁹⁵ No society can survive if its constituents

⁹¹ See COUNCIL OF EUROPE, CONVENTION ON CYBERCRIME (ETS No. 185), Nov. 23, 2001, <http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm>. According to the Explanatory Report accompanying the Convention, it seeks to establish “a common minimum standard of relevant offences.” COUNCIL OF EUROPE, EXPLANATORY REPORT – CONVENTION ON CYBERCRIME ¶ 33, Nov. 8, 2001, <http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm>. Parties to the Convention would agree to adopt such legislative and other measures as may be necessary to establish “certain activities as cybercrimes under their “domestic law”. See CONVENTION ON CYBERCRIME, Article 2. The activities are set out in the five titles contained in Section 1 of Chapter II of the Convention: (1) illegal interception of and/or interference with computer data, illegal access to and/or interference with computer systems, and the misuse of devices to commit any of these offenses; (2) computer-related forgery and fraud; (3) child pornography; (4) the infringement of copyright and related rights; and (5) provisions governing the imposition of aiding and abetting and corporate liability. *Id.* at Articles 2-10.

⁹² See, e.g., S. SHAVELL, PRINCIPLES OF ECONOMIC ANALYSIS OF LAW Ch. 24 p. 2 (2000), <http://econ.bu.edu/Weiss/Ec337/Shavell/bg24-2e.pdf> (“Imprisonment is a sanction that is unique to criminal law, as are . . . whipping, amputation of limbs, . . . banishment and the death penalty”).

⁹³ Compare Indian Penal Code (1860), <http://www.indialawinfo.com/bareacts/ipc.html>, with American Law Institute, Model Penal Code (1962).

⁹⁴ See, e.g., The Code of Hammurabi, <http://www.yale.edu/lawweb/avalon/hamframe.htm>. See also ROLLIN M. PERKINS & RONALD N. BOYCE, CRIMINAL LAW 5 (3d ed. 1982) (“The purpose of the criminal law is to define socially intolerable conduct, and to hold conduct within the limits which are reasonably acceptable from the social point of view”).

⁹⁵ See, e.g., Portugal, Código Penal, <http://www.cea.ucp.pt/lei/penal/penalind.htm>; Criminal Code of the Russian Soviet Federated Socialist Republic (1934),

are free to harm each other at will, to appropriate each other's property, to undermine the political order and/or to flout the moral principles the citizenry hold dear. Every society will therefore formulate penal prohibitions defining (i) crimes against persons (e.g., murder, assault, rape); (ii) crimes against property (e.g., theft, arson, fraud); (iii) crimes against the state (e.g., treason, rioting, obstruction of justice); and (iv) crimes against morality (e.g., obscene materials, defiling a place of worship).⁹⁶ The greatest degree of consistency will be found in the first two categories which represent the *malum in se* crimes, the absolute prohibitions a society must establish if it is to maintain a modicum of social order because they involve the direct infliction of harm by one person upon another or others.⁹⁷ There will be consistency as to a core of offenses in the third category, e.g., treason, riot, and obstructing justice, because every society must also ensure the stability of its political order.⁹⁸ But there will be more overall deviation in this category because nations vary in terms of the extent to which they feel it necessary to discourage political dissidence.⁹⁹ Finally, there will be a great deal of inconsistency as to offenses in the fourth category because they are the product of a society's values and religious principles and, as such, tend to be much more idiosyncratic in nature.¹⁰⁰

How is this relevant to the development of consensus related to high-tech crimes? For one thing, any effort to devise consensus crimes as an instrument for harmonizing national cybercrime laws needs to take account of, and build upon,

<http://www.tiac.net/users/hcunn/rus/uk-rsfsr.html>. See generally 4 WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND *5-*7. See also ANDREW ASHWORTH, PRINCIPLES OF CRIMINAL LAW 11 (1991).

⁹⁶ See, e.g., H.L.A. Hart, *Law as the Union of Primary and Secondary Rules*, THE NATURE OF LAW 144, 145 (M. P. Golding ed. 1966) (a society must enact "in some form restrictions on the free use of violence, theft, and deception to which human beings are tempted but which they must, in general, repress if they are to coexist in close proximity to each other"). See also Criminal Code of the Republic of Belarus, <http://www.belarus.net/softinfo/lowcatal.htm>;

⁹⁷ "A crime which is malum in se is . . . 'naturally evil, such as murder, rape, arson, burglary, and larceny'. . . . A crime which is malum prohibitum is one prohibited by statute . . . 'although no moral turpitude or dereliction may attach.'" [State v. Hertzog, 615 P.2d 480, 489 \(Wash. Ct. App. 1980\)](#) aff'd in part, rev'd in part, [635 P.2d 694 \(Wash. 1981\)](#).

⁹⁸ See, e.g., Fiji Islands Penal Code, §§ 50 (treason), 87 (unlawful assembly) & 130 (destroying evidence), http://www.vanuatu.usp.ac.fj/paclawmat/Fiji_legislation/Consolidation_1978/Fiji_Penal_Code.html; Revised Penal Code of the Philippines, Articles 114 (treason), 153 (tumults and other disturbances of public order) & 180-181 (false testimony), <http://www.chanrobles.com/revisedpenalcodeofthephilippinesbook2.htm>.

⁹⁹ See, e.g., Criminal Code of the Russian Soviet Federated Socialist Republic (1934), § 58-12, <http://www.tiac.net/users/hcunn/rus/uk-rsfsr.html> ("Failure to denounce a counterrevolutionary crime, reliably known to be in preparation or carried out, shall be punishable by . . . deprivation of liberty for a term not less than six months").

¹⁰⁰ Compare Zamfara State of Nigeria, Shari'ah Penal Code Law (Jan. 2000), §§ 126 & 127 (fornication and adultery offenses), <http://www.nigerianlaws.com/frames/docs/stats/ShariaCodeContents.html> with CONN. GEN. STAT. § 53a-81 (adultery offense repealed) and D.C. CODE ANN. § 22-1001 (fornication offense repealed).

consistencies that exist in the articulation of terrestrial crimes. The more these consensus crimes mirror the definitions of traditional crimes, the more likely it is that countries will be willing to incorporate them into their penal codes. It will, for example, be easier to devise consensus crimes that deal with *malum in se* offenses such as burglary, larceny and property damage than with crimes such as pornography or gambling because the definitions of the former will be far more consistent across national boundaries than the latter. All countries will outlaw acts falling into the first category, and will do so in relatively standard terms because the prohibitions are directed at a finite range of conduct.¹⁰¹ As to pornography and gambling, countries will vary widely in their prohibitions of the former,¹⁰² and some will, and some will not, prohibit the latter.¹⁰³ Building upon previously existing legal concepts also makes the process more efficient and more effective; trying to create new law from scratch is a very time-consuming process, and the technology and the threat is constantly marching on.

For another, identifying fundamental consistencies in the structure of penal codes can help to identify those areas where consensus crimes are most likely to be needed. Unlike civil statutes, which tend to prescribe standards and behaviors,¹⁰⁴ criminal statutes are prohibitory, i.e., they prohibit the behaviors used to achieve specified results.¹⁰⁵ A criminal statute is designed to prevent a forbidden result, or “harm,” by outlawing it and imposing a more or less heinous penalty upon those who achieve (and who endeavor to achieve) that result.¹⁰⁶ The focus of such a statute is therefore on the prohibited result, and its ability to encompass the use of computer technology in achieving that result will depend on the extent to which the statute is phrased in terms that transcend the differences between physical reality and virtual reality.¹⁰⁷

¹⁰¹ Compare Criminal Law of the People's Republic of China, Article 263 (robbery), <http://www.qis.net/chinalaw/prclaw60.htm#Chapter%20V2> with German Penal Code §§ 249 & 250 (robbery), http://www.bmj.bund.de/publik/e_stgb.pdf and United Arab Emirates Penal Code Articles 383 & 384 (1988) (robbery).

