Journal of Criminal Law and Criminology

Volume 97
Issue 2 *Winter*

Article 2

Winter 2007

At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare

Susan W. Brenner

Follow this and additional works at: https://scholarlycommons.law.northwestern.edu/jclc

 Part of the Criminal Law Commons, Criminology Commons, and the Criminology and Criminal Justice Commons

Recommended Citation

Susan W. Brenner, At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare, 97 J. Crim. L. & Criminology 379 (2006-2007)

This Symposium is brought to you for free and open access by Northwestern University School of Law Scholarly Commons. It has been accepted for inclusion in Journal of Criminal Law and Criminology by an authorized editor of Northwestern University School of Law Scholarly Commons.

0091-4169/07/9702-0379
THE JOURNAL OF CRIMINAL LAW & CRIMINOLOGY
Vol. 97, No. 2
Copyright © 2007 by Northwestern University, School of Law
Printed in U.S.A.

"AT LIGHT SPEED": ATTRIBUTION AND RESPONSE TO CYBERCRIME/TERRORISM/WARFARE

SUSAN W. BRENNER*

This Article explains why and how computer technology complicates the related processes of identifying internal (crime and terrorism) and external (war) threats to social order of responding to those threats. First, it divides the process—attribution—into two categories: what-attribution (what kind of attack is this?) and who-attribution (who is responsible for this attack?). Then, it analyzes, in detail, how and why our adversaries' use of computer technology blurs the distinctions between what is now cybercrime, cyberterrorism, and cyberwarfare. The Article goes on to analyze how and why computer technology and the blurring of these distinctions erode our ability to mount an effective response to threats of either type. Finally, it explores ways in which we can modify how we currently divide responsibility for identifying and responding to the three threat categories among law enforcement and the military, respectively. The goal here is to identify techniques we can use to improve attribution and response processes for emerging cyberthreats.

I. INTRODUCTION

> The speed and anonymity of cyber attacks makes distinguishing among the actions of terrorists, criminals, and nation states difficult . . . .[1]

In October 2006, a "sensitive Commerce Department bureau"—the Bureau of Industry and Security (BIS)—suffered a "debilitating attack on its computer systems."[2] The attack forced the BIS to disconnect its

* NCR Distinguished Professor of Law & Technology, University of Dayton School of Law.

[1] THE WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE 19, 64 (2003), *available at* http://www.whitehouse.gov/pcipb/ ("Cyber attacks cross borders at light speed . . . .").

[2] Alan Sipress, *Computer System Under Attack*, WASH. POST, Oct. 6, 2006, at A21, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/10/05/AR2006

computers from the Internet, which interfered with its employees' ability to perform their duties.[3] It was traced to websites hosted by Chinese Internet service providers (ISPs), but the attackers were never identified.[4]

Consider for a moment the statement: the attackers were never identified. This statement has several implications, the most obvious of which is that the *individuals* who carried out the attack were never identified. That is far from remarkable; given the opportunities cyberspace creates for the remote commission of attacks and attacker anonymity, it is more common than not for cybercriminals to go unidentified and unapprehended.[5]

That, though, assumes we are dealing with cybercriminals, which brings us to another implication of the statement above: Not only were the BIS attackers never identified, the *nature* of the attack was never identified. It was apparently clear the attack came from China,[6] but what kind of attack was it? Was it cybercrime—the Chinese hackers launching a counting coup[7] on U.S. government computers? Was it cyberterrorism—an initial effort toward a takedown of U.S. government computers by terrorists (who may or may not have been Chinese) pursuing idiosyncratic ideological goals? Or was it cyberwarfare—a virtual sortie by People's Liberation Army hackers?[8]

100501781.html ("[T]he Bureau of Industry and Security . . . is responsible for controlling U.S. exports of commodities, software and technology having both commercial and military uses.").

[3] *Id.* "A source familiar with the security breach said the hackers had penetrated the computers with a 'rootkit' program, a stealthy form of software that allows attackers to mask their presence and then gain privileged access to the computer system." *Id.* The BIS computers were so compromised that officials decided they could not be salvaged, so they will be replaced with "clean hardware and clean software." *Id.*

[4] *Id.*

[5] *See* Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security*, 10 B.U. J. SCI. & TECH. L. 1, 65-76 (2004) [hereinafter Brenner, *Toward a Criminal Law for Cyberspace*].

[6] Sipress, *supra* note 2 ("The attacks were traced to Web sites registered on Chinese Internet service providers, Commerce officials said."). Cyberattackers can route their attacks through intermediate systems to disguise the true originating point of an attack. *See, e.g.*, *Tiny Nevada Hospital Attacked by Russian Hacker*, USA TODAY, Apr. 7, 2003, *available at* http://www.usatoday.com/tech/webguide/internetlife/2003-04-07-hospital-hack_x.htm (reporting that the Russian hacker routed an attack on a Nevada hospital through Al-Jazeera's website to make it appear the attack came from Qatar).

[7] Counting coup—Wikipedia, http://en.wikipedia.org/wiki/Counting_coup (last visited Apr. 21, 2007).

[8] *See, e.g.*, Dawn S. Onley & Patience Wait, *Red Storm Rising*, GOV'T COMPUTER NEWS, Aug. 21, 2006, *available at* http://www.gcn.com/print/25_25/41716-1.html; John Rogin, *China Fielding Cyberattack Units*, FCW.COM, May 25, 2006, http://www.fcw.com/article94650-05-25-06-Web; *see also* JOHN ROLLINS & CLAY WILSON,

The BIS episode illustrates why we need to assess how we approach attribution (Who launched the attack? What kind of attack is it?) and the corresponding problem of response (Who should respond to an attack—civilian law enforcement, the military, or both?). As Sections II, III, and IV explain, the essentially ad hoc approaches we currently use for both attribution and response worked well in the past but are becoming increasingly unsatisfactory as cyberspace becomes a viable vector for attacks, of whatever type.

My goal in this Article is to explore these issues in terms of the conceptual and legal issues they raise. I will also analyze some non-traditional ways of structuring our response to ambiguous attacks, such as the one that targeted the BIS computers. My hope is that this Article provides a basis for further discussion of these issues, the complexity of which puts their ultimate resolution outside the scope or ambitions of any single law review article.

Section II constructs a taxonomy of cyberthreats (crime, terrorism, and war) and explains why these evolving threat categories can make who- and what-attribution problematic. Section III explains how these difficulties with attribution impact the process of responding to cyberthreats. Section IV continues our examination of this issue by analyzing how we might improve our response capability without surrendering principles we hold dear. Section V is a brief conclusion, which summarizes the preceding arguments and analysis and offers some final thoughts on both.

II. IDENTIFYING CYBERCRIME, CYBERTERRORISM, AND CYBERWARFARE: TAXONOMY

> [T]he . . . "blurring of crime and war" at the operational level. . . . has accelerated over the last few decades.[9]

As Section I noted, the continuing evolution and proliferation of computer technology has created a new class of threats—"cyberthreats"—which societies must confront. These cyberthreats can be generically defined as using computer technology to engage in activity that undermines a society's ability to maintain internal or external order.[10]

CONG. RESEARCH SERV., TERRORIST CAPABILITIES FOR CYBERATTACK: OVERVIEW AND POLICY ISSUES 14-15 (2005), *available at* http://www.fas.org/sgp/crs/terror/RL33123.pdf.

[9] Robert J. Bunker, *Combatants or Non-Combatants?*, J. INT'L PEACE OPERATIONS, July 2006, at 17, *available at* http://ipoaonline.org/journal/index.php?option=com_content&task=view&id=96&Itemid=28.

[10] *See* Brenner, *Toward a Criminal Law for Cyberspace*, *supra* note 5, at 6-49.

Societies have historically used a two-pronged strategy to maintain the order they need to survive and prosper. Societies maintain internal order by articulating and enforcing a set of proscriptive rules (criminal law enforcement) that discourage the members of a society from preying upon each other in ways that undermine order, such as by killing, robbing, or committing arson.[11] Societies maintain external order by relying on military force (war) and, to an increasing extent, international agreements.[12] I call this the internal-external threat dichotomy, and the choice between law enforcement and military the attack-response dynamic.

As we will see, computer technology erodes the empirical realities that generated and sustain this dichotomous approach to maintaining order. This approach is based on the assumption that each society occupies a territorially-defined physical locus—that, in other words, sovereignty and "country" are indistinguishable.[13] One consequence of the presumptive isomorphism between sovereignty and territory is that threats to social order are easily identifiable as being *either* internal (crime/terrorism) or external (war). Computer-mediated communication erodes the validity of this binary decision tree by making territory increasingly irrelevant; as a study of cybercrime laws noted, "In the networked world, no island is an island."[14] In the twenty-first century, those bent on undermining a society's ability to maintain order can launch virtual attacks from almost anywhere in the world. As a result, these attacks may not fit neatly into the internal-external threat dichotomy and the attribution hierarchy (crime/terrorism, war) derived from that dichotomy.

Section II outlines a taxonomy of the three categories of cyberthreats: cybercrime, cyberterrorism, and cyberwarfare. Section III explains how these online variations of real-world threat categories challenge the processes we currently use for threat attribution.

A. CYBERCRIME

An online dictionary defines "cybercrime" as "a crime committed on a computer network."[15] The basic problem with this definition is that

---

[11] *See id.*

[12] *See id.*

[13] *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 201 (1987); *see, e.g.*, BLACK'S LAW DICTIONARY 377 (8th ed. 2004) (defining "country" as "a nation or political state"); *see also* Country—Wikipedia, http://en.wikipedia.org/wiki/Country (last visited Apr. 21, 2007).

[14] MCCONNELL INT'L, CYBER CRIME . . . AND PUNISHMENT? ARCHAIC LAWS THREATEN GLOBAL INFORMATION 8 (2000), *available at* http://www.witsa.org/papers/McConnell-cybercrime.pdf.

[15] Cybercrime—definitions from Dictionary.com, http://dictionary.reference.com/

American lawyers need to be able to fit the concept of "cybercrime" into the specific legal framework used in the United States and into the more general legal framework that ties together legal systems around the world in their battle against cybercrime.[16] That leads me to ask several questions: Is cybercrime different from regular crime? If so, how? If not, if cybercrime is merely a boutique version of crime, why do we need a new term for it?

The first step in answering these questions is parsing out what cybercrime is and what it is not. When we do this, we see that the definition quoted above needs to be modified for two reasons.

The first reason is that this definition assumes every cybercrime constitutes nothing more than the commission of a traditional crime by non-traditional means (using a computer network instead of, say, a gun). As I have argued elsewhere,[17] that is true for much of the cybercrime we have seen so far. For example, online fraud such as the 419 scam[18] is nothing new as far as the law is concerned; it is simply "old wine in new bottles."[19] Until the twentieth century, people had only two ways of defrauding others: they could do it face to face by offering to sell someone the Brooklyn Bridge for a *very* good price; or they could do the same thing by using snail mail.[20] The proliferation of telephones in the twentieth century made it possible for scam artists to use the telephone to sell the bridge, again at a *very* good price.[21] And we now see twenty-first century versions of the same scams migrating online.

The same is happening with other traditional crimes, such as theft, extortion, harassment, and trespassing.[22] Indeed, it seems reasonable to

---

browse/cybercrime (last visited Apr. 21, 2007).

[16] It might be more accurate to cite the *evolving* framework that is intended to unite legal systems in the battle against cybercrime. *See* Convention on Cybercrime, Council of Europe, Nov. 23, 2001, C.E.T.S. No. 185, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm [hereinafter Convention on Cybercrime Treaty]; Convention on Cybercrime, Council of Europe, Signatures and Ratifications, Nov. 23, 2001, C.E.T.S. No. 185, *available at* http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=12/11/2006&CL=ENG.

[17] *See* Susan W. Brenner, *Is There Such a Thing as Virtual Crime?*, 4 CAL. CRIM. L. REV. 1 ¶¶ 120-29 (2001), http://www.boalt.org/CCLR/v4/v4brenner.htm [hereinafter Brenner, *Virtual Crime*].

[18] *See* Advance fee fraud—Wikipedia, http://en.wikipedia.org/wiki/Advance_fee_fraud (last visited Apr. 21, 2007); Nigeria—The 419 Coalition Website, http://home.rica.net/alphae/419coal/ (last visited Apr. 21, 2007).

[19] *See* Advance fee fraud—Wikipedia, *supra* note 18.

[20] *See, e.g.*, DAVID W. MAURER, THE BIG CON 31-102 (1999).

[21] *See, e.g.*, FED. TRADE COMM'N, PUTTING TELEPHONE SCAMS . . . ON HOLD (2004), *available at* http://www.ftc.gov/bcp/conline/pubs/tmarkg/target.htm.

[22] *See* Brenner, *Virtual Crime*, *supra* note 17, ¶¶ 39-50, 61-68.

believe that many, if not most, of the crimes with which we have traditionally dealt will migrate online in some fashion. Admittedly, a few traditional crimes—such as rape and bigamy—probably will not migrate online because the commission of these particular crimes requires physical activity that cannot occur online (unless, of course, we revise our definition of bigamy to encompass virtual bigamy).[23]

The same cannot be said of homicide: while we have no documented cases in which computer technology was used to take human life, this scenario is certainly conceivable and will no doubt occur.[24] Those who speculate on such things have postulated instances in which someone would hack into the database of a hospital and kill people by altering the dosage of their medication.[25] The killer would no doubt find this a particularly clever way to commit murder because the crime might never be discovered. The deaths might well be put down to negligence on the part of hospital staff;[26] and even if they were identified as homicide, it might be very difficult to determine which of the victims were the intended targets of the unknown killer and thereby begin the investigative process.

My point is that while most of the cybercrime we have seen to date is simply the commission of traditional crimes by new means, this will not be true of *all* cybercrime. We already have at least one completely new cybercrime: a distributed denial of service (DDoS) attack. A DDoS attack overloads computer servers and "make[s] a computer resource [such as a website] unavailable to its intended users."[27] In February 2000, a Canadian known as "Mafiaboy" launched attacks that effectively shut down websites operated by CNN, Yahoo!, Amazon.com, and eBay, among others.[28]

---

[23] *Id.* ¶¶ 104-26.

[24] There are reports of attempts to use computer technology to cause injury or death: "[H]ackers have infiltrated hospital computers and altered prescriptions . . . . [A] hacker prescribed potentially lethal drugs to a nine-year old boy who was suffering from meningitis. The boy was saved only because a nurse caught the deviation prior to the drug being administered." Howard L. Steele, Jr., *The Prevention of Non-Consensual Access to "Confidential" Health-Care Information in Cyberspace*, 1 COMP. L. REV. & TECH. J. 101, 102 (1997), *available at* http://www.smu.edu/csr/Steele.pdf. This same interloper had also prescribed unnecessary antibiotics to a seventy-year-old woman. *Id.*

[25] *Stealing the Network: How to Own A Continent* outlines a creative cyber-homicide scenario: *Uber*-hacker Bob Knuth tricks Saul, a student, into hacking into a hospital's wireless network. FX ET AL., STEALING THE NETWORK: HOW TO OWN A CONTINENT 39-75 (2004).

[26] *See id.*

[27] Denial of service attack—Wikipedia, http://en.wikipedia.org/wiki/Denial-of-service_attack (last visited Apr. 21, 2007).

[28] *See, e.g.*, Pierre Thomas & D. Ian Hopper, *Canadian Juvenile Charged in Connection with February "Denial of Service" Attacks*, CNN.COM, Apr. 18, 2000, http://archives.cnn.com/2000/TECH/computing/04/18/hacker.arrest.01/.

DDoS attacks are increasingly used for extortion.[29] Someone launches an attack on a website, then stops the attack and explains to the website owner that the attack will continue unless and until the owner pays a sum for "protection" against such attacks.[30] This is the commission of an old crime (extortion) by a new means, little different from tactics the Mafia used over half a century ago, though they relied on arson instead.[31]

But a "pure" DDoS attack, such as the 2000 attacks on Amazon.com and eBay, is not a traditional crime. It is not theft, fraud, extortion, vandalism, burglary, or any crime that was within a pre-twentieth century prosecutor's repertoire.[32] It is an example of a new type of crime: a "pure" cybercrime.[33] As such, it requires that we create new law that would make it a crime to launch such an attack.[34]

To summarize, one reason why the definition quoted above is unsatisfactory is that it does not encompass the proposition that cybercrime can consist of committing "new" crimes—crimes we have not seen before and therefore have not outlawed—as well as "old" crimes. The other reason I take issue with this definition is that it links the commission of cybercrime with the use of a computer network.[35]

Certainly, use of computer networks is usually true for cybercrime. In fact, it is probably the default model of cybercrime. But it is also possible that computer technology, not network technology, can be used for illegal purposes. A non-networked computer can, for example, be used to counterfeit currency or to forge documents.[36] In either instance, a

---

[29] *See, e.g.*, MCAFEE NA VIRTUAL CRIMINOLOGY REPORT 6-19 (2005), *available at* http://www.softmart.com/mcafee/docs/McAfee%20NA%20Virtual%20Criminology%20Report.pdf; Paul McNamara, *Addressing "DDoS Extortion,"* NETWORK WORLD, May 23, 2005, *available at* http://www.networkworld.com/columnists/2005/052305buzz.html; Jose Nazario, *Cyber Extortion, A Very Real Threat*, IT-OBSERVER, June 7, 2006, http://www.it-observer.com/articles/1153/cyber_extortion_very_real_threat/.

[30] *See, e.g.*, Erik Larkin, *Web of Crime: Enter the Professionals*, PC WORLD, Aug. 22, 2005, *available at* http://pcworld.about.com/news/Aug222005id122240.htm.

[31] *See, e.g.*, PRESIDENT'S COMM'N ON LAW ENFORCEMENT AND ADMIN. OF JUSTICE, CRIME IN A FREE SOCIETY: EXCERPTS FROM THE PRESIDENT'S COMMISSION ON LAW ENFORCEMENT AND ADMINISTRATION OF JUSTICE 192-209 (1968).

[32] *See* Brenner, *Virtual Crime*, *supra* note 17, ¶¶ 73-76.

[33] *See id.*

[34] Otherwise, there is no crime. In fact, until recently this was the case in the United Kingdom: the U.K.'s 1990 Computer Misuse Act outlawed hacking and other online variants of traditional crime, but it did not address DDoS attacks. Tom Espiner, *U.K. Outlaws Denial-of-Service Attacks*, CNET NEWS.COM, Nov. 10, 2006, http://news.com.com/2100-7348_3-6134472.html.

[35] *See* Cybercrime—definitions, *supra* note 15.

[36] *See, e.g.*, Convention on Cybercrime Treaty, *supra* note 16; United States Secret Service: Know Your Money—Counterfeit Awareness, http://www.secretservice.gov/

computer—but not a computer network—is being used to commit a crime. Here, the computer is being used to commit an "old" crime, but it is at least conceptually possible that a non-networked computer could be used to commit a "new" crime of some type.

Thus, a better definition of cybercrime is the use of computer technology to commit crime; to engage in activity that threatens a society's ability to maintain internal order. This definition encompasses both traditional and emerging cybercrimes. It also encompasses *any* use of computer technology, not merely the use of networked computer technology.

This generic definition does not, of course, provide the legal predicate needed to respond to cybercrime, as it is a conceptual definition of a category of crime rather than the definition of a particular offense or particular offenses. To ensure they can respond to new types of cybercrime, societies must monitor online activity in an effort to identity emerging activities that constitute a threat to their ability to maintain internal order. Once identified, these activities should be criminalized, just as the United Kingdom recently criminalized DDoS attacks.[37]

B. CYBERTERRORISM

> [G]et ready . . . . terrorists are preparing . . . cyberspace based attacks . . . .[38]

Generically, cyberterrorism consists of using computer technology to engage in terrorist activity.[39] This definition mirrors the generic definition of cybercrime articulated in the previous section, which is appropriate given that societies treat terrorism as a type of crime. However, societies conflate crime and terrorism because both threaten their ability to maintain internal order. The assumption, which derives from the dichotomy noted earlier, is that all threats to internal order should be dealt with in the same way.[40]

---

money_technologies.shtml (last visited Apr. 21, 2007).

[37] *See, e.g.*, Espiner, *supra* note 34.

[38] John Arquilla, *Waging War Through the Internet*, S.F. CHRON, Jan. 15, 2006, at E1, *available at* http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2006/01/15/ING2AGLP021.DTL [hereinafter Arquilla, *Waging War Through the Internet*].

[39] *See, e.g.*, CLAY WILSON, CONG. RESEARCH SERV., COMPUTER ATTACK AND CYBERTERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS (2005).

[40] For the proposition that crime and terrorism both threaten internal order, see *supra* Section I.

The move to criminalize terrorism began in the 1930s as a reaction to the assassination of King Alexander I of Yugoslavia. *See* Ben Saul, *The Legal Response of the League of Nations to Terrorism*, 4 J. INT'L CRIM. JUST. 78, 79 (2006). It resulted in the adoption of the 1937 League of Nations' Convention for the Prevention and Punishment of Terrorism, which required parties to adopt legislation criminalizing terrorism. *See* Reuven Young, *Defining*

Although societies conflate crime and terrorism, we need to distinguish them because they differ in ways that are relevant to how societies need to respond to them. Basically, crime is personal while terrorism is political.[41] Crimes are committed for individual and personal reasons, the most important of which are personal gain and the desire or need to harm others psychologically and/or physically.[42]

Terrorism often results in the infliction of harms indistinguishable from those caused by certain types of crime (such as death, personal injury, or property destruction), but the harms are inflicted for very different reasons.[43] A federal statute, for example, defines "terrorism" as committing acts constituting crimes under the law of any country to intimidate or coerce a civilian population; to influence government policy by intimidation or coercion; or to affect the conduct of government by mass destruction, assassination, or kidnapping.[44] We will return to the issue of terrorism-as-crime in a moment, but first we need to focus on what precisely is involved in the commission of terrorist acts.

As the above definition suggests, terrorism is usually intended to directly or indirectly demoralize a civilian population;[45] this distinguishes

---

Terrorism: The Evolution of Terrorism as a Legal Concept in International Law and Its Influence on Definitions in Domestic Legislation, 29 B.C. INT'L & COMP. L. REV. 23, 35-36 (2006). One proponent of the 1937 Convention, Czechoslovakia, said that "criminalization was necessary to protect 'security of life and limb, health, liberty and public property intended for the common use.'" Saul, *supra*, at 81 (quoting J. Starke, *The Convention for the Prevention and Punishment of Terrorism*, 19 BRITISH YEAR BOOK INT'L. L. 60 (1938)). As one author noted, "Ordinary criminal offences aim to achieve the same object." Saul, *supra*, at 82.

The 1937 Convention never went into effect, but its approach proved influential; its successor, the United Nations, has consistently defined terrorism as criminal activity. *See* Young, *supra*, at 36-40; *see, e.g.*, G.A. Res. 49/60, U.N. Doc. A/RES/49/60 (Feb. 17, 1995), *available at* http://www.un.org/documents/ga/res/49/a49r060.htm.

[41] *See, e.g.*, PAUL R. PILLAR, TERRORISM AND U.S. FOREIGN POLICY 13-14 (2001).

[42] *Id.*

[43] *See, e.g.*, Pippa Norris, Montague Kern & Marion Just, *Introduction: Framing Terrorism*, *in* FRAMING TERRORISM: THE NEWS MEDIA, THE GOVERNMENT, AND THE PUBLIC 3, 8 (Pippa Norris, Montague Kern & Marion Just eds., 2003) [hereinafter FRAMING TERRORISM] (distinguishing terrorism from "crimes motivated purely by private gain, such as blackmail, murder, or physical assault directed against individuals, groups, or companies, without any political objectives").

[44] 18 U.S.C. § 2331 (2000). For more definitions, see, e.g., Mohammad Iqbal, *Defining Cyberterrorism*, 22 J. MARSHALL J. COMPUTER & INFO. L. 397 (2004).

[45] We are familiar with terrorist acts that are intended directly to demoralize a civilian population, such as the 9/11 attacks in the United States and the 3/11 Madrid bombings. In both instances, violence was used for symbolic purposes, and the goal was to shock and demoralize the populace of societies with which Al-Qaeda deems itself to be at war—an ideological war aimed at allowing the restoration of the "ancient Islamic caliphate." *See*

terrorism from warfare, which is not supposed to target civilians.[46] In the real-world, terrorism usually achieves its primary goal[47] of demoralizing civilians by destroying property and injuring or killing civilians.[48] The 9/11 attacks on the World Trade Center are a perfect example of real-world

---

LAWRENCE WRIGHT, THE LOOMING TOWER: AL-QAEDA AND THE ROAD TO 9/11 175, 234-35 (2006); *see also* Norris, Kern & Just, *supra* note 43, at 7-8.

The goal in these and similar attacks is to demoralize civilians by directly demonstrating their vulnerability through the inability of their government to protect them from seemingly random violence. One source explains how this demoralization ties into the terrorists' goals:

> Terrorists may create . . . fear . . . to influence their negotiations with . . . governments, but fear has secondary consequences that further undermine government authority . . . . [F]ear fragments and isolates society into anxious groups of individuals concerned only with their personal survival . . . "Terrorism destroys the solidarity, cooperation, and interdependence on which social functioning is based, and substitutes insecurity and distrust." The breakdown of social trust and cooperation could have serious effects on how society functions.

Leonie Huddy et al., *Fear and Terrorism*, *in* FRAMING TERRORISM, *supra* note 43, at 255, 255 (quoting Martha C. Hutchinson, *The Concept of Revolutionary Terrorism*, 6 J. CONFLICT RESOL. 288 (1973)); *see also* INFORMATION OPERATIONS: WARFARE AND THE HARD REALITY OF SOFT POWER 92 (Leigh Armistead ed. 2004) [hereinafter INFORMATION OPERATIONS] ("[T]errorism is an attack on the legitimacy of the established order."). For more on this, see *infra* Sections II.B.2-3.

[46] *See* U.N. Office of the High Comm'r for Human Rights, *Geneva Convention Relative to the Protection of Civilian Persons in Time of War*, Aug. 12, 1949, *available at* http://www.unhchr.ch/html/menu3/b/92.htm; *see also* Terrorism—Wikipedia, http://en.wikipedia.org/wiki/Definition_of_terrorism (last visited Apr. 21, 2007).

[47] It is important to realize—especially when analyzing cyberterrorism—that terrorists also have secondary goals. Their secondary goals involve the successful conducting of activities that sustain and promote their ability to work toward achieving their primary goal. These goals include disseminating propaganda; recruiting news members of a terrorist group and retaining existing members; fundraising to support terrorist activities and the terrorists themselves; training terrorists in attack strategies; coordinating attacks; and researching attack targets. *See, e.g.*, EBEN KAPLAN, COUNCIL ON FOREIGN REL., TERRORISTS AND THE INTERNET (2006), *available at* http://www.cfr.org/publication/10005/; *see also* U.S. DEP'T OF STATE, COUNTRY REPORTS ON TERRORISM 2005 17 (2006), *available at* http://www.state.gov/documents/organization/65462.pdf [hereinafter COUNTRY REPORTS ON TERRORISM 2005] ("Terrorists exploit electronic infrastructure . . . for recruitment, training, planning, resource transfer, and intelligence collection between and among . . . terrorist groups . . . . Harnessing the Internet's potential for speed, security, and global linkage gives terrorists the ability to conduct many of the activities that once required physical haven, yet without the associated security risks. With the ability to communicate, recruit, train, and prepare for attacks, any computer may function essentially as a 'virtual' safe haven.").

This Article focuses exclusively on terrorists' use of computer technology to further their primary goal of demoralizing civilians for two reasons: 1) brevity; and 2) using computer technology to further primary goals is the essence of cyberterrorism.

[48] "[A]cts done to advance an ideological . . . cause and to induce terror in any population . . . are terrorism if they cause one of the following outcomes: death or serious injury; serious risk to public health or safety; destruction or serious damage to property." Young, *supra* note 40, at 86 (summarizing Terrorism Suppression Act, 2002, § 5 (N.Z.)).

terrorism; they were intended to destroy a premier symbol of capitalism and in so doing undermine the morale of U.S. citizens and the stability of the U.S. society.[49]

To date, there have been no known instances of cyberterrorism.[50] There have been cases which media has incorrectly described as cyberterrorism: in 2000, an Australian man hacked into a municipal waste-management system and dumped "millions of litres of raw sewage" into parks, rivers, and businesses.[51] Elsewhere, in 1997 a Massachusetts hacker shut down all communications to a Federal Aviation Administration (FAA) control tower at an airport for six hours.[52] These and similar cases, however, involved *cybercrime*, not cyberterrorism. In each instance, the perpetrator acted out of individual motivations—a desire for revenge or power—instead of out of a desire to advance a particular ideology by demoralizing segments of a civilian population.[53]

To understand what cyberterrorism can and will be, we must parse out how terrorists can use computer technology to demoralize a civilian population and thereby undermine a society's ability to sustain internal order.[54] Conceptually, computer technology's use for this purpose falls into

---

[49] *See, e.g.*, WRIGHT, *supra* note 45, at 308.

[50] *But see* Arquilla, *Waging War Through the Internet*, *supra* note 38, at E1.

[51] Tony Smith, *Hacker Jailed for Revenge Sewage Attacks*, REGISTER, Oct. 31, 2001, http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/.

[52] Bill Wallace, *Next Major Attack Could Be Over Net*, S.F. CHRON., Nov. 12, 2001, at A1, *available at* http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2001/11/12/MN29929.DTL.

[53] Probably the closest thing we have to a reported cyberterrorist attack came in 1998 when:

> Tamil guerrillas swamped Sri Lankan embassies with 800 e-mails a day over a two-week period. The messages read, "We are the Internet Black Tigers and we're doing this to disrupt your communications." Intelligence authorities characterized it as the first known . . . attack by terrorists against a country's computer systems.

Rohas Nagpal, *Cyber Terrorism in the Context of Globalization*, 2 WORLD CONGRESS ON INFORMATICS & L. 22 (2002), *available at* http://www.ied.org/congreso/ponencias/Nagpal,%20Rohas.pdf. The Tamil Tigers have certainly proven to be terrorists, and their e-mail bombing was undertaken to promote an ideological agenda. *See* COUNCIL ON FOREIGN REL., LIBERATION TIGERS OF TAMIL EELAM (2006), *available at* http://www.cfr.org/publication/9242/. Some might argue that this attack did not constitute cyberterrorism because it targeted computer systems at embassies located in countries other than Sri Lanka and therefore did not impact Sri Lanka's civilian populace. But the attack did shut down the embassy computers and "had the desired effect of generating fear in the embassies." Dorothy E. Denning, *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, *in* NETWORKS AND NETWARS: THE FUTURE OF TERROR, CRIME, AND MILITANCY 236, 239 (John Arquilla & David F. Ronfeldt eds., 2001), *available at* http://www.nautilus.org/archives/info-policy/workshop/papers/denning.html.

[54] While some dismiss the possibility of cyberterrorism, others correctly understand that

three categories: (1) weapon of mass destruction; (2) weapon of mass distraction; and (3) weapon of mass disruption.[55] I now examine each, in order.

1. Weapon of Mass Destruction

This is a conceptual option, but not a real possibility. The notion that computer technology can be a weapon of mass destruction is based on a flawed premise: the concept that computers, alone, can be used to inflict the kind of demoralizing carnage the world saw in New York and Washington, D.C., on 9/11 or in Madrid on 3/11.[56] Computers, as such, cannot inflict physical damage on persons or property; that is the province of real-world implements of death and destruction.[57]

However, computers *can* be used to set in motion forces that produce physical damage. Instead of hacking into a municipal waste-management system for revenge, cyberterrorists could disable the systems that control a nuclear power plant and cause an explosion like the one at Chernobyl in 1986.[58] By claiming responsibility for the catastrophe, the cyberterrorists

---

it is not merely a possibility, but an inevitability. *See, e.g.*, Arquilla, *Waging War Through the Internet*, *supra* note 38, at E1.

> Despite . . . al Qaeda's long-standing interest in cyber terror, we have been . . . dismissive of this burgeoning threat. In part, that's because we doubt terrorists will focus on using computers to attack computer systems, believing instead that "real terrorists" want to kill people and blow things up . . . .
>
> From a purely psychological point of view, this idea makes sense, as traditional terrorists have been leg-breakers . . . . But over the past four years, we have made it very hard for al Qaeda to mount new attacks within the United States.
>
> So, if Osama bin Laden wants to pursue his goal of attacking our economy, disruptive cyber-terror strikes via the Internet are likely to be an increasingly important element in his offensive.

Id. Arquilla also attributes our tendency to dismiss cyberterrorism to our misplaced confidence "in our defensive capabilities." *Id.*

[55] The discussion that follows focuses on terrorists' use of computer technology to further their *primary* goal of advancing an ideological agenda. It does not address the use of computer technology to further the secondary goals noted earlier.

[56] 2004 Madrid train bombings—Wikipedia, http://en.wikipedia.org/wiki/11_March_2004_Madrid_train_bombings (last visited Apr. 21, 2007).

[57] The erroneous assumption that computer technology is merely another mode of mass destruction accounts for the skepticism many express about the prospects of a "digital Pearl Harbor" or a "digital 9/11." *See, e.g.*, Drew Clark, *Computer Security Officials Discount Chances of "Digital Pearl Harbor,"* GOVEXEC.COM, June 3, 2003, http://www.govexec.com/dailyfed/0603/060303td2.htm.

[58] *See, e.g.*, Chernobyl disaster—Wikipedia, http://en.wikipedia.org/wiki/Chernobyl_accident (last visited Apr. 21, 2007); *see also* Barton Gellman, *Cyber-Attacks by Al-Qaeda Feared*, WASH. POST, June 27, 2002, at A1, *available at* http://www.washingtonpost.com/ac2/wp-dyn/A50765-2002Jun26?start=24&per=24

could exploit the resulting illness, death, and radioactive contamination to undermine citizens' faith in their government's ability to protect them and maintain order.

This is a viable terrorism scenario, but it is not a *cyber*terrorism scenario. While computer technology would be used to trigger the explosion, the victims would recall it as a *nuclear* catastrophe, not as a *computer* catastrophe. Here, as in other computer as weapon of mass destruction scenarios, computer technology plays an incidental role in the commission of a terrorist act, serving merely as a detonator. To describe this scenario as cyberterrorism is as inappropriate as describing the 1998 U.S. embassy bombings carried out by Al-Qaeda as automotive-terrorism because vehicles were used to deliver the bombs to the target sites.[59]

2. Weapon of Mass Distraction

This is both a conceptual and a realistic possibility. Here, computer technology plays a pivotal role in the commission of a terrorist act, an act that differs in essential ways from the real-world terrorism to which we are accustomed. Computer technology is used to manipulate a civilian population psychologically. This manipulation saps civilian morale by undermining citizens' faith in the efficacy of their government.[60] Depending on the type of manipulation involved, it can also result in the infliction of personal injury, death, and property destruction.

To understand how computer technology could be used purely for psychological manipulation, consider this scenario: on September 11, 2001, as planes crashed into the World Trade Center and the Pentagon, millions of Americans watched the events unfold on television; many also used the Internet to try to find out more about what was happening.[61] The CNN site experienced particularly heavy traffic that day.[62] What if, instead of finding CNN-generated content, these visitors had encountered a Web page that announced, in appropriately terrifying graphics, "World War—Nuclear

---

(reporting that in 1998 a twelve-year-old hacker "broke into the computer system that runs Arizona's Roosevelt Dam" and could have released 489 trilliion gallons of water, which would have flooded the cities of Mesa and Tempe).

[59] *See, e.g.*, WRIGHT, *supra* note 45, at 270-72.

[60] Susan W. Brenner & Marc D. Goodman, *In Defense of Cyberterrorism: An Argument for Anticipating Cyber-Attacks*, 2002 U. ILL. J.L. TECH. & POL'Y 1, 31-40.

[61] *See, e.g.*, September 11, 2001 timeline for the day of the attacks—Wikipedia, http://en.wikipedia.org/wiki/September_11,_2001_timeline_for_the_day_of_the_attacks (last visited Apr. 21, 2007) ("8:49:34 a.m.—CNN and MSNBC's websites receive such heavy traffic that many servers collapse.").

[62] *See id.*

Holocaust in Europe and Australia, Japan Devastated by Chemical Attack"?[63]

As this was 2001, an over-the-top Orson Welles "War of the Worlds" reaction would have been unlikely,[64] since for the last decade, people typically have been obtaining their news from several types of media and from various sources within each type. But the posting of such a falsified page could have acted as a terror multiplier, enhancing the unnerving effects of the day's real-world terrorist events.[65] It could also have left lingering doubts in the public's mind as to whether "the government" had actually "covered up" the extraterritorial disasters once reported on CNN. These doubts could have provided the predicate for a long-term campaign of eroding public confidence in public officials and news outlets.

Now consider a scenario coupling psychological manipulation with injury, even death. At 1:00 p.m. on a Wednesday in San Francisco, the local Office of Emergency Services and Homeland Security receives messages via a secure government computer system informing them that a "suitcase nuclear device" is on the Bay Area Rapid Transit (BART) system, the public transportation system that serves San Francisco and surrounding cities.[66] The officials are told the device is in the hands of terrorists who will detonate it in two hours, at 3:00 p.m. If such a device were detonated, the death and destruction would be unimaginable—far greater than that inflicted on 9/11. The officials issue an immediate evacuation order for the San Francisco area. This produces chaos as panicked citizens desperately try to flee an impending nuclear disaster: cars clog the streets and accidents ensue, while those without cars clamor for other means of public transportation, leading to stampedes. Death, injury and property damage result—except that there is no impending disaster, no suitcase nuke. Terrorists hacked the government computer system and sent credible, fake messages, which the local officials reasonably believed. The net result is that the terrorists could achieve injury, death, and destruction as well as a dramatic erosion in the public's confidence in the government's ability to ensure their security without having to deploy an actual weapon.[67]

---

[63] For analogous, but much less dramatic attacks, see Brenner & Goodman, *supra* note 60, at 32-34.

[64] The War of the Worlds (radio)—Wikipedia, http://en.wikipedia.org/wiki/The_War_of_the_Worlds_(radio) (last visited Apr. 21, 2007).

[65] *See* Brenner & Goodman, *supra* note 60, at 26.

[66] Bay Area Rapid Transit—Wikipedia, http://en.wikipedia.org/wiki/Bay_Area_Rapid_Transit (last visited Apr. 21, 2007).

[67] For a similar, equally-fictive account of how false information can be used to create confusion and a resulting risk of injury, see Chris Suellentrop, *Sim City: Terrortown*, WIRED, Oct. 2006, at 103, 103-04, *available at* http://www.wired.com/wired/archive/

In these and other computer as weapon of mass distraction scenarios, computer technology is used primarily for psychological manipulation. The first scenario is a "true" computer as weapon of mass distraction scenario; the second scenario tends to blend weapon of mass distraction with hypothesized weapon of mass disruption effects. The point, though, is that neither scenario involves the actual use of real-world weapons; the computer is the only implement the terrorists employ.

3. Weapon of Mass Disruption

When terrorists use computer technology as a weapon of mass disruption, their goal is to undermine a civilian populace's faith in the stability and reliability of essential infrastructure components such as mass transit, power supplies, communications, financial institutions, and health care services.[68] Although the weapon of mass disruption and weapon of mass distraction alternatives both target civilians' faith in essential aspects of their society, they differ in how computer technology is used to corrode civilian confidence in societal infrastructure and services.

As we saw in the previous section, terrorists launch a psychological attack when they use computer technology as a weapon of mass distraction; the goal is to undermine civilians' confidence in one or more of the systems they rely on for essential goods or services. The cyberterrorists accomplish this by making citizens *believe* a system has been compromised and is no longer functioning effectively. The terrorists do not actually impair the functioning of the system. Their goal is to inflict psychological, not systemic, damage.

However, when computer technology is used as a weapon of mass disruption, terrorists' goal *is* the infliction of systemic damage on one or more target systems. This version of cyberterrorism is closer to the scenarios that sometimes appear in the popular media in which cyberterrorists shut down an electrical grid or the systems supplying natural gas or petroleum to a particular populace.[69]

Like the weapon of mass distraction alternative, this scenario is a conceptual yet realistic possibility. Here, terrorists utilize computer technology in a fashion that is analogous to, but less devastating than, their utilization of real-world weapons of mass destruction. Their goal is not to

---

14.10/posts.html?pg=2.

[68] *See* Brenner & Goodman, *supra* note 60, at 26.

[69] *See, e.g.*, DAN VERTON, BLACK ICE: THE INVISIBLE THREAT OF CYBER-TERRORISM 1-16 (2003); *see also* Jeremy Kirk, *Russian Expert: Terrorists May Try Cyberattacks*, INFOWORLD.COM, Dec. 13, 2006, http://www.infoworld.com/article/06/12/13/HNcyberterroralert_1.html?sour.

inflict the catastrophic carnage and destruction we saw on 9/11.[70] Rather, it is more insidious: to demoralize a civilian populace by making civilians question the government's ability to keep things working. In other words, terrorists seek to undermine citizens' faith in their government's ability to maintain the essential fabric of their lives by ensuring that the systems on which they rely function as they are intended to.

As many have noted, our increasingly urbanized, increasingly technologized lifestyle makes us more vulnerable to this type of terrorism than traditional, rural societies:

> The key to unlocking the disruptive potential of cities . . . is to attack key points . . . within target infrastructure . . . to force a change in the city's dynamic. Infrastructure attacks, particularly on power/fuel/water, negate the ability of the government to deliver political goods . . . . This halts economic activity and . . . damages the ability of the government to deliver political goods, which are the key to legitimacy.[71]

In this excerpt, the author is assuming attacks of a more drastic character, such as those inflicted in war.[72] He cites contemporary Baghdad as an example of how cities can

> be engineered to radiate instability . . . . This is accomplished through acts that leverage three attributes of modern cities. These include:
>
> - Extreme mobility and interconnectedness (for example, high rates of automobile and cell phone ownership).
> - Complete reliance on high volume infrastructure networks.
> - Complex and heterogeneous social networks that are held together under pressure.[73]

The same effect can be achieved, less dramatically, with cyberterrorist attacks that disrupt the functioning of infrastructure components. A recent exercise conducted by the U.S. Secret Service and Department of Homeland Security demonstrates this. In February 2006, more than three hundred participants from the American public and private sectors and from four other countries conducted a simulated cyberterrorism assault, called Cyber Storm, on U.S. government agencies and businesses.[74] The attacks were

---

[70] *See supra* note 57.

[71] John Robb, *The Role of Cities*, GLOBAL GUERRILLAS, Oct. 21, 2006, http://globalguerrillas.typepad.com/globalguerrillas/2006/10/the_role_of_cit.html.

[72] *See id.*

[73] *Id.*

[74] U.S. DEP'T OF HOMELAND SECURITY, NATIONAL CYBER EXERCISE: CYBER STORM 1 (2006), *available at* www.automationalley.com/MiRSA/Studies/prep_cyberstormreport_sep06.pdf [hereinafter CYBER STORM REPORT]:

> Cyber Storm was a coordinated effort between international, Federal and State governments, and

meant to disrupt "critical infrastructure, . . . leading to cascading effects" within the participating countries' "economic, societal, and governmental structures."[75] The exercise revealed problems in coordination between the public and private sectors and between different agencies in the public sectors. It also showed that talented, determined attackers can inflict serious damage on components of the United States' infrastructure.[76]

The Cyber Storm attacks were launched by a loosely knit coalition of domestic terrorists and opportunistic attackers, including a "cyber saboteur," a disgruntled airport employee, and German hackers.[77] Among other things, the disparate attackers crashed the FAA computer control system, caused electrical power and Internet outages, shut off the heat in government buildings, compromised medical data, posted a false Amber alert, altered one "No Fly" list and posted another one online, shut down commuter trains, and altered account balances in financial institutions.[78]

Cyber Storm was intended to test how collaborating government agencies and private sector representatives would respond to cyberattacks.[79] The exercise demonstrated that these cyberattacks can be launched with a

---

private sector organizations to exercise their response, coordination, and recovery mechanisms in reaction to . . . cyber events. . . .

Over 100 public and private agencies, associations, and corporations participated in the exercise from over 60 locations and 5 countries. . . .

The . . . scenario simulated a large-scale cyber campaign affecting or disrupting . . . critical infrastructure elements primarily within the Energy, Information Technology (IT), Telecommunications and Transportation sectors. The exercise was conducted primarily on a separate exercise network without impacting real world information systems.

[75] *Id.* at 1.

The exercise simulated a sophisticated cyber attack campaign through . . . scenarios directed against critical infrastructures. The intent . . . was to highlight the interconnectedness of cyber systems with the physical infrastructure and to exercise coordination . . . between the public and private sectors. Each of the scenarios . . . was executed in a closed and secure environment.

Id. at 11.

[76] *See id.* at 6-9.

[77] *Id.* at 14 ("The simulated adversaries did not represent a specific . . . terrorist group. . . .The[y] . . . were a loose coalition of well financed 'hacktivists.'").

The Cyber Storm attackers are consistent with emerging threats that have been identified elsewhere. A recent State Department report notes that "technologically empowered . . . 'micro actors'" who are "extremely difficult to detect or counter" are an emerging trend in terrorism. *See* COUNTRY REPORTS ON TERRORISM 2005, *supra* note 47, at 11.

[78] *See* U.S. Dep't of Homeland Sec., Presentation, National Cyber Exercise: Cyber Storm, New York City Metro ISSA Meeting 11 (June 21, 2006), *available at* http://www.cryptome.org/cyberstorm.ppt [hereinafter Cyber Storm powerpoint].

[79] *See* CYBER STORM REPORT, *supra* note 74, at 1.

fair degree of efficacy.[80] The Cyber Storm report noted that while the "good guy" players were "generally effective in addressing single threats/attacks, ... [p]layers were challenged when attempting to develop an integrated situational awareness picture and cohesive impact assessment across sectors and attack vectors."[81] It also noted that improved "processes, tools and technology" would "enhance the quality, speed and coordination of response," particularly for "cascading attacks or consequences."[82] The Cyber Storm report at least implicitly indicates that improvements are needed in interagency (and inter-sector) coordination, contingency planning, risk assessment, and definition of "roles and responsibilities across the entire cyber incident response community."[83]

The effects of the Cyber Storm attacks were localized and somewhat limited because the goal of the exercise was to test responses, not to explore how cyberattacks can demoralize civilians.[84] Still, shutting down FAA systems, commuter trains, electrical power, Internet access, and heat would unnerve the victim populace. Arguably, one of the most effective ways to mount a weapon of mass disruption attack would be to structure outages or other interferences of essential services in a way that dramatically demonstrates that these systems are now under the control of some anonymous, hostile agency.

One way to do this would be to launch sequenced, synchronized attacks shutting down ATMs and other financial systems in carefully selected U.S. cities.[85] They should be minor cities, perhaps Des Moines, Ithaca, Tulsa, Lexington, Eugene, and Fresno. The reason for this is that

---

[80] We are left to wonder how effectively these entities would have responded had they not been anticipating such attacks and/or had the attacks targeted more than three infrastructure sectors. *See supra* note 74.

[81] CYBER STORM REPORT, *supra* note 74, at 2.

[82] *Id.* at 10 (italics omitted).

[83] *See id.* at 1-2. Interestingly, the Cyber Storm report also concluded that "[p]ublic messaging must be an integral part of . . . incident response to . . . empower the public to take appropriate individual protective or response actions consistent with the situation." *Id.* at 2.

[84] *See generally id.* at 1.

[85] *See* Brenner & Goodman, *supra* note 60, at 39-40. In 2003, the Slammer worm "disrupted more than 13,000 Bank of America" ATMs, apparently as an unintended consequence of its propagation. CLAY WILSON, CONG. RESEARCH SERV., COMPUTER ATTACK AND CYBER TERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS 34 n.90 (2003), *available at* http://www.fas.org/irp/crs/RL32114.pdf ("[T]he effects would likely have been more severe had Slammer carried a malicious payload."). In August 2003, the Nachi worm compromised ATMs at financial institutions "in the first confirmed case of malicious code penetrating cash machines." Kevin Poulsen, *Nachi Worm Infected Diebold ATMs*, REGISTER, Nov. 25, 2003, http://www.theregister.co.uk/2003/11/25/nachi_worm_infected_diebold_atms/.

we are more likely to expect terrorist attacks on major cities. The bombing of the Oklahoma City federal building was especially horrific because until then, we had not expected catastrophes in the Heartland. Many still do not.

As the financial system attacks progressed from city to city, it would become increasingly apparent they were neither random, nor the product of software bugs, nor otherwise explainable, but were instead the product of terrorist activity. While attacks such as these would not inflict the sheer horror of the 9/11 attacks, they could further terrorist goals by creating a climate of insecurity and anger at the government, something analogous to what we saw with the Hurricane Katrina fiasco. The negative effects could be magnified if the attacks were sporadically repeated in other cities or if they were coupled with similar attacks on other non-financial systems, such as electrical power, telephone communication, or air traffic control.[86]

Another kind of attack might target health care systems. We have already seen an inadvertent example of this. In 2005, a botnet, a network of compromised computers,[87] controlled by Christopher Maxwell attacked a Seattle hospital.[88] The botnet shut down computers in the Intensive Care Unit and caused operating room doors and doctors' pagers not to function.[89] Maxwell did not intend for his botnet to attack Seattle's Northwest Hospital or any other hospital; rather, he was using it to earn commissions for surreptitiously installing adware on users' computers.[90] The attack, if such it was, occurred because the botnet was searching for computers to add to its system; in so doing, it overloaded the hospital's computer systems and shut down various functions.[91] Because the attack was inadvertent, its effects were not as serious as they would have been had there been a sustained attack. Hospital staff was therefore able to improvise solutions that prevented patients from being harmed and ensured uninterrupted quality patient care.[92]

---

[86] *See* Brenner & Goodman, *supra* note 60, at 39-42.

[87] "Botnet" refers "to a collection of compromised machines running programs . . . , under a common command and control infrastructure. A botnet's originator . . . can control the group remotely, usually through a means such as IRC, and usually for nefarious purposes." Botnet—Wikipedia, http://en.wikipedia.org/wiki/Botnet (last visited Apr. 21, 2007).

[88] Press Release, U.S. Attorney, W. Dist. of Wash., California Man Pleads Guilty in "Botnet" Attack that Impacted Seattle Hospital and Defense Department (May 4, 2006), *available at* http://seattle.fbi.gov/dojpressrel/2006/botneck050406.htm.

[89] *Id.*

[90] *Id.*

[91] *Id.*

[92] *See* Maureen O'Hagan, *Three Accused of Inducing Ill Effects on Computers at Local Hospital*, SEATTLE TIMES, Feb. 11, 2006, at A1, *available at* http://seattletimes.nwsource.com/html/localnews/2002798414_botnet11m.html; *see also*

As the Seattle episode illustrates, weapon of mass disruption attacks can cause personal injury or even death (along with property damage).[93] They can also be, but are not necessarily, blended attacks, which combine the infliction of real harms with psychological manipulation.[94]

4. Cyberterrorism as Crime

Having analyzed how terrorists can use computer technology to advance their primary goals of demoralizing civilians and destabilizing governments, by logical extension, it is fair to define terrorism as a crime rather than as war. Terrorism is defined and prosecuted as a crime in the U.S. and elsewhere.[95] A federal statute makes terrorism a federal crime in the United States.[96] Other countries criminalize terrorism, and both the United Nations and the European Union have defined terrorism in a criminal context.[97]

The practice of treating terrorism as crime no doubt evolved for two reasons. First, terrorists historically tended to be home-grown; they might, like the first-century Zealots or eleventh-century Hashhashin, target foreigners in their own country, but they were still a local, domestic threat.[98] Second, their efforts generally target a society's ability to maintain order in the face of internal threats, and the activities in which they engage are functionally indistinguishable from many crimes.[99] Real-world terrorists

---

Michael S. Mimoso & Marcia Savage, *Today's Attackers Can Find the Needle*, INFO. SEC., June 2006, at 24, *available at* http://informationsecurity.techtarget.com/magPrintFriendly/0,293813,sid42_gci1191313,00.html.

[93] The prosecutor handling the case noted afterward that while no patients were harmed, "this kind of attack could easily endanger lives." O'Hagan, *supra* note 92.

[94] *See* Brenner & Goodman, *supra* note 60, at 39-42.

[95] *See, e.g.*, Note, *Responding to Terrorism: Crime, Punishment, and War*, 115 HARV. L. REV. 1217, 1224 (2002).

[96] 18 U.S.C. § 2332b (2000). Section 1030(a)(5) of title 18 can also be used to prosecute cyberterrorism. *See* 18 U.S.C.S. § 1030(a)(5) (LexisNexis 2006). The USA PATRIOT Act made modifications to § 1030 that were intended to enhance its applicability to cyberterrorism. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, Title V, § 506(a), Title VIII, § 814, 115 Stat. 366, 382 (codified as amended at 18 U.S.C.S. § 1030(a)(5)).

[97] *See supra* note 40; *see also* Terrorism—Wikipedia, *supra* note 46.

[98] *See, e.g.*, Sharon Harzenski, *Terrorism, A History: Stage One*, 12 J. TRANSNAT'L L. & POL'Y 137, 140 n.17 (2003); History of Terrorism—Wikipedia, http://en.wikipedia.org/wiki/History_of_terrorism (last visited Apr. 21, 2007); Terrorism—Wikipedia, http://en.wikipedia.org/wiki/Terrorism (last visited Apr. 21, 2007).

[99] *See, e.g.*, United States v. Sarkissian, 841 F.2d 959, 965 (9th Cir. 1988) ("[Terrorism,] by definition, requires the investigation of activities that constitute crimes.").

kill, injure, and kidnap people and destroy property. The activity is the same as that conducted by criminals—only the motivation differs.

It seems reasonable to continue this approach of treating cyberterrorists as criminals, even though cyberterrorism, unlike most traditional, real-world terrorism, can be committed remotely.[100] For example, in the Cyber Storm exercise, three hackers operating from Germany contributed to the disruption of services in the United States.[101] One might argue that this remote commission capacity warrants treating cyberterrorism differently—approaching it as an external, rather than an internal, threat to social order. To do that, we would have to define "remote" cyberterrorism as something other than crime.[102] Alternatively, we could expand our definition of crime to encompass at least one type of external threat.[103]

As I noted earlier, cybercrime can also be committed remotely. This has certain consequences for how we approach the investigation and

---

[100] Note that real-world terrorism *can* be committed remotely, as Ramzi Yousef proved in 1994, when he left a triggered time-bomb on a Philippines Airlines plane bound from Manila to Tokyo. *See, e.g.*, DENNIS PISKIEWICZ, TERRORISM'S WAR WITH AMERICA: A HISTORY 91 (2003). The bomb went off two hours after Yousef had disembarked from the airliner; it killed the man who had taken his seat, seriously injured other passengers, and nearly disabled the airplane (which had been Yousef's goal). *See id.* Fortunately, the pilot was able to safely land the plane, saving the lives of all those who survived the explosion. *See id.*

Yousef also triggered the bomb he used in the first World Trade Center attack remotely by lighting a twelve-minute fuse. *See id.* at 87. But while these and similar instances involve the remote commission of terrorist acts in the literal sense, they still require that the terrorist be, or have recently been, in physical proximity to the attack target. Real-world terrorist attacks simply cannot be committed by terrorists who are spatially remote from the attack site. (By "spatially remote," I mean that they are in another country or in another part of the country from where the attack is carried out.) These real-world remote terrorist attacks are therefore functionally more analogous to crime than they are to cyberterrorism. Here, as with real-world crime, the terrorist-perpetrators' physical proximity to the attack site increases the risk that they will be identified and apprehended; it also makes the task of carrying out the attack more difficult, as they have to deal with constraints imposed by acting in the real, physical world. *See* Brenner, *Toward a Criminal Law for Cyberspace*, *supra* note 5, at 65-76.

[101] *See* Cyber Storm powerpoint, *supra* note 78, at 10.

[102] This, in turn, might result in our employing a dichotomous approach to cyberterrorism in which non-remote cyberterrorism was defined as crime, while remote cyberterrorism was defined as something other than crime.

[103] If we were to do this, we would also have to decide how we should respond to this new, not-crime phenomenon. We would presumably not prosecute apprehended not-criminal cyberterrorists in our domestic courts because these courts are reserved for criminals. We might set up specialized tribunals—perhaps analogous to war crimes tribunals—to prosecute them. We will return to this issue later, when we analyze the process of responding to cybercrime/cyberterrorism/cyberwarfare. *See infra* Section IV.

apprehension of those who commit cybercrime,[104] but for "mere" cybercrime, the capacity to act remotely is clearly irrelevant to the inherent nature of the phenomenon itself. Theft is theft, fraud is fraud, and extortion is extortion, regardless of whether they are committed by the victim's next-door neighbor or by someone halfway around the world. The same is true for the other categories of harm-infliction we define as crime. As long as the remote (or local) perpetrator acts out of personal motives, the dynamic is that of crime—the victimization of one individual by another.[105] Therefore, instead of focusing on means (how harm is inflicted), we focus on the harm itself, because it is the infliction of these types of harm (criminal harms) that threatens internal order.[106]

The same should be true for terrorism. Insofar as terrorist acts are designed to undermine a society's ability to maintain internal order, they are indistinguishable from, and should be treated as, crime regardless of whether they are perpetrated locally or remotely.

Before we conclude this discussion, I need to make one caveat: the approach I outline above is satisfactory when the only factor differentiating crime or terrorism from cybercrime or cyberterrorism is local versus remote commission. Indeed, as the next section explains, the analysis can become more complex when crimes or terrorist acts are carried out in Nation-State A by individuals who are acting as agents of Nation-State B.

C. CYBERWARFARE

> [T]he intruders retained an ability to keep coming back into our systems, even . . . . as our cyber warriors tried . . . to block . . . them . . . .[107]

In the fall of 2006, the U.S. Air Force adopted a new mission statement in which it pledged to "fight in Air, Space, *and Cyberspace*."[108]

---

[104] *See* Brenner, *Toward a Criminal Law for Cyberspace*, *supra* note 5, at 65-76.

[105] *See id.* at 40-65. When I say "individual," I mean to denote, at least as far as the victim is concerned, both real and fictive persons. So far anyway, the victimizers are necessarily human, but the victims could be human, corporate, or another artificial entity.

[106] *See also id.* If citizens do not believe their society can protect them from crime "harms," they are likely to resort to self-help measures, which can lead to chaos. *See, e.g.*, Andrew Ashworth, *Responsibilities, Rights and Restorative Justice*, 42 BRIT. J. CRIMINOLOGY 578, 585 (2002) (stating that societies undertake "the duty of administering justice and protecting citizens in return for citizens giving up their right to self-help").

[107] Arquilla, *Waging War Through the Internet*, *supra* note 38, at E1.

[108] Air Force Link—Welcome, http://www.af.mil/main/welcome.asp (emphasis added) (last visited Apr. 21, 2007). The new mission statement added the reference to cyberspace. *See* Michael W. Wynne, Sec'y of the Air Force, Cyberspace as a Domain in Which the Air Force Flies and Fights (Nov. 2, 2006), *available at* http://www.af.mil/library/speeches/speech.asp?id=283.

The new statement recognizes what has been apparent for some time: warfare can and will migrate into cyberspace.[109]

Cyberwarfare is the conduct of military operations by virtual means.[110] It consists of nation-states' using cyberspace to achieve the same ends that they pursue through the use of conventional military force: achieving advantages over a competing nation-state or preventing a competing nation-state from achieving advantages over them.[111]

---

[109] *See, e.g.*, CLAY WILSON, CONG. RESEARCH SERV., INFORMATION OPERATIONS AND CYBERWARFARE: CAPABILITIES AND RELATED POLICY ISSUES CRS-1 to CRS-8 (2006), *available at* http://www.fas.org/irp/crs/RL31787.pdf. A recent congressional report described China's commitment to cyberwarfare:

> China is actively improving its non-traditional military capabilities. . . . China's approach to exploiting the technological vulnerabilities of adversaries extends beyond destroying or crippling military targets. Chinese military writings refer to attacking key civilian targets such as financial systems.
>
> The Commission believes Chinese intelligence services are capable of doctoring computer systems. It has seen clear examples of computer network penetrations coming from China, some of which were publicized in the "Titan Rain" exposé that received substantial press coverage. In August and September 2006. . . .
>
> The PLA [People's Liberation Army], leveraging private sector expertise, steadily increases its focus on cyber-warfare capabilities and is making serious strides in this field. . . . [T]he PLA's cyber-warfare strategy has evolved from defending its own computer networks to attacking the networks of its adversaries. . . .

U.S.-CHINA ECON. & SEC. REVIEW COMM'N, 109TH CONG., REPORT TO CONGRESS 137 (2006), *available at* http://www.uscc.gov/annual_report/2006/annual_report_full_06.pdf (notes omitted); *see also* OFFICE OF THE SEC'Y OF DEF., 109TH CONG., ANNUAL REPORT TO CONGRESS: MILITARY POWER OF THE PEOPLE'S REPUBLIC OF CHINA 35-36 (2006), *available at* http://www.defenselink.mil/pubs/pdfs/China%20Report%202006.pdf.

[110] *See, e.g.*, STEVEN A. HILDRETH, CONG. RESEARCH SERV., CYBERWARFARE (2001), *available at* http://www.fas.org/irp/crs/RL30735.pdf; *see also supra* note 108. For a cyberwarfare scenario, see John Arquilla, *The Great Cyberwar of 2002*, WIRED, Feb. 1998, *available at* http://www.wired.com/wired/archive/6.02/cyberwar_pr.html [hereinafter Arquilla, *The Great Cyberwar*].

[111] *See, e.g.*, The Brig Amy Warwick (The Prize Cases), 67 U.S. 635, 652 (1863) ("[W]ar" is "the exercise of force by bodies politic, or bodies assuming to be bodies politic, against each other, for the purpose of coercion."); *see also* YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENSE 4-5 (2001) (identifying the four constituent elements of war as: "(i) there has to be a contention between at least two States; (ii) the use of the armed forces of those States is required; (iii) the purpose must be overpowering the enemy (as well as the imposition of peace on the victor's terms); and . . . (iv) both parties are expected to have symmetrical, although diametrically opposed, goals").

The modern conception of war was expanded in the twentieth century beyond state-to-state conflicts; it now encompasses "armed conflict[s] between or among states or groups like states capable of supporting a uniformed military." Steve Sheppard, *Passion and Nation: War, Crime, and Guilt in the Individual and the Collective*, 78 NOTRE DAME L. REV. 751, 789 (2003) (citing INGRID DETTER DE LUPIS, THE LAW OF WAR 24 (1987)). As one commentator notes, the Geneva Conventions "recognize . . . four distinct categories of armed

This is already happening, according to some accounts. There are reports that the People's Republic of China is launching cyberattacks that are intended to cripple Taiwan's infrastructure and paralyze that island nation's government and economy.[112] The attacks allegedly target Taiwan's public utility, communications, transportation, and operational security networks.[113]

As noted above, the distinguishing characteristic of war is that it is a struggle between nation-states;[114] war—like all human activity—is carried out by individuals, but here individuals act on behalf of a particular nation-state.[115] Like terrorism, warfare tends to result in the destruction of property (often on a massive scale) and in the injury and deaths of

---

conflict: inter-state armed conflict under Common Article 2; internal 'wars of national liberation' as defined in Protocol I; 'civil wars' . . . as defined in Protocol II; and 'armed conflicts not of an international character' under Common Article 3." Derek Jinks, *September 11 and the Laws of War*, 28 YALE J. INT'L L. 1, 27 (2003). While the latter three categories do not represent traditional state-versus-state warfare, each is predicated, at least to some extent, on the premise that a conflict is between a traditional state and a group that aspires or purports to have the characteristics of a nation-state. *See, e.g.*, Derek Jinks, *The Applicability of the Geneva Conventions to the "Global War on Terrorism,"* 46 VA. J. INT'L L. 165, 182-85 (2005). General Rupert Smith uses "war amongst the people" to refer the "modern warlike situations" in which "there is no secluded battlefield upon which armies engage." RUPERT SMITH, THE UTILITY OF FORCE 5 (2007).

I am not concerned with these nuanced conceptualizations of war. The discussion in the text above assumes inter-state conflict can be traditional armed conflict; it can also encompass inter-state conflicts that utilize other means, such as cyberwarfare and economic warfare. I focus on war as inter-state conflict because this conceptual category encompasses challenges to a state's ability to maintain external order. This focus on challenges to external order differentiates warfare from crime and terrorism, both of which have traditionally been concerned exclusively with challenges to internal order. I will therefore use warfare as the analytical construct that allows us to examine how, and why, the utilization of computer technology can blur the distinction between challenges to internal order (crime and terrorism) and challenges to external order (warfare), and thus make attribution problematic.

[112] Bill Gertz, *Chinese information warfare threatens Taiwan*, WASH. TIMES, Oct. 13, 2004, at A3; *see also supra* note 109.

[113] Gertz, *supra* note 112, at A3; *see also supra* note 109. China is not alone in developing the capacity for cyberwarfare. According to one expert, "at least 20 nations . . . have their own cyberattack programs." Onley & Wait, *supra* note 8 (quoting John Thompson, chairman and chief executive officer of Symantec Corp.).

[114] *See supra* note 111; *see also* DINSTEIN, *supra* note 111, at 5 ("One element seems common to all definitions of war. In all definitions it is clearly affirmed that war is a contest between states." (quoting Clyde Eagleton, *An Attempt to Define War*, 291 INT'L. CONCIL. 237, 281 (1933))).

[115] *See, e.g.*, Hague Convention No. IV Respecting the Laws and Customs of War on Land art. I, Oct. 18, 1907, 36 Stat. 2277, *available at* http://www.yale.edu/lawweb/avalon/lawofwar/hague04.htm [hereinafter Hague Convention No. IV]; Geneva Convention III, Relative to the Treatment of Prisoners of War arts. 1 & 2, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135, *available at* http://www.genevaconventions.org/.

individuals (also often on a massive scale).[116] Unlike terrorism, war is limited, at least in theory, to clashes between the aggregations of individuals (armies), who respectively act for the warring nation-states.[117] Injuring and killing civilians occurs, but like most property damage and destruction, it is a collateral event.[118] The primary focus of war in general and of particular wars is to "triumph" over the adversarial nation-state(s), whatever that means in a given context.[119]

In the real-world, there can be ambiguity as to whether an event is a crime or an act of terrorism,[120] but war is always unambiguous.[121] When Japan bombed Pearl Harbor in 1941,[122] it was clearly an act of war; the same was true when Hitler invaded Poland in 1939 and has been true throughout recorded history.[123]

War is unambiguous in the real-world because it is unique; only nation-states can summon the resources needed to launch a physical land, sea, or air attack on another nation-state. The clarity of war is further enhanced by the fact that those who conduct an attack wear uniform clothing and insignia that identify them as members of a particular nation-

---

[116] *See, e.g.*, NIALL FERGUSON, THE PITY OF WAR 248-317 (1999) (describing economic losses and loss of life in World War I).

[117] *See* Karma Nabulsi, *Evolving Conceptions of Civilians and Belligerents: One Hundred Years After the Hague Peace Conference*, *in* CIVILIANS IN WAR 9, 9-24 (Simon Chesterman ed., 2001).

[118] *See* Geneva Convention IV, Relative to the Protection of Civilian Persons in Time of War arts. 3, 28, 53, Aug. 12, 1949, *available at* http://www.genevaconventions.org/; *see, e.g.*, Bombing of Dresden in World War II—Wikipedia, http://en.wikipedia.org/wiki/Bombing_of_Dresden_in_World_War_II (last visited Apr. 21, 2007); *see also* Nabulsi, *supra* note 117, at 9-21. *See generally* The Paquete Habana, 175 U.S. 677, 710-15 (1900).

[119] *See* DINSTEIN, *supra* note 111, at 4 ("War is a contention between two or more States through their armed forces, for the purpose of overpowering each other and imposing such conditions of peace as the victor pleases." (quoting II LASSA OPPENHEIM, INTERNATIONAL LAW 202 (7th ed. 1952) (1905))).

[120] *See, e.g.*, Alan Cooperman, *Capture Focuses on Christian Terrorism*, GRAND RAPIDS PRESS, June 2, 2003, *available at* 2003 WLNR 13819663 (reporting that authorities were trying to determine if Atlanta Olympic bomber Eric Rudolph was a "Christian terrorist" or merely a criminal); Patrick May & Martin Merzer, *No Place to Hide*, MIAMI HERALD, Apr. 21, 1995, *available at* 1995 WLNR 2638059 (writing that authorities were not sure if the bombing of the Oklahoma City federal building was terrorism or a crime).

[121] In this and subsequent discussions, we will use the term "war" to refer to a state of armed conflict between two nation-states. *See supra* note 111.

[122] *See, e.g.*, Attack on Pearl Harbor—Wikipedia, http://en.wikipedia.org/wiki/Attack_on_Pearl_Harbor (last visited Apr. 21, 2007).

[123] *See, e.g.*, Battle of Thermopylae—Wikipedia, http://en.wikipedia.org/wiki/Battle_of_Thermopylae (last visited Apr. 21, 2007); Invasion of Poland (1939)—Wikipedia, http://en.wikipedia.org/wiki/Invasion_of_Poland (last visited Apr. 21, 2007); Six-Day War—Wikipedia, http://en.wikipedia.org/wiki/Six-Day_War (last visited Apr. 21, 2007).

state's armed forces.[124] And, of course, real-world warfare involves the violation of territorial boundaries. Nation-states are defined by the territory they control;[125] acts of war have, as a result, historically involved breaching the integrity of the victim state's borders.[126] This, after all, is why war is a nation-state's response to an external threat—though not the only possible response. The threat to social order comes not from "insiders" who are at least ostensibly legitimately in the state's territorial boundaries but from another nation-state—a necessary externality.[127]

The threat dichotomy (internal versus external threat, crime and terrorism versus war) we reviewed earlier is consequently a stable, reliable way of parsing real-world attacks. We may be somewhat uncertain as to whether a particular event is crime or terrorism, but that is ultimately of little moment because we use the same approach for both, since both threaten internal order. And the monopolization of territory and military force by nation-states means that in the real-world, we will never be uncertain as to whether we are confronted with a threat to internal order (crime/terrorism) or a threat to our nation-state's ability to maintain external order (war).[128] In the real-world, only nation-states wage war.[129]

As the scenario we began with implicitly illustrates, this threat dichotomy breaks down when attacks are vectored through the virtual world. By giving non-state actors access to a new, diffuse kind of power,[130] cyberspace ends nation-states' monopolization of the ability to wage war and effectively levels the playing field between all actors.[131] In the twenty-

---

[124] *See, e.g.*, Hague Convention No. IV, *supra* note 115.

[125] *See* MARTIN VAN CREVALD, THE RISE AND DECLINE OF THE STATE 133 (1999) ("[T]he most important characteristic of the modern state is its territoriality."); *see also* SASKIA SASSEN, TERRITORY, AUTHORITY, RIGHTS: FROM MEDIEVAL TO GLOBAL ASSEMBLAGES 76-82 (2006).

[126] *See supra* note 111.

[127] *See* Brenner, *Toward a Criminal Law for Cyberspace*, *supra* note 5, at 105-06 ("[N]ation-states are defined by and primarily operate within specific territorial boundaries. Nation-states maintain . . . external order by protecting their citizens from 'outside' threats, which have historically been encroachments by other nation-states.").

[128] *See also id.* at 9-10, 105-06.

[129] *See* Steven Brayton, *Outsourcing War: Mercenaries and the Privatization of Peacekeeping*, 55 J. INT'L AFF. 303, 303 (2002); *see also* Glenn M. Sulmasy, *The Law of Armed Conflict in the Global War on Terror: International Lawyers Fighting the Last War*, 19 NOTRE DAME J.L. ETHICS & PUB. POL'Y 309, 311 (2005).

[130] *See, e.g.*, INFORMATION OPERATIONS, *supra* note 45, at 10-14.

[131] *See id.* at 70 ("[T]echnology . . . has revolutionized warfare by taking the elements of power and dispersing them to the people."); *see also* LT. COL. WILLIAM R. FAST, NAT'L DEF. UNIV., INST. FOR NAT'L STRATEGIC STUDIES, KNOWLEDGE STRATEGIES: BALANCING ENDS, WAYS, AND MEANS IN THE INFORMATION AGE (2002), *available at* http://www.ndu.edu/inss/siws/ch1.html.

first century, states generate crime and terrorism as well as war, and individuals wage war in addition to committing crimes and carrying out acts of terrorism. I examine these issues next.

III. IDENTIFYING CYBERCRIME, CYBERTERRORISM, AND CYBERWARFARE: ATTRIBUTION

For our purposes, attribution encompasses two issues:[132] who carried out an attack, and what kind of an attack it was. The first issue goes to assigning responsibility for *committing* an attack. The second goes to assigning responsibility for *responding* to an attack. We will call the first "attacker-attribution" and the second "attack-attribution." The sections below examine how we currently approach both. Section IV then considers how we can improve our approach to what is becoming the most problematic aspect of attribution: attack response.

A. ATTACKER-ATTRIBUTION

The task of identifying those who are responsible for an attack has been, and will remain, a constant. As we will see, identification of the attacker can play an integral role in ascertaining the nature of an attack; and ascertaining the nature of an attack is usually the first step in formulating a response to an attack, of whatever type.

---

[132] *See, e.g.*, THE WHITE HOUSE, *supra* note 1, at 50; *see also* THOMAS J. BARRETT & ANDREW W. CUTTS, NAT'L CTR. AT NORWICH UNIV., NATIONAL CYBERGUARD: DEFENDING AMERICA'S CYBERSPACE AGAINST THE STRATEGIC THREAT (2005), *available at* http://www.ncatnu.org/ccri/NationalCyberGuardWP.pdf.

The characterization given in the text above focuses on attribution as a legal, rather than as a technical or technical-legal, concept. It therefore focuses on the information decision-makers need to decide whether an attack is a matter to be resolved by civilian or military law, by law enforcement officers, or by military personnel. As we shall see, information about the attackers (Are they acting on their own? Are they agents of a foreign nation-state?) can be as important as information about the attack when one is making this decision.

Because we are focusing solely on legal decision-making, the characterization of attribution given above contains fewer elements than the characterization used by those who parse the technical aspects of attack attribution. For a technically-legally focused characterization of attribution, see, e.g., Dorothy E. Denning, Cyber Conflict Studies Ass'n, Presentation-Attribution Workshop, Cyber Attack Attribution: Issues and Challenges 2, (March 2005), *available at* http://www.cyberconflict.org/attributionworkshop.asp (follow "Cyber Attack Attribution: Issues and Challenges" hyperlink; then open PowerPoint presentation; then see slide 2) (describing four levels of attribution: identification of attacking machines; identification of primary controlling machines; identification of humans responsible for attack; and identification of sponsor organization). For a more technical approach to the issue, see, e.g., SANS Institute—Network Attack Attribution Research Group, http://www.sans.org/projects/aarg/?portal=3844d624dbae783333b30e399b89ccce (last visited Apr. 21, 2007).

We will divide our consideration of attacker-attribution into two stages. First, we review how attacker-attribution is currently approached for real-world attacks. Second, we will consider how attacker-attribution becomes problematic as attacks migrate online, in whole or in part.

1. Real-world Attribution

Attacker-attribution has historically been less problematic for war than for crime or terrorism.[133] The laws of war require states launching an attack on another state to identify themselves, though this convention is apparently honored more in the breach than in its realization.[134] Even if that is true, it is generally not difficult to identify the state responsible for an act of war in the real-world. The initial attack may be a surprise, as with Pearl Harbor, but attributing the attack to a specific state tends to be a relatively simple process. Military attackers wear distinctive, uniform clothing and use equipment with insignias or characteristics indicating their national affiliation. The language the attackers use will be another indicator of their country of origin, as well as circumstances of the attack itself.[135] The location from which an attack is launched can be another clue: if Nation-State A is under attack by missiles being launched from Nation-State B, Nation-State A's decision-makers can reliably infer that either Nation-State B, or another nation with which Nation-State B is affiliated (Nation-State C, say) is responsible for the attack.[136]

---

[133] Here, as earlier, we are using "war" to denote an armed conflict between two or more nation-states. *See* Nabulsi, *supra* note 117, at 9-21.

[134] *See* Hague Convention No. III Relative to the Opening of Hostilities art. I, Oct. 18, 1907, 36 Stat. 2259, 2271, T.S. 598, *available at* http://www.yale.edu/lawweb/avalon/lawofwar/hague03.htm; Yoram Dinstein, *Comments on War*, 27 HARV. J.L. & PUB. POL'Y 877, 885-86 (2004); *see also* DINSTEIN, *supra* note 111, at 29-32 (declaration of war is not essential to establish state of war; armed attack suffices). A declaration of war "served the legal function of triggering international law governing neutral and belligerent states . . . ." William C. Peters, *On Law, Wars and Mercenaries: The Case for Courts-Martial Jurisdiction over Civilian Contractor Misconduct in Iraq*, 2006 BYU L. REV. 367, 404 (quoting CURTIS A. BRADLEY & JACK L. GOLDSMITH, FOREIGN RELATIONS LAW 177, 178 (2003)). The United Nations Charter "abolished" war "as a category of international law," so declarations of war no longer serve any legal purpose. *See* Paul W. Kahn, *War Powers and the Millennium*, 34 LOY. L.A. L. REV. 11, 17 (2000).

[135] These attribution factors apply whenever a classic state of war exists, and can also apply when nations are embroiled in "incidents short of war." DINSTEIN, *supra* note 111, at 3-13.

[136] *See, e.g.*, Gulf War—Wikipedia, http://en.wikipedia.org/wiki/Desert_Storm (last visited Apr. 21, 2007) (illustrates real-life example where U.S.-led coalition forces, representing "Nation-State A," launched initial air sorties against Iraq, "Nation-State B," from Saudi Arabia, "Nation-State C").

Identifying those responsible for a crime is usually much more difficult. Criminals have a strong incentive to avoid identification because it is generally the first step to being apprehended, tried, convicted, and sanctioned for their misdeeds.[137] With rare exceptions,[138] criminals do not intentionally identify themselves as the architects of their crimes (though they may do so indirectly by using a *nom de crime*, such as "the Zodiac Killer").[139] Since crime control is essential for the maintenance of internal order, nation-states have developed a standardized, generally effective approach for identifying those who commit crimes in their territory.[140]

This criminal investigation approach assumes activity in the real-world because, until recently, physical reality was the only arena of crime commission.[141] The approach therefore focuses on finding attribution evidence at a physical crime scene by locating witnesses who saw the perpetrator and can describe and hopefully identify him, and physical evidence (such as DNA or fibers) that can be traced to a particular individual who was suspiciously at the crime scene. Since it is predicated on conduct in the real-world, this approach assumes that the perpetrator of an attack—a crime—was, and still is, physically in the local geographical area.[142] The latter assumption gives rise to the "dragnet" tactic, in which officers comb the area for sightings of the perpetrator and for people who know him.[143] If attacker-attribution fails for a crime, officers will assume the attacker remains in the local area and will consequently be alert for the possibility that he will re-offend and then be identified.[144]

With regard to attacker-attribution, terrorism occupies a middle ground between war and crime. While those who carry out a terrorist attack may

---

[137] *See* Brenner, *Toward a Criminal Law for Cyberspace*, *supra* note 5, at 49-59.

[138] *See, e.g.*, Bonnie and Clyde—Wikipedia, http://en.wikipedia.org/wiki/Bonnie_and_Clyde (last visited Apr. 21, 2007) (Bonnie Parker wrote poems about the pair's exploits and sent them to newspapers, which published them).

[139] *See, e.g.*, Zodiac Killer—Wikipedia, http://en.wikipedia.org/wiki/Zodiac_killer (last visited Apr. 21, 2007). The *nom de crime* tactic is not, of course, intended to reveal the perpetrator's true identity. Instead, it is a compromise—a way of letting the perpetrator "take credit" for the crimes she commits while still retaining the anonymity that increases her chances of avoiding capture.

[140] *See* Brenner, *Toward a Criminal Law for Cyberspace*, *supra* note 5, at 55-65; *see also* Denning, *supra* note 132, at 5-6 (discussing the Uniform Crime Reporting program for real-world crimes). We will review the basic tactics used in this approach in the next section.

[141] *See* Brenner, *Toward a Criminal Law for Cyberspace*, *supra* note 5, at 65-76.

[142] *See id.*

[143] *See id.*

[144] *See id.* Officers can also rely on identifiable geographical and offense patterns in local crimes to assist in identifying perpetrators. *See id.*

not identify themselves personally,[145] they often identify themselves as acting on behalf of a terrorist group so the group can take credit for the attack.[146] Increasingly, terrorism-perpetrators identify themselves as representatives of a particular terrorism group in "martyrdom messages" recorded prior to an attack, especially a suicide attack.[147] It is also increasingly common for the group sponsoring a terrorist attack to claim credit for it in a message posted online or on a videotape delivered to media outlets.[148] And if the sponsoring group does not claim credit for an attack, the structure and style of the attack may inferentially identify the organization responsible for it.[149] In terrorism, as in war, it is usually possible to identify the entity responsible for an attack; but, as with crime, it can be difficult to identify the individuals who actually carried out an attack. Since the current strategy treats terrorism as a type of crime, the

---

[145] Terrorists are more likely to identify themselves if they do not anticipate escaping to commit further attacks. Terrorists whose goal is to commit further attacks eschew self-identification for the same reason crime-perpetrators try to avoid identifying themselves. Identification facilitates apprehension, which, for terrorists, negates their ability to commit further acts of terrorism. *See, e.g.*, Carlos the Jackal—Wikipedia, http://en.wikipedia.org/wiki/Ilich_Ram%C3%ADrez_S%C3%A1nchez (last visited Apr. 21, 2007).

[146] Terrorist groups differ in terms of their attitude toward publicly taking credit for attacks. *See, e.g.*, KIM CRAGIN & SARA A. DALY, THE DYNAMIC TERRORIST THREAT 37-38 (2004) (explaining that RIRA, the "Real Irish Republican Army," and Hamas take credit for the attacks they sponsor, while FARC, the Revolutionary Armed Forces of Colombia, and al-Qaeda generally do not).

[147] *See id.* at 38; *see also Video Shows Laughing 9/11 Hijackers in Afghan Hideout,* CNN.COM (Oct. 1, 2006), http://edition.cnn.com/2006/WORLD/meast/10/01/hijackers.video/index.html; Martyrdom Video—Wikipedia, http://en.wikipedia.org/wiki/Martyrdom_video (last visited Apr. 21, 2007).

[148] *See, e.g.*, 7 July 2005 London bombings—Wikipedia, http://en.wikipedia.org/wiki/7_July_2005_London_bombings#Claims_of_responsibility (last visited Apr. 21, 2007) (explaining that multiple groups claimed responsibility for the London subway bombing attacks via statements posted online and that two of the bombers left videotaped messages). The increasing tendency of groups to claim responsibility can produce conflicting claims of responsibility for an attack. *See, e.g.*, Hugh Miles, "*We Heard a God Almighty Bang. Then Another, and Then Another,*" TELEGRAPH (London), July 23, 2005, *available at* http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2005/07/24/wegypt124.xml; John Ward Anderson, *Suicide Blast Kills Four in Tel Aviv*, WASH. POST, Feb. 26, 2005, at A01, *available at* http://www.washingtonpost.com/wp-dyn/articles/A55514-2005Feb26.html.

[149] *See, e.g.*, Scott MacLeod, *Is Al-Qaeda in Sinai?*, TIME, Oct. 12, 2004, at 17, 17, *available at* http://www.time.com/time/magazine/article/0,9171,1101041018-713210,00.html (reporting that "synchronized attacks are a common al-Qaeda tactic"); *World Nations Beef Up Security after London Bombings*, AL JAZEERA (Qatar), July 8, 2005, http://www.aljazeera.com/me.asp?service_ID=8870 (quoting a security expert who explains that synchronized attacks are "pretty classic for al Qaeda"). It is also possible to infer responsibility for an attack from the likely motive for the attack.

criminal investigation approach outlined above is often used to identify and apprehend individual terrorists.[150]

2. Online Attribution

The BIS episode[151] illustrates how online attacks complicate attacker-attribution across all three dimensions of crime, terrorism, and war. Attacker-attribution becomes problematic at each level because the approaches we use to identify attackers implicitly assume territorially-based activity in the physical world. Since cyberattacks do not take place in physical reality, the attack signatures[152] of cybercrime, cyberterrorism, and cyberwarfare generally display few of the empirical characteristics common to their real-world counterparts.

To understand why that is true, we need to parse the BIS attacks. As we saw in the previous section, the real-world crime-terrorism and war attacker-attribution calculi rely on the "place" where an attack occurred or originated from in determining attacker identity. With virtual attacks, a "place" tends to be at once more ambiguous and less conclusive than in real-world analyses.

a. Attack Origin

With cybercrimes, a "place" is ambiguous because while attacks may be routed through Internet servers located in China, this does not necessarily mean that they originated in China. It is common for online attackers to use "stepping stones"—computers the attacker controls but that are owned by innocent parties—in their assaults.[153] These "stepping stone" computers can be located anywhere in the physical world because real-space is irrelevant to activity in cyberspace. So, while use of the Chinese servers might mean the attacks came from China, it also might mean they did *not* come from China. Rather, the attacker might be in Russia, Brazil, or Peoria. Indeed, an attacker located somewhere other than in China and who knew of U.S. concern about China's efforts to develop cyberwarfare capabilities might use Chinese servers deliberately to mask the true source

---

[150] *See, e.g.*, DENNIS PISZKIEWICZ, TERRORISM'S WAR WITH AMERICA: A HISTORY 85-96 (2003) (describing the investigation and apprehension of 1993 World Trade Center bomber Ramzi Yousef, which mirrors the steps involved in the criminal investigation approach).

[151] *See supra* Section I.

[152] Essentially, an attack signature encompasses the essential elements of an attack. *See, e.g.*, Bryan Sartin, *Tracking the Cybercrime Trail*, SEC. MGMT., Sept. 2004, at 95, 95-96 ("FBI agents . . . looked at . . . audit logs to find the hacker's . . . attack signature—that is, how the hacker broke in and what the hacker did once he . . . had access.").

[153] *See, e.g.*, Denning, *supra* note 132, at 7.

of the attack and mislead the investigators trying to identify him.[154] Unless and until investigators reliably establish that the attacks originated in Chinese real-space, we cannot predicate attacker-attribution on inferences drawn from the place of attack origin.[155]

What if BIS-style attacks were repeated over a period of time, with each attack coming from Chinese servers and each targeting computers used by U.S. government agencies? Can we now predicate attacker-attribution on inferences drawn from the repetitive use of what seems to be the same point of origin? It would be risky to rely on mere repetition; aside from anything else, a virtual Machiavelli might be "framing" China by routing structurally similar attacks through its real-space.[156]

Repetition coupled with other circumstances might support using point of attack origin inferences to establish attacker-attribution. Assume that BIS-style attacks are launched against another U.S. government agency's computers. Investigators trace these attacks to servers in Guangdong, China. Over the last, say, six years, sporadic attacks targeting U.S. government and civilian computers have been traced to Guangdong; some say the attacks were conducted by Chinese military hackers, others say Guangdong University students were responsible for them.[157] Can we predicate attacker-attribution inferences on the discontinuous repetition of similar target attacks coming from the same real-world locus in China? Does the (reasonably reliable) identification of a single point of origin support the inference that the recent BIS-style attacks came from Guangdong?[158]

---

[154] *See, e.g.*, Nathan Thornburgh, *The Invasion of the Chinese Cyberspies*, TIME, Sept. 5, 2005, at 34, 34, *available at* http://www.time.com/time/magazine/article/0,9171,1098961-1,00.html ("China . . . is known for having poorly defended servers that outsiders from around the world commandeer as their unwitting launchpads.").

[155] News reports of the attacks indicate that investigators were able to determine that they came "through Chinese servers" but not necessarily from China. *See, e.g.*, Gregg Keizer, *Chinese Hackers Hit Commerce Department*, TECH WEB, Oct. 6, 2006, http://www.techweb.com/showArticle.jhtml;jsessionid=OM4E5LCHY4W0WQSNDLRCKHSCJUNN2JVN?articleID=193105174.

[156] *See, e.g.*, Jeremiah Grossman—The devil made me do it, http://jeremiahgrossman.blogspot.com/2006/07/devil-made-me-do-it.html (July 18, 2006) (describing how XSS exploitation could be used to frame someone for launching attacks on government or other websites).

[157] *See, e.g.*, Robert Vamosi, *Is China's Guangdong Province Ground Zero for Hackers?*, ZD NET, Aug. 30, 2001, http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2808609,00.html; *Hacker Attacks in U.S. Linked to Chinese Military*, BREITBART.COM, Dec. 12, 2005, http://www.breitbart.com/news/2005/12/12/051212224756.jwmkvntb.html.

[158] One can argue that basing attacker-attribution on the above facts produces errors analogous to those known as the "prosecutor's fallacy." *See* Michael N. Schmitt & Laura H.

Of course, one can still argue that Guangdong's status as the point of origin of the attacks has not been conclusively established. But while certainty is reassuring, it is a luxury decision-makers often cannot afford. In the cyber-world (and the real-world), it can be difficult to conclusively establish the circumstances of an event; here, as is often true for real-world events, decision-makers will sometimes have to rely on inference. For the purposes of analysis, therefore, we will assume the facts in the previous paragraph support the inference that the hypothesized BIS-style attacks were launched by "someone" in Guangdong. That brings us to the next question: how, if at all, does the inference that the attacks came from Guangdong advance the process of identifying the "someone" who is responsible for the attacks?

i. War

Point of attack origin has historically played an important role in attacker-attribution for acts of war because war is a conflict between nation-states. The victims of such attacks have therefore typically inferred with a high degree of confidence that an attack originating in another nation-state is attributable to that nation-state. If we apply this logic to the scenario given above, the U.S. could rationally infer that the BIS-style attacks on U.S. government agency computers were acts of war launched by China. It could, in effect, construe the attacks as the virtual equivalent of Japan's real-world attack on Pearl Harbor. The problem with this derivative inference[159] of responsibility lies in equating an attack inferentially launched *from* Chinese territory with an attack launched *by* the Chinese nation-state.

Historically, it was reasonable to equate transnational attacks with acts of war because only a nation-state could launch such an attack.[160] That is

---

Crocker, *DNA Typing: Novel Scientific Evidence in the Military Courts*, 32 A.F. L. REV. 227, 301 (1990) ("The prosecutor's fallacy is essentially overstating the statistical case . . . . [A]ssume a blood match results in a ninety percent probability of the accused being the source of the sample found at the crime scene. The prosecutor's fallacy is citing this figure without taking into account exculpatory evidence."); *see also* State v. Bloom, 516 N.W.2d 159, 162-63 (Minn. 1994).

[159] This inference, unlike the primary inference that the attacks came from Guangdong, is based not on ascertained facts, but on inferences from the primary inference. *See, e.g.*, Wabash Corp. v. Ross Elec. Corp., 187 F.2d 577, 601-03 (2d Cir. 1951) (Frank, J., concurring and dissenting).

[160] *See* G.A. Res. 3314, Annex Article I, U.N. GAOR, 29th Sess., U.N. Doc. A/RES/3314 (Dec. 14, 1974) ("Aggression is the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations."); *see also* Military and Paramilitary Activities (Nicar. v. U.S.), 1986 I.C.J. 14, 103 (June 27) (defining an act of war

still true for the real-world, but cyberspace gives each nation-state an incremental, highly permeable set of "virtual" national borders. Anyone with Internet access and certain skills can launch a cross-border virtual attack, not on the territory but on the machinery of an external nation-state.[161] A virtual attack is not territorially invasive, but it produces effects in the victim-state's territory that are damaging in various ways and in varying degrees. The character and extent of the damage inflicted will tend to be a function of the nature of the attack and will be examined in Section III.B.

In terms of the war calculus, there are two reasons why point of attack origin plays a more problematic role in analyzing online attacks. First, identifying the point of origin is likely to depend more on inference in online attacks than in real-world attacks; this introduces an element of ambiguity into the attribution calculus. Second, an identified external point of origin (that is, an attack originated in Nation-State X's territory) can be inconclusive. An identified external point of origin cannot routinely be construed as an attack by the point of the originating state because cyberspace gives essentially anyone the ability to launch transnational attacks.

ii. Crime-terrorism

This leaves the role that point of attack origin plays in the crime-terrorism calculus. While crime and terrorism are conceptually distinct phenomena, we will consider them jointly in this analysis because both represent threats to internal order (and, as discussed earlier, law treats terrorism as crime). Unlike war, which threatens a society's ability to maintain external order, crime and terrorism are the product of individual rather than state action.[162]

Point of attack origin has historically played a much more limited role in crime and terrorism attacker-attribution than in war attribution. While point of attack origin can inferentially indicate who may have been

---

as "action by regular armed forces across an international border" and sending "armed bands . . . which carry out acts of armed force against another State" (quoting G.A. Res. 3314, Annex Article 3(g)), *supra*).

[161] *See, e.g.*, Peter Warren, *Smash and Grab, the Hi-Tech Way*, GUARDIAN (Manchester, U.K.), Jan. 19, 2006, *available at* http://technology.guardian.co.uk/weekly/story/0,,1689093,00.html (writing of the virtual attack "aimed at stealing sensitive information" on computers used by Parliament).

[162] This proposition becomes problematic for state-sponsored crime and state-sponsored terrorism, which we will consider briefly in Section III.A.2.a.iii, *infra*, and in more detail in Section III.B.2, *infra*.

responsible for a crime or an act of terrorism, the link between origin and attribution is much more attenuated than in war analysis.

The primary reason for this is that in the real-world, point of attack origin and point of attack occurrence are often so closely related as to be indistinguishable for crime, and even for terrorism.[163] A crack dealer buys and sells crack in his neighborhood;[164] the points of origin and occurrence of his drug crimes are functionally identical. In 1982, the Irish National Liberation Army (INLA), a terrorist group, bombed a disco frequented by British soldiers in Ballykelly, Northern Ireland, killing eleven soldiers and six civilians; the INLA agents who carried out the bombing operated out of nearby Derry.[165] Since the points of attack origin and occurrence for this act of terrorism were separated by only a short distance, one can argue that they are functionally identical here as well.

If there is little or no differentiation between the point of attack origin and the point of attack occurrence, identifying the point of origin is unlikely to markedly advance the process of identifying the attacker. Assume a woman is raped as she leaves Ladies Night at a neighborhood bar. She left at closing time and was attacked in the nearby parking lot where she left her car.[166] Police are likely to infer that the attacker is an opportunistic local who is familiar with the bar's closing time, with its Ladies Nights, and with the fact that patrons use the rather isolated parking lot.[167] This inference establishes that, insofar as an attack such as this has a distinct point of origin, it is in the local area. This inference would also play a role in the police's attempt to identify the rapist by focusing their efforts on the area the bar serves. Police would interview people who might have seen

---

[163] As I have explained elsewhere, spatial proximity between attacker and victim has historically been an inevitable element of real-world crime and, to a somewhat lesser extent, of real-world terrorism. *See* Brenner, *Toward a Criminal Law for Cyberspace*, *supra* note 5, at 65-76. Proximity has been unavoidable because both have required direct physical action by the attacker against the victim. *See id.*; *see also* History of Terrorism—Wikipedia, *supra* note 98. The development of timing devices created a limited potential for the remote commission of crime and terrorism, but physical proximity remains the norm for real-world activity. *See, e.g.*, discussion *supra* note 100.

[164] *See, e.g.*, GEORGE F. RENGERT, THE GEOGRAPHY OF ILLEGAL DRUGS 67-90 (1996).

[165] *See* Dominic McGlinchey—Wikipedia, http://en.wikipedia.org/wiki/Dominic_McGlinchey (last visited Apr. 21, 2007); Irish National Liberation Army—Wikipedia, http://en.wikipedia.org/wiki/INLA (last visited Apr. 21, 2007).

[166] We will assume that the victim cannot identify her attacker and that he left no DNA for searching within police databases.

[167] It is possible he is an out-of-towner who simply happened to be driving by when the victim was walking to her car. While this inference is logically permissible, experience tells us that it is less likely to be correct than the inference given above. The police will, therefore, base their investigation on the higher probability inference.

someone in the area that night or might have heard someone talking about the rape. They would also check the location and alibis of locals with sex crime convictions and pursue other, similar leads.

As this hypothetical illustrates, point of attack origin tends to be merely one factor in the inferential and evidence-gathering processes law enforcement officers use to identify those responsible for real-world crime and terrorism. It has played a lesser, implicit role in crime and terrorism attacker-attribution because these threats to internal order have, at least until recently, come primarily, if not exclusively, from domestic actors.[168] Domestic actors are presumptively in the nation-state where the attack occurred, and investigators tend to assume that the domestic actors responsible for an attack remain in the locality where it occurred. Even when there is significant spatial differentiation between point of origin and point of occurrence, identifying the former serves at most as a clue—an inferential datum that can contribute to the identification of the attackers and, if terrorism, of the sponsoring terrorist organization.[169]

As crime and terrorism migrate online, point of attack origin can assume more importance in attacker-attribution. As we saw in our discussion of war attribution, cyberspace eliminates the need for physical proximity between attacker and victim and thereby creates the potential for increased differentiation between point of attack origin and point of occurrence.

In 1994, workers at the Rome Air Development Center (Rome Labs) in upstate New York discovered that the lab's computer systems had been hacked by unknown persons.[170] The hackers had, among other things, copied data from computers containing sensitive Air Force research and development data.[171] Since hacking (unauthorized access) is a federal crime, Air Force, Secret Service, and Federal Bureau of Investigation agents immediately began investigating the incidents, hoping to identify the perpetrators.[172] They found a complex attack signature: the attackers had

---

[168] *See* Brenner, *Toward a Criminal Law for Cyberspace*, *supra* note 5, at 65-76; Larry Copeland, *Domestic Terrorism: New Trouble at Home*, USA TODAY, Nov. 15, 2004, at 1A, *available at* http://www.usatoday.com/news/nation/2004-11-14-domestic-terrorism_x.htm.

[169] *See generally Search Continues for Witness in Clinic Bombing*, CNN.COM, Jan. 31, 1998, http://www.cnn.com/US/9801/31/clinic.bombing/?related; World Trade Center bombing—Wikipedia, http://en.wikipedia.org/wiki/World_Trade_Center_bombing (last visited Apr. 21, 2007) (in these bombings, identification of the point of origin was merely a clue in the process of identifying the attacker).

[170] *See, e.g.*, RICHARD POWER, TANGLED WEB: TALES OF DIGITAL CRIME FROM THE SHADOWS OF CYBERSPACE 66-75 (2000).

[171] *See id.*

[172] *See id.*

routed their attacks through multiple computers in various countries.[173] Through a process too intricate to describe here, the U.S. investigators eventually traced the attacks to the United Kingdom where, with Scotland Yard's assistance, they identified two adolescents as the Rome Labs attackers.[174] Both were prosecuted, though with mixed results.[175]

The Rome Labs case illustrates how and why the use of cyberspace can make attacker-attribution more difficult. Cyberspace erodes law enforcement's ability to assume that an attacker is parochial. The viability of that default assumption still holds for real-world crime, and *can* also hold for real-world terrorism, but its applicability to online crime and terrorism is increasingly problematic.

When it comes to cybercrime and even some types of cyberterrorism, the parochial-attacker assumption is most likely to hold for "personal" attacks: crimes and acts of terrorism in which the perpetrator's motives are idiosyncratically emotional.[176] In these cases—where John uses cyberspace to stalk his former girlfriend or Jane uses it to attack her employer—the perpetrator and victim are in the same area, but instead of using physical

---

[173] *See id.*

[174] *See id.* For more on the investigation, see *infra* notes 231-239 and accompanying text.

[175] *See* POWER, *supra* note 170, at 70-75 (one pled guilty, charges were dropped against the other).

[176] These cybercrimes include revenge attacks by former spouses/lovers and current or former employees, as well as more generalized cyberstalking and harassment. *See* Susan W. Brenner, *Should Criminal Liability Be Used to Control Online Speech?*, 76 MISS. L.J. (forthcoming 2007); Drew Cullen, *UBS Logic Bomber Jailed for Eight Years*, REGISTER (London), Dec. 13, 2006, http://www.theregister.co.uk/2006/12/13/ubs_logic_bomber_sentenced/; Devin Smith & Marsha Kranes, *Match.creep: Cop Hounded Ex on Dating Site*, N.Y. POST, Apr. 4, 2006, at 19, *available at* 2006 WLNR 6494179.

Terrorist attacks of this type can include the efforts of groups such as the Red Hackers Association, a "revolutionary" organization that seems primarily to target Turkish government and political websites. *See, e.g.*, Press Release, Red Hackers Ass'n (Dec. 24, 2006) (on file with author); Press Release, Red Hackers Ass'n (Dec. 18, 2006), *available at* http://istanbul.indymedia.org/news/2006/12/161565.php. In December 2006, for example, the Red Hackers Association posted messages on target sites condemning the 2000 "massacre" of revolutionaries being held in Turkish prisons. *See* Justus Leicht, *Turkish State Suppresses Prison Revolts*, WORLD SOCIALIST WEB SITE, Dec. 22, 2000, *available at* http://www.wsws.org/articles/2000/dec2000/turk-d22.shtml; Press Release, Red Hackers Ass'n (Dec. 24, 2006), *supra*. Since their efforts are intended to promote an ideological agenda, the Red Hackers might be characterized as domestic terrorists, given their focus on localized issues. Their latest efforts would fall within the category noted above because they have a specific emotional component, that is, the efforts are reactions to the 2000 prison "massacre."

activity in that real-space to conduct the attack, the perpetrator vectors it through cyberspace.[177]

This creates an epistemological issue: When attacker and attacked are in the same real-space area throughout an attack conducted online, did the attack originate in the real-space occupied by attacker and victim, online, or in both? For the purposes of attacker-attribution, the answer should be both.

In "personal" attack cases, the connections between attacker and victim mean that the parochial-attacker assumption is likely to be very useful in identifying the attacker. Thus far, cyber-vendettas seem primarily to originate in real-world contacts between attacker and victim.[178] This assessment means that investigators can profitably rely on the approach used for real-world crime and terrorism, focusing on inferences derived from a real-world context. Therefore, for the purposes of this approach, the attack should be construed as originating in the real-space occupied by attacker and victim.[179]

But the origin of the attack should not be the only focus of their investigation. When a "personal" attacker uses cyberspace, it, too, becomes a "place" of origin of the attack. Its role in the investigation of "personal" attacks is analogous to the role that a physical point of attack origin plays in the traditional investigative process. Cyberspace, like a real-world point of attack origin, becomes a source of inferential data that can be used to identify the attacker.[180] If, for instance, a stalker consistently uses a specific website in tormenting his victim, that website becomes "a" point of origin of the attack and should be treated as such.[181] Even if the attacker has not

---

[177] *See* Paul Shukovsky, *Cyberstalker Just out of Reach of Law, But Finally, He Stops*, SEATTLE POST-INTELLIGENCER, Feb. 11, 2004, *available at* http://seattlepi.nwsource.com/local/160201_cyberstalking11.html; Press Release, Office of the U.S. Attorney, S. Dist. of Cal. (Aug. 28, 2006), *available at* http://www.usdoj.gov/ usao/cas/press/cas60828-1.pdf.

[178] *See also* Leroy McFarlane & Paul Bocij, *An Exploration of Predatory Behaviour in Cyberspace: Towards a Typology of Cyberstalkers*, FIRST MONDAY, Sept. 2003, *available at* http://www.firstmonday.org/issues/issue8_9/mcfarlane/index.html (writing that investigators are in fact likely to assume a real-space point of origin for a "personal" attack case and proceed accordingly).

[179] *See, e.g.*, People v. Vijay, No. H024123, 2003 WL 23030492 (Cal. Ct. App. Dec. 19, 2003); State v. Hoying, No. 2004-CA-71, 2005 WL 678989 (Ohio Ct. App. Mar. 25, 2005); State v. Cline, No. 2002-CA-05, 2003 WL 22064118 (Ohio Ct. App. Sept. 5, 2003), *rev'd*, 816 N.E.2d 1069 (Ohio 2004); State v. Askham, 86 P.3d 1224 (Wash. 2004).

[180] It can also, as noted earlier, become a source of physical evidence. *See supra* note 169.

[181] *See, e.g.*, Smith & Kranes, *supra* note 176.

revealed his identity to the site operator, his use of that particular website may provide inferential data as to his identity.[182]

What about attacks in which the attacker is *not*, by any definition, in the same real-space as the victim? In the BIS attacks, the target was in Washington, D.C., while the attackers were (presumably) in China; in the Rome Labs attacks, the target was in upstate New York, while the attackers were in Cardiff, Wales, and London.[183] An identified point of attack origin serves a very different function in cases like these, for several reasons.

First, identifying the point of attack origin in attacks such as these serves an initial, essentially negative function in attacker-attribution. It tells the investigators that the parochial-attacker assumption and derivative investigative approach that they use for real-world crime and terrorism will probably be of little use in identifying the attackers. When an attack presents functionally coterminous points of attack origin and occurrence, we have a localized crime scene that becomes the focal point of the investigation. Evidence, inferences, observations of witnesses, and connections between victim and attacker all radiate from and revolve around this unitary crime scene. It creates a comprehensible focus for the investigation and, in so doing, makes the investigation a manageable task. In complex serial-killer cases, we have seen how expanding a single crime scene into a variegated network of geographically-dispersed, victim-idiosyncratic, real-space crime scenes can test the limits of the traditional investigative approach.[184]

But even ambitious serial killers operate on a limited geographical scale: in the U.S., they have tended to confine their activities to a smaller

---

[182] *See id.*

[183] *See, e.g.*, *Targeting the Pentagon*, SUNDAY TIMES (London), Mar. 30, 1998, *available at* http://marc.theaimsgroup.com/?l=isn&m=100434567710396&w=2-.

[184] *See, e.g.*, ANN RULE, GREEN RIVER, RUNNING RED: THE REAL STORY OF THE GREEN RIVER KILLER—AMERICA'S DEADLIEST SERIAL KILLER (2004); *see also* Andrei Chikatilo—Wikipedia, http://en.wikipedia.org/wiki/Andrei_Chikatilo (last visited Apr. 21, 2007). Serial killers are a useful analog here because while their attacks take place in real-space, they are not "personal" in the sense used earlier:

> Murder is usually either a crime of personal relationships . . . or an unintended consequence of other crimes. Because of this, most murders are . . . simple to solve; in most familial deaths, the murderer makes little . . . effort to conceal the crime . . . ; in other cases, the murderer is usually a local . . . . These assumptions, with which any law enforcement officer naturally approaches a single murder, are barriers to catching a serial killer.
>
> Another barrier to serial killers' early capture is their . . . choices of victim . . . . They almost never have any links to their victims—they pick by whim or impulse, seeking types or opportunity rather than any easily detectable link.

Serial killer—Wikipedia, http://en.wikipedia.org/wiki/Serial_killer (last visited Apr. 21, 2007).

area within a state, sometimes to the state itself, and in unusual instances, to surrounding states.[185] The physical constraints of the real-world limit the frequency and geographical dispersion of the attacks real-world serial killers can successfully carry out.[186] However, this limitation is not true for other offenses once cyberspace becomes a component of criminal and/or terrorist activity. Instead, one can strike anonymously from any point connected to the Internet and iterate the attacks with a frequency impossible in the real-world.[187]

Cyberspace fractures the crime-scene into shards, the number of which depends on the particular circumstances of an attack. One constant shard is the alpha point of attack origin—the place where the attacker is physically located and from which she launches the attack. Other, variable crime scene shards (beta, gamma) are the intermediary points of transmission used in the attack; each represents the occurrence of a constituent, spatially diverse event that contributed to the success of the ultimate attack.[188] The other constant shard, the omega shard, is the place of attack occurrence, which we will examine in the next section.

Fracturing the crime scene into shards makes identifying the point of attack origin and linking it to the attacker much more difficult. Aside from anything else, a fractured crime scene can result in false positives—in investigators assuming that an intermediary point of transmission of an attack is the originating point for the attack.

This situation could have happened in the Rome Labs case. Here, the investigators initially traced the two intruders back to an ISP, "mindvox.phantom.com, in New York City."[189] The provider allegedly had ties to the Legion of Doom, a hacker group several members of which had been convicted of unlawful intrusion crimes a few years earlier.[190] The investigators could logically have assumed that this ISP was the originating point for the attack on the Rome Labs computers, given its immediate

---

[185] *See, e.g.*, Ted Bundy—Wikipedia, http://en.wikipedia.org/wiki/Ted_Bundy (last visited Apr. 21, 2007) (Bundy is an example of a serial killer who murdered in several states).

[186] *See* Brenner, *Toward a Criminal Law for Cyberspace*, *supra* note 5, at 65-76.

[187] *See id.*

[188] *See supra* note 124 and accompanying text; *see also* Jeanne Sahadi, *Credit Card Breach: Tracing Who Dunnit*, CNN/MONEY.COM, June 29, 2005, http://money.cnn.com/2005/06/28/pf/security_hackers/.

[189] POWER, *supra* note 170, at 68. Investigators also traced part of the attack to a Seattle ISP. *Id.* This discussion focuses only on the New York ISP because it provides a better illustration.

[190] *See id.* at 68.

connection to the attack and its apparent ties to hackers.[191] This assumption would have been consistent with the real-world approach to investigating crime because it tends to incorporate the notion that point of attack origin is a binary concept. Real-world "places" tend to be mutually exclusive: a real-world "place" is either the point of attack origin or it is not; if it is the point of attack origin, other "places" cannot be. Since it was clear that the immediately-proximate source of the attack was the New York ISP, it could, logically, have been deemed to be "the" point of attack origin for the Rome Labs attack.

Identifying the New York ISP as the point of origin would have been a false positive, one that most certainly would have derailed the investigation. Fortunately, the investigators continued to investigate and eventually identified a trail of attack increments that utilized many computers in various countries.[192] However, they were not able to track the increments back to their true points of origin. Ironically, the Rome Labs investigators ultimately identified the perpetrators—"Datastream Cowboy" and "Kuji"—the old-fashioned way: by using informants.[193] They knew that the attackers used these *noms de hack*, so the investigators sent people to chat rooms to see if either was taking credit for the attacks.[194] Datastream Cowboy not only took credit, he also revealed that he was from the United Kingdom and gave an informant his home telephone number.[195] It became a simple matter to identify and apprehend him, though doing the same for Kuji took a while longer.[196] This episode illustrates the way that cyberspace can fracture the crime scene into shards, which makes it more difficult to determine the point of origin of an attack.[197] Making this determination proved impossible for the Rome Labs investigators because of the intricate paths the attackers used.[198]

---

[191] Indeed, it could also have seemed a logical choice for the point of attack origin because it was in the same state where the attack occurred.

[192] *See* POWER, *supra* note 170, at 68-69.

[193] *See id.* at 70.

[194] *See id.* at 71-75.

[195] *See id.*

[196] *See id.*

[197] *See, e.g.*, DANIEL A. MORRIS, U.S. DEP'T. OF JUSTICE, TRACKING A COMPUTER HACKER (2001), http://www.cybercrime.gov/usamay2001_2.htm.

[198] Difficulty unraveling the point of origin in an attack is not unique to the Rome Labs case. *See, e.g.*, Tom Young, *IT Industry Core to Global E-Crime Battle*, IT WEEK, Nov. 9, 2006, http://www.itweek.co.uk/computing/analysis/2168266/industry-core-global-crime (quoting an FBI Special Agent who "estimates that fewer than five per cent of international e-criminals are caught." The agent also notes that "evidence is in many different areas—personal PCs, corporate databases, all over the world—which makes it particularly difficult.").

Another issue that can complicate the process of backtracking through a series of incremental attack stages is the legal process involved.[199] Incremental attack stages will almost certainly involve the use of computers in different countries.[200] To gain access to the necessary information to trace an attack back through those computers, law enforcement will have to obtain assistance from government and civilian entities in the countries in which the computers were used.[201] This process can be difficult and time-consuming. The formal methods used to obtain assistance can take months or even years when digital evidence is fragile and can disappear by the time the investigators obtain the assistance they need.[202] Furthermore, not all countries have criminalized hacking or other computer malfeasance, sometimes making it impossible to obtain assistance from the authorities.[203]

Even if the investigators obtain the assistance they need and are confident they have traced an attack back to its true point of origin, this may not markedly advance their effort to identify the attacker. The BIS attacks are instructive in this regard. Investigators in that case accurately ascertained that the attacks came from servers in China. However, this information could neither directly nor inferentially establish who was responsible for the attacks or, indeed, what *kind* of attacks they were.

In some instances, identifying the ultimate extraterritorial point of attack origin can serve the same function an identified point of origin serves in investigating real-world crime—it can become an inferential datum that contributes to identifying the attacker.[204] Assume the FBI has information independently derived from informants or from other online investigations that a Romanian gang is engaged in phishing.[205] If the FBI then traces a phishing attack to Romania, it would be reasonable to infer that it came from the gang already under suspicion.[206] The inference would be

---

[199] *See, e.g.*, MORRIS, *supra* note 197.

[200] *See, e.g.*, Young, *supra* note 198 (reporting that the FBI Special Agent said international cybercriminals "are specialists in . . . covering their tracks").

[201] *See, e.g.*, Susan W. Brenner & Joseph J. Schwerha IV, *Transnational Evidence-Gathering and Local Prosecution of International Cybercrime*, 20 J. MARSHALL J. COMPUTER & INFO. L. 347, 354-88 (2002).

[202] *See id.*; *see also* Young, *supra* note 198.

[203] *See* Brenner & Schwerha IV, *supra* note 201.

[204] *See supra* note 169 and accompanying text.

[205] *See, e.g.*, Rene Millman, *Half of all phishes from Romanian cyber gang*, PC PRO, Dec. 18, 2006, http://www.pcpro.co.uk/news/100351/half-of-all-phishes-from-romanian-cyber-gang.html. Phishing is, essentially, using online techniques to trick people into giving online criminals useful information, such as their credit card numbers, Social Security number, passwords, and usernames. *See, e.g.*, Phishing—Wikipedia, http://en.wikipedia.org/wiki/Phishing (last visited Apr. 21, 2007).

[206] This example suggests a longitudinal way in which point of attack origin can

strengthened if, say, the attack were traced to the city out of which the gang is known to operate or if the attack signature displayed elements peculiar to this gang's operations.

In sum, while point of attack origin can play a role in identifying the attackers in a cybercrime or cyberterrorism event, its function tends to be limited, and will probably become more so as cyberattackers become more sophisticated about hiding their tracks.[207]

iii. State-sponsored crime/terrorism

In the previous sections, we considered attacker-attribution and other issues presented by crime and terrorism, cyber and otherwise. We have assumed for the purpose of analysis that there is a distinct conceptual divide between war, which is conducted by nation-states, and crime and terrorism, which are carried out by individuals. While this distinction is still useful for analyzing attacker-attribution in real-world and online attacks, it is not as stable as it once was.

Over the last several decades, the hybrid phenomena of state-sponsored terrorism and state-sponsored crime have emerged as increasingly serious threats.[208] Both present distinct legal issues, most notably with regard to the efficacy of attempting to use criminal sanctions

---

contribute to the identification of an attacker or attackers. If investigators can establish point of attack origin with a high level of confidence for successive attacks, then they should be able to use the repeated occurrence of attacks emanating from this same point of origin to infer some consistency in the identity of the person or persons responsible for those attacks. *But see supra* Section III.A.2.a.

[207] *See generally* Brian Krebs, *Cyber Crime Hits the Big Time in 2006*, WASH. POST, Dec. 28, 2006, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/12/22/AR2006122200367_pf.html (reporting that 2006 saw an "unprecedented spike" in "sophisticated online attacks").

[208] *See, e.g.*, Christopher C. Joyner & Wayne P. Rothbaum, *Libya and the Aerial Incident at Lockerbie: What Lessons for International Extradition Law?*, 14 MICH. J. INT'L L. 222, 229 (1993) ("State-sponsored terrorism has emerged since the 1970s as a dangerous strain of international violence."). *But see* Susan W. Brenner & Anthony C. Crescenzi, *State-Sponsored Crime: The Futility of the Economic Espionage Act*, 28 HOUS. J. INT'L L. 389 (2006) (economic espionage as state-sponsored crime); Douglas R. Burgess, Jr., *Hostis Humani Generi: Piracy, Terrorism and a New International Law*, 13 U. MIAMI INT'L & COMP. L. REV. 293, 302-03 (2006) (writing that sixteenth-century British government regarded piracy "in much the same way as state-sponsored terrorism is viewed today"). In the discussion above "state-sponsored crime" denotes state involvement in the commission of conventional crimes, such as the theft of intellectual property. *See* Brenner & Crescenzi, *supra*. This Article is not concerned with the distinct phenomenon of state-sponsored war crimes or crimes against humanity. For more on that topic, see, e.g., Jean-Marie Simon, *The Alien Tort Claims Act: Justice or Show Trials?*, 11 B.U. INT'L L.J. 1, 50 (1993).

to deter an activity sponsored by a nation-state.[209] Aside from anything else, a sponsoring state may not cooperate in the investigation, apprehension, and extradition of those who acted on its behalf in committing criminal or terrorist acts.[210]

Notwithstanding the complexities associated with the mechanics of bringing these offenders to justice,[211] analysis of attacker-attribution for individually-perpetrated attacks and for acts of war can be useful in a state-sponsored cybercrime and cyberterrorism context. Yet, the ultimate determination of responsibility for attacks falling into these categories will require ascertaining the nature of the attacks—an issue we take up below.

To understand why this is true, reconsider the BIS attacks. We are assuming they were launched from Guangdong, China. We know they targeted computer systems used by a sensitive U.S. government agency in Washington, D.C. We analyzed how the attacker-attribution calculus should proceed if the attacks were cyberwarfare or "personal" cybercrime/cyberterrorism. Inherent in this analysis was the need to differentiate the two categories of attacks. The act of distinguishing involves both identifying an attacker and identifying the nature of an attack, because for cyberwarfare, the same factor establishes both. If the attacker-attribution calculus indicated that an attack "came from" a nation-state (command and control), we concluded it was war; otherwise, it fell into the residual category of cybercrime or cyberterrorism.

One problem with this analysis is that determining whether a cyberattack "comes from" a specific nation-state can be difficult because territorial point of attack origin can be ambiguous in this context. An attack from Guangdong might "come from" China itself or it might "come from" sport hackers[212] who are adventitiously in Guangdong. Essentially, point of attack origin's utility in attacker-attribution has, to this point, been limited to negating the proposition that an attack is an instance of cyberwarfare. If we conclude with some confidence that an attack did not "come from" a nation-state actor, we inferentially assign it to the cybercrime/cyberterrorism category and embark upon the tasks of determining precisely what it is and who is responsible for it.

---

[209] *See* Brenner & Crescenzi, *supra* note 208. *But see* COUNTRY REPORTS ON TERRORISM 2005, *supra* note 47 (describing the use of economic and other sanctions against state supporters of real-world terrorism).

[210] *See* Brenner & Crescenzi, *supra* note 208.

[211] For an examination of this issue, see *infra* Section IV.

[212] *See Secure Your Wi-Fi Network*, ACCENT, Aug. 2005, http://www.emphasisonsuccess.com/htmlArchive/aug2005/aug2005page3.html.

The other problem with our earlier analysis is that nation-state "involvement" in an attack is no longer synonymous with warfare.[213] In the real-world, we now have intermediate categories of nation-state involvement that, among other things, have given us state-sponsored crime and state-sponsored terrorism.[214] State-sponsored crime has already migrated online, and state-sponsored terrorism will certainly follow.[215] The problem, for the moment, is parsing out whether an attack is "mere" cybercrime or state-sponsored cybercrime, "mere" cyberterrorism or state-sponsored cyberterrorism.

State sponsorship necessarily involves a level of state participation in a cyberattack, but identifying a nation-state's involvement in a less-than-cyberwarfare attack will surely be difficult. Point of attack origin is unlikely to be helpful in this effort, for at least two reasons. First, the fact that an attack originates in the territory of a nation-state, even one known to be inclined to sponsor terrorist activity, is inconclusive. Attack origination on its territory *might* mean the state is involved in the attack, but it might not;[216] territorial origination is inferentially even less significant here than it is for cyberwarfare. Second, the fact an attack originates *outside* the territory of a particular nation-state does not necessarily mean the nation-state is not sponsoring the attack. As we have seen in the real-world, state sponsorship can take many forms, such as providing terrorists with "funding, weapons, training and sanctuary."[217]

A Machiavellian nation could fund and otherwise support terrorists (or criminals) who launch cyberattacks from outside its territory on a nation-state it wants to see "harmed"—economically undermined, harassed, rendered vulnerable to overtures, or intimidated in the real-world.[218] The point of attack origin might be traced and used to identify the individual attackers, but it would reveal nothing about the sponsoring nation-state's complicity in the attack; indeed, since the attacks originated outside the

---

[213] *See supra* note 208 and accompanying text.

[214] *See supra id.*; *see also supra* note 111.

[215] *See, e.g.*, ROLLINS & WILSON, *supra* note 8.

[216] *See* COUNTRY REPORTS ON TERRORISM 2005, *supra* note 47, at 16 ("The presence of terrorist safe havens in a nation . . . is not necessarily related to state sponsorship of terrorism.").

[217] State Sponsors: Iran—Council on Foreign Relations, http://www.cfr.org/publication/9362/ (last visited Apr. 21, 2007).

[218] *See* Brenner & Crescenzi, *supra* note 208; *see, e.g.*, OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXECUTIVE, ANNUAL REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE—2005 10 (2006), *available at* http://www.ncix.gov/publications/reports_speeches/reports/fecie_all/Index_fecie.html.

physical "presence" of this rogue nation-state, this nation-state would plausibly be able to deny any association with them.[219]

If the attacks were launched from within its territory, our hypothetical state sponsor of cybercrime and cyberterrorism could still credibly deny involvement with them. Physical attacks involve detectable staging efforts that can be difficult to conceal, which can make it challenging for a nation-state to disavow knowledge of (and at least tacit complicity in) activity within its borders.[220] State-sponsored cyberattacks, like their civilian counterparts, are presumably clandestine in staging and in execution, and, unlike physical attacks, involve computer activities which are harder to detect and easier to conceal. The sovereign-sponsor of such domestically-launched attacks could therefore plausibly deny knowledge of and involvement with them in the same way and for the same reasons nation-states concede their inability to identify cybercriminals ex ante (or even ex post).[221] A devious nation-state might even be able to conceal its involvement in self-interested cyberattacks by encouraging "civilian" cybercriminals and cyberterrorists to conduct their operations from within its borders since the fog of "civilian" cyberattacks would obscure the purpose and origins of the state-sponsored attacks.

As these examples illustrate, point of attack origin will not be particularly helpful in attributing state responsibility for sponsored cyberattacks because we are dealing with tiered responsibility: primary responsibility for an attack rests with the individuals who carry it out, while secondary responsibility rests with the nation-state that sponsored their efforts.[222] As discussed earlier, an identified point of attack origin can play a role in primary attacker-attribution for cybercrime and cyberterrorism; however, that role diminishes for secondary attacker-attribution because of the sponsor's indirect participation in the attack.

---

[219] This becomes easier as the state's level of sponsorship diminishes. *See, e.g.*, PILLAR, *supra* note 41, at 157-96 (distinguishing state-sponsors of terrorism, state-enablers of terrorism, and state-cooperators in terrorism).

[220] *See, e.g.*, Michael Elliott, *They Had a Plan*, TIME, Aug. 2, 2002, *available at* http://www.time.com/time/covers/1101020812/story.html (discussing al-Qaeda in Afghanistan prior to 9/11); Bay of Pigs Invasion—Wikipedia, http://en.wikipedia.org/wiki/Bay_of_Pigs_Invasion (last visited Apr. 21, 2007).

[221] *See* Brenner, *Toward a Criminal Law for Cyberspace*, *supra* note 5, at 65-76.

[222] *See* COUNTRY REPORTS ON TERRORISM 2005, *supra* note 47, at 173, 176-77 (listing Iran and Syria as nation-states with secondary responsibility).

b. Occurrence

As we saw above, point of attack occurrence plays a pivotal role in real-world attacker-attribution. We shall see below that its role diminishes as attacks move online.

i. War

For real-world warfare, point of attack occurrence is the essential complement to point of attack origin, its inevitable counterpoint in the attack dynamic. Point of attack origin tells us which country (or countries, since war can be a plural dynamic) has initiated war; point of attack occurrence tells us which country is the "victim." The points of attack origin and occurrence will therefore be in different countries when the attack constitutes an act of war.

This calculus is unambiguous in the real-world because "place" is unambiguous in the real-world. For example, when Germany invaded Poland in 1939, it clearly initiated war.[223] The calculus becomes ambiguous if and when warfare migrates online. We saw earlier how defining point of attack origin becomes problematic in this context. Even if we can ascertain with the requisite level of confidence that an online act of war "came from" a specific nation-state, we cannot reflexively attribute that attack to the nation-state from which it came.[224]

Similar problems arise as to point of attack occurrence. We return to the BIS attacks. They occurred here in the United States. What, if anything, can that tell us about who is responsible for the attacks?

We will again assume for the purposes of analysis that these attacks originated in Guangdong, China. Can we infer that cyberattacks originating in China and occurring "in" the United States represent acts of war attributable to the Chinese government? Unlike real-world acts of war, in this situation, we do not have the presence of enemy personnel and armament on U.S. soil. We have only the virtual "presence" of signals, bits and bytes, which traveled through cyberspace by routine means, the same means used by civilian and government traffic every second of every day. The signals bear neither state insignia nor other markers of military allegiance or intent.[225] Our only bases for possibly concluding they

---

[223] *See* Invasion of Poland (1939)—Wikipedia, *supra* note 123.

[224] Recall that the points of attack origination and occurrence have historically been in the same nation-state when an attack constitutes crime or terrorism.

[225] We are assuming the effects triggered by bits and bytes can constitute acts of war. *See, e.g.*, Davis Brown, *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, 47 HARV. INT'L L.J. 179, 179-81 (2006).

constitute components of an act of war by the Chinese government are their point of origin, their geographic destination, and the nature of the harm they inflicted (damage to U.S. government computers). I will defer my consideration of the third factor until later, because it concerns the nature of the attack,[226] but will analyze the other two factors now.

We have already analyzed the inherent ambiguity of the point of origin of this attack, which lies in *determining* the point of origin. Here, the point of attack occurrence is not ambiguous in and of itself; we know it occurred in the United States. The ambiguity lies in the implications of this point of attack occurrence. In the real-world, the occurrence of an act of war on Nation-State A's territory is equivalent to a declaration of war by the nation responsible for the attack. This is because war has historically been about territory; the violation of one nation-state's territorial integrity by agents of another nation-state is a challenge to its ability to maintain external order, that is, to sustain its existence as an autonomous entity.[227]

In the real-world, then, the singular inference to be drawn from an attack originating in the territory of one nation-state and occurring inside the territory of another is war; real-world transborder attacks have been equated with warfare because only nation-states could (and did) launch such attacks. If we were dealing with real-world attacks, therefore, the rational (if not exclusive) inference would be that they were acts of war launched by China.

But we are not in the real-world; we are in the cyberworld, where transborder attacks are not the exclusive province of nation-states. We therefore cannot infer from the mere fact that the attacks targeted computers on U.S. territory that this is the equivalent of Hitler invading Poland. Instead, it could be adolescent sport hackers in Guangdong exploring U.S computers.[228] In utilizing point of attack occurrence as a factor in attacker-attribution, we must modify the assumption that equates transborder attacks with war so it incorporates a basic reality of the online environment. U.S. government and civilian computers now come within an analog of the

---

[226] *See infra* Section III.B.2.

[227] *See* Brenner, *Toward a Criminal Law for Cyberspace*, *supra* note 5, at 45-46.

[228] *See, e.g.*, *Interview with John Arquilla*, *Frontline* (PBS television broadcast Apr. 24, 2003), *available at* http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/arquilla.html:

> Moonlight Maze, this intrusion into Defense Department computers that went on over a considerable period of time . . . highlights the problem of identifying the ultimate user. Some tracking was done back to systems in Moscow . . . . But that, by no means, suggests that these were Russians doing this. It could easily have been someone operating in an entirely other part of the world who bounced off of a computer in Russia. Or it could have been the Russians . . . . You simply don't know who's coming at you.

Willie Sutton rule; that is, they are attacked because they are particularly attractive targets for criminals, terrorists, and, ultimately, nation-states bent on war.[229] Since U.S. computers are attractive targets for all three categories of attackers, and since any of them can launch transborder attacks, the mere fact that an externally-launched attack occurs "in" the United States cannot sustain the conclusion that the attack was an act of war on the part of the nation-state from whose territory it originated.[230]

For cyberwarfare, determining attacker identity is often associated with establishing the nature of an attack. Those charged with uncovering attacker-attribution will have to determine if an attack is actually cyberwarfare before they can begin assigning blame to sovereign entities. We will return to this issue later, in our consideration of attack-attribution.[231]

ii. Crime-terrorism

Point of attack occurrence is an integral component of attacker-attribution for crimes and acts of terrorism. Real-world investigations concentrate on the scene of the crime or terrorist event, on the place where the attack occurred. This investigative model is based on the assumption that the players in the attack dynamic (criminals/terrorists and victims) occupied shared real-space; this assumption derives from the inescapable fact that physical proximity is an essential prerequisite for the commission of real-world crime or terrorism.

Thus, the point of attack occurrence plays a central role in the investigation of these real-world events. It is the most likely source of physical evidence and eyewitness testimony that can be used to identify an attacker and link him to the crime/act of terrorism. The larger spatial context in which the immediate crime scene resides provides a potential source of further testimony and data that can become the basis of inferential linkages between victim and attacker. And sometimes the place where the attack occurs can itself become a source of inference as to the likely identity of an attacker. If someone is murdered in a home with an armed alarm system, this suggests the attacker knew the victim; but if jewelry disappears from a locked safe in a jewelry store, this suggests the thief was an insider who had access to the safe's combination.[232]

---

[229] Apocryphally Willie Sutton said he robbed banks "because that's where the money is." Willie Sutton—Wikipedia, http://en.wikipedia.org/wiki/Willie_Sutton (last visited Apr. 21, 2007).

[230] However, as described immediately below, it can contribute to that conclusion.

[231] *See infra* Section III.B.

[232] *See, e.g., Sex, Lies And The Doctor's Wife*, CBS NEWS, June 6, 2006,

Here, again, the importance of point of attack occurrence diminishes as attacks move online. A real-space attacker's gaining entry to a home that has an armed alarm system suggests the attacker knew the victim, but a cyberspace attacker's gaining entry to a home computer hooked to a cable modem does not. Similarly, a hacker's transferring funds from online bank accounts is likely not an inside job. Although the bank presumably had measures in place that were intended to limit virtual access to the accounts, the compromise of those measures, unlike the compromise of the jewelry store safe, did not necessarily involve privileged physical access either to the accounts or to "inside" information needed to access them. Investigators can infer with a high degree of confidence that the compromise of the jewelry store safe came from an employee or a former employee who was given the combination as a routine part of his employment or from someone with whom that employee shared the information. The physical constraints that govern action in the real-world make it eminently reasonable to draw certain inferences from the place where an attack occurred; the absence of those constraints makes it problematic, if not impossible, to predicate similar inferences on the place where a virtual attack occurred. Cyberspace nullifies the influence of the three spatial dimensions that constrain action in the real-world and, in so doing, erodes the significance of place in attacker-attribution.

The point of attack occurrence still plays a role in attacker-attribution for online crimes and acts of terrorism because it is literally the place where an attack occurred. More precisely, it is the place where the virtual attack was consummated. Real-world attacks are initiated and consummated in a single physical place, which then becomes the crime scene. As we saw earlier, the utilization of cyberspace breaks the crime scene into shards. Here, the place where the attack actually occurs—where the harm is inflicted on the victim—is part of a larger crime scene. Like a real-world crime scene, it will contain evidence that can be used in an attempt to track the person(s) responsible for the attack. Unlike a real-world crime scene, however, it is not self-contained; the evidence found at this virtual crime scene is part of a sequence of digital evidence that is strewn around cyberspace and stored on the computers used in the attack. Since the ultimate crime scene accounts for only part of the available evidence, its role in the inferential process of identifying the attacker is accordingly reduced.

---

http://www.cbsnews.com/stories/2005/11/09/48hours/main1028132.shtml; Ali Winston, *$13G "Inside Job" Jewelry Theft*, JERSEY J. (Jersey City, N.J.), Dec. 8, 2006, *available at* http://www.nj.com/news/jjournal/index.ssf?/base/news-3/116556105967210.xml&coll=3.

And as with cyberwarfare, determining the identity of the attacker responsible for crimes or acts of terrorism will often be bound up with determining the nature of an attack. I return to this issue in Section III.B.

iii. State-sponsored crime/terrorism

The role of point of attack occurrence in attacker-attribution for state-sponsored cybercrime and cyberterrorism is functionally indistinguishable from the role it plays in assigning individual responsibility for online crime and acts of terrorism. Here, too, it is simply part of the total crime scene—the point at which an attack is consummated. Digital evidence retrieved from the point of attack occurrence can be used in efforts to backtrack the attack to its source and can be the basis for an inference as to primary and secondary responsibility for an attack, once investigators determine that it was state-sponsored. In making this determination, investigators should factor the analog of the Willie Sutton rule into the calculus because, as we saw earlier, point of attack occurrence cannot itself sustain a finding of nation-state responsibility.

And here, as with cyberwarfare, cybercrime, and cyberterrorism, determining the identity of the attacker will often be bound up with determining the nature of an attack. We consider this issue in the next section.

B. ATTACK-ATTRIBUTION

As we saw earlier, attacker-attribution (who-attribution) has historically been problematic in the real-world, at least for crime and terrorism, but attack-attribution (what-attribution) has not. The reason for this lies in the distinction societies have drawn between threats to internal order and threats to external order.[233] In the real-world, that distinction traditionally divided attacks into two categories: crime/terrorism (internal) and war (external).[234]

This division, and the distinction upon which it was predicated, arose from the realities of the physical world. At least until the last century, the limitations of travel and state monopolization of military-grade weaponry made it functionally impossible for non-state actors to challenge a nation-state's ability to maintain its territorial integrity as a sovereign entity.[235]

---

[233] *See* Brenner, *Toward a Criminal Law for Cyberspace*, *supra* note 5, at 49-65.

[234] *See id.*

[235] This assumes the challenge is to the core territory that gives a nation-state its identity, rather than to satellite territory to which the nation-state additionally lays claim. One could, for example, point to the American Revolution as an instance in which non-state actors challenged a nation-state's territorial integrity, since Britain claimed the colonies and the

External order was a purely sovereign concern; nation-states challenged each other in the international arena and resolved matters with military combat. Non-state actors were limited to challenging a state's ability to maintain internal order; criminals' pursuit of self-gratification and the more doctrinaire activities of terrorists threatened to erode social order in varying ways and to varying degrees. For at least a century and a half, nation-states have employed a unique strategy—civilian law enforcement—to control internal threats.[236] This two-pronged strategy consists of adopting laws that criminalize crime and terrorism and using a specialized, quasi-military force to identify and apprehend those who violate the laws.[237] Violators are prosecuted, convicted, and sanctioned, which presumptively deters them from re-offending and others from following their example.[238]

The sections below examine attacker-attribution, in the real-world and then in the virtual world of cyberspace. As part of this analysis, the first section incorporates some consideration of the response mechanisms we employ for each category of threats in the real-world; the next section continues that approach by demonstrating how the attribution ambiguity in online attacks impacts response mechanisms.

---

territory they comprised as its own.

One problem with characterizing this incident as an exception to the rule set out above is that the American revolutionaries regarded themselves as agents of another nation-state, a newly-emerged nation-state that now exercised sovereign authority over territory that had been under British control. If we accept that characterization, then the American Revolution (and similar colonial revolts) becomes a struggle between two nation-states that threatened the new American sovereignty's ability to maintain external order. One could argue that the struggle also threatened Britain's ability to maintain external order insofar as the American colonies were a component of its territorial integrity. The conceptual problem with this argument is that Britain was not confronting an external enemy nation-state, the activities of which threatened its ability to survive as a sovereign entity; instead, it essentially confronted a challenge to internal order in a satellite territory. Since the revolutionaries succeeded, Britain lost control over internal order in that territory to a new sovereign composed of local actors; if Britain had succeeded, it would have restored the "old" internal order and, no doubt, treated the revolutionaries as criminals.

The general point is that while non-state actors did challenge nation-state authority prior to the twentieth century, those challenges did not make the internal/external threat configuration problematic. Nation-states might use military force to deal with protestors and revolutionaries, but they ultimately approached them as threats to internal order—as "criminals."

[236] *See* Brenner, *Toward a Criminal Law for Cyberspace*, *supra* note 5, at 49-65.

[237] *See id.*

[238] *See id.*

1. Real-world

As a combined function of history and empirical circumstance, real-world attacks have fallen discretely into either of two categories: crime/terrorism or warfare. In analyzing attacker-attribution, we saw how and why the respective distinguishing characteristics of crime/terrorism and warfare have been apparent and unambiguous in the real-world.

Crime is easy to identify because it involves the civilian-on-civilian infliction of familiar categories of harm, such as theft, robbery, rape, murder, fraud, and arson.[239] Crime also tends to be limited in scale because of the constraints that physical reality imposes on action in the real-world.[240] The next most common crime scale model in the real-world is many-to-one victimization; however, the one-to-many victimization typical of cybercrime is almost unknown in the real-world because of the physical constraints noted above.[241]

Real-world terrorism is also usually easy to identify even though it involves activity that can fall within the definition of crime, harming people and destroying property. Real-world terrorism can usually be distinguished from crime because (1) it seems irrational in that it has no obvious mundane motive, such as self-enrichment or revenge; and (2) the scale on which it is committed often vastly exceeds what we encounter with crime. Take the attacks on the World Trade Center: they were irrational in that they produced no financial gains (unlike bombing one of the towers to rob a bank) and redressed no personal grievances. We regard crime as rational when it is committed for financial gain or for emotional reasons that have an underlying logical calculus, such as revenge.

There are irrational crimes. In the U.S., one can read daily about murders that were committed for no rational reason, such as ridding oneself of an unwanted spouse. But those crimes tend to be "personal"—to be the product of relationships. Family members kill each other; employees "go postal" and kill co-workers. In these crimes there is a link, a factual nexus between the perpetrator and the victims. And as with all crimes, they also tend to be limited in scale; the perpetrator kills the person she knows and with whom she is angry.

We do on occasion have what seem to be purely irrational incidents of mass murder and serial killings, but here, too, it is usually obvious that we are dealing with crime, not terrorism. As one source noted, in mass murder the motive "is likely to be personal," while serial killings "'often [have] a

---

[239] *See id.*

[240] *See id.*

[241] *See id.*

sexual component.'"[242] Even though the underlying rationale (if any) of these crimes may not be immediately apparent, we understand from the circumstances of their commission that they are, in fact, crimes. We realize that the mass murderer who climbs a tower and shoots anyone who comes within range is engaged in an act that is one step removed from "personal" assault—that is, he is taking revenge for real or wholly perceived wrongs fortuitously and indiscriminately. We also realize that the activities of serial killers—which otherwise seem incomprehensible—are the product of what seems to be a distinct psychopathology that drives them to "hunt humans."[243]

Terrorism is fundamentally different. It derives not from "personal" concerns or skewed psyches but from ideology. In real-world terrorism, the activity is *actually* but not *ostensibly* rational: Why would anyone fly a plane into the World Trade Center? The motivations of the Al Qaeda members who actually did this are quite rational if one accepts the ideological premises from which they operated. But to the uninitiated, the conduct seems irrational because of the nature of the act itself and because the actors forfeited their lives. Nearly all criminals (even mass murderers) try to survive; their motives come from self-interest, not sacrifice.

As noted above, another factor is the scale on which harm is inflicted. Because crime is the product of individual motivations and the physical constraints governing activity in the real-world, it tends to be committed on a limited scale.[244] A mugger robs one victim, a rapist assaults another, a killer murders yet another; in each instance, as with most crime, we have one-to-one victimization.[245] The scale on which terrorism is committed tends to be more inexact, regardless of whether it involves flying planes into buildings or suicide bombing. Consider the suicide bomber. He wants to inflict as much death, injury, and property destruction as possible, and takes that into account in selecting the area where he will detonate his bomb. However, the scale on which he will actually inflict harm remains uncertain until the attack has been consummated because the context in which suicide bombers operate (unannounced attacks in public areas) is fluid. The harm the bomber inflicts will almost certainly exceed that attributable to any crime, because whereas crime inflicts a focused harm

---

[242] Sara Knox, *A Gruesome Accounting: Mass, Serial and Spree Killing in the Mediated Public Sphere*, 1 J. FOR CRIME, CONFLICT & MEDIA 1, 4 (2004) (quoting Elliott Leyton, *Serial and Mass Murderers*, *in* THE ENCYCLOPEDIA OF VIOLENCE 279, 281 (Lester Kurtz & Jennifer Turpin eds., 1998)).

[243] *See, e.g.*, ELLIOTT LEYTON, HUNTING HUMANS: THE RISE OF THE MODERN MULTIPLE MURDERER 5-10 (2005).

[244] *See* Brenner, *Toward a Criminal Law for Cyberspace*, *supra* note 5, at 49-65.

[245] *See id.*

(profit, revenge, sexual control), terrorism inflicts generalized, variegated harms. Aside from anything else, the theatrical nature of terrorist violence usually serves to distinguish it from criminal violence.

Finally, as we saw in analyzing attacker-attribution, it has been easy to identify warfare in the real-world. When the Japanese bombed Pearl Harbor, no one who saw the attack could have had the slightest doubt that this was war—not crime, nor terrorism. One nation-state's using military force to launch an attack on another nation-state's territory immediately indicates that we have left the arena of internal threats to social order and entered the theater of war.

Overall, the internal-external threat dichotomy and resulting allocation of responsibility for responding to threats has proven quite satisfactory in the real-world. There can be initial definitional ambiguity between crimes and acts of terrorism; but since both have represented purely internal threats to social order and since internal threats are addressed by civilian law enforcement, ambiguity as to whether an attack was crime or terrorism has little, if any, impact on the civilian response process. For our purposes, the residual category of war has had no corresponding definitional ambiguity[246] and no operational uncertainty; the military is exclusively responsible for responding to acts of war.[247]

2. Virtual World

Here we turn again to the BIS attacks, but now our focus is on identifying the nature of the attack, not the attacker. We addressed this issue implicitly, in our consideration of online attacker-attribution, but we

---

[246] The concept of warfare is not the unitary construct it once was. The beginning of the twenty-first century has seen "a decrease in conventional warfare with large armies and an increase in conflicts characterized as Military Operations Other Than War (MOOTW)." Eugene B. Smith, *The New Condottieri and US Policy: The Privatization of Conflict and Its Implications*, 17 PARAMETERS 104, 104 (2002), *available at* http://www.carlisle.army.mil/usawc/Parameters/02winter/smith.htm. The dissociation of warfare into discrete modes of conflict is relevant in analyzing how societies should adapt their military posture to this evolving military threat matrix, but is not relevant to the analysis we pursue here. Our focus is on how the use of computer technology impacts the attribution of and response to two generic categories of attacks: military-conducted attacks and civilian-conducted attacks.

[247] *See id.* at 106-07.

> As states matured and the concept of sovereignty developed, legitimacy was defined . . . by the ability of states to protect and control their citizens . . . . An immediate result was the withdrawal of the right of private citizens to conduct private war. The army and navy became the primary manifestation of a state's legitimacy . . . as the sole holder of the legitimate means to enforce order.

Id.

need to articulate why online attack-attribution becomes problematic and how this impacts our response processes.

We begin by parsing out what we know of the BIS attacks. It is clear they were deliberate, orchestrated attacks, not computer malfunctions; they targeted computers used by a federal agency; they originated in China; and we assume they came from Guangdong, which is reputationally associated with China's efforts to develop cyberwarfare capability. We do not know what the attackers sought to accomplish,[248] but because we know we were attacked, we must decide how to respond.[249]

Deciding how to respond requires determining what kind of attacks these were; as we saw earlier, the attack-response dynamic is consistent across all three categories of attacks—crime, terrorism, and war. Under our current attack-response model, once we know what kind of attack we are dealing with (internal threat versus external threat), we know what response process is appropriate. If the BIS attacks were crime or terrorism, civilian law enforcement (of whatever level) will respond;[250] if they were cyberwarfare, the military will respond.[251]

We explored the inherent ambiguity of the attack in our analysis of attacker-attribution and the same issues arise here as well. The circumstances of the attack suggest it was a sortie into cyberwarfare—an attack launched at the behest of the Chinese government. As we saw

---

[248] *See* Sipress, *supra* note 2.

[249] We assume for the purpose of analysis that a response is in order. If we decide the attacks were cybercrime or cyberterrorism, then that will certainly be the case. If we decide they were a foray into cyberwarfare, we may or may not want to respond; if we believe the attacks represent the efforts of military hackers who were testing the strength of our online defenses, then we might not want to respond actively, at least not immediately. We might decide on a passive response, in which we observe any future efforts of this type to see what we can learn about our adversary; indeed, we might want to create a federal computer honeypot so we can learn as much as possible about our uncertain adversary and the tactics it employs. For more on honeypots, see, e.g., Honeypot (computing)—Wikipedia, http://en.wikipedia.org/wiki/Honeypot_%28computing%29 (last visited Apr. 21, 2007).

[250] *See* Brenner, *Toward a Criminal Law for Cyberspace*, *supra* note 5, at 49-65. Since the attacks targeted computers used by the federal government, federal law enforcement agents responded. If they had targeted computers used by state or local government, state or local law enforcement officers would have responded, possibly with the assistance of federal law enforcement agents. If they had targeted computers used by a large corporation, the response could have come from federal or state law enforcement agents or, more likely, from a combination of both.

[251] *See also Missile Defense: Hearing Before the S. Armed Forces Servs. Comm. Subcomm. on Strategic Forces*, 109th Cong. (2005) (statement of Gen. James E. Cartwright, USMC, Commander, U.S. Strategic Command) (stating that Network Warfare Joint Functional Component Command "will facilitate . . . engagement with other national entities in computer network defense and offensive information warfare"), *available at* http://www.nti.org/e_research/official_docs/congress/senate040705Cartwright.pdf.

earlier, an attack originating from the territory of one nation-state and terminating on the territory of another nation-state has presumptively constituted an act of war; the validity of that conclusion is reinforced here by the fact that the attacks targeted federal computers rather than civilian or state computers. The nature of the target therefore provides inferential support for the premise that the attacks were an initial, even tentative foray into cyberwarfare. While we do not know precisely what the attacks were meant to accomplish, we could logically conclude that they were a virtual reconnaissance by China's military, a testing of the security of U.S. government computer systems. If we were to arrive at this conclusion with the requisite level of confidence, we would have to decide whether to respond, and if we decided a response was in order, we would have to decide what type of response would be appropriate.[252] Since we have, in this analytical branch, concluded that the attacks were cyberwarfare, these decisions and any response will come from the U.S. military. Since we have, at least to this point, decided we are dealing with an external threat to order, civilian law enforcement will not be involved in the decision-making or response processes.

The problem with this analysis is that we cannot conclude the BIS attacks constituted cyberwarfare with the requisite level of confidence because the circumstances—the indicators—we must rely on take on an ambiguity lacking in the real-world. The fact that the attacks originated from the territory of another nation-state is a circumstance we can consider in attack-attribution, but it carries much less weight than in the real-world; as we saw earlier, cyberspace makes it possible for anyone with an Internet connection and a base level of computer skills to attack a computer in another country. The transnational aspect of the attack *may* be significant, but it also may not be; and the same is true of the attacks' origination in Guangdong and targeting of computers used by a federal agency. Guangdong province has been producing hackers for years,[253] and civilian hackers of many nationalities have been exploring federal computers for years.[254] It is therefore equally as possible that the attacks came from sport hackers in Guangdong[255] as it is that they came from the Chinese government.

---

[252] *See supra* note 249.

[253] *See, e.g.*, Vamosi, *supra* note 157.

[254] *See, e.g.*, Colin Barker, *The NASA Hacker: Scapegoat or Public Enemy?*, ZD NET, July 13, 2005, http://news.zdnet.co.uk/security/0,1000000189,39208862,00.htm.

[255] *See* Vamosi, *supra* note 157. It might also be *possible* that the attacks came from cyberterrorists operating out of Guangdong, but since we have no facts pointing to terrorists operating out of Guangdong, we cannot logically arrive at that conclusion. It is also possible that the attacks constitute state-sponsored cyberterrorism, but, again, the bare facts we have

If we decide the BIS attacks were civilian hacks, then they constitute cybercrime and civilian law enforcement will respond.[256] If we decide they were cyberwarfare, then the military will respond. But how do we decide—how do we resolve this inherently ambiguous situation?

As I noted earlier, our response strategy is predicated on the premise that we know, or can quickly determine, what *kind* of an attack occurred and only need to identify and neutralize the attacker(s). Our legal system incorporates that premise; as will be discussed in Section IV, it allocates responsibility for crime/terrorism to law enforcement and for war to the military. The allocation is scrupulously partitioned; civilian law enforcement does not respond to war and the military does not respond to crime.

This rigidly partitioned response authority gives rise to several concerns. One, as we saw above, is that the response process will be delayed while decision-makers try to determine the nature of an attack. Another is that the decision-makers will misunderstand the nature of an attack. What if a BIS-style attack were to target a corporate computer system? The nature of the attack target inferentially supports the conclusion that it was cybercrime, because we tend to assume criminals target civilians.[257] That conclusion would further be reinforced if the attackers' actions conformed to what we expect of cybercriminals; for example, if their efforts consisted of trying to extract funds from corporate accounts or personal information from its customer databases. Since we assume civilians are the targets of crime, not war, an attack such as this would almost certainly be construed as cybercrime and responded to by law enforcement.

---

simply provide no basis for drawing that inference with the requisite level of confidence.

[256] The same, of course, is true if we decide they were state-sponsored or "civilian" cyberterrorist attacks.

[257] This assumption derives from the internal-external threat dichotomy. We know civilians, and civilian entities, suffer harm of varying types and degrees in warfare but, as noted earlier, this is a collateral consequence of war. *See supra* notes 118-119 and accompanying text. We have therefore equated direct, intentional attacks on civilians with crime and, to a lesser degree, with terrorism. This assumption is also based in the limitations of physical reality: in the real-world, it is simply not possible for Nation-State A to physically attack Corporation XY, which is located entirely in the territory of Nation-State B, without launching a war. If Nation-State A used long-range missiles to damage Corporation XY's headquarters, that would in a sense constitute the commission of a crime against Corporation XY, but the criminal offense would be subsumed in the larger consequences of the attack; Nation-State B would construe it as war because while the attack inflicts harm on a civilian entity, it also represents an external threat to Nation-State B's sovereign integrity.

The problem is that relying on this assumption could be a mistake. The attack on our fictive corporate entity could be cyberwarfare, not cybercrime. China's focus on cyberwarfare specifically includes attacks on civilian entities, including financial and infrastructure entities.[258] If our default approach to attacks continues to be the civilian-attacks-are-crime assumption, we will certainly have a situation (or many situations) in which an act of cyberwarfare is construed, and responded to, as if it were merely cybercrime. The consequent, possibly lengthy, delay in realizing what we truly confront could have serious consequences for our financial system or other parts of our infrastructure, especially if we misinterpret a *series* of cyberattacks.

An analogous, but perhaps less serious, problem arises if the attack on our hypothetical corporate entity is cyberterrorism. Cyberterrorist attacks are unlikely to be isolated incidents; it is far more likely that a cyberterrorist event will be part of a sequence of attacks which may be separated spatially, temporally, and have different points of origin.[259] Because the corporate attack we hypothesized above seems to be "mere" cybercrime, it would be dealt with by civilian law enforcement. Except for serial killers and the odd career robber or serial arsonist, civilian law enforcement is not accustomed to approaching an attack—a crime—as part of a sequence; the officers who respond to our fictive attack will therefore not likely consider whether it may be part of a much larger attack sequence.[260] This means the civilian law enforcement response to a coordinated, sequenced cyberterrorism attack would probably be discrete and isolated; officers in different locations would respond to incidents without realizing that they were, in fact, part of a single, larger attack. As we saw above, the same could be true for cyberwarfare.[261]

This problem arises both because of our partitioned responsibility for responding to crime/terrorism versus warfare and because we tend to assume that crime, of whatever type, is a localized phenomenon. A subsidiary factor contributing to the problem is that the markers we rely

---

[258] *See supra* note 109.

[259] *See supra* notes 74-75 and accompanying text.

[260] The likelihood that they will consider this possibility will diminish, accordingly, if the attacks constituting the larger attack sequence (1) occur discretely at locations in different states or in widely-separated parts of a single state; (2) occur over a week, two weeks, a month, or longer; and (3) display different attack signatures. As to (3), the discrete attacks in a sequenced effort could target one or more financial institutions, commuter trail transport, a power grid, and communication systems. The spatial, temporal and target differentiation in the attacks would mask the fact that they are components of a single event.

[261] For essentially this scenario, see Arquilla, *The Great Cyberwar*, *supra* note 110 ("This time it is real. The great cyberwar has begun. I am sure of it.").

upon to differentiate crime/terrorism from warfare in the real-world are absent or unreliable when it comes to virtual attacks. In the real-world, we rely on three markers—or indicia—to determine the nature of an attack: (1) point of attack origin, (2) point of attack occurrence, and (3) the motive for an attack.

As we have seen, the utility of the first two markers erodes as attacks migrate online. The same is also true, but in a different way and for different reasons, of the third factor—the motive for an attack. Technology enhances our ability to inflict harm, but does not alter the human psyche; unless and until technology transforms us into cyborgs or some other variety of post-human life,[262] it is reasonable to assume that the motives which have historically driven us to inflict harm will continue to account for our doing so, on- or offline. Motive, therefore, is and will continue to be a valid differentiating factor for cyberattacks: profit drives most cybercrime; ideology drives most cyberterrorism; and nation-state rivalries drive cyberwarfare. The difficulty arises not with our ability to rely upon established motivations as a "marker" which inferentially indicates the nature of an attack. It arises instead with our ability to ascertain the motive behind a specific attack.

We saw this with the BIS attacks. We know *what* the BIS attackers did, but we cannot ascertain *why* they did it. The same has been true of other highly-publicized U.S. government and corporate attacks, including "Titan Rain" and "Moonlight Maze."[263] And the same is likely to be true of many future attacks, as well: while the motive behind what are almost certainly routine cybercrime incidents is usually apparent (greed, revenge, power over another), that may not always be true. Terrorists, for example, are increasingly using cybercrime to finance their real-world efforts, which give us a mixed-motive scenario: the motive for the commission of the cybercrimes is profit, a criminal motive; but the motive for obtaining the profit is to engage in acts of terrorism, a non-criminal motive. This mixed message scenario has few, if any, implications for the response process because civilian law enforcement responds to crime and terrorism; the efficacy of a response to a specific attack will therefore be a function of the extent to which the state targeted by the attack can adequately respond to cybercrime and cyberterrorism.

---

[262] *See, e.g.*, Transhumanism—Wikipedia, http://en.wikipedia.org/wiki/Transhumanism (last visited Apr. 21, 2007).

[263] *See, e.g.*, Thornburgh, *supra* note 154; Moonlight Maze—Wikipedia, http://en.wikipedia.org/wiki/Moonlight_Maze (last visited Apr. 21, 2007); Titan Rain—Wikipedia, http://en.wikipedia.org/wiki/Titan_Rain (last visited Apr. 21, 2007).

A variation of this "mixed message" scenario can have serious implications for a state's ability to respond to attacks. When what is ostensibly cybercrime is state-sponsored—as is often the case with economic espionage—the efficacy of the civilian law enforcement response process breaks down.[264] The sponsoring state will almost certainly refuse to cooperate with the investigative efforts of the victim state's law enforcement officers and thereby thwart the crime response process.[265] The same result will ensue when a nation-state sponsors cyberterrorism. In neither instance does the sponsoring state have any incentive to cooperate with those who are attempting to bring its agents to justice in the victimized state; indeed, the opposite is true.[266] The sponsoring state has every incentive *not* to cooperate with law enforcement from the victim state, especially if the state-sponsored cybercrime/cyberterrorism is an instance of war-but-not-war, that is, a covert campaign aimed at undermining the economic or structural stability of the victim nation-state.[267] This is a class of attacks with which we must be especially concerned, because the harm sought to be inflicted here is systemic, not individual, harm.

Another class of attacks with which we must be especially concerned is the BIS-style attack—attacks in which no apparent motive exists. The scenario in which we cannot ascertain whether attacks are cybercrime, cyberterrorism, or cyberwarfare creates the greatest challenges for our current response model, and consequently creates the greatest risks for the victim state. It creates marked risks for countries such as the United States, which rigidly partition response authority between civilian and military agents. In these systems, if potential responders cannot ascertain what kind of an attack occurred, they can neither assume nor assign responsibility for responding to it—which creates the possibility that no appropriate response will ensue.[268]

This, in turn, creates the possibility that a country like the United States could be the targets of cyberwarfare and not realize it until the attacker had inflicted substantial systemic damage; this would be particularly true if a dispersed attack seemed to represent cybercrime. Local authorities would deal discretely with each node of the attack, not

---

[264] *See* Brenner & Crescenzi, *supra* note 208.

[265] *See id.*

[266] *See id.*

[267] *See id.*

[268] *See, e.g., Cyber Attack: Is the Government Safe?: Hearing Before the S. Comm. on Governmental Affairs*, 106th Cong. (2000) (testimony of James Adams, Chief Executive Office, Infrastructure Defense, Inc.), *available at* http://www.senate.gov/~gov_affairs/030200_adams.htm (criticizing the lack of response to Moonlight Maze).

realizing they were responding to part of a greater whole.[269] It also creates the possibility that a concerted attack—cybercrime or cyberterrorism—by an organized group of non-nation-state actors could inflict similar, though perhaps not as substantial, systemic harm on the victim nation-state.[270] This latter scenario raises yet another possibility—that of sporadic, concerted attacks by one or more organized groups of non-nation-state actors.[271] While the harm these attacks inflicted would not be the immediately devastating kind of harm associated with real-world warfare or real-world terrorism on a 9/11 scale, it would be damaging, particularly if it were repeated.

This last possibility highlights another difficulty with our current, segmented response processes: civilian law enforcement and military personnel have a very limited ability to join forces in combating attacks. This is due to the persistence of the internal-external threat dichotomy.[272] Civilian law enforcement and military personnel have an even more limited ability to join forces with each other and with civilians to respond to attacks. In the nation-state model, the state monopolizes the response processes; civilians can become recruits in the military response process, but otherwise can play no legitimate role in responding to threats.[273] This is also due to the internal-external threat dichotomy. Nation-states assume they can maintain internal order with law enforcement personnel and external order with military personnel and that by doing this they establish a secure internal enclave in which civilians need have no concern with, and no responsibility for, attacks.[274] As we have seen, cyberspace erodes the validity of both assumptions.[275]

We therefore need to reconsider how we respond to cyberthreats, of whatever type. The next section undertakes that task.

IV. RESPONSE: THE CURRENT MODEL AND BEYOND

> Our enemies . . . do not recognize the artificial construct between law enforcement and national defense.[276]

---

[269] *See, e.g.*, Arquilla, *The Great Cyberwar*, *supra* note 110.

[270] *See, e.g., id.*

[271] *See, e.g., id.*

[272] *See* Brenner, *Toward a Criminal Law for Cyberspace*, *supra* note 5, at 65-76.

[273] *See id.*

[274] *See id.*

[275] *See id.*

[276] Gary Felicetti & John Luce, *The Posse Comitatus Act: Setting the Record Straight on 124 Years of Mischief and Misunderstanding Before Any More Damage Is Done*, 175 MIL. L. REV. 86, 87 (2003).

The first section below describes how our laws create the partitioned response authority cited in Section III.B.2. The next section considers how we can modify the partitioned model to improve our ability to respond to cyberattacks.

A. WHERE WE ARE

As Section III.B.2 noted, in the United States response authority is scrupulously bifurcated between military and civilian law enforcement personnel,[277] with military personnel responding to external threats (acts of war) and law enforcement personnel responding to internal threats (crime and terrorism). Further, "pure" civilians have absolutely no role in responding to crime or terrorism, and the only role they play in responding to acts of war is as recruits for a country's military forces.

This seems an eminently logical state of affairs to us because it is all we know. In the United States, the basic components of this model have been in place since the Revolutionary War ended, though they have been refined somewhat over the years. The two sections below briefly review the legal principles that are responsible for this bifurcated response authority; the first examines the military-law enforcement bifurcation, while the second examines the non-role "pure" civilians have in attack response processes.

1. Military-Law Enforcement Bifurcation

The United States' commitment to bifurcated response authority has its roots in English common law and more immediate origins in the American colonists' experience with the British military.[278] In the Declaration of Independence, colonists complained that the King's actions had "render[ed] the military independent of and superior to the Civil Powers."[279] According

---

[277] The discussion that follows makes explicit what has been implicit in what I have written so far; that is, it explicitly assumes the model of response authority in effect in the United States, both because it is the model with which I am the most familiar and because it seems to be the most extreme instance of the partitioned response authority model. The partition is not as defined, nor as rigid, in some countries. *See, e.g.*, DONALD E. SCHULZ, THE UNITED STATES AND LATIN AMERICA: SHAPING AN ELUSIVE FUTURE 37 (2000). *But see* DANIELLA ASHKENAZY, THE MILITARY IN THE SERVICE OF SOCIETY AND DEMOCRACY: THE CHALLENGE OF THE DUAL-ROLE MILITARY 5 (1994) ("[T]he military in democratic societies have not been assigned a role as a domestic law enforcement agency, with the exception of extreme circumstances of insurrection or collapse of domestic public order beyond the capabilities of civilian police.").

[278] *See, e.g.*, Nathan Canestaro, *Homeland Defense: Another Nail in the Coffin for Posse Comitatus*, 12 WASH. U. J.L. & POL'Y 99, 101-10 (2003).

[279] THE DECLARATION OF INDEPENDENCE para. 14 (U.S. 1776); *see also id.* at para. 13, 16

to one scholar, the Declaration of Independence's "'repudiation of military intervention in domestic law enforcement,' which the founders viewed as an offense against civil liberties, became 'the bedrock of due process on which the American government was built.'"[280]

The concern with limiting military power carried over to the drafting of the Constitution. The delegates to the Constitutional Convention accepted the need for a standing military force, but only "on the condition that there be safeguards established to keep the military under civilian control."[281] The Constitution consequently "allowed for a standing army and navy, but restricted military appropriations to two years, and . . . appointed a civilian commander-in-chief."[282] While the Constitution itself "did not include an explicit provision regarding the domestic use of military forces,"[283] some argue that the Bill of Rights achieves this indirectly: "Hamilton chose the Fifth Amendment's due process clause to satisfy the delegates who demanded a clear separation between civil and military authority. The Amendment's emphasis on the full and unhindered process of the law implies the superiority of the civil sphere over . . . military authority."[284]

Notwithstanding these efforts, in "the first ninety years of the republic, there was no clear . . . legal barrier to the use of federal troops to enforce the laws."[285] The Militia Act of 1792 authorized federal marshals to use state militias in enforcing civil law on the premise that the militia members were acting "as private citizens, not as soldiers."[286] In the years leading up to the Civil War, federal marshals' use of army troops to enforce federal law

---

& 27.

[280] Canestaro, *supra* note 278, at 108 (quoting David E. Engdahl, *Foundations for Military Intervention in the United States*, 7 U. PUGET SOUND L. REV. 1, 7 (1983)). The dichotomization of the civilian-military spheres of authority and the military's consequent subservience to civilian authority are essential organizing principles in democratic societies. *See* ASHKENAZY, *supra* note 277, at 4-5.

[281] Canestaro, *supra* note 278, at 109.

[282] *Id.*

[283] *Id.*

[284] *Id.*

[285] *Id.* at 109-10 (quoting Edward F. Sherman, *Contemporary Challenges to Traditional Limits on the Role of the Military in American Society*, *in* MILITARY INTERVENTION IN DEMOCRATIC SOCIETIES 216, 219 (Peter J. Rowe & Christopher J. Whelan eds., 1985)).

[286] *Id.* at 110; *see* Militia Act of 1792, ch. 28, § 2, 1 Stat. 264 (1792). The Act only permitted use of the militia "in limited circumstances where law enforcement officers . . . could not suppress a violent internal disorder." Sean J. Kealy, *Re-examining the Posse Comitatus Act: Toward a Right to Civil Law Enforcement*, 21 YALE L. & POL'Y REV. 383, 392 (2003). And it drew a "clear distinction between the citizen soldiers who may be used in emergencies and the standing army, indicating that Congress sought to exclude the regular army from law enforcement matters." *Id.*

"became commonplace," and in 1854, the Attorney General issued an opinion upholding the legality of the practice.[287]

The use of federal military personnel for law enforcement continued until its abuse in the post-Civil War South brought calls for a change.[288] "As a result, in 1878 the post-Reconstruction Congress passed the Posse Comitatus Act . . . to put an end to the use of military for ordinary law enforcement purposes."[289] The Posse Comitatus Act (PCA) is still in force, and currently provides as follows: "Whoever, except in cases . . . expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force . . . to execute the laws shall be fined . . . or imprisoned not more than two years, or both."[290] While the PCA only applies to the Army and Air Force, Department of Defense regulations extend its restrictions to the Navy and Marines.[291] It has not been applied to the Coast Guard because the Coast Guard has traditionally functioned more as a law enforcement agency than as a military entity.[292]

---

[287] Canestaro, *supra* note 278, at 110 (citing 6 Op. Att'y Gen. 466, 473 (1854)); *see also* Kealy, *supra* note 286, at 392-93.

[288] *See, e.g.*, Comment, *The Posse Comitatus Act Applied to the Prosecution of Civilians*, 53 U. KAN. L. REV. 767, 771 (2005) [hereinafter *The Posse Comitatus Act*] ("Never before or after, within the continental boundaries of the United States, did [the military] exercise police . . . functions . . . on the scale it did in the eleven ex-Confederate states from 1865 to 1877" (quoting ROBERT W. COAKLEY, THE ROLE OF FEDERAL MILITARY FORCES IN DOMESTIC DISORDERS 1789-1878 268 (1988))).

[289] *The Posse Comitatus Act*, *supra* note 288, at 772 (citing Army Appropriations Act, ch. 263, § 15, 20 Stat. 145, 152 (1878)). As one author notes, "the PCA was rarely mentioned for a century after its passage, and the courts so rarely had to interpret the law that one court described the PCA as 'obscure and all-but-forgotten.' The obscurity may have been a result of the Act's effective curtailment of military involvement in law enforcement." Kealy, *supra* note 286, at 398 (quoting Chandler v. United States, 171 F.2d 921, 936 (1st Cir. 1948)).

[290] 18 U.S.C. § 1835 (2000).

[291] *See The Posse Comitatus Act*, *supra* note 288, at 772-73 (citing U.S. Dep't of Defense, Directive No. 5525.5, DoD Cooperation with Civilian Law Enforcement Officials, encl. 4 at 4.3 (Jan. 15, 1986)). A federal statute requires the Secretary of Defense to establish regulations which ensure that law enforcement activity "does not include or permit direct participation by a member of the Army, Navy, Air Force or Marine Corps." 10 U.S.C. § 375. Prior to the enactment of the Department of Defense regulations, the Fourth Circuit had held that the Act applies all branches of the armed services. *See* United States v. Walden, 490 F.2d 372, 375 (4th Cir. 1974).

[292] *See The Posse Comitatus Act*, *supra* note 288, at 773; *see also* United States v. Chaparro-Almeida, 679 F.2d 423, 425-26 (5th Cir. 1982); Jackson v. State, 572 P.2d 87, 93 (Alaska 1977). At least two circuits have held that the Posse Comitatus Act does not apply to the Navy when it is under the control of or supporting the Coast Guard. *See* United States v. Klimavicius-Viloria, 144 F.3d 1249, 1259 (9th Cir. 1998); United States v. Kahn, 35 F.3d 426, 432 (9th Cir. 1994); United States v. Mendoza-Cecelia, 963 F.2d 1467, 1477-78 (11th Cir. 1992).

As many commentators have noted, the restrictions imposed by the PCA have eroded over the last several decades: "Since the 1970s, the courts have narrowed the scope of the Act's application, and during the 1980s, Congress specifically exempted certain military actions from the PCA, particularly in the context of the war on drugs."[293] In 1981, for example, Congress passed the Military Cooperation with Law Enforcement Officials Act, which let the military

> help enforce drug, immigration, and tariff laws. The Act . . . [allowed] the military to cooperate with law enforcement by providing equipment, research facilities, and information; by training and advising police on the use of loaned equipment; and by assisting law enforcement personnel in keeping drugs from entering the country.[294]

After 9/11, there were calls to abandon the PCA to let the military play a "greater role" in homeland defense,[295] but the general sentiment seems to be that it should neither be repealed nor further eroded.[296]

The PCA is the primary legal principle barring the military from participating in civilian law enforcement, but other federal statutes and regulations also contribute to the bifurcation.[297] The correlate aspect of this bifurcation—law enforcement's exclusion from the conduct of military operations—is a fundamental principle of the modern laws of warfare.[298] It is also implicit in the Constitution's authorizing Congress to "raise and support Armies."[299] The military is, as a treatise notes, "separate from civilian society, with a jurisprudence that exists . . . apart from the law

---

[293] Kealy, *supra* note 286, at 398; *see, e.g.*, Laird v. Tatum, 408 U.S. 1, 19 (1972).

[294] Kealy, *supra* note 286, at 409 (citing Department of Defense Authorization Act of 1982, Pub. L. No. 97-86, § 905, 95 Stat. 1115 (codified as amended at 10 U.S.C. §§ 371-78)).

[295] *See, e.g.*, *id.* at 424; *see also* Stewart M. Powell, *Bush Considers Changes to Posse Comitatus Act*, HOUS. CHRON., Oct. 2, 2005, *available at* 2005 WLNR 24636542.

[296] *See, e.g.*, Dan Bennett, Comment, *The Domestic Role of the Military in America: Why Modifying or Repealing the Posse Comitatus Act Would Be a Mistake*, 10 LEWIS & CLARK L. REV. 935 (2006); *see also* Michael T. Cunningham, *The Military's Involvement in Law Enforcement: The Threat Is Not What You Think*, 26 SEATTLE U. L. REV. 699, 717 (2003) (arguing that utilizing the military in domestic law enforcement would threaten the military's ability to "project effective, overwhelming force" in the interests of national defense).

[297] *See, e.g.*, Adam Burton, *Fixing FISA for Long War: Regulating Warrantless Surveillance in the Age of Terrorism*, 4 PIERCE L. REV. 381, 389 (2006) (asserting that the Foreign Intelligence Surveillance Act creates "a 'wall' of separation between agencies responsible for law enforcement and those responsible for military and foreign intelligence").

[298] *See, e.g.*, Hague Convention No. IV, *supra* note 115.

[299] U.S. CONST. art. I, § 8, cl. 12.

which governs" the civilian realm.[300] Its unique and exclusive function is, as the Supreme Court said, "to fight or be ready to fight wars."[301]

2. Civilian Exclusion from Attack Response

The sections below examine civilian exclusion from the law enforcement and military response processes. The first section considers law enforcement; the second analyzes the military.

a. Law Enforcement

Until the nineteenth century, civilians not only participated in law enforcement, they essentially *were* law enforcement.[302] As I have explained in more detail elsewhere, until Sir Robert Peel established the first professional police force in early nineteenth-century London, civilian law enforcement was an ad hoc process that relied heavily on the efforts of citizens.[303] Pre-nineteenth century England and the American colonies had laws that required able-bodied men to participate in apprehending criminals; American civilians, at least, were initially reluctant to surrender this function to armed professionals for fear of government over-reaching.[304] Their reluctance waned, and by the twentieth century, policing had become the sole province of law enforcement officers.[305]

The process of professionalizing policing has been so successful that civilians no longer need to assume any responsibility for controlling or preventing crime.[306] Those tasks are now monopolized by professional police forces organized in a hierarchical, quasi-military fashion.[307] Civilians' only roles in this model of crime control and prevention are as sources of evidence—witnesses or victims.[308]

---

[300] 6 C.J.S. ARMED SERVICES § 11 (note omitted).

[301] Toth v. Quarles, 350 U.S. 11, 17 (1955).

[302] *See* Brenner, *Toward a Criminal Law for Cyberspace*, *supra* note 5, at 65-76.

[303] *See id.*

[304] *See id.*

[305] *See id.*

[306] *See id.*

[307] *See id.*

[308] *See id.* The model of "community policing" that emerged at the end of the last century seeks to incorporate a level of civilian participation into the law enforcement process, but here, too, the civilians function almost exclusively as sources of information about actual or potential crimes. *See id.* Even when they take a rather more active role in crime control, civilian participants in community policing do not participate in the processes of investigating crime and apprehending perpetrators. *See id.*; *see, e.g.*, Community Policing, http://www.hawaiipolice.com/topPages/cpo.html (last visited Apr. 21, 2007).

Indeed, civilian exclusion from law enforcement is so complete that when citizens *do* participate, their actions have been given a distinct, pejorative descriptor: vigilantism. Vigilantism is essentially a civilian's "taking the law into her own hands": engaging in action that would be lawful if it were carried out by an authorized law enforcement agent.[309] Since the vigilante is not an authorized law enforcement agent, she will be prosecuted for her conduct if it violates an established criminal prohibition and she cannot raise a statutory defense to criminal charges.[310]

"Pure" vigilantism almost always involves "volunteers"—untrained, rogue actors who have taken it upon themselves to "assist" law enforcement by operating on their own.[311] Societies have long deemed "pure" vigilantism intolerable for several reasons, one of which is that the activities of "pure" vigilantes create unacceptable risks of error in offender identification and apprehension.[312] Another argument against tolerating "pure" vigilantism is that it tends to undermine legal guarantees that are designed to safeguard civil liberties. It also undermines respect for lawfully-established authority, such as law enforcement and the judicial system. For these and other compelling reasons, societies have rigorously, and successfully, discouraged "pure" vigilante efforts for the last century or so, in large part as a function of professionalizing law enforcement.

Our suppression of "pure" vigilantism will, however, continue to be successful only so long as law enforcement is perceived as effective in combating crime.[313] This is so far not a problem for real-world crime, at

---

[309] One scholar characterizes vigilantism as "lawless law." LAWRENCE M. FRIEDMAN, CRIME AND PUNISHMENT IN AMERICAN HISTORY 172 (1993). He describes it as follows: "'Taking the law into one's own hands' . . . expresses two thoughts: first, that the action is *private*, the action of individuals . . . who seize . . . the state's role as enforcer of law. But equally important is the second idea, that it is *law* that one is taking into one's hands . . . ." *Id.*

[310] *See* Kelly D. Hine, *Vigilantism Revisited: An Economic Analysis of the Law of Extra-Judicial Self-Help or Why Can't Dick Shoot Henry for Stealing Jane's Truck?*, 47 AM. U. L. REV. 1221, 1227-28 (1998).

[311] *See, e.g.*, Vigilante—Wikipedia, http://en.wikipedia.org/wiki/Vigilante (last visited Apr. 21, 2007).

[312] It can also, in extreme circumstances, create the potential for the erroneous application of sanctions to those whom "pure" vigilantes have misidentified as offenders.

[313] Although the *perception* that law enforcement is effectively combating crime necessarily encompasses the premise that law enforcement *actually* enjoys a level of success in this regard, it does not mean law enforcement must apprehend the perpetrator of every crime it is unable to prevent. Modern societies rely on a crime-control, not a crime-negation, strategy to maintain the baseline of internal order they require to survive and prosper. *See* Brenner, *Toward a Criminal Law for Cyberspace*, *supra* note 5, at 65-76. Crime-control strategies maintain that baseline of internal order by persuading citizens that the risks of apprehension are high enough that they dissuade all but a subset of the population from

least not in most countries, but it is for cybercrime. As we saw earlier, cybercrime represents a significant challenge for law enforcement because it differs in several critical respects from the real-world crime that shaped the current law enforcement model.[314] Law enforcement is losing its battle with sophisticated, transnational cybercrime, and will continue to do so unless and until we can adapt our current law enforcement model to an increasingly online environment.[315]

While many citizens remain unaware of this reality, others understand that online law enforcement is failing. Some of those in the latter category have consequently become "pure" online vigilantes: rogue actors whose goals are, variously, to frustrate online criminal activity or to initiate the apprehension and prosecution of online perpetrators. And the incidence of "pure" online vigilante activity is almost certain to increase unless we improve the efficacy of online law enforcement; "pure" vigilantism emerges when citizens perceive that there is a law enforcement vacuum, that crime control is ineffective.[316] The already-notable online vacuum encourages "pure" vigilantism, as do several other factors. One is the ease with which online vigilantes can affiliate with like-minded others; websites and e-mail let them share information and join in collaborative vigilante activity directly targeting online offenders. Another factor prompting online vigilantism is that it is a relatively low-risk activity. Since they have no reason to be in physical proximity with those they pursue, online vigilantes run little risk of physical violence from their prey; a vigilante can be in a different city, a different state, or a different country from those he targets. And because online vigilantes can conceal their identities as well as their locations, they are unlikely to be identified and prosecuted as vigilantes.

The eroding efficacy of our current model of law enforcement is therefore compounding the problem of maintaining internal or external order online: the model's increasing inefficacy in controlling crime qua crime is eroding societies' disparate abilities to discourage criminal activity in cyberspace; this not only undermines the perception that social order is being maintained "in" cyberspace, it also erodes the perception that societies are maintaining order in the real-world. Criminal laws are

---

engaging in criminal activity. *See id.* This keeps crime at an acceptable level. *See id.* There can be a disconnect between the actual and perceived risks of perpetrator apprehension, but the disconnect will be irrelevant to the efficacy of the crime-control strategy as long as the perceived risk of apprehension is significant enough to act as a default crime-deterrent.

[314] *See id.*

[315] *See id.*

[316] *See, e.g.*, FRIEDMAN, *supra* note 309, at 158-68.

designed to prevent the citizens of a society from preying on each other;[317] the problem we now confront is that while the enforcement of these laws in their real-world societal context continues to be efficacious enough to maintain order within a given society, the inefficacy with which criminal laws are enforced in cyberspace bleeds into the real-world, where it undermines our faith in our government's ability to protect us. That, in turn, encourages "pure" vigilantism, which itself threatens societies' ability to maintain internal order; while vigilantes claim to be acting on behalf of the law, their conduct actually erodes the fabric and integrity of the law.

It would seem, then, that we must continue to exclude civilians from law enforcement because to do otherwise would at least implicitly sanction vigilantism.[318] And that is true as far as it goes: For the reasons noted above, we cannot tolerate "pure" vigilantism in the real-world, in cyberspace, or in the intersection of the two. But "pure" vigilantism—vigilantes substituting for law enforcement officers—is not our only option. Another possibility is to return to the past—to institute a limited revival of the traditional Anglo-American system in which civilians legitimately participated in (rather than replaced) law enforcement.

One of the reasons law enforcement is struggling with cybercrime is a lack of resources and trained personnel. Agencies operating essentially on the same budgets that barely sufficed for real-world crime must now respond to real-world crime *plus* cybercrime. Cybercrime also increases the complexity, as well as the quantity, of the crime with which officers must deal; because cybercriminals exploit computer technology in more or less sophisticated ways, investigators need special training and equipment, both of which must be continually upgraded. The obvious solution would be to increase law enforcement budgets so that they can support the personnel, resources, and training necessary to increase the efficacy with which law enforcement responds to cybercrime. Unfortunately, this appealingly straightforward solution is ultimately impracticable because the cost would be prohibitive, at least in terms of what taxpayers in the United States and elsewhere would be willing to bear.[319]

---

[317] *See* Brenner, *Toward a Criminal Law for Cyberspace*, *supra* note 5, at 65-76.

[318] As I note in Section IV.B, *infra*, an early twentieth-century experiment with bringing civilians into law enforcement had the apparently unintended effect of sanctioning—and thereby encouraging—the worst kind of "pure" vigilantism.

[319] There are several reasons why taxpayers would not—and probably could not—fund the personnel and other resources needed to maintain an effective law enforcement response to cybercrime.

One is the sheer magnitude of the problem: Criminal law enforcement in the United States primarily takes place at the state and local level; there are, consequently, over 17,500 state and local law enforcement agencies in the United States. Bringing these agencies up to

We could achieve essentially the same end indirectly if we were to utilize the above noted approach, that is, incorporating a level of civilian participation into law enforcement. The Anglo-American practice of incorporating such participation derived from the then-acknowledged need to supplement available law enforcement resources. Of course, at that time officers needed manpower, weapons, and horses, while today's officers need hardware, software, and individuals trained in their use. The principle, though, remains the same: civilian participation can serve as an in-kind supplement to formal law enforcement resources.

We will assume for the purpose of analysis that corporate and individual civilians are able and willing to participate in the law enforcement response to cybercrime. Therefore, the difficulty, if any, of implementing this strategy lies in (1) identifying precisely *how* civilians would participate in that endeavor and (2) resolving any legal obstacles to such participation. We will defer the first issue for now, and return to it later in Section IV.B. Our concern here is with how the law does, and should, approach civilian participation in what has long been a purely sovereign function. It seems that re-establishing the principle of civilian participation in law enforcement would, at a minimum, require resolving two legal issues. One is the vigilantism issue noted earlier: how can we integrate civilian participation into law enforcement without sanctioning vigilantism and its attendant evils? The other issue is perhaps more

---

speed in the battle against cybercrime would require hiring and training an appropriate number of officers in each agency and equipping each agency with some to-be-identified quantum of specialized computer hardware and software. The initial costs would be staggering because the process would certainly require purchasing new equipment and would almost certainly require hiring new officers; new hires would be necessary both because of the need to maintain current force levels to deal with real-world crime and because traditional officers often have neither the interest nor the aptitudes needed to pursue cybercrime. As to personnel costs, we can only speculate as to how many officers would need to be hired, but if it averaged, say, two officers per agency, 35,000 officers would have to be hired for this purpose. The initial costs of bringing the agencies up to speed would, therefore, encompass salaries, benefits, and initial training for these new hires, as well as the purchase of the hardware and software they would need in their work.

If we were dealing with real-world law enforcement, the initial costs would basically be a one-time expense. While officers do continue to train in the use of weapons and other tactics, their equipment and police vehicles last for years. Cybercrime, on the other hand, is an exponentially evolving arms race: computer hardware and software evolve at an amazing pace, a circumstance cybercriminals exploit. Optimally, cybercrime investigators should be equipped with and trained in the latest technology, and their efficacy as investigators will decline if they do not have access to current technology and training. But providing them with what they need is an expensive proposition; more precisely, it is a recurring expensive proposition since hardware and software quickly become obsolete. It is conceivable, but exceedingly unlikely, that taxpayers could and would bear the expense involved in keeping law enforcement competitive with cybercriminals.

straightforward: what, if any, statutory or other obstacles currently ban civilian participation in law enforcement?

i. Vigilantism

The vigilantism issue is concededly problematic, as history demonstrates. I address this issue in more detail in Section IV.B, when I speculate about the mechanics of integrating civilians into the cyberconflict attack processes. For now, I want to note only that the strategy currently under consideration involves utilizing civilians to *supplement*, rather than *replace*, law enforcement efforts. It does not legitimize "pure" vigilantism. The critical distinction between "pure" vigilantism and the hypothesized strategy is that the civilians work under the supervision of authorized law enforcement officers.[320] Whatever else they do, civilians do not initiate or control the course of investigations; the adoption and rigorous implementation of this proposition should eliminate the evils associated with "pure" vigilantism. Since the civilians remain subordinate to law enforcement officers, the perception will be that crime control—efficacious crime control—is being implemented by law enforcement.[321]

ii. Existing law

Does existing law create any obstacles to the strategy posited above? There is a federal statute, the Anti-Pinkerton Act, that seems to prohibit such an effort, but probably does not. To understand why, we need to review a bit of history.

When the Civil War began, the federal government had no law enforcement officers of its own. Because it was written before professional policing had been invented, the Constitution requires Congress to create and maintain "Armies" but not law enforcement agencies.[322] As a result, when President Lincoln's life was threatened, federal authorities had to turn to a private agency for help. Allan Pinkerton, founder of what would become Pinkerton's National Detective Agency, was hired to guard the President.[323] Pinkerton then not only guarded Lincoln, he also took over the Secret

---

[320] Federal law, for example, already allows this practice with regard to the execution of search warrants. *See* 18 U.S.C. § 3105 (2000) (private citizen may assist an officer in executing a search warrant); *see, e.g.*, United States v. Schwimmer, 692 F. Supp. 119, 126-27 (E.D.N.Y. 1988) (holding that the execution of search warrant by "computer expert" acting under supervision of federal agent was proper).

[321] This negates the "perceived law enforcement vacuum" which, as noted earlier, tends to encourage the rise of vigilantism.

[322] *See supra* notes 298, 302-307 and accompanying text.

[323] *See* David Sklansky, *The Private Police*, 46 UCLA L. REV. 1165, 1212 (1999).

Service—"the Union army's intelligence operation."[324] As a result, throughout the Civil War, "the United States continuously employed 'Pinkertons' as security officers, intelligence gatherers, and counterintelligence operatives" because there was no other alternative.[325]

After the war, Pinkerton and his agents returned to providing security and guard services for businesses, which led to their involvement in "strike-breaking" for companies opposed to unionization.[326] Pinkerton's anti-labor activities, combined with an infamous riot in which Pinkerton guards and strikers were killed, caused "great public concern over the use of private security forces."[327] This concern and union pressure resulted in Congress' adopting what is known as the Anti-Pinkerton Act.[328] The Act, which has changed very little since it was adopted in 1893, states that "[a]n individual employed by the Pinkerton Detective Agency, or similar organization, may not be employed by the Government of the United States."[329]

While the Act seems to bar the federal government from hiring private individuals to participate in federal law enforcement activities, this may not be true. The only court so far to interpret the Anti-Pinkerton Act held that an organization "is not 'similar' to the . . . Pinkerton Detective Agency unless it offers quasi-military armed forces for hire."[330] The then-Fifth Circuit based its holding on the premise that the Act was meant to prevent the federal government from hiring the kind of "armed guards" who precipitated injury and death in the nineteenth century labor riots, not from retaining the services of companies (or individuals) who merely provide investigative services.[331]

The *Weinberger* court's holding is one reason why the Anti-Pinkerton Act is presumably not an impediment to implementing the civilian participation strategy outlined above, at least not at the federal level. Since the strategy contemplates civilian participation in law enforcement

---

[324] *See id.*

[325] Gregory L. Bowman, *Transforming Installation Security: Where Do We Go from Here?*, 178 MIL. L. REV. 50, 55 (2003).

[326] *See id.*

[327] *See id.*

[328] *See id.* It was also "spurred in part by the employment of 25 Pinkerton guards at the 1889 presidential inauguration." Sklansky, *supra* note 323, at 1214 n.297. Hostility toward Pinkerton and its strikebreaking activities was a factor in changing American attitudes toward the professionalization of policing. *See id.* ("Hostility to private policing mounted during the second half of the nineteenth century, fueled by . . . stories of malfeasance and by a growing notion that the responsibility for peacekeeping should not be placed in private hands.").

[329] 5 U.S.C. § 3108 (2000).

[330] United States ex rel. Weinberger v. Equifax, Inc., 557 F.2d 456, 463 (5th Cir. 1977).

[331] *See id.* at 462-63.

investigations, the civilians' efforts should fall within the "safe harbor" this court carved out for investigative services.

The other reason why the Anti-Pinkerton Act does not seem to preclude implementation of a civilian participation strategy derives from the language of the Act itself: as noted above, it bars the federal government from "employing" individuals who work for the Pinkerton Agency or similar organizations. This prohibition does not apply to the strategy outlined above because it does not contemplate "employing" civilians; "employing" individuals denotes paying them for their efforts, and that would be impracticable in this context for the same reasons increasing law enforcement budgets is impracticable.[332] Since the strategy is predicated on volunteer civilian participation, the Anti-Pinkerton Act seems inapposite. It is also inapposite insofar as the strategy does not encompass hiring civilians to act as "quasi-military armed forces."

No statutory obstacles seem to exist at the state level. States do not seem to have adopted analogs of the Anti-Pinkerton Act.[333]

The de facto exclusion of civilians from the law enforcement process is apparently more a product of custom or culture rather than of law—a byproduct of the professionalization of policing that emerged in the nineteenth century and evolved in sophistication in the last century.

b. Military

Civilian participation in the military attack response process falls into two categories. In one, civilians surrender their civilian status and become members of the armed forces; a civilian who joins the military is not only authorized, but required, to participate in responding to attacks of war.[334] The more problematic category involves participation by civilians who have remained civilians, that is, who have not officially joined the military.

As one author notes, the law of war "attempts to regulate state utilization of civilians in combat operations in the course of international armed conflicts by prohibiting civilians from directly participating in

---

[332] *See supra* note 319 and accompanying text. Hiring civilians to supplement law enforcement efforts could be even more expensive than increasing law enforcement budgets, since civilian consultants would probably cost more, per hour, than would law enforcement investigators.

[333] In the late nineteenth century, some states adopted laws restricting the use of private, armed guards "brought in from out of state," but these laws seem to have had little effect and have apparently disappeared. *See* Sklansky, *supra* note 323, at 1215 n.296.

[334] *See* Jeffrey F. Addicott, *Contractors on the Battlefield*, 28 HOUS. J. INT'L L. 323, 340-41 (2006) (writing that the Geneva Conventions require "militaries to distinguish between combatants (armed forces) and noncombatants (civilians)"); *see also* 10 U.S.C. § 802(a); 32 C.F.R. §§ 1624.9 & 1627.1 (2002).

combat."[335] The goal is to protect civilians from retaliatory attacks, but the "effectiveness of this prohibition has been substantially undercut . . . by the failure of the law of war to provide a clear definition of what constitutes direct participation in combat."[336] Until relatively recently, no precise definition was needed because the demarcation between civilians as noncombatants and civilians as combatants was quite apparent in an era of "simple weapons systems operating at short range."[337]

As warfare becomes more sophisticated and remote warfare becomes more common, the distinction between civilian noncombatants and civilian combatants has eroded.[338] In order to "save money and gain access to superior technical expertise," countries are increasingly using civilians "to operate and maintain sophisticated military equipment and to support combat operations."[339] The increasing integration of civilians into military efforts can create uncertainty as to whether a civilian is acting as a "civilian" or as a military actor.[340]

Under the current law of war, a "civilian" is someone who is not a member of a country's armed forces.[341] Ambiguity as to someone's status is resolved by construing him as a civilian.[342] Civilians involved in military efforts fall into two classes: employees and contractors.[343] "Civilian employees are hired and supervised by the armed forces and have an employment relationship with them. Contractors work independently or for a private company and have a contractual relationship with the armed forces."[344] Civilian employees are "subject to supervision, control, and discipline" by military personnel to a far greater degree than are civilian contractors.[345]

---

[335] J. Ricou Heaton, *Civilians at War: Reexamining the Status of Civilians Accompanying the Armed Forces*, 57 A.F.L. REV. 155, 157 (2005). For more on this, see *id.* at 168-84.

[336] *Id.*

[337] *Id.*

[338] *See id.* at 157, 159-63. "Combatants" and "noncombatants" are all members of the armed forces, the distinction being that one engages in combat activities while the other does not. *See id.* at 172-73. Noncombatant members of a military force are barred from engaging in combat by the laws of their own state, not by the laws of war. *See id.*

[339] *Id.* at 157; *see also id.* at 191-92.

[340] *See id.* at 157, 159-63.

[341] *Id.* at 173 (citing 1977 Geneva Protocol I Additional to the Geneva Conventions of Aug. 12, 1949, and Relating to the Protection of Victims of International Armed Conflicts, Dec. 12, 1977 arts. 43 and 51, 1125 U.N.T.S. 3 (entered into force Dec. 7, 1978)).

[342] *See id.*

[343] *See id.* at 184.

[344] *Id.* at 174 (citation omitted).

[345] *Id.* at 184.

In the U.S. military, the role of civilian employees has been limited to providing combat support for real-world military operations; consequently, they work in "areas such as weapons system maintenance, logistics, and intelligence."[346] Civilian contractors, on the other hand, are "involved in almost every aspect of military activity."[347] They "train, feed, equip, and house" soldiers; they also "maintain weapons, gather intelligence, provide security at forward locations, and even fight."[348] Civilian contractors who train military units may accompany the units into combat, and contractor-consultants can be "actively involved" in planning combat operations.[349]

The roles contractors are assuming in real-world military operations can conflict with the law of war; under current law, civilians cannot participate directly in military activities.[350] Civilian employee participation in U.S. military endeavors generally comports with this requirement, but contractor participation may not, depending on how one defines "direct" participation in military activities.[351] The extent to which civilians of either type can participate in cyberwarfare is even more uncertain:

> The law of war provides limited guidance to help determine when computer network attack and exploitation [CNAE] actions are considered combat. No treaties specifically regulate CNAE, but it is governed by the law of war. Those aspects of CNAE which cause physical damage can be treated like attacks with more conventional weapons, with the consequence that carrying out such attacks is limited to combatants. Other types of CNAE, particularly those involving attacks on networks to steal, destroy, or alter information within them, do not necessarily constitute direct participation in hostilities and are arguably open to lawful civilian participation.[352]

Under current law, then, civilians can legitimately participate in certain aspects of cyberwarfare, a circumstance attributable to the increasing superannuation of the law of war. That law will eventually have to be modernized so it encompasses the various manifestations of cyberwarfare. And that process will also need to include a reassessment of the role civilians can legitimately play in cyberwarfare, as the rationale for excluding them from traditional combat operations either does not apply, or applies with less force, to cyberwarfare. This rationale existed to protect civilians from retaliatory attacks by an opposing military force. But as we

---

[346] *Id.*

[347] *Id.* at 186.

[348] *Id.*

[349] *Id.* at 184.

[350] *Id.* at 192-93.

[351] *Id.* at 190-93.

[352] *Id.* at 194 (notes omitted). As noted above, "combatants" are members of a nation's armed forces. *See supra* note 338.

saw earlier, cyberwarfare tends to eradicate distinctions between civilian and military targets; indeed, civilian infrastructure components will become a prime target in cyberwarfare.

B. WHERE DO WE GO FROM HERE?

> No more was I part of a world . . . in which the civilian and military establishments each had its distinct role . . . .[353]

In the above-quoted comment, General Rupert Smith is speaking of his experience with twenty-first century warfare—with what he calls "war amongst the people."[354] His point is that real-world warfare has become a more nuanced, complex phenomenon than the symmetric battlefield confrontation between armies of opposing nation-states that has been the norm for centuries. As we have seen, the same is true—to an even greater extent—of conflicts in the cyberworld.

General Smith argues that military organizations need to re-think and restructure their approach to warfare in order to accommodate the realities of this century. I, of course, am making a similar argument for an even more intricate phenomenon: cyberconflict. General Smith argues that to adapt to new varieties of warfare, military organizations must incorporate a concern with achievable political objectives into their historic focus on using force to realize purely military ends.[355] My argument—which we will dissect and analyze below—is that the only way countries can achieve effective attribution and response capabilities for the inherently ambiguous spectrum of cyberattacks is to abandon the model in which military personnel exclusively respond to acts of war, civilian law enforcement officers exclusively respond to crimes and acts of terrorism, and "pure" civilians play no role in either process.[356]

---

[353] SMITH, *supra* note 111, at xiii.

[354] *See id.*; *see also supra* note 110.

[355] *See* SMITH, *supra* note 111, at 3-28.

[356] By "pure" civilians I mean those who are not currently employed by the military or by a civilian law enforcement agency.

The list given above and the discussion that follows do not include a fourth category: individuals employed by agencies such as CIA and MI6. *See, e.g.*, Intelligence (information gathering)—Wikipedia, http://en.wikipedia.org/wiki/Intelligence_(information_gathering) (last visited Apr. 21, 2007). These civilian agencies concentrate on collecting strategic information—"intelligence"—that is then utilized in efforts to promote "national security." *See, e.g.*, Intelligence Agency—Wikipedia, http://en.wikipedia.org/wiki/Intelligence_agencies (last visited Apr. 21, 2007); *see also* Central Intelligence Agency, https://www.cia.gov/cia/information/mission.html (last visited Apr. 21, 2007). "National security" denotes the need to deal with external threats, that is, the need "to maintain the survival of the nation-state through the use of economic, military and political power and the

I have already explained *why* I believe countries must do this. Now I need to address *how* they can do it. While an improved strategy of the type for which I am arguing must logically be unitary in nature, that is, it must incorporate the efforts of all three constituencies into the attribution and response processes, I am dividing the "how" analysis into two sections: the first considers how to integrate military and law enforcement personnel into these processes; the second considers how, and to what extent, it is possible to incorporate civilian participation into the new, integrated military-law enforcement strategy.

1. Military-Law Enforcement Integration

Integrating military and law enforcement personnel into the attribution and response processes raises distinct issues for the two broad categories of cyberattack, cyberwarfare and cybercrime/cyberterrorism. As an initial matter, it is important to note that my argument is based on integrating the efforts of the military and law enforcement constituencies, not on fusing

---

exercise of diplomacy." National security—Wikipedia, http://en.wikipedia.org/wiki/National_security (last visited Apr. 21, 2007); *see also* 50 U.S.C.S. § 401a(1)-(5) (LexisNexis 2005). In the post-9/11 world, intelligence agencies have assumed more responsibility in the battle against state-initiated and non-state-initiated threats; as a result, their operations increasingly incorporate both law enforcement and military characteristics. *See, e.g.*, RON SUSKIND, THE ONE PERCENT DOCTRINE (2006); *see also* Central Intelligence Agency, *supra* (the CIA now focuses on "counterterrorism, . . . international organized crime and narcotics trafficking, . . . and arms control").

While civilian intelligence agencies play an important role in helping nation-states fend off external threats, and while they will no doubt continue to play this role as these threats move online, they are not included in the discussion above because they do not constitute a distinct operational category. Intelligence agencies have historically functioned to support the military, which has primary responsibility for fending off external threats. *See* Norman C. Bay, *Executive Power and the War on Terror*, 83 DENV. U. L. REV. 335, 369-75 (2005); *see also* Grant T. Harris, Note, *The CIA Mandate and the War on Terror*, 23 YALE L. & POL'Y REV. 529, 531 (2005) (writing that the CIA was "born from the collective memory of the surprise attack on Pearl Harbor, . . . and a growing fear of communism"). As such, they fall into the category of civilian employees whose efforts support the military.

In the United States, civilian employees of intelligence agencies are explicitly barred from becoming involved in domestic law enforcement. *See, e.g.*, Fred F. Manget, *Intelligence and the Criminal Law System*, 17 STAN. L. & POL'Y REV. 415, 416 (2006) (asserting that the National Security Act of 1947 specifically prohibits the CIA "from having law enforcement powers").

Given that alignment, there should be no need separately to analyze the contributions intelligence agencies can make to the cyberconflict attribution and response processes. To the extent intelligence agencies continue to function primarily as adjuncts to the military, their role in dealing with cyberconflicts will be subsumed in the military's role in this area. If and when they legitimately move into supporting law enforcement as well, that aspect of their role in dealing with cyberconflicts will be subsumed in the analysis of law enforcement's role in that area.

them into a single entity. There are very good reasons to maintain the institutional separation of these entities.[357] Therefore, we are concerned only with how to achieve a specific, limited level of operational integration.

a. Cyberwarfare

The threshold problem here is what-attribution, determining the nature of the attack. Integrating the efforts of military and law enforcement personnel into this process should not present insurmountable conceptual or practical difficulties because all we are concerned with, to this point, is identifying that there has been an attack or an attack is in progress and the nature of that attack. We can achieve an effective level of military-law enforcement integration in the "what-attribution" process and still maintain the institutional integrity of both the military and law enforcement constituencies.

Once an attack is determined to be cyberwarfare, the focus shifts to who-attribution and the need to respond. Who-attribution can be an independent inquiry or a subsidiary component of the what-attribution process. If it is initially apparent that an attack represents cyberwarfare, then who-attribution becomes an independent inquiry as it is not bound up with the process of what-attribution. If it is not initially apparent that an attack represents cyberwarfare, then who-attribution becomes a subsidiary component of the what-attribution process; here, determining the identity of the attackers is an essential component of the what-attribution process.

Integration proceeds no further in this analysis;[358] law enforcement-military integration here is necessarily limited to the attribution processes. The responsibility for responding to identified acts of cyberwarfare will continue to rest exclusively with the military;[359] to do otherwise would effectively eradicate the institutional separation between civilian and military response authority. The military therefore must continue to maintain institutional and operational control over the process of responding to external threats, however they present themselves.[360] I will

---

[357] Aside from anything else, keeping the military separate from and subordinate to civilian authority helps ensure the survival of democracy and incorporating the military into the battle against crime and terrorism could undermine its ability to carry out its primary function of combating external threats.

[358] *But see* Section IV.B.1.b, *infra*.

[359] *See, e.g.*, Patience Wait, *Defense Domain, Civilian Awareness*, GOV'T COMPUTER NEWS, Jan. 22, 2007, *available at* http://www.gcn.com/print/26_2/42958-1.html (reporting that the general in charge of Air Force's new Cyberspace Command is responsible "for creating 'cyberspace warriors,' who can react to any threats 24/7").

[360] This, alone, would eliminate concerns about running afoul of the Anti-Pinkerton Act. One can argue, of course, that the Anti-Pinkerton Act should not impede integrating non-

later consider the extent to which civilian participation can be utilized to support the military response process.

This analysis, therefore, is concerned only with the propriety, and the practicalities, of integrating the military and law enforcement constituencies into the attribution processes for cyberwarfare. Since attribution is based upon information, it follows that this integration must focus exclusively on sharing information that may pertain to actual or potential attacks and attackers. More precisely, it must focus on law enforcement unilaterally sharing information it has lawfully collected with the military. There are at least two reasons why that is the appropriate focus of this particular integration effort. The most obvious is that the additional information provided by law enforcement can, and should, improve the military's ability to identify cyberwarfare attacks and attackers.

The perhaps less obvious reason is that this unilateral, delimited integration preserves the institutional division between civilian law enforcement and the military. If law enforcement were to be charged with affirmatively locating information relevant to identifying cyberwarfare attacks and attackers, such a charge would alter its function in impermissible ways. Law enforcement would be able to use its civil investigative authority to investigate cyberwarfare, as well as criminal activity. That, in turn, would mean law enforcement would act as a de facto agent of military authorities—scrutinizing civilian activities for purposes quite unrelated to its legitimate function of controlling criminal activity and maintaining internal order. However much we trust our military, that is a path we must not take.

So, how should this one-way information-sharing strategy work? We begin with the rather obvious premise that military personnel will be on alert for potential cyberwarfare. This premise should hold not only for personnel assigned to special "cyber commands," but rather to all military personnel who interact with cyberspace as part of their duties.[361] Personnel

---

federal law enforcement into the what-attribution process for cyberwarfare because it only bars the federal government from hiring *private* security personnel. Since state and local law enforcement are not private security operatives, they presumably do not come within this prohibition. Also, the Act only prohibits the federal government's "employing" private security operatives; non-federal law enforcement officers' participation in the what-attribution process for cyberwarfare would be a function of their employment by their own, non-federal agency.

And since the military will respond only if an attack is reasonably determined to constitute cyberwarfare, the provisions of the Posse Comitatus Act should not be implicated by the law enforcement-military integration I have outlined.

[361] Arguably, this obligation to be on alert for acts of cyberwarfare could also extend to off-duty military personnel's encounters with cyberspace, in the same way an off-duty police officer who encounters criminal activity will almost certainly respond in some fashion, even

in both categories (but especially the latter category) should be trained to recognize the indicia of cyberwarfare attacks and report any evidence of such attacks to their superiors or the appropriate, designated agency. None of this is novel; we are simply transporting obligations military personnel have always had to the arena of cyberspace.

The novel task is conceptualizing the process by which civilian law enforcement shares information with the military. We begin with the premise that law enforcement is merely transmitting information it has collected in the routine course of its official duties; it is not gathering information specifically for the purpose of assisting the military with cyberwarfare attribution.

One issue we need to resolve is whether law enforcement should filter the information before providing it to the military in an effort to narrow its focus to likely indicia of cyberwarfare or whether it should transmit all the information it collects about every cyber-incident law enforcement officers encounter. The argument for filtering is that selective reporting reduces the risk of overwhelming the military with extraneous data. The argument against filtering is that computer systems can analyze large amounts of data, thereby reducing the possibility of overwhelming military analysts. The best approach would probably be to require both. If the circumstances of an attack warranted, law enforcement officers could initially vet the attack, using a set of criteria supplied by military personnel. If they concluded that there was a fair probability the attack was cyberwarfare, the officers would transmit the information to the military expeditiously and flag it as priority data. If, on the other hand, officers saw nothing indicating that an event implicated cyberwarfare, they would transmit information about those attacks routinely, as data to be incorporated into a more general analysis. Law enforcement agencies would presumably transmit this routine attack data with a pre-determined frequency, perhaps daily.

Admittedly, law enforcement's sharing of information in the second category with military personnel might produce concerns about the potential for eroding the partition between civilian and military authority. The information shared in the first category (likely about cyberwarfare attacks) does not violate the partition because here law enforcement is merely giving the military something to which it is legitimately entitled.

---

if it is only to alert on-duty officers as to what is occurring. Indeed, we could encourage this type of activity by explicitly authorizing it and/or giving off-duty military personnel immunity from suit for actions they take in an effort to ascertain if a cyber-event constitutes an act of cyberwarfare. *See generally* ALASKA STAT. § 09.65.330(a)(1) (2006) (off-duty law enforcement officer is immune from a suit for injury caused while engaging in "official duties"); WIS. STAT. § 175.40(6m)(a) (2006) (off-duty law enforcement officers may arrest a person in certain circumstances).

Since this information presumptively concerns warfare, it only has operational relevance to and value for the military. Sharing this information with the military therefore poses no threat to the segregation of civilian and military authority.

Logically, the same holds for the information in the second category because it is being provided not as domestic operational data, as information to be used against civilians, but as external operational data—as information the military can use in an effort to identify cyberwarfare attacks and attackers. Logic, though, should not be dispositive, given the potential for this aspect of our information-sharing endeavor to be perceived as having sinister purposes. The civilian populace might come to believe law enforcement was involved in a cabal with the military, the purpose being to spy on domestic activities for frightening, but no doubt nebulous, purposes. The best way to address this concern would be to adopt legislation or regulations that ensure that the military's use of the second category data is limited to the purpose for which is it provided—for cyberwarfare attribution and response.[362]

b. Cybercrime and cyberterrorism

The analysis here is essentially a mirror image of our cyberwarfare analysis. Here, too, response authority is rigidly partitioned: civilian law enforcement has exclusive responsibility for responding to cybercrime and cyberterrorism. Given that, the only contribution the military can make to the cybercrime/cyberterrorism *attribution* process is to assist civilian law enforcement officers with determining that an attack has occurred or is in progress; and ascertaining the nature of the attack. This assistance dynamic is the counterpoint to the dynamic analyzed above. But while the dynamics are functionally analogous, the conceptual analysis of the cybercrime/cyberterrorism assistance dynamic is more complex for at least two reasons. One is that the military's capacity to assist law enforcement is not necessarily limited to providing information about attacks. The other is that the military's assisting law enforcement with its designated function of enforcing civilian criminal law raises concerns about eroding the civilian-military authority partition that do not exist when the roles are reversed. We will begin with two implementation issues—the rationale for institutionalizing this dynamic and the nature of the information it encompasses—and then consider these conceptual questions.

[362] Since cyberwarfare response is the exclusive province of the military, and since the data law enforcement shares with the military cannot be used for domestic purposes, there seems to be no reason why the military cannot use information lawfully shared by the process outlined above to respond to cyberwarfare, as well as to identify it.

It is only reasonable to assume that while they perform their constitutionally-authorized function of identifying cyberwarfare attacks and attackers, military personnel will encounter attacks that clearly are not cyberwarfare. Unless and until we parse cyberassaults into new categories, these attacks will by default constitute cybercrime or cyberterrorism. Since it is also reasonable to assume the military's ability to scan cyberspace for attacks is superior to that of civilian law enforcement, it is logical to conclude that the military will acquire information about cybercrime and cyberterrorism events that may not be available to civilian law enforcement. It would seem both logical and prudent to allow the military to share this information with civilian law enforcement because this is not information the military can act upon, and sharing it with civilian law enforcement is likely to enhance the latter's ability to identify and respond to cybercrimes and acts of cyberterrorism.

Assuming for the moment that this is an appropriate strategy, the parameters of the military's authority to transmit attack information to civilian law enforcement still needs to be resolved. Here, there seems to be no reason to filter the information according to the type of attack involved; that is, there seems to be no reason why the military could not periodically provide law enforcement with all of the unclassified information it collects concerning cyberattacks on the United States.[363] Such a transmission of data would be over-inclusive in that it would provide information about cyberwarfare, for which law enforcement has no response authority, but there seems to be no downside to allowing this as long as the information is not classified. Civilian law enforcement, after all, has neither the authority, the resources, nor the inclination to respond to cyberwarfare. And there is a good argument for allowing it: The more empirical data civilian law enforcement has about cyberwarfare attack signatures, the more effective law enforcement officers can be in identifying potential acts of cyberwarfare and sharing that information with the military. Absent other, non-operational concerns, this seems to be an appropriate way of integrating the military and law enforcement sectors in our battle against cyberattacks.

---

[363] The argument for excepting classified information about cyberwarfare and non-cyberwarfare attacks is that even information in the latter category could implicate national security concerns.

Unless and until we give law enforcement officers high-level security clearances, we cannot allow the military to routinely share classified information with them. The same is also true, of course, for civilian intelligence agencies and other civilian entities that support the military and lawfully have access to classified information. *See supra* note 356. The discussion above assumes they, too, would share non-classified cyberattack information with law enforcement.

That brings us to the first conceptual issue noted above: information-sharing is not the only type of assistance the military could at least potentially provide to law enforcement. A major challenge that law enforcement, especially non-federal law enforcement, faces in identifying and responding to cybercrime and cyberterrorism is the lack of non-personnel resources, such as hardware, software, and training for officers assigned to cybercrime/cyberterrorism units.[364] While the military cannot provide personnel,[365] it could, perhaps, alleviate this challenge by providing technical training to law enforcement officers and by donating its superfluous or out of date equipment to law enforcement. Recall that in the 1980s, Congress authorized precisely this type of assistance to improve law enforcement's ability to combat the illegal drug trade;[366] there seems, then, no doctrinal reason why the military could not provide such assistance to law enforcement for the purpose of enhancing their ability to combat cybercrime and cyberterrorism. Indeed, the argument for instituting a similar program becomes even more compelling when we note that cybercrime and cyberterrorism are analogous to the drug trade in that all three tend to encompass transborder criminal activity. The same policy considerations that justified allowing the military to provide non-personnel resources to enhance law enforcement's effectiveness in combating the drug trade consequently seem to militate in favor of allowing similar assistance in the cybercrime/cyberterrorism context.

That brings us to the second conceptual issue: the concern that letting the military assist law enforcement will erode the military-civilian law enforcement partition. This concern is not likely to be compelling with regard to the military's providing non-personnel resources; as noted above, Congress has already, and uneventfully, authorized this type of assistance in the context of a battle against a different kind of transborder crime. Now, that does not mean this issue would not be raised were this resource-support program to be instituted for civilian cybercrime and cyberterrorism units. In fact, if it were raised and if the drug war precedent did not prove dispositive, it would be necessary to analyze whether, and how, the contribution of non-personnel resources by the military could undermine the authority partition. One could credibly argue that erosion could result

---

[364] *See, e.g.*, NAT'L INST. OF JUSTICE, ELECTRONIC CRIME NEEDS ASSESSMENT FOR STATE AND LOCAL LAW ENFORCEMENT 16-19 (2001), *available at* http://www.ojp.usdoj.gov/nij/pubs-sum/186276.htm.

[365] Allowing the military to provide its own personnel to supplement law enforcement's resources would almost certainly violate the Posse Comitatus Act. It would also raise serious, legitimate concerns about eroding the partition between civilian and military authority.

[366] *See supra* notes 293-294 and accompanying text.

from law enforcement's essentially becoming indebted to the military. In this case, the postulated erosion would result not from a quid pro quo kind of indebtedness but from a shift in allegiance, in which law enforcement would begin to look to military rather than civilian authority for support. Support builds bonds between individuals, and those bonds could eventually transmute into allegiance. By that I do not mean civilian law enforcement would promptly become vassals of the military. I merely mean that institutionalizing this type of non-personnel resource assistance effort should be approached cautiously because it could have unforeseen consequences in the decades ahead.

Another argument those who oppose the non-personnel resource assistance effort could make is that the risks associated with providing assistance to combat the drug trade were much less than the risks that could ensue from providing assistance to combat cybercrime and cyberterrorism. Arguably law enforcement's efforts to combat the drug trade focused to a great extent on offshore activities and non-citizens; its efforts to combat cybercrime and cyberterrorism, on the other hand, are likely to focus to a greater extent on activity that takes place in the territorial United States and is conducted by U.S. citizens. Thus, theoretically, what was acceptable when law enforcement was concentrating primarily on "them" is not acceptable when law enforcement is concentrating primarily on "us." Doctrinally, this theory could be grounded in the Supreme Court's interpretation of the Fourth Amendment as applying to law enforcement activity that targets U.S. citizens and/or persons or places within the territorial United States but not applying to extraterritorial law enforcement activity directed at non-citizens.[367] Those who supported the non-personnel resource assistance effort could counter by pointing out that the effectiveness of the Fourth Amendment and similar measures in protecting citizens from over-reaching by law enforcement officers would in no way be diminished by law enforcement's relying on alternate sources of material support.

Actually, the concern that military assistance could erode the civilian-military authority partition would be more compelling with regard to the military's sharing information with civilian law enforcement. The military's providing information to law enforcement about civilian offenses (cybercrimes and cyberterrorism) could create the perception—if not the reality—that the military was spying on citizens to assist law

[367] *See, e.g.*, United States v. Verdugo-Urquidez, 494 U.S. 259, 266 (1990) (holding that the Fourth Amendment was intended to protect U.S. citizens against arbitrary action by their own government, not to restrain actions of the federal government against aliens outside of U.S. territory).

enforcement.[368] The prospect of this perception (and reality) could doom the information assistance option unless there were a reliable way to ensure that the military's information-collecting would be conducted only for lawful military purposes. In so doing, the non-cyberwarfare data the military collected and shared with law enforcement would merely have been collected as an inadvertent byproduct of the military's carrying out its legitimate constitutional functions.

In the previous section, I suggested that the version of this issue that arises for law enforcement's sharing information with the military could be addressed by adopting statutes and/or regulations which limit the recipient's—the military's—use of data provided by law enforcement. A similar approach could work here, but it should target the provider (the military), rather than the recipient (law enforcement); statutes and other measures that bar the military from sharing any data with law enforcement except that routinely collected as an inadvertent byproduct of the military's carrying out its legitimate constitutional functions would act, in essence, as an exclusionary rule.

This approach should eliminate any incentive for the military to engage in impermissible activity in order to assist law enforcement and thereby reinforce the military-civilian authority partition; the incentive would be lacking because law enforcement could not use the information provided. Measures designed to limit law enforcement's use of data obtained from the military would not be an effective way to prevent the military from becoming a de facto agent of law enforcement because these measures would only prohibit on-record use of the data in the investigation and prosecution of cybercrimes and acts of cyberterrorism. Such an approach would be under-inclusive, as law enforcement could still use the information for strategic purposes, such as for developing initiatives or attack profiles.[369]

---

[368] *See, e.g.*, Posting of Bruce Schneier, Schneier on Security: Giving the U.S. Military the Power to Conduct Domestic Surveillance, http://www.schneier.com/blog/archives/2005/11/giving_the_us_m.html (Nov. 28, 2005) ("The police and the military have fundamentally different missions. The police protect citizens. The military attacks the enemy. When you start giving police powers to the military, citizens start looking like the enemy.").

If the military were to cross the line from dispassionately compiling cybercrime/cyberterrorism data as an incident of cyberwarfare monitoring to intentionally seeking out such data to assist civilian law enforcement, that would clearly violate the Posse Comitatus Act. It would also be an indication that the civilian-military partition was becoming unstable.

[369] The Supreme Court long ago recognized that the exclusionary rule is ineffective in controlling police behavior "where the police either have no interest in prosecuting or are willing to forego successful prosecution in the interest of pursuing some other goal." Terry

2. Civilian-Military-Law Enforcement Integration

In this section, we will analyze the next step in the integration effort we are postulating: the possibility—and mechanics—of incorporating a level of civilian participation into the type of military-law enforcement integration examined above. Before we begin that analysis, however, I need to define a term that will be used in the analysis and note a premise that implicitly structures the analysis.

The term is "pure" civilian. By "pure" civilian, I mean a citizen of the United States (or of any other country that decides to implement an institutionally-integrated strategy for dealing with cyberattacks) who is neither: (1) directly employed by a branch of the military, by a military-related government agency, or by a law enforcement agency; nor (2) works as a consultant or contract employee for the military or for either type of agency. This definition also includes corporate and other artificial entities that are recognized as U.S. citizens. "Pure" civilians are completely "outside" the military and law enforcement institutional structures; under the law, they have no role in, and no responsibility for, maintaining either internal or external order.[370] The issue we analyze below is how to incorporate a level of "pure" civilian participation into the integrated military-law enforcement efforts we have already hypothesized without turning the United States into a military-police state or eroding the effectiveness of either the military or law enforcement. The goal—which may be difficult to achieve—is to use "pure" civilian efforts to enhance, but not dilute, the efficacy of either constituency.

The premise is simply that we are exploring the potential for integrating "pure" civilian participation into an integrated military-law enforcement effort of the type hypothesized above. To this point, our analysis has been based on the fundamental premise that an appropriately-circumscribed integration of these constituencies can enhance the efficacy of national efforts to address external (military) and internal (law enforcement) cyberthreats. In the sections below, we will pursue an analysis based on the secondary premise that the selective incorporation of "pure" civilian participation can further enhance the efficacy of these efforts.

One might ask why there should be any need to incorporate "pure" civilian participation into this already-integrated effort? Why not simply incorporate "pure" civilian participation into the efforts of law enforcement (only)? Additively, or alternatively, why not simply incorporate "pure"

---

v. Ohio, 392 U.S. 1, 14 (1968).

[370] *See supra* Sections II-III.

civilian participation into the efforts of the military (only)? The answers to both questions lie in the different roles, and different cultures, of the two institutions.

Integrating the efforts of "pure" civilians into the law enforcement function essentially entails orchestrating a collaboration between civilian constituencies. While law enforcement officers play an institutional role that differentiates them from "pure" civilians in their professional capacity, their status remains, at base, that of civilians.[371] Law enforcement officers work in the civilian world with civilian personnel. Their official purpose is to maintain order in civilian society, and when they are not performing their professional duties, they effectively return to "pure" civilian status.[372] As a result, there is less of an institutional and cultural gulf between civilian law enforcement officers and "pure" civilians than there is between "pure" civilians and military personnel.[373]

Military personnel are governed by different laws than "pure" civilians.[374] For instance, they mostly work and live in an environment that is culturally and environmentally quite distinct from the civilian culture that is the default experience of both "pure" civilians and law enforcement officers.[375] Another differentiating factor is the institutional goals military personnel are committed to achieving. Their professional role is to confront and overcome external threats to the nation-state to which they have sworn allegiance; to accomplish this, they are authorized to use methods and machineries that are not found in civilian society.[376] The activities they engage in are therefore alien to and rigidly segregated from civilian society, and civilians of all types are strictly denied access to information concerning some of these activities.

Logic and pragmatism therefore suggest we should not concentrate on integrating "pure" civilian efforts discretely into law enforcement and into the military. The institutional and cultural divide between "pure" civilians

---

[371] *See, e.g.*, Judith Berkan, *Manu Dura—Official Police Department Bias Takes a Hit*, 69 REV. JUR. U.P.R. 1267, 1274 (2000) (writing that the difference between police and the military "is that police officers are civilians and the military is not"); *see also* ROBERT M. PERITO, WHERE IS THE LONE RANGER WHEN WE NEED HIM?: AMERICA'S SEARCH FOR A POSTCONFLICT STABILITY FORCE 85-86 (2004).

[372] In some states, off-duty officers can make arrests for offenses committed in their presence. *See, e.g.*, State v. Brown, 672 P.2d 1268, 1269 (Wash. App. 1983). Of course, in some states civilians can make arrests under certain circumstances. *See, e.g.*, 5 AM. JUR. 2D ARREST § 56 (2006).

[373] *See, e.g.*, PERITO, *supra* note 371, at 85-86.

[374] *See id.*

[375] *See id.*

[376] *See id.*

and the military would make it difficult to design and implement a stand-alone integration of their respective efforts. It seems the best approach is to use law enforcement as the "gateway" for incorporating a level of "pure" civilian participation into the law enforcement-military integration outlined above. This is the approach we will analyze below.

The pivotal issue in this analysis is the conceptual and doctrinal gap that separates the military and law enforcement from "pure" civilians. In the United States, this gap is the product of two established dichotomies: One is the constitutionally-mandated partitioning of civilian and military authority; the other is the de facto and de jure distinction between "pure" civilians and civilian law enforcement officers. The cumulative effect of these dichotomies is to segregate "pure" civilians from military personnel and law enforcement officers. Given that, how can we incorporate "pure" civilian efforts into the integrated law enforcement-military strategy outlined above without undermining the integrity of either or both of these dichotomies? That is, how can we do this without eroding institutionally essential distinctions between "pure" civilians and military personnel and/or law enforcement officers?[377]

Logically, there are two ways to approach this task. One is formally institutionalizing the "pure" civilian effort. This would require creating a new social institution that would serve as the conduit for "pure" civilian participation in efforts to combat cyberattacks. The other option is to proceed informally—to rely on voluntary, ad hoc participation by "pure" civilians. We will analyze each option in the sections below.

a. Formal

The alternatives noted above should really be labeled "more formal" and "less formal" because this alternative does not actually contemplate the creation of a "real" societal institution analogous to, say, law enforcement, education, or state government. A defining characteristic of "real" institutions is that they have an independent "presence" in society (facilities, personnel) and are the occupational focus of individuals who "belong to" that institution.[378]

---

[377] For the far foreseeable future, anyway, we must retain these distinctions in order to preserve the institutional arrangement that provides the necessary baseline of protection from internal and external threats to social order. We want to incorporate a level of civilian participation into the law enforcement and military efforts, but we do not want to undermine those institutions so that we sink either into anarchy or autocracy.

[378] *See, e.g.*, MICHAEL HECHTER, KARL-DIETER OPP & REINHARD WIPPLER, SOCIAL INSTITUTIONS: THEIR EMERGENCE, MAINTENANCE AND EFFECTS 13-16 (1990).

There are several reasons why we cannot use a "real" societal institution as the conduit for "pure" civilian efforts against cyberattacks. One is that formally institutionalizing civilians' efforts would effectively eliminate their status as "pure" civilians; they would become more or less professionalized constituents of that new institution. Such a result would defy both logic and pragmatism.

Logically, the result would be absurd; every "pure" civilian in the United States would become a (possibly recalcitrant) constituent of this new societal institution—the "pure" Civilian Cybercorps, or whatever it might be called. This result is absurd because the gravamen of a societal institution is specialization; institutions such as the military, government, and education exist to perform a specialized task that is essential for the survival of a society.[379] Integrating the entire civilian populace of a society as large as the United States into one institution would represent the antithesis of specialization, with its attendant divisions of labor. Institutionalized divisions of labor and responsibilities have become standard features of modern societies for good reason; they are effective at carrying out essential tasks. A global institution of the type outlined above would not be effective because it repudiates specialization.

Mandating participation in a new, global institution—the "pure" Civilian Cybercorps—would also require establishing governance and enforcement structures to ensure that civilians were "doing their part" to contribute to this obligatory effort. And that brings me to the second objection to this approach—the pragmatic objection. Creating and sustaining an institution such as this would require resources that simply are not available. As I noted earlier, perhaps the most significant challenge law enforcement confronts in its battle against cybercrime and cyberterrorism is a lack of resources. If we do not have the resources available to support an existing institution in its efforts to combat these threats, it is highly unlikely we could find the massive additional resources needed to create and maintain a new institutional structure.

Consequently, what I will instead analyze here is something far less formal: a voluntary organization that would recruit, train, and coordinate the activities of "pure" civilians willing to donate their time and effort to support military-law enforcement efforts against cyberattacks. The use of such an organization has certain advantages, including the following:

---

[379] *See, e.g.*, Functionalism (sociology)—Wikipedia, http://en.wikipedia.org/wiki/Functionalism_%28sociology%29 (last visited Apr. 21, 2007).

- Institutional leaders could implement a vetting process for applicants in an effort to ensure that only committed, serious individuals are allowed to participate.
- Since participation would be voluntary, this institution would not have to "police" the civilian participants to be sure they were "doing their part." The vetting process should further ensure that only willing, committed civilians participate.
- Representatives of this institution could work with the military and law enforcement to create taxonomies and other operational criteria that would structure the efforts of participants in consistent, optimally-effective ways.
- Representatives of the institution could also develop and implement training programs to ensure that new participants had the skills needed to participate effectively and all participants were regularly instructed in new tactics and new issues.
- Members of the institution could establish consistent, regularized standards for the civilian participants, so they would know what was expected of them (and what was forbidden to them).
- Use of such an institutional structure would facilitate the process of establishing routine, reliable channels of communication between institutional participants and law enforcement-military personnel.

Essentially, I am proposing a larger-scale analog of the law enforcement support programs used in community-policing.[380] I think these programs provide a useful conceptual model for the type of effort we are considering both because of the way they are structured and because of the type of support they provide.

Here, as in the earlier discussion of integrating the efforts of law enforcement officers and military personnel, I am assuming that the civilians' contribution will be limited to providing information about cyberthreats. Earlier, we assumed that (1) law enforcement's only contribution to the military's efforts against cyberwarfare would be providing information about incidents that might constitute cyberwar, and (2) the military's primary (and perhaps only) contribution to law enforcement would be providing information about actual or potential cybercrime/cyberterrorism. I made these assumptions because of legal and pragmatic constraints that derive from the institutional separation of the military and law enforcement. Here, we are writing on a blank slate—

[380] *See, e.g.*, San Antonio Police Department—Cellular on Patrol, http://www.sanantonio.gov/saPD/cop2.asp (last visited Apr. 21, 2007); *see also* WESLEY G. SKOGAN, & SUSAN M. HARTNETT, COMMUNITY POLICING, CHICAGO STYLE 110-93 (1997).

creating an entirely new institution with a new purpose and a new and distinct legal status. We could, therefore, incorporate a level of civilian participation that goes beyond mere information-sharing. We could design this hypothesized institution so that it would allow citizens to take a proactive role in investigating cyberattacks; we could even involve them in the apprehension of cyberattackers and, perhaps, in retaliating against such attacks. While some, at least, would find this appropriate,[381] it would be inadvisable in practice.

Ninety years ago, concerns about German spies and saboteurs resulted in the creation of the American Protective League (League), a "volunteer organization to aid the Bureau of Investigation of the Department of Justice" in identifying, apprehending, and generally frustrating the efforts of foreign agents operating inside the United States.[382] The League came into existence because neither federal nor state law enforcement had the personnel or other resources to mount effective investigative and enforcement campaigns targeting what was perceived to be a serious threat of espionage and sabotage.[383] A well-meaning group of civilians therefore organized what became a national effort intended to supplement the official resources available for this and related security efforts.[384] Unfortunately, the nature and scope of the activities authorized for League members was not well-defined at the outset, and the definitions deteriorated as time passed.[385] Like participants in the institution postulated above, members of the League took on the responsibility of passing pertinent information concerning "enemy" activities to state and federal law enforcement officers; unlike what has so far been postulated for the participants in our hypothesized institution, members of the League went much further, actively conducting investigations, "arresting" suspects, and, in some tragic instances, administering their own form of "justice."[386]

---

[381] *See, e.g.*, Tim Mullen, *When Striking Back Is the Best Defense*, SECURITYFOCUS, Dec. 15, 2003, http://www.securityfocus.com/columnists/203.

[382] JOAN M. JENSEN, THE PRICE OF VIGILANCE 22 (1968).

[383] *See id.* at 17-32.

[384] *See id.*; *see also* HOMER CUMMINGS & CARL MCFARLAND, FEDERAL JUSTICE: CHAPTERS IN THE HISTORY OF JUSTICE AND THE FEDERAL EXECUTIVE 421 (1937) (writing that by June 1917, the League "had branches in almost six hundred cities and towns" and nearly 100,000 members; and by 1918, it had almost 250,000 members). According to a reliable estimate, during its existence the League investigated three million cases for the War Department and "perhaps another" three million cases for the Department of Justice. *See* JENSEN, *supra* note 382, at 155.

[385] *See* JENSEN, *supra* note 382, at 17-31.

[386] *See id.*

The League serves as an object lesson in the need to take great care in formally incorporating any level of civilian participation in government-monopolized activities. The advantage of creating an institution like the League is that it solves the vigilante problem; since the participants in such an institution operate on behalf of and with the approval of a government agency, they occupy a position midway between that of "regular" law enforcement and "pure" civilians. One disadvantage of creating an institution such as this is that it can shield members from liability for violating law in their efforts to assist with its enforcement.[387] A related disadvantage is that the quasi-official status that membership in such an institution confers can, as the sad history of the League demonstrates, encourage excess and lawlessness.[388]

Our goal in this endeavor is to identify how "pure" civilian participation can be used to increase the effectiveness of the integrated law enforcement-military effort outlined above. An essential aspect of this endeavor is incorporating civilian participation in such a way that it does not undermine the integrity and professionalism of our attribution and response processes for cyberthreats. We seek to improve, not to degrade, the methods we use to protect ourselves.

An American Protective League-style approach creates a voluntary civilian organization that *actively* works to support law enforcement (or, for our purposes, an integrated military-law enforcement effort). I believe it is inherently inadvisable to allow active civilian participation in law enforcement or in joint military-law enforcement efforts. The organizers of the League created a detailed set of rules and operating standards for their members, and created a complex national organization to enforce these rules and standards,[389] but things still went tragically awry.

Things went awry for the League because its civilian members were actively engaged in law enforcement without having been trained in law enforcement and without being supervised by professionals with such training.[390] There were no resources for training, and the size of the League's membership and the scope of its activities made supervision impossible.[391]

---

[387] *See id.* at 17-32.

[388] *See id.*

[389] *See id.* at 130-50. The American Protective League's membership manual is available online at the University of North Carolina at Asheville's American Protective League website. American Protective League, http://toto.lib.unca.edu/findingaids/mss/biltmore_industries/american_protection_league/default_league.htm (last visited Apr. 21, 2007).

[390] *See* JENSEN, *supra* note 382, at 130-50.

[391] *See id.*

The same would be true if we were to institutionalize active civilian participation in the integrated military-law enforcement effort outlined above. Even if participation were purely voluntary, as it was with the League, such an effort would attract hundreds of thousands, even millions, of participants.[392] Assigning law enforcement and military personnel to supervise the efforts of these volunteers would reduce the number of professionals available to deal directly with cyberthreats. That is very likely to be counterproductive. Not assigning law enforcement and military personnel to supervise volunteer efforts invites a degradation of effort; the participants in a "pure" Civilian Cybercorps might well descend into spying, harassment, public humiliation, and misplaced retaliation against those they believe to be cybercriminals, cyberterrorists, and cyberwarriors. In other words, without supervision they are likely to drift toward vigilantism.

I, therefore, conclude that sanctioning active civilian participation creates a potential for abuse and over-reaching which is simply unacceptable.

b. Informal

The better path, I believe, is to create a voluntary organization along the lines I outline above in which the civilian participants' sole role is to report information about cyberevents that they have observed. This information can be transmitted to law enforcement, which passes it along to the military, or it can be sent directly to both. I suspect the best approach would be to let law enforcement serve as the conduit for transmitting information to the military except, perhaps, in what seem to be exigent circumstances. Alternatively, the organization posited above could transmit information directly to the military; it would be up to the military whether they preferred to have law enforcement vet the civilian-provided data or receive it directly.

The civilian organization should be as virtual as possible; it should consist of a web of civilians networked by e-mail and secure websites. As I noted above, the organization should provide the volunteers with at least some initial and continuing training and should provide them with a set of operating standards and cyberevent identification criteria. The role these volunteers would play in the cyberattack attribution and response effort is analogous to the role civilian aircraft spotters played in the United States during World War II: the Civil Air Patrol "enrolled civilian spotters in reconnaissance. Towers were built in coastal and border towns, and

[392] *See supra* note 384.

spotters were trained to recognize enemy aircraft, so as to report if any were seen."[393] The effort proved successful "almost to a fault," as in the "Plains states where many dedicated aircraft spotters took up their posts night after night . . . in an area of the country that no enemy aircraft of that time could possibly hope to reach."[394] Like this effort, the voluntary organization I posed above would recruit civilians to help provide information about potential threats, although they would be virtual, rather than physical, threats.

The primary virtue of this approach is that it gives law enforcement and the military access to information they have not yet received or, in some instances, might not otherwise receive. In this way, the procedure helps to alleviate the current under-reporting of cybercrime that makes it difficult, if not impossible, for law enforcement to identify patterns and trends in cybercrime and cyberterrorism. This approach can provide a similar benefit for the military. As explained earlier, cyberwarfare, unlike its real-world counterpart, is very likely to be directed at civilian targets. As we also saw earlier, cyberwarfare is not likely to begin with a dramatic, Pearl Harbor-style attack; it is far more likely to begin with a series of probes, smaller attacks testing security on particular systems. If the participants in the voluntary organization postulated above include representatives of the corporate and other entities that comprise a nation-state's critical infrastructure, they can provide information to law enforcement and to the military about what their organization may not even realize are acts of cyberwarfare. That would markedly enhance a nation-state's attribution and response capability for this category of cyberattack.

There are at least two possible disadvantages to utilizing this approach. One is that requiring would-be volunteers to go through a vetting and training process might discourage participation. I am afraid I do not see that as a true disadvantage. If the vetting and training processes were implemented correctly, they should serve only to eliminate potential volunteers who are undesirable because they lack the responsibility, maturity, or other qualities required for acceptable participation.

The other possible disadvantage is that by recruiting civilians into a quasi-formal, law enforcement-sanctioned organization, we would almost certainly establish the participants as state agents for the purposes of applying the Fourth Amendment.[395] I see that as a necessary and inevitable

---

[393] United States home front during World War II—Wikipedia, http://en.wikipedia.org/wiki/Homefront-United_States-World_War_II (last visited Apr. 21, 2007).

[394] *Id.*

[395] The volunteers would be acting with the purpose of assisting law enforcement and,

consequence of implementing an approach such as this, a consequence that ensures this effort would not undermine our constitutional rights. While this would no doubt require courts to address novel issues, the applicability of the Fourth Amendment to the efforts of these civilian volunteers should not present significant difficulties. For one thing, most of the data to which they would have access would be public, not private; a cyberattacker cannot, for example, claim a Fourth Amendment expectation of privacy in his efforts to assault a corporate or other private computer system. To the extent information supplied by the civilian volunteers does incorporate proprietary and other information that can be deemed private for Fourth Amendment (or other) purposes, the sanctity of that information can in many instances be shielded by redacting it or by pseudonymizing it.

V. CONCLUSION

We live in a world that is changing. The proliferation and evolution of computer and computer-related technologies alters the threat landscape in unprecedented ways. We may be on the threshold of a paradigm shift that threatens our conception of the nation-state and its boundaries.[396]

Historically, the evolution of the nation-state was the product of several factors, but its defining characteristic has always been the exercise of sovereign authority within a specific territory.[397] Territorial authority is, and perhaps will always be, an essential component of organized human society. The migration of crime and terrorism into cyberspace does not mean those evils will disappear from the real-world; people will continue to harm each other and each other's possessions in the real-world, as well as the virtual one. And, as we have seen, the same is and will be true of cyberwarfare, at least for the foreseeable future.

We may be in a transitional period, to a world in which territorial authority recedes in importance and other factors take its place. Or, we may be in the world as it will be—a place in which human societies must maintain order in both physical and empirical realms. In either event, we will have to re-conceptualize how we approach the task of fending off internal and external threats from whatever realm. As we have seen, our current models of law enforcement and the military are historical artifacts—each evolved at a particular point in time to address a specific type of real-world threat. We cannot, for the foreseeable future, completely discard

---

given its cooperative relationship with the umbrella organization in which the volunteers participated, law enforcement would be deemed to have acquiesced in and/or encouraged their efforts. *See, e.g.*, United States v. Hall, 142 F.3d 988, 993 (7th Cir. 1998).

[396] *See* VAN CREVALD, *supra* note 125, at 126-88.

[397] *See, e.g., id.* at 1, 126-88.

either model because these real-world threats persist; what we must do, unless and until the threat environment changes further, is to evolve strategies that expand the capabilities of both models.

In so doing, we must explore different approaches, approaches that are suited to the fluid, unstable, territorially-unbounded nature of activities in cyberspace. We must resist the temptation to rely on what we know and merely create new institutions assigned to improve cyberthreat attribution and response. Instead, we must consider the distinct and evolving nature of the threats we face and attempt to devise strategies suitable for dealing with them—in the same way modern policing evolved to deal with urban crime and the modern military evolved to deal with traditional warfare.

I cannot and would not presume to say that the approaches I have analyzed in this Article are *the* solution to this problem, or even that they are *a* solution to the problem. All I can hope is that what I offer in this article will contribute to a dialog on these issues, one that results in our devising tactics that enhance our ability to deal with the perils that emerge from cyberspace.