IN DEFENSE OF CYBERTERRORISM: AN ARGUMENT FOR ANTICIPATING CYBER-ATTACKS

Susan W. Brenner
Marc D. Goodman

The September 11, 2001, terrorist attacks on the United States brought the notion of terrorism as a clear and present danger into the consciousness of the American people. In order to predict what might follow these shocking attacks, it is necessary to examine the ideologies and motives of their perpetrators, and the methodologies that terrorists utilize. The focus of this article is on how Al-Qa'ida and other Islamic fundamentalist groups can use cyberspace and technology to continue to wage war against the United States, its allies and its foreign interests.

Contending that cyberspace will become an increasingly essential terrorist tool, the author examines four key issues surrounding cyberterrorism. The first is a survey of conventional methods of "physical" terrorism, and their inherent shortcomings. Next, a discussion of cyberspace reveals its potential advantages as a secure, borderless, anonymous, and structured delivery method for terrorism. Third, the author offers several cyberterrorism scenarios. Relating several examples of both actual and potential syntactic and semantic attacks, instigated individually or in combination, the author conveys their damaging political and economic impact.

Finally, the author addresses the inevitable inquiry into why cyberspace has not been used to its full potential by would-be terrorists. Separately considering foreign and domestic terrorists, it becomes evident that the aims of terrorists must shift from the gross infliction of panic, death and destruction to the crippling of key information systems before cyberattacks will take precedence over physical attacks. However, given that terrorist groups such as Al Qa'ida are highly intelligent, well-funded, and globally coordinated, the possibility of attacks via cyberspace should make America increasingly vigilant.

O ALLAH! Inspire Muslims . . . around the world, to use their skills, whether it be computer knowledge or financial ability, to RETALIATE against the enemy in every part of the World![1]

In the wake of the September 2001 attacks, the nation's attention irresistibly and inevitably turned to terrorism.[2] In the aftermath of 9/11,

---

1. YOSSEF BODANSKY, BIN LADEN: THE MAN WHO DECLARED WAR ON AMERICA 223-225 (2001) (explaining that a dua is a voluntary prayer, a "prayer-sermon instructing the believer how to answer the call of Islam."). *See also,* JOHN GILCHRIST, MUHAMMED AND THE RELIGION OF ISLAM (1984), http://answering-islam.org/Gilchrist/Vol1/7c.html (explaining the "Five Pillars of Islam") (on file with the University of Illinois Journal of Law, Technology & Policy). *Al Qaeda Is Not New to US Intelligence,* BUSINESS DAY, Sept. 26, 2001, *at* http://www.bday.net/sep26/p04-261.htm (on file with the University of Illinois Journal of Law, Technology & Policy). Issued by the Azzam Organization, the "mother organization of the . . . mujahadin," the dua incorporated "all the challenges and threats of jehad into a single global struggle against a common enemy," the United States and Israel. *Id. See also* BODANSKY, *supra* at 223 ("This dua codified the role of the anti-American jihad . . . in the context of the escalating worldwide jihad.").

2. The U.S. Code defines "terrorism" as "premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents." 22 U.S.C. § 2656f (2000). *See also* 22 U.S.C. § 2656f(d)(1) ("'international terrorism' means terrorism involving citizens or the territory of more than 1 country"); 22 U.S.C. § 2656f(d)(3) ("'terrorist group' means any group practicing, or which has significant subgroups which practice, international terrorism"). For a more expansive definition, *see, e.g., Threat of Terrorism in the United States, Statement before the Senate Committee on Appropriations, Armed Services and Select Committee on Intelligence,* 107th Cong. (May 10, 2001), *at* http://www.fbi.gov/congress/congress01/freeh051001.htm (statement of Louis J. Freeh, Director, Federal Bureau of Investigation) [hereinafter Freeh].

> International terrorism involves violent acts, or acts dangerous to human life, that are a violation of the criminal laws of the United States or any state, or that would be a criminal violation if committed within the jurisdiction of the United States or any state, and which are intended to intimidate or coerce a civilian population, influence the police of a government, or affect the conduct of a government. Acts of international terrorism transcend national boundaries in terms of the means by which they are accomplished, the intended persons they appear to intimidate, or the locale in which the perpetrators operate.

Id.

Terrorism is a form of "asymmetric warfare" or, perhaps more accurately, the use of asymmetric "counters or stratagems" as a way to deal with an opponent who possesses vastly superior resources and capabilities. NATIONAL DEFENSE UNIVERSITY, 1998 STRATEGIC ASSESSMENT: ENGAGING POWER FOR PEACE 169, *available at* http://www.ndu.edu/inss/sa98/sa98ch11.html. *See also "Asymmetric Warfare", the USS Cole, and the Intifada,* THE ESTIMATE, Nov. 3, 2000, *available at* http://www.theestimate.com/public/110300.html [hereinafter *Asymmetric Warfare*](explaining that in asymmetric warfare, an "opponent – a state, a 'transnational' group (such as an international terrorist organization or a drug cartel), or various other types of players seeks to counter the superior technology or firepower of a superpower or regional power with unconventional, 'asymmetric' means").

> Put simply, asymmetric threats or techniques are a version of not 'fighting fair,' which can include the use of surprise in all its operational and strategic dimensions and the use of weapons in ways unplanned by the United States. Not fighting fair also includes the prospect of an opponent designing a strategy that fundamentally alters the terrain on which a conflict is fought . . . .
>
> Four broad options could be part of an asymmetric response to current and foreseeable U.S. superiority in regional combined-arms warfare capability. The first option is the acquisition of weapons of mass destruction (WMD) and long-range ballistic or cruise missiles. A future regional opponent could threaten U.S. and allied forces with a dramatic form of military escalation. Even without operational use, the mere presence of such capability would act as a regional-strategic shadow and might weaken the commitment of key allies to any future U.S. military response to regional aggression. The second is the selected acquisition of high-technology sensors, communications, and weapon systems. This is the strategy of the niche player. The third, the exploitation of cyberweapons, could be used to disrupt the next generation of information-technology (IT) military logistics systems or to bring the war home by attacking the national strategic infrastructure (NSI), itself rapidly exploiting IT in the name of economic efficiency. And in the fourth, opponents could choose to fight in environments, such as large cities or jungles, that

as it has come to be called, government officials and the public alike began spinning scenarios in an attempt to forecast what will come next. Forecasting what will come next requires consideration of two factors: (1) the ideologies and motives of those who have made us victims; and (2) the methods these persons will use to deliver terror to us again.

As to ideologies, it is appropriate to concentrate on Islamic fundamentalists, as they are the group that has expressed the most implacable hostility toward our society and that has clearly demonstrated the intent and ability to act on that hostility. The ideologies and motives that animate Al-Qa'ida and associated Islamic fundamentalist groups have been addressed with great expertise and insight elsewhere, and are not the focus of this article.[3] The focus of this article is on why and how these groups can use cyberspace and information technology to implement their jihad against the United States and its allies.

Therefore, for the purposes of this article, it is sufficient to note that the Islamic fundamentalists, or "Islamists,"[4] who comprise Al-Qa'ida and its associated entities subscribe to a new, "modern" form of terrorism. Until recently, terrorists tended to be loath to use weapons of mass destruction which left a large body count in the wake of a terrorist event; traditional terrorists found this to be counterproductive.[5] A large civilian body count is detrimental to the achievement of the aims of any terrorist group that pursues a political agenda because mass civilian casualties tend to turn a populace against the architects of those casualties.[6]

---

degrade the U.S. capacity to find and attack militarily significant targets. This could include conducting acts of aggression that purposely blur boundaries between actions considered crimes and those viewed as warfare.

NATIONAL DEFENSE UNIVERSITY, *supra*. *See also Asymmetric Warfare, supra* (noting that "asymmetric warfare includes conventional terrorism, classic guerrilla war and the use of weapons of mass destruction, but also such innovative approaches as cyber-attacks and information warfare.").

3. *See* Press Release, Office of the Coordinator for Counterterrorism, U.S. Department of State, Patterns of Global Terrorism 2000 (April 30, 2001), *at* http://www.state.gov/s/ct/rls/pgtrpt/2000/index.cfm?docid=2450.

4. The term "Islamist" is often used by Islamic radical groups and scholars of the Islamic revival, to emphasize the distinction between orthodox Islamic groups and movements that follow orthodox Islam, and radical or fundamental groups." Reuven Paz, *Is There an "Islamic Terrorism"?*, THE INT'L POL'Y INST. FOR COUNTER-TERRORISM, Sept. 7, 1998 *at* http://www.ict.org.il/articles/articledet.cfm?articleid=46. Islamist "denotes the overwhelming prevalence of the political aspect—particularly radicalism, extremism, and militancy—as pursued and perpetrated under the banner of Islam as interpreted by the practitioners" of Islamist views. BODANSKY, *supra* note 1, at ix. The term is used to differentiate "the majority of Muslims and a minority comprising extreme terrorists." *Id.* It reflects the proposition that the ideology espoused by Islamist groups "does not represent true Islam but stems from a misinterpretation of the religion, and even heresy", since "Islam cannot be used for terrorist activity because of its peaceful elements." Paz, *supra*, at n.1.

5. *See* Steve Bowman & Helit Barel, *Weapons of Mass Destruction—The Terrorist Threat*, Congressional Research Service Report for Congress, at CRS-2, Dec. 8, 1999, *available at* http://www.fas.org/irp/crs/RS20412.pdf.

6. *See* D.W. Craig, Canadian Forces College, *Asymmetrical Warfare and the Transnational Threat: Relearning the Lessons from Vietnam*, *at* http://wps.cfc.dnd.ca/irc/amsc/amsc1/006.html (last visited Nov. 4, 2002). *See also* NATIONAL COMM'N ON TERRORISM, COUNTERING THE CHANGING THREAT OF INTERNATIONAL TERRORISM, at § 1 (June 7, 2000), *available at* http://www.terrorism.com/documents/bremercommission/index.shtml [hereinafter COUNTERING THE CHANGING THREAT].

Infliction of a large number of civilian casualties is not a detriment to the goals of "new" terrorists who pursue other-than-political ends. In fact, groups such as Al-Qa'ida which are motivated by transcendental goals[7] such as the destruction of Western culture and the triumph of Islam, see the infliction of mass civilian casualties as a very desirable end because their objective is to demoralize and ultimately destroy the population from which these casualties are drawn.[8] This distinction is

---

Terrorist attacks are becoming more lethal. Most terrorist organizations active in the 1970s and 1980s had clear political objectives. They tried to calibrate their attacks to produce just enough bloodshed to get attention for their cause, but not so much as to alienate public support . . . .

Id.

7. One study identifies three "terrorist paradigms": "terror as coercive diplomacy, terror as war, and terror as the harbinger of a 'new world.'" *See* John Arquilla et al., *Networks, Netwar, and Information-Age Terrorism*, in ZALMAY KHALILZAD ET AL., STRATEGIC APPRAISAL: THE CHANGING ROLE OF INFORMATION IN WARFARE 101 (1999), *available at* http://www.rand.org/publications/MR/MR1016/MR1016.chap4.pdf [hereinafter Networks in KHALILZAD]. In the coercive diplomacy paradigm, terrorism is "designed to achieve specific goals, and the level of violence is limited, or proportional, to the ends being pursued." *Id.* at 102. In the war paradigm,

terrorist acts arise when weaker parties cannot challenge an adversary directly and thus turn to asymmetric methods. A war paradigm implies taking a strategic, campaign-oriented view of violence that makes no specific call for concessions from, or other demands upon, the opponent. Instead, the strategic aim is to inflict damage, in the context of what the terrorists view as an ongoing war . . . . [T]his paradigm, unlike the coercive diplomacy one, does not seek a proportional relationship between the level of force employed and the aims sought. When the goal is to inflict damage generally, and the terrorist group has no desire or need to claim credit, there is an attenuation of the need for proportionality—the worse the damage, the better.

Id. For an explanation of "asymmetric methods," *see Asymmetric Warfare*, *supra* note 2. The "new world" paradigm seeks

the vast disruption of political, social, and economic order. Accomplishing this goal may involve lethal destruction, even a heightened willingness to use [weapons of mass destruction]. Religious terrorists may desire destruction for its own sake, or for some form of "cleansing." But the ultimate aim is not so much the destruction of society as a rebirth after a period of chaotic disruption.

Networks in KHALILZAD, *supra*, at 104. The authors of the study put the Palestinian struggle for independence into the coercive-diplomacy paradigm, cite Al-Qa'ida as an example of a group that exemplifies the war paradigm, and list the Aum Shinrikyo cult as an example of the "new world" terrorist paradigm. *See id.* at 101-03. For a description of Aum Shinrikyo and its activities, *see infra* notes 16, 17, 19, 21, and 24 and accompanying text.

8. *See, e.g.*, Craig, *supra* note 6.

The new terrorist is driven by a different set of motives . . . rage, ethnic hatred, mass murder, extortion or embarrassment or any combination of these. What is so dangerous about this new terrorist is that the previous paradigm of reluctance to use WMD [Weapons of Mass Destruction] does not apply. Traditional terrorism shied away from WMD as the consequences of the use of these weapons would have been counter-productive to their cause. Mass casualties would be seen to discredit the cause for which state terrorists were fighting for and would be certain to evoke strong governmental response.

The new breed of terrorist . . . has no compunction against inflicting mass casualties. In fact, they may desire that many people are killed for revenge and there is no threshold for violence or destruction that they will not exceed.

Id. See also COUNTERING THE CHANGING THREAT, *supra* note 6, at § 1.

Now, a growing percentage of terrorist attacks are designed to kill as many people as possible. In the 1990s a terrorist incident was almost 20 percent more likely to result in death or injury than an incident two decades ago. The [1993] World Trade Center bombing . . . killed six and wounded about 1,000, but the terrorists' goal was to topple the twin towers, killing tens of thousands of people. The thwarted attacks against New York City's infrastructure in 1993—which included plans to bomb the Lincoln and Holland tunnels—also were intended to cause mass casualties. In 1995, Philippine authorities uncovered a terrorist plot to bring down 11 U.S. airliners in Asia. The circumstances surrounding the millennium border arrests of foreign nationals suggest that the suspects planned to target a large group assembled for a New Year's celebration. Overseas

important for the purposes of this article because a terrorist group's tolerance for mass civilian casualties, along with its ultimate objectives, will influence the choice of methods the group uses to deliver terror to the target populace.

With a very few and essentially minor exceptions, terrorists have exclusively used "physical world" methods to deliver terror. Cyberspace has not yet played a notable role as the mechanism used to inflict terror upon a target population. That will change. To understand why it will change, it is necessary to consider four related issues: 1) the "physical world" methods[9] that are used to deliver terror; 2) the reasons why terrorists might find it advantageous to adapt computer technology to this end; 3) the type of cyber-attack that could be mounted to achieve a terrorist event; and 4) the reasons why computer technology as of yet has been neglected as an instrument for inflicting terror.

I. CBERN: "PHYSICAL WORLD" DELIVERY METHODS

At one time, the "physical world" methods used to deliver terrorism were summarized by the acronym "NBC terrorism."[10] NBC terrorism translated as "nuclear, biological, chemical terrorism."[11] More recently, the acronym has been expanded to "CBERN terrorism." CBERN terrorism translates as "chemical, biological, explosive, radiological, nuclear terrorism."[12]

---

attacks against the United States in recent years have followed the same trend. The bombs that destroyed the military barracks in Saudi Arabia and two U.S. Embassies in Africa inflicted 6,059 casualties . . . .

The trend toward higher casualties reflects . . . the changing motivation of today's terrorists. Religiously motivated terrorist groups, such as Usama bin Ladin's group, al-Qaida, . . . represent a growing trend toward hatred of the United States. Other terrorist groups are driven by visions of a post-apocalyptic future or by ethnic hatred. Such groups may lack a concrete political goal other than to punish their enemies by killing as many of them as possible, seemingly without concern about alienating sympathizers. Increasingly, attacks are less likely to be followed by claims of responsibility or lists of political demands.

Id. *See also* JESSICA STERN, THE ULTIMATE TERRORISTS 6-7 (1999).

9. The phrase "physical world" methods" is used to differentiate traditional devices such as conventional explosives, chemical and biological weapons from the "virtual world" methods that can be used to mount terrorist assaults via cyberspace.

10. *See* FEDERATION OF AMER. SCIENTISTS, COUNTERPROLIFERATION PROGRAM REVIEW COMM., ANNUAL REPORT TO CONG. 1997 § 3, *at* http://www.fas.org/spp/starwars/program/cprc97/cprc9703.htm (last visited Nov. 4, 2002).

11. *See* Rodney L.M. Stark, Rats, Bugs, and Gas: The Threat of NBC Terrorism (May 1999) (unpublished M.S. dissertation, Southwest Missouri State University), *at* http://www.infowar.com/survey/ 99/survey_062299b_j.shtml (last visited Nov. 4, 2002).

12. For a good overview of physical world terrorism delivery methods, *see generally* ASSESSING THE THREAT, FIRST ANNUAL REPORT TO THE PRESIDENT AND CONGRESS OF THE ADVISORY PANEL TO ASSESS DOMESTIC RESPONSE CAPABILITIES FOR TERRORISM INVOLVING WEAPONS OF MASS DESTRUCTION (Dec. 15, 1999), *available at* http://www.infowar.com/class_3/00/class3_tp-terr.shtml.

Chemical weapons . . .

. . . .

. . . release toxic gases or liquids that attack the body's nerves, blood, skin or lungs. They may produce surface effects such as tears, blistering, or vomiting, or cause hallucinations or loss of nervous control. Chemical attacks can contaminate an area for between several hours and

several days, compromising equipment and forcing troops to wear highly restrictive protective clothing (reducing their efficiency) and/or take chemical antidotes whose side effects remain largely unknown. Chemical attacks cause widespread panic amongst both military and civilian populations, and their terror effects on civilians are potent.

CTR. FOR DEF. AND INT'L SEC. STUDIES, *Devil's Brews in Details: Chemical Weapons*, *at* http://www.cdiss.org/cw.htm (last visited Nov. 4, 2002). Chemical weapons, "unlike nuclear weapons, which require a large, specialised [sic], and costly scientific-industrial base,... can be made with commercial equipment generally available to any country." *Id. See also* STERN, *supra* note 8, at 49-54.

Biological weapons...

....

... contain either living organisms or their derivatives, such as toxins, which cause disease or death. Living organisms can multiply within the living targets to produce their effects, while toxins cannot reproduce themselves. Toxins are generally more lethal, and act relatively quickly causing incapacitation or death within minutes or hours. Living organisms (microbial pathogens), require incubation periods of 24 hours to 6 weeks between infection and appearance of symptoms. This incubation period... means that biological weapons can continue to have a significant impact many weeks after the initial attack (e.g. by causing a long-term pandemic). Likewise, this delayed incubation period may mean that a biological attack can be completed before those on the ground have realised that it has occurred, or even take place entirely covertly, the effects being confused with a natural outbreak of disease....

....

A biological attack can contaminate an area for between several hours and several weeks.... The relatively poor warning devices available against biological attack and the potential delayed effects of some agents make mis-identification of the agent or agents used more likely, leading to the failure of defence measures....

CTR. FOR DEF. AND INT'L SEC. STUDIES, *Devil's Brews in Details: Biological Weapons*, *at* http://www.cdiss.org/bw.htm (last visited Nov. 4, 2002). *See also* STERN, *supra* note 8, at 49-54.

A nuclear weapon is "any weapon in which the explosion results from the energy released by reactions involving atomic nuclei, either fission or fusion or both." CTR. FOR DEF. AND INT'L SEC. STUDIES, *Devil's Brews in Details: Nuclear Weapons*, *at* http://www.cdiss.org/nw.htm (last visited Nov. 4, 2002). Nuclear weapons are similar to "conventional"

high-explosive