¹⁰² Compare KAN. STAT. ANN. § 21-4302 (promoting obscenity) with Sweden, Penal Code (1999), <http://justitie.regeringen.se/propositionermm/ds/pdf/Penalcode.pdf> (no obscenity offense).

¹⁰³ See, e.g., William R. Edington, *Casinos and Tourism in the 21st Century*, <http://www.unr.edu/business/econ/trends2000.html> (surveying legalization of gambling).

¹⁰⁴ See, e.g., German Civil Code, Part II – Seventh Section, <http://www.hull.ac.uk/php/lastcb/bgbeng2.htm>; The Civil Code of Mongolia, Articles 160-178, <http://www.indiana.edu/~mongsoc/mong/civilcode.htm>. Civil statutes that sound in tort, especially those which deal with intentional torts, tend to be more prohibitory than prescriptive because they deal with conduct which is analogous to that at issue in criminal statutes.

¹⁰⁵ See, e.g., New South Wales Consolidated Acts: Crimes Act 1900, Part 3 (“offences against http://www.austlii.edu.au/au/legis/nsw/consol_act/ca190082/”; Sweden, Penal Code, Part Two (“on crimes”), <http://justitie.regeringen.se/propositionermm/ds/pdf/Penalcode.pdf>.

¹⁰⁶ See, e.g., Susan W. Brenner, *Is There Such a Thing as Virtual Crime?*, 4 California Criminal Law Review 1 (2001), <http://boalt.org/CCLR/v4/v4brenner.htm>.

¹⁰⁷ See, e.g., Susan W. Brenner, *Is There Such a Thing as Virtual Crime?*, 4 California Criminal Law Review 1 (2001), <http://boalt.org/CCLR/v4/v4brenner.htm>.

A. CRIMES AGAINST PERSONS

It is, for example, almost certain there will be no need to devise consensus crimes addressing homicide and rape, albeit for different reasons. The purpose of developing consensus crimes is to provide a means of filling the gaps in a country's existing penal law that do not allow the prosecution of cybercrimes.¹⁰⁸ Gaps exist either (a) because a country has not yet outlawed entirely "new" types of criminal activity (such as cyberstalking)¹⁰⁹ or (b) because the language a country has employed to define traditional crimes is so based in physical reality it cannot encompass the use of computer technology to commit those crimes.¹¹⁰ Since both homicide and rape, perhaps the oldest forms of criminal activity, are crimes that are firmly grounded in physical reality, neither falls into the first category; every country will have long ago outlawed the acts of taking another person's life and of forcibly having sexual intercourse.¹¹¹ Homicide does not fall into the second category because homicide crimes are defined in terms of a prohibited result—the death of another person or persons—that transcends the differences between physical and virtual reality.¹¹² The focus is on the result—the method is for the most part irrelevant.¹¹³ Penal codes do not, for instance, parse the result into "homicide by gun," "homicide by strangulation," "homicide by poison" and so on; they simply prohibit causing the death of another human being.¹¹⁴ Existing

¹⁰⁸ See, e.g., *Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information*, McConnell International, <http://www.mcconnellinternational.com/services/cybercrime.htm>.

¹⁰⁹ See, e.g., Susan W. Brenner, *Is There Such a Thing as Virtual Crime?*, 4 California Criminal Law Review 1 (2001), <http://boalt.org/CCLR/v4/v4brenner.htm>.

¹¹⁰ See, e.g., Jari Raman, *Computer Crime*, ENLIST, Nov. 7, 2000, <http://itlaw.law.strath.ac.uk/ENLIST/subjects/is/commentary/> ("Some countries are reluctant to apply the traditional provision of theft and embezzlement to . . . gathering secret data because these provisions require the taking of tangible property with the intention of permanently depriving the victim of it").

¹¹¹ See, e.g., Criminal Law of the People's Republic of China, Articles 232 (homicide) & 236 (rape), <http://www.qis.net/chinalaw/prclaw60.htm#Chapter%20IV2>; Fiji Islands Penal Code, §§ 149 (rape) & 199 (murder); Indian Penal Code, §§ 300 (homicide) & 375 (rape), http://www.indialawinfo.com/bareacts/ipc.html#_Toc496765173; Sweden, Penal Code, Chapter 3 § 1 (homicide) & Chapter 6 § 1 (rape), <http://justitie.regeringen.se/propositionerm/ds/pdf/Penalcode.pdf>; United Arab Emirates Penal Code, Articles 332 (homicide) & 354 (rape). See also *The Code of Hammurabi*, <http://www.yale.edu/lawweb/avalon/hamframe.htm>; *The Visigothic Code*, <http://libro.uca.edu/vcode/>.

¹¹² See, e.g., Susan W. Brenner, *Is There Such a Thing as Virtual Crime?*, 4 California Criminal Law Review 1 (2001), <http://boalt.org/CCLR/v4/v4brenner.htm>.

¹¹³ Some statutes do, of course, provide for the imposition of enhanced penalties if particular weapons (notably firearms) are used to commit a crime against persons. For more on this, and more on its applicability to cybercrime, see Susan W. Brenner, *Is There Such a Thing as Virtual Crime?*, 4 California Criminal Law Review 1 (2001), <http://boalt.org/CCLR/v4/v4brenner.htm>.

¹¹⁴ See, e.g., Criminal Law of the People's Republic of China, Article 232 (homicide), <http://www.qis.net/chinalaw/prclaw60.htm#Chapter%20IV2>; Indian Penal Code, § 300, http://www.indialawinfo.com/bareacts/ipc.html#_Toc496765173; Sweden, Penal Code, Chapter 3 § 1 (homicide), <http://justitie.regeringen.se/propositionerm/ds/pdf/Penalcode.pdf>; United Arab

homicides statutes should therefore encompass the use of computer technology to cause the death of another person or persons.¹¹⁵ Rape will not fall into the second category as long as it continues to prohibit coerced physical sexual intercourse between two or more people because such an act cannot be consummated in cyberspace or via the medium of computer technology;¹¹⁶ existing rape statutes should therefore apply even if computer technology were somehow to be used as the means of perpetrating rape (to identify a victim, say).¹¹⁷ As to other physical crimes against persons, assault-type statutes and kidnapping statutes should be able to encompass whatever role computer technology comes to play in the commission of these crimes,¹¹⁸ as should child abuse and suicide statutes.¹¹⁹ The same should generally be true for statutes defining non-physical crimes against persons, such as invasions of privacy and defamation.¹²⁰ So far, the truly problematic crimes in this category are those targeting

Emirates Penal Code, Article 332. See also Susan W. Brenner, *Is There Such a Thing as Virtual Crime?*, 4 California Criminal Law Review 1 (2001), <http://boalt.org/CCLR/v4/v4brenner.htm>.

¹¹⁵ See, e.g., Indian Penal Code, § 300 (murder), http://www.indialawinfo.com/bareacts/ipc.html#_Toc496765173. The Indian Penal Code was originally promulgated on October 6, 1860; its definition of murder is quite adequate to encompass the use of computer technology to take someone's life.

¹¹⁶ See, e.g., Julian Dibbell, *A Rape in Cyberspace*, <http://www.levity.com/julian/bungle.html>. See also, Susan W. Brenner, *Is There Such a Thing as Virtual Crime?*, 4 California Criminal Law Review 1 (2001), <http://boalt.org/CCLR/v4/v4brenner.htm>.

¹¹⁷ See, e.g., Sandro Cohen, *Oliver Jovanovic: First Sacrifice of the Digital Age*, May 19, 1998, <http://www.ishipress.com/sandro.htm> (man accused of raping woman he met over the Internet).

¹¹⁸ See, e.g., Criminal Law of the People's Republic of China, <http://www.qis.net/chinalaw/prclaw60.htm#Chapter%20IV2> Article 239 (kidnapping); Sweden, Penal Code, Chapter 3 § 5 (assault) & Chapter 4 § 1 (kidnapping), <http://justitie.regeringen.se/propositionermm/ds/pdf/Penalcode.pdf>; Zamfara State of Nigeria, Shari'ah Penal Code Law (Jan. 2000), § 223 (assault) & § 229 (kidnapping), <http://www.nigerianlaws.com/frames/docs/stats/ShariaCodeContents.html>.

¹¹⁹ See, e.g., Sweden, Penal Code, Chapter 6 § 7 (child molestation), <http://justitie.regeringen.se/propositionermm/ds/pdf/Penalcode.pdf>; Zamfara State of Nigeria, Shari'ah Penal Code Law (Jan. 2000), § 213 (cruelty to children) <http://www.nigerianlaws.com/frames/docs/stats/ShariaCodeContents.html>; Fiji Islands Penal Code §§ 155 (child molestation) & 219 (liability for another's suicide), http://www.vanuatu.usp.ac.fj/paclawmat/Fiji_legislation/Consolidation_1978/Fiji_Penal_Code.html.

See also Indian Penal Code §§ 306 & 309 (aiding suicide & attempting suicide), <http://www.indialawinfo.com/bareacts/ipc.html>.

¹²⁰ See, e.g., Indian Penal Code, § 499, http://www.indialawinfo.com/bareacts/ipc.html#_Toc496765395:

Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, to defame that person.

harassment or intimidation: The prohibited result is usually a direct threat to cause physical harm to the victim or the victim's family; statutes that prohibit the generic communication of such a threat should reach the use of computer technology to that end.¹²¹ Unfortunately, the Internet and its facilitation of anonymous communication have generated varieties of harassment that do not involve the transmission of a direct threat to cause physical injury and so cannot be prosecuted under existing law; to reach this type of conduct, nations will have to enact statutes that broaden the prohibited result.

B. CRIMES AGAINST PROPERTY

What about crimes against property? The prohibited results are wrongfully taking another's property (embezzlement, theft, robbery, fraud, forgery); wrongfully damaging or destroying another's property (vandalism, arson); and wrongfully intruding upon another's property (trespass, burglary).¹²² Since crimes against property are also among the oldest types of criminal activity, prohibitions directed at these results are standard features of every penal code.¹²³

Computer technology makes the application of these prohibitions problematic in certain respects. Unlike the harassment statutes discussed in the preceding paragraph, the problem here lies not with the characterization of the prohibited results but with the conceptualization of "property." The formulations of offenses falling into this category have always been predicated upon the notion that "property" is a real-world, physical construct, i.e., a tangible item.¹²⁴ Conceptualizing property in this way imposes significant limitations upon the application of theft, damage and intrusion statutes to conduct occurring in and via cyberspace because in cyberspace property becomes an intangible item. Cyberspace property can consist, for instance, of electronic data which has value because it represents funds one can expend in the "real world"; cyberspace property also consists of software, of domain names and of "pure" information, all of which are valuable in and of themselves. Some transgressions against intangible

This provision—from a penal code that was drafted in 1860—is broad enough to encompass the use of the Internet to distribute defamatory comments.

¹²¹ Cf. New South Wales Consolidated Acts, Crimes Act 1900, § 31 ("documents containing http://www.austlii.edu.au/au/legis/nsw/consol_act/ca190082/s317.html).

¹²² See, e.g., Criminal Code of the Republic of Belarus, Chapter 7 (Crimes Against Property"), http://www.belarus.net/softinfo/catal_la/100097.htm; Canada, Criminal Code, Part IX ("Offenses Against Rights of Property"), <http://laws.justice.gc.ca/en/C-46/index.html>; Criminal Law of the People's Republic of China, Articles 363-276, <http://www.qis.net/chinalaw/prclaw60.htm#Chapter%20IV2>; Fiji Islands Penal Code, §§ 258-351, http://www.vanuatu.usp.ac.fj/paclawmat/Fiji_legislation/Consolidation_1978/Fiji_Penal_Code.html; Indian Penal Code, §§ 378-480, http://www.indialawinfo.com/bareacts/ipc.html#_Toc496765051; Zamfara State of Nigeria, Shari'ah Penal Code Law (Jan. 2000), §§ 144, 161, 173, & 179 <http://www.nigerianlaws.com/frames/docs/stats/ShariaCodeContents.html>.

¹²³ See *id.*

¹²⁴ See, e.g., Indian Penal Code, § 22 ("corporeal property of every description, except land and http://www.indialawinfo.com/bareacts/ipc.html#_Toc496765051).

OHIO REV. CODE § 2909.05 (vandalism as causing “serious physical
See also CAL. PENAL CODE § 7(9) (defining real property) & § 10 (defining
personal property as including “money, goods, chattels, things in action and evidences of debt”).

¹²⁷ See, e.g., Indian Penal Code, §§ 441-453,
http://www.indialawinfo.com/bareacts/ipc.html#_Toc496765051.

¹²⁸ See, e.g., Charlie Baggett, *Denial of Service: The New Cyber Terror*, BIZMONTHLY.COM,
March, 2000, <http://www.bizmonthly.com/news2000/march/baggett.html>.

C. CRIMES AGAINST THE STATE

The third category—crimes against the state—consists of a set of core offenses every country will outlaw plus another set of distinctive offenses found in one or more nations. The core offenses include treason, counterfeiting, rioting and obstructing justice crimes.¹²⁹ Treason, the act of levying war against one's country or supporting its enemies, is a crime the prohibitions of which, like those directed at homicide, are very much focused on a specific result;¹³⁰ traditional treason statutes should therefore encompass the use of computer technology to achieve this result, so that neither new, cyber-treason statutes nor modifications in existing statutes will be required. Traditional rioting statutes may not encompass the use of computer technology to instigate rioting or other forms of public disorder,¹³¹ so this is an area where new legislation can be needed. Computer technology should not affect the application of traditional counterfeiting statutes since, as one author noted, "[u]sing a computer, a scanner, graphics software, and a high-quality color laser printer for forgery or counterfeiting is the same crime as using an old-fashioned printing press with ink".¹³² Obstructing justice is an area where existing laws may need to be modified: Statutes in this area prohibit, among other things, creating, modifying or destroying evidence; to the extent that such statutes conceptualize evidence solely as a tangible commodity,¹³³ they will need to be modified to include acts directed at electronic evidence. Also, existing obstruction of justice statutes may not address acts such as, for example, hacking into a court system's computers and altering or deleting charges against a perpetrator or warrants issued for his arrest.¹³⁴ While it might seem that these issues are a matter of local concern, and

¹²⁹ See, e.g., Criminal Law of the People's Republic of China, Articles 102-113, 170, <http://www.qis.net/chinalaw/prclaw60.htm#Chapter%20V2>; Fiji Islands Penal Code, §§ 50-68, 79-105, 117-136, 352-368, http://www.vanuatu.usp.ac.fj/paclawmat/Fiji_legislation/Consolidation_1978/Fiji_Penal_Code.html

¹³⁰ See, e.g., Fiji Islands Penal Code, § 50, http://www.vanuatu.usp.ac.fj/paclawmat/Fiji_legislation/Consolidation_1978/Fiji_Penal_Code.html

¹³¹ See, e.g., Fiji Islands Penal Code, § 86, http://www.vanuatu.usp.ac.fj/paclawmat/Fiji_legislation/Consolidation_1978/Fiji_Penal_Code.html; Indian Penal Code, § 146, http://www.indialawinfo.com/bareacts/ipc.html#_Toc496765051. But see Indian Penal Code, § 150, http://www.indialawinfo.com/bareacts/ipc.html#_Toc496765051 ("Whoever . . . promotes . . . any person to become a member of any unlawful assembly" is guilty of unlawful assembly, or rioting).

¹³² Ronald B. Standler, *Computer Crime* (1999), <http://www.rbs2.com/ccrime.htm>. But see Indian Penal Code, § 231, http://www.indialawinfo.com/bareacts/ipc.html#_Toc496765051 (offense to counterfeit "coin").

¹³³ See, e.g., Indian Penal Code, § 192, http://www.indialawinfo.com/bareacts/ipc.html#_Toc496765051. See generally Criminal Law of the People's Republic of China, Article 306, <http://www.qis.net/chinalaw/prclaw60.htm#Chapter%20V2>; New South Wales Consolidated Acts, Crimes Act 1900, § 317, http://www.austlii.edu.au/au/legis/nsw/consol_act/ca190082/s317.html.

¹³⁴ See, e.g., Jonathan Saltzman, *Traffic Clerk Charged with Erasing Fines*, PROVIDENCE J, March 7, 2000, A1, 2000 WL 5096652.

therefore not the likely focus of consensus crime categories, that is in fact not the case; the transnational character of cybercrime means that countries depend upon each other, in large part, to gather and preserve evidence and, to a lesser extent, to facilitate the identification and apprehension of known offenders. If a cybercriminal can exploit loopholes in one country's obstruction of justice laws, this can have a negative impact on other countries, the citizens of which have been victimized by that cybercriminal's activities.

D. CRIMES AGAINST MORALITY

The fourth and final category—crimes against morality—is the one in which there will be the least consistency in the creation and definition of offenses.¹³⁵ This lack of consistency has two implications for the articulation of consensus crimes: The lack of consistency means that what is a crime in some countries (gambling, say) is not a crime elsewhere, so this category is *generally* not likely to be a source of consensus crimes; the lack of consistency also means that it would *generally* be difficult to gain acceptance for consensus crimes developed for this category. The qualifications are necessary because it is sometimes difficult to decide whether an activity—such as child pornography—is a “crime against persons” or a “crime against morality.” Child pornography, at least non-virtual child pornography, clearly falls into both categories: A crime against persons is committed when real children are used to produce child pornography;¹³⁶ and the creation, distribution and possession of child pornography is considered a crime against morality in many nations,¹³⁷ just as the dissemination of adult pornography is often considered to be a crime against morality.¹³⁸ Child pornography in some guise is therefore an area that will almost certainly be the focus of one or more consensus crimes. Victimless crimes like the use of drugs and alcohol, gambling and prostitution fall into the category of crimes against morality,¹³⁹ but this type of prohibition tends to be so tied into parochial standards of morality it is unlikely to yield consensus crimes. The same is true of offenses that prohibit acts directed at religious observances or symbols.

¹³⁵ Compare Fiji Islands Penal Code §§ 145-186, http://www.vanuatu.usp.ac.fj/paclawmat/Fiji_legislation/Consolidation_1978/Fiji_Penal_Code.html with Criminal Law of the People's Republic of China, Articles 249-252, 258-261, <http://www.qis.net/chinalaw/prclaw60.htm#Chapter%20IV2> and Estonian Criminal Code, §§ 115-119, 200, 202, <http://www.legaltext.ee/en/andmebaas/ava.asp?m=022>.

¹³⁶This is not true when child pornography is “virtual.” See, e.g., *Ashcroft v. Free Speech Coalition*, ___ U.S. ___, 122 S.Ct. 1389 (2002).

¹³⁷ Cf. Sweden, Penal Code (child pornography not criminalized), <http://justitie.regeringen.se/propositionermm/ds/pdf/Penalcode.pdf>.

¹³⁸ See, e.g., *Bia³ystok Blue*, WARSAW VOICE (August 18, 1996), <http://www.warsawvoice.pl/v408/News01.html> (spokesperson for Ministry of Justice quoted as stating that “[p]ornography is a crime against morality”).

¹³⁹ See, e.g., Gerard V. Bradley, *Retribution and the Secondary Aims of Punishment*, 44 AM. J. JURIS. 105, 108-109 (1999) (“The reason for blanket legal prohibitions . . . of drinking or gambling is a concern for the character of the morally weak. A culture stripped of certain temptations helps the weak to be good”).

There are other activities that, like child pornography, do not fit neatly into any one category. Terrorism is one: It can be considered a crime against persons because terrorist acts inflict injury and death, a crime against property because property is often damaged by terrorist acts, and/or a crime against the state because the terrorist's goal is to undermine the stability of that state by generating chaos and destruction. The characterization of terrorism is further complicated by the fact that nations disagree as to what is, and is not, a terrorist act; the British described the American revolutionaries as terrorists but to modern Americans they were heroic freedom fighters. For that reason, perhaps, countries tend to prosecute terrorist acts as crimes against persons and crimes against property,¹⁴⁰ reducing the acts to their constituent results instead of treating them as a distinct category of criminal activity. This suggests terrorism is not a likely candidate for a consensus crime.

Analyzing consistencies in the articulation of traditional crimes suggests that consensus crimes are needed and are likely to be accepted in these areas:

- defining “new” crimes against persons, for example, online stalking and harassment;
- revising extant crimes against property so they encompass acts directed at intangible property;
- defining “new” crimes against property that encompass denial of service attacks and other emerging types of property damage;
- revising obstruction of justice crimes so they encompass, *inter alia*, the creation, alteration, admissibility and destruction of electronic evidence;
- defining “new” crimes directed at obstructing justice, such as tampering with court records; and
- revising some crimes against morality, notably child pornography, to encompass the use of computer technology.

Since the property crimes are the most consistently problematic, and since the business community and global financial markets have an enormous stake in ensuring the safety of property, this area will no doubt be among the first of these to be addressed. The analysis of consistencies in the articulation of traditional crimes also suggests that consensus crimes are otherwise not likely to be developed (a) because cybercrimes can be prosecuted under existing offense-definitions or (b) because there is a lack of agreement between nations as to what should and should not be criminalized. And while it may seem as if consensus might be an impossible goal to reach, evidence would suggest that more and more nations around the world are moving towards consensus in their approaches to crime in cyberspace.

¹⁴⁰ See, e.g., Criminal Law of the People's Republic of China, Articles 114-124, <http://www.qis.net/chinalaw/prclaw60.htm#Chapter%20V2>. See also United States v. Bin Laden, et al., Indictment (S(9) 98 Cr. 1023 (LBS), Southern District of New York, <http://www.fbi.gov/maicases/eastafrica/indictment.pdf> (indictment in Kenya and Tanzania embassy bombings charged defendants with 229 counts of murder plus conspiracy, perjury, attempted murder, attempt to take hostage and assaults).

2. THE LIMITS OF PENAL LAW CONSISTENCY

The analysis above--indeed, the notion of consensus crimes--is predicated on the principle that fundamental commonalities exist in the penal laws of every nation because penal law has a common, constant function, namely, to maintain order within a society by prohibiting behaviors that produce socially-intolerable results. A society's inevitable need for this function and the consequent emergence of these commonalities make this principle the logical basis for developing consensus crimes. Unfortunately, it incorporates a qualifying condition that will to some extent limit their acceptance.

Penal law has evolved to maintain order *within* a society. Each nation-state is concerned with fulfilling its obligations to its citizens (protecting their lives, property and morality) and with ensuring its own survival. As noted earlier, prohibitions barring crimes against persons and property arose because no nation can survive if its citizens are free to prey upon each other. But what if they prey upon citizens of *another* society? What if the citizens of Nation A use cyberspace to prey upon the citizens of Nations B and C? Is this a matter that is likely to be of great concern to Nation A?

There are no ready answers to these questions, but there are historical precedents for this type of behavior that may shed some light on what will ensue in cyberspace. The most analogous of these involve high-seas piracy and intellectual piracy.

High-seas piracy has been around for centuries; indeed, until the seventeenth century it was "widely sanctioned" in most countries, a "national industry."¹⁴¹ Early in the seventeenth century, the nations of Europe banded together to battle the "infidel" Turkish pirates who had expanded from the Mediterranean into the North Atlantic; by the end of the century, increased trade was transforming attitudes toward piracy.¹⁴² "The advantage to be derived from stealing from one another was giving way to the greater advantage of stable commercial relations."¹⁴³ In the eighteenth century, European countries began a war on piracy that included warning other nations "to cease sponsoring pirate expeditions and to crack down on . . . pirates operating . . . from their territories."¹⁴⁴ These efforts were not immediately successful, in part because many non-European nations and even some European colonies resisted, regarding them as unwelcome infringements.¹⁴⁵ This was certainly true in the American colonies, where "business executives and public officials alike continued to provide havens . . . for pirate

¹⁴¹C.M. SENIOR, A NATION OF PIRATES: ENGLISH PIRACY IN ITS HEYDAY 151 (1976). See Ethan A. Nadelmann, *Global Prohibition Regimes*, 44 INTERNATIONAL ORGANIZATION 479-556 (1990), <http://www.criminology.fsu.edu/transcrime/articles/GlobalProhibitionRegimes.htm> ("Kings . . . and other political magnates . . . viewed piracy as a valued source of wealth and

¹⁴²See Nadelmann, *Global Prohibition Regimes*, *supra*.

¹⁴³ *Id.*

¹⁴⁴ *Id.*

¹⁴⁵ *Id.*

ships for decades after London ordered a halt to such activities”.¹⁴⁶ Piracy therefore persisted well into the nineteenth century; it was not until 1849, for instance, that British forces finally eliminated pirate bases in Crete and Borneo after local rulers refused to act, and pirate havens in the West Indies survived until the 1820s.¹⁴⁷ But by the end of the nineteenth century, piracy had been pretty much eliminated around the world:¹⁴⁸ “As . . . the high seas ceased to be perceived as a no-man’s-land, larceny at sea became

¹⁴⁹ The prohibition against piracy has been described as the first consensus crime.¹⁵⁰

High-seas pirates looted tangible property—gold, silver, jewels and other objects. For intangible, intellectual piracy to develop there had to be a means by which intellectual property could be widely produced, marketed and controlled.¹⁵¹ That process began with the printing press, brought to England in 1476; by 1534, a Crown decree forbade anyone from publishing without a license and approval from royal censors.¹⁵² This measure was meant to promote censorship, not protect property; but by the sixteen century, Britain had begun to protect intellectual property, a process that culminated in the adoption of the first copyright law, the Statute of Anne, in 1709.¹⁵³ The statute barred the reproduction of a published work without the copyright owner’s consent and shifted ownership of copyrights from publishers to authors.¹⁵⁴ The Statute of Anne is generally considered to have provided the model for modern copyright law “in the

¹⁵⁵ it was widely copied by other countries, including the United

¹⁴⁶ *Id.*

¹⁴⁷ *Id.*

¹⁴⁸ It still survives on a small scale. See, e.g., United Nations, Reports on Piracy: Oceans and the Law of the Sea, Report of the Secretary-General, Fifty-fifth Session, 2000, <http://www.geocities.com/Tokyo/Garden/5213/unrep00.htm>.

¹⁴⁹ *Id.*

¹⁵⁰ *Id.*

¹⁵¹ See generally Christophe Kervegant, *Intellectual Property and Electronic Communication*, 10TH BILETA CONFERENCE, 1995, <http://www.law.warwick.ac.uk/confs/95-7.html>; Debora Halbert, *Computer Technology and Legal Discourse: The Potential for Modern Communication Technology to Challenge Legal Discourses of Authorship and Property*, 1 E LAW (May 1994), <http://www.austlii.edu.au/au/other/elaw/v1no2/halbert.html>.

¹⁵² See, e.g., Marshall Leaffer, *Protecting Authors' Rights in a Digital Age*, 27 U. TOL. L. REV. 1, 3 (1995).

¹⁵³ 8 Anne, c. 19. See, e.g., Lyman Ray Patterson, *The Statute of Anne: Copyright Misconstrued*, 3 HARV. J. ON LEGIS. 223 (1966).

¹⁵⁴ See, e.g., Marshall Leaffer, *Protecting Authors' Rights in a Digital Age*, 27 U. TOL. L. REV. 1, 3 (1995); Peter Burger, *The Berne Convention: Its History and Its Key Role in the Future*, 3 J. LAW & TECH. 1, 5 (1988).

¹⁵⁵ See, e.g., Sharon Appel, *Copyright, Digitization Of Images, And Art Museums: Cyberspace and Other New Frontiers*, 6 UCLA ENT. L. REV. 149, 156 (1999).

¹⁵⁷ When the Act was adopted, there were no American authors who needed international copyright protection, and this approach—meant to foster the growth of an American publishing industry—let publishers infringe British copyrights “without paying royalties to authors from a country against which the United States had just revolted”.¹⁵⁸ For a century, American publishers pirated the works of foreign authors, which eventually had an unforeseen result: Pirated works could be sold so cheaply they created a market “that provided high quality foreign books at a price lower than an
¹⁵⁹ In 1891, the complaints of American authors finally led to the adoption of the Chace Act, which gave non-resident foreign authors copyright protection under American law.¹⁶⁰

What do these episodes have in common? And if such commonalities exist, what do they reveal about the prospects for achieving transnational consensus on outlawing at least the basic types of cybercrimes against persons and property?

Both episodes involved instances in which societies were willing to allow (or even encourage) their citizens to steal from citizens of other societies. In both, the focus was on crimes against property, not against persons; the motivation was purely economic.¹⁶¹ In both the conduct took place at the “margins” of the law: high-seas piracy occurred outside the territorial boundaries of any nation and therefore outside the scope of any laws; eighteenth-century American intellectual property piracy occurred at a time when the legal status of intellectual property as “property” was still evolving.¹⁶² Both types of conduct were outlawed when they became economically disadvantageous for the host countries; high-seas piracy was criminalized when it became a threat to the economic

¹⁵⁶ See *id.* at 156-156 (“It became the model for copyright law in the United States, and is reflected in both the Constitutional provision that authorizes Congress to legislate copyright protection, and the . . . Copyright Act of 1790”).

¹⁵⁷ Act of May 31, 1790, ch. 15, 1 Stat. 124,
<http://www.earlyamerica.com/earlyamerica/firsts/copyright/centinel.jpg>.

¹⁵⁸ Binyomin Kaplan, Note, *Determining Ownership of Foreign Copyright: A Three-Tier Proposal*, 21 CARDOZO L. REV. 2045, 2050 n. 18 (2000). See also Thomas Bender & David Sampliner, *Poets, Pirates, and the Creation of American Literature*, 29 N.Y.U. J. INT’L L. & POL. 255, 256-258 (1996-1997).

¹⁵⁹ Bender & Sampliner, *Poets, Pirates, and the Creation of American Literature*, *supra*, 29 N.Y.U. J. INT’L L. & POL. at 262.

¹⁶⁰ See Act of March 3, 1891, ch. 565, 26 Stat. 1106.

¹⁶¹ While high-seas piracy was a violent occupation, the infliction of injury and death was incidental to the primary goal of enriching the pirates and/or their sponsors.

¹⁶² See, e.g., Ronald A. Cass, *Copyright, Licensing, and the “First Screen”*, 5 MICH. TELECOMM. & TECH. L. REV. 35 (1999), <http://www.mttl.org/volfive/cass.html>. See also ADAM SMITH, AN INQUIRY INTO THE NATURE AND CAUSES OF THE WEALTH OF NATIONS 330-31 (R. H. Campbell & A. S. Skinner eds, Clarendon Press 1976) (1776).

advantages derivable from legitimate commerce; and America prohibited intellectual piracy of foreign works when it began to undermine the economic prospects of native authors and the value of domestic intellectual property.

One can, therefore, hypothesize that countries may be inclined to tolerate their citizens' victimizing citizens of other nations if (a) the conduct takes place at the "margins" of the law, that is, involves activity that is not definitely proscribed by an applicable set of legal standards and (b) results in a benefit to the victimizing nation. The former gives the victimizing nation at least plausible deniability when confronted with its tolerance of illegal activity; the latter is an obvious motive for tolerating the activity at issue, and may even reinforce the rationale given for tolerating that activity. That is, as to the latter proposition, the victimizing nation may assert, and may believe, that the activity in question is simply a reallocation of scarce resources from a wealthy nation to a poorer nation.

Countries are moving to adopt consensus crimes in certain areas. Significant progress has been made toward achieving consensus with regard to outlawing cybercrimes against property, and there is also a solid, and growing, consensus on outlawing the use of computers and the Internet to produce and disseminate child pornography. So far, neither crimes against persons nor obstruction of justice activities have been a focal point of the movement toward consensus crimes, but this will change, for the reasons set forth above.

There are areas in which consensus will not be achieved. Crimes against morality are the most systemically idiosyncratic types of crime because they are intrinsically bound up with a nation's religious and moral principles. It is true that the essentially-irresistible proliferation of the Internet will lead to some eroding of national moral proscriptions, some leveling in the definitions of crimes against morality, because it is more difficult for nations to maintain stringent standards of moral interdiction when their citizens are exposed to the permissive standards in force elsewhere. Countries have tried to avoid this outcome by restricting or eliminating access to the Internet,¹⁶³ but that is likely to prove futile.¹⁶⁴ The effects of this are apparent with regard to gambling, which already enjoys vastly increased legal and social acceptance as a result of online gambling.¹⁶⁵ This does not, of course, mean that a "reverse consensus" will develop which calls for the elimination of crimes against morality; indeed, the opposite will continue to be the case as, for example, online sales of alcohol and/or tobacco find acceptance in some countries but are outlawed in others. Past efforts to develop consensus crimes have been notably unsuccessful with regard to the articulation of offenses directed at gambling and other crimes against morality.

¹⁶³ See, e.g., R. Frank Lebowitz, *Internet Cafes Closed in Iran*, DIGITAL FREEDOM NETWORK (May 17, 2001) (Iranian officials closed Internet cafes "in order to purify materials which go awry

¹⁶⁴ See, e.g., Gary R. Bunt, *The Islamic Internet Souq*, Q-NEWS (Nov. 2000), <http://www.lamp.ac.uk/cis/liminal/virtuallyislamic/souqnov2000.html> ("the Internet is difficult to censor").

¹⁶⁵ See, e.g., Sarah Tippit, *Internet Gambling Grows at Torrid Rate Worldwide*, INFOSEC.COM (May 31, 2000), http://www.info-sec.com/commerce/00/commerce_053100d_j.shtml.

The same is true of a related area that involves the limitations which are placed on what can be disseminated online. Consensus generally exists as to the imposition of one such limitation, namely, prohibitions on creating, posting and disseminating child pornography, but child pornography seems destined to be a special case. Many countries do, of course, censor what can be posted on the Internet; some make it a crime to post prohibited material.¹⁶⁶ The forms this censorship assumes range from sweeping prohibitions designed to block the dissemination of political statements to narrowly-crafted statutes criminalizing the publication of particular types of material—such as racist/hate speech--on the Internet.¹⁶⁷ Relatively few countries fall into the first category but many outlaw the dissemination of racist/hate speech, which might lead one to assume that consensus could be achieved in this area. Indeed, a provision to this effect was proposed for inclusion in the Council of Europe's Draft Convention on Cyber Crime.¹⁶⁸ Like some other countries, the United States does not, indeed, cannot outlaw the dissemination of hate speech because of the strong protections its law accords free speech. Consequently, the attempt to include a prohibition on hate speech in the Draft Convention failed. As this episode demonstrates, consensus will almost certainly not be achieved with regard to content-based restrictions other than those targeting child pornography; and prohibitions on child pornography can be distinguished, to some extent at least, from other content-based prohibitions because the primary impetus behind laws against child pornography has traditionally been to address a crime against persons, i.e., the use of children in the production of pornography.

Nor will it be achieved with regard to prohibitions targeting online terrorism. The obstacle here is the divergent views countries take as to what is and is not a terrorist act. But while the failure to establish consensus crime categories encompassing terrorism *qua* terrorism may let the perpetrators of some terrorist acts avoid prosecution, nations can still pursue and prosecute them for the underlying crimes against persons and crimes against property they commit as part of terrorist agendas.

¹⁶⁶ See, e.g., Tony Taylor, *The Internet: The New Free Speech Battleground*, <http://www.cosc.georgetown.edu/~denning/cosc450/papers/taylor.html>. See also William Yurcik & Zixiang Tan, *The Great (Fire)Wall of China: Internet Security and Information Policy Issues*, TPRC, <http://www.tprc.org/abstracts/tan.txt>.

¹⁶⁷ See, e.g., Richard S. Rosenberg, *Free Speech on the Internet: Legal, Social and Political Issues*, 9 CSS JOURNAL (July/Sept. 2001), <http://www.webcom.com/journal/rosenber.html>.

¹⁶⁸ See *Racism and Xenophobia in Cyberspace – Motion for a Recommendation*, Parliamentary Assembly, Council of Europe (Nov. 7, 2000), <http://stars.coe.fr/doc/doc00/EDOC8886.htm> (motion calling for including in the Draft Convention on Cyber-Crime a provision defining “as criminal acts the distribution of racist and xenophobic materials, hate speech and racial discrimination on the Internet”).

D. BEYOND CONSENSUS CRIMES

*In the networked world, no island is an island.*¹⁶⁹

This lack of consensus postulated above will be the product of two mutually-exclusive phenomena: One—which will be the most common of the two—is the *failure* to achieve consensus at the national level, i.e., the failure by some nations to adopt the necessary body of core cybercrime legislation. This failure, in turn, will take at least two forms, one of which is attributable to national variations in the kinds of conduct that are criminally proscribed and in the ways criminal proscriptions are structured. This type of failure is the product of a conscious, intentional act: a country's reviewing its existing laws and affirmatively deciding not to incorporate certain cybercrime prohibitions because they are deemed to be inconsistent with those laws or with the penal philosophy responsible for them. This type of failure is most likely to occur in areas that have traditionally reflected idiosyncratic national values and concerns, such as the articulation of crimes against morality. One notable example of this type of failure is the United States' refusal to enact laws criminalizing racist/hate speech on the Internet, something many countries regard as an urgent priority. This type of failure is likely to be the least common of the two varieties of failure, at least for the foreseeable future.

The most common type of failure to achieve consensus will be inaction which is attributable to the fact that cybercrime is not an urgent priority for countries where few citizens have access to the Internet. Cybercrime is simply not being addressed in many of the countries around the world; very few of the nations of Africa, the Caribbean and Asia have considered cybercrime as a problem or as a potential problem. In a world where no island is an island, the failure of these nations to address the need for cybercrime legislation may have grave consequences for the rest of the world.

Failures to achieve consensus at the national level are unsurprising though still regrettable outcomes; transnational criminal law has, after all, never achieved perfect consensus on real world crimes. But the lack of consensus in outlawing cybercrimes may be the product of a different, rather more unusual phenomenon, namely, the *rejection* of efforts to persuade nations to adopt consistent, comprehensive cybercrime laws. This possibility raises a number of interesting conceptual issues.

The most obvious is the question of why a nation would deliberately reject the notion of adopting cybercrime legislation that would bring it into consensus with the penal laws adopted by other nations. The discussion above created a framework for answering this question; it derived two propositions from a review of historical instances in which citizens of one nation were allowed to—even encouraged to—prey on citizens of other nations. The propositions are that this type of behavior—which reflects a rejection of criminal proscriptions adopted by at least a subset of the other nations of the world—is most likely to occur: (a) when the conduct at issue exists at the margins of the law, i.e., involves conduct that has not been traditionally criminalized; and (b) when the conduct at issue produces some benefit—an economic benefit or another type of benefit—to the victimizing nation. These propositions can be used to hypothesize “consensus rejection scenarios” that explore the conditions under which nations might

¹⁶⁹ *Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information*, McConnell International, <http://www.mcconnellinternational.com/services/cybercrime.htm>.

deliberately rebuff efforts to achieve consensus in the proscription of cybercrimes. These scenarios are set out below.

Since economic benefits have traditionally been the driver of much criminal behavior, it is only logical to begin by considering how economic benefit might prompt a nation to refuse to proscribe some or all cybercrimes. The most obvious analogy here is to the “bank secrecy” havens that proliferated in the 1980’s. Bank secrecy laws became a source of economic benefit for some nations as others, notably the United States, began aggressively tracking the domestic flow of funds in an effort to target money laundering, tax evasion and drug trafficking. Countries discovered that strong bank secrecy laws were a marketable commodity which attracted deposits from those who—for whatever reasons—wished to shield the existence and career of their funds from government scrutiny.

How might the derivation of economic benefits lead to the creation of “cybercrime havens”? First of all, nations could derive economic benefits from their haven status in any of several ways: Their citizens and residents might emulate the American copyright pirates of the nineteenth century and illegally appropriate software and other intellectual property belonging to citizens of other nations. Or, the haven states might follow in the footsteps of the bank secrecy and high-seas pirate havens and profit from funds which the cybercriminals deposit and/or expend in their jurisdiction.

One example of this is already emerging: Countries in various parts of the world are competing to encourage online gambling server farms to physically locate within their borders—often by offering to lower the taxes assessed on the casinos—even as they recognize that gambling is illegal in most nations.¹⁷⁰ These countries see online casinos as an excellent source of revenue derivable from the gaming operations themselves which, as one source noted, represent “earnings which are dollar-based and generated from outside the economy and jurisdiction” which hosts the casino. They also tend to charge those seeking to establish online casinos in their territory exorbitant licensing and application fees that far exceed those assessed for other types of commercial activities. Like the high-seas pirates of the eighteenth century and the American copyright pirates of the nineteenth century, twenty-first century countries that host online casinos realize an economic benefit by letting the casinos prey upon citizens of other nations, nations that have most likely outlawed gambling within their own borders.

A nation might also use its status as a “cybercrime haven” to derive economic benefits in a rather more indirect fashion: The United States pays Israel and Egypt a combined total of \$5-6 billion dollars a year to maintain peace,¹⁷¹ and it gives Colombia, Bolivia and other South American countries hundreds of millions of dollars each year to

¹⁷⁰ See, e.g., National Centre For Academic Research Into Gaming, Project South Africa – Internet Gaming and South Africa: Implications, Costs, Opportunities 7-8, 22-23 (August 1999), <http://www.gamingtech.com/news/report.doc>.

¹⁷¹ See, e.g., Hamdesa Tuso, *Constructed on a Sand Foundation: The Crisis of U.S. Foreign Policy Toward the Horn of Africa During the Post Cold War Era – A Critical Review*, Part III, http://www.sidamaconcern.com/articles/us_policy3.html.

fight the war on drugs.¹⁷² So it is not difficult to imagine a scenario in which a country approached the United States and said, in effect, “we know our citizens are committing tens of millions in crimes perpetrated against Ebay, Amazon, and other United States interests but, unfortunately, we do not have the expertise needed to stop this activity. If you give us millions (or even billions) of dollars in support we will make an effort to do so.” The country would be using its status as a cybercrime haven to extort an economic benefit from the United States and/or other nations that were being victimized by the activities of its citizens and/or residents.

How might a nation go about becoming a “cybercrime haven”? It could do so by design or by default.

As to default, many of the former Soviet Republics are already major cybercrime havens already--de facto havens, not de jure. Their status as cybercrime havens results not only from what is often an absence of penal law that can be used to prosecute cybercrime activity but also from a paucity of cybercrime investigative experience and expertise, technical knowledge and forensic and computer hardware. These countries also decline to assist law enforcement officials seeking to apprehend cybercriminals operating within their borders; in one recent case Russian authorities repeatedly ignored FBI requests for assistance in apprehending Russian hackers who were breaking into the computers of U.S. companies as part of an ongoing extortion scam.¹⁷³

As to design, there are several ways this could be done: A nation desiring to become a cybercrime “extradition haven” might simply refuse to execute extradition treaties encompassing the commission of cybercrimes. It might direct its law enforcement officials not to cooperate with officials from other countries who were trying to secure evidence pertaining to the commission of cybercrimes against citizens of those countries. Or it might frustrate the application of extradition treaties by refusing to outlaw some or all cybercrimes. Or the haven country might exploit definitional problems, i.e., even though a treaty might be in force between Countries X and Y that provided for the extradition of those who commit economic crimes such as financial fraud, when asked to extradite certain persons Country Y could decline on the grounds that their activity constituted a cybercrime, not a financial fraud, and was therefore outside the scope of the treaty. A more imaginative approach would be for the haven state to set up an arrangement which lets cybercriminals who are physically located either in the haven state or elsewhere vector their criminal activities through the haven state in such a way that they are untraceable. This would effectively render their activities immune from the investigative efforts of law enforcement officials located in other countries. Pragmatically, this would be as effective as the non-extradition of offenders located within the haven state but it would also let the haven state extend its shield to encompass the activities of non-resident cybercriminals. In a sense, this is already

¹⁷² See, e.g., *The Effective National Drug Control Strategy 1999*, <http://www.csdp.org/edcs/page47.htm>; Steven Wisotsky, *A Society of Suspects: The War on Drugs and Civil Liberties*, POLICY ANALYSIS (Oct. 2, 1992), <http://www.cato.org/pubs/pas/pa-180.html>.

¹⁷³ See, e.g., Mike Bruner, *Cyberspace Evidence Seizure Upheld*, MSNBC (May 30, 2001), <http://stacks.msnbc.com/news/563379.asp> (“Eastern Europe and nations of the former Soviet Union have become a hotbed in recent years for computer crime aimed at businesses in the United States and other Western nations”).

happening; countries that do not keep log files or require their Internet Service Providers to do so effectively frustrate all cybercrime investigations because the perpetrator of a cybercrime cannot be traced back to a given IP address or machine.

The rise of cyberspace, of course, means that a crime haven no longer needs to be a conventional, land-based sovereignty. A haven might be a “virtual country,” and virtual countries have already been created.¹⁷⁴ A ship on the high seas or a platform built five hundred miles off the coast of Australia could be a server farm that evades current legal regimes while hosting cybercrime activities. Or the haven might be an airborne server farm that carried out a variety of network instructions while hovering over international waters; a great deal of illegal material could be switched and sent, and before the plane landed all hard drives could be erased and wiped so that forensics recovery was impossible.

What kinds of non-economic benefit might prompt a nation to become a “cybercrime haven”? The most obvious, of course, is the realization of some political benefit; the most likely scenario here would be for a country to shelter the activities of terrorists who use computer technology to carry out their activities. If the haven state’s motivations were purely non-economic, it might shield terrorism activities out of a sense of loyalty, of identification with the terrorist group’s agenda. Of course, the haven state could also act out of mixed motives, at once sympathizing with the terrorist group’s agenda and profiting from the terrorist group’s presence and/or from hosting its cyber-terrorist activity.

One can postulate yet another scenario in which a country becomes a cybercrime haven for other than economic reasons: A country—like the United States—which has strong laws protecting freedom of expression can become a haven for those who wish to express views that are outlawed elsewhere in the world. Many countries outlaw the dissemination of racist/hate speech,¹⁷⁵ and, indeed, a provision to this effect was proposed for inclusion in the Council of Europe’s Convention on Cybercrime.¹⁷⁶ The proposal failed due in large part to opposition from the United States.¹⁷⁷ Because of its

¹⁷⁴ See, e.g., Bertil Lintner, *Cyberfraud – The Fictitious “Domain of Melchizedek”*, http://www.infowar.com/law/99/law_060299a_j.shtml

¹⁷⁵ See, e.g., Brendan Fowler, et al., Can You Yahoo!? The Internet’s Digital Fences, 2001 DUKE L. & TECH. REV. 0012, <http://www.law.duke.edu/journals/dltr/articles/2001dltr0012.html>.

¹⁷⁶ See Racism and Xenophobia in Cyberspace – Motion for a Recommendation, Parliamentary Assembly, Council of Europe (Nov. 7, 2000), <http://stars.coe.fr/doc/doc00/EDOC8886.htm> (motion calling for including a provision defining “as criminal acts the distribution of racist and xenophobic materials, hate speech and racial discrimination on the Internet). See also COUNCIL OF EUROPE – PARLIAMENTARY ASSEMBLY, SPRING SESSION (23-27 APRIL 2001), REPORT OF DEBATES OF THE SECOND PART OF THE 2001 ORDINARY SESSION (24 APRIL 2001), http://www.cyber-rights.org/documents/coe_assembly.htm.

¹⁷⁷ See COUNCIL OF EUROPE – PARLIAMENTARY ASSEMBLY, SPRING SESSION (23-27 APRIL 2001), REPORT OF DEBATES OF THE SECOND PART OF THE 2001 ORDINARY SESSION (24 APRIL 2001), http://www.cyber-rights.org/documents/coe_assembly.htm. The Council of Europe subsequently “decided to draw up an additional Protocol” to the Convention on Cybercrime that addresses hate speech. See COUNCIL OF EUROPE, COMMITTEE OF EXPERTS ON THE CRIMINALISATION OF ACTS OF RACIST OF [S/C] XENOPHOBIC NATURE COMMITTED THROUGH COMPUTER NETWORKS (PC-RX), SPECIFIC TERMS OF REFERENCE 2 (December 13, 2001). If adopted, it would be a separate legal instrument, so countries could sign the Convention without binding themselves to enforce the Protocol. See, e.g., U.S. Department of Justice, Frequently Asked

strong First Amendment protections for free speech, the United States is, in a sense, a haven for those who create and maintain web sites that disseminate hate speech, racist views, Nazi and Neo-Nazi philosophies and other viewpoints the expression of which are outlawed by other nations.

This notion that a country can be a “cybercrime speech haven” implicates the second proposition set out above, namely, that a country is more likely to host illegal activity, which may involve letting its citizens prey on citizens of other countries, when the activity at issue exists on the margins of the law, i.e., has not been traditionally defined as a “crime.” This is certainly true of the racist/hate speech laws that are found in some nations but that would be unconstitutional in the United States; it can also be true, at least to some extent, of cyberterrorism activities since there is some disagreement at the transnational level as to what does, and does not, constitute “terrorism.” The definition of political offenses and of crimes against morality tends to be more idiosyncratic than the definition of crimes against persons and crimes against property, which means that a haven state’s conduct with regard to activities falling into the first two categories may not be so clearly regarded as tolerating or even facilitating illegal conduct as would conduct pertaining to crimes against persons or crimes against property.

Why is this important? It is important because it gives the haven state plausible deniability. If, say, a nation refused to sign a cybercrime *extradition* treaty in order to set itself up as a cybercrime haven, it would no doubt prefer to predicate its refusal on some at least ostensibly neutral principle, such as the argument that the offenses encompassed by the treaty were not “crimes” under its historical penal law. If such a nation were take an indirect approach to becoming a cybercrime haven—such as allowing cybercriminals to vector their activities through facilities it maintained—it might prefer to be able to claim ignorance as to the criminality of the activities at issue.

II. CONCLUSION

Cybercrime presents the nations of the world with a problem they have never had to address before, i.e., the permeability of national borders. As long as crime remained a “real world” phenomenon which required the commission of some overt act or omission which, by definition, had a circumscribed geographical reach, localized, idiosyncratic criminal laws were sufficient to protect a nation’s citizens from those who would do them harm.

It is true, of course, that the rise of modern transportation—planes, trains, ships and automobiles—made it possible for criminals to commit offenses in one country and then flee to another. Nations responded to this phenomenon by developing extradition treaties which allowed the country in which a miscreant took refuge to hand him or her off to the country whose citizens had been victimized, as long as certain conditions-- notably the proscription of the conduct at issue by both countries--were met. The

Questions and Answers About the Council of Europe Convention on Cybercrime (Final Draft, released June 29, 2001), C-5 (July 10, 2001) (“if the U.S. decides to become a signatory to the Convention, it is not required to adopt the Protocol”).

requirement of dual criminality was seldom an obstacle under these extradition regimes—until recently—because the crimes at issue were “real world” crimes and there are basic commonalities in the structure of penal codes developed to deal with “real

As the “Love Bug” episode demonstrated, the varieties of cybercrime can make the operation of these regimes problematic. The obstacle that barred efforts to prosecute the accused architect of the “Love Bug” in any of the countries that were victimized by his efforts was inadvertent, the Philippines’ unintentional failure to have adopted even the most basic of cybercrime prohibitions. If future “Love Bug” episodes are to be avoided, countries must work together to devise a set of core consensus crimes that can be used to pursue cybercriminals wherever they may operate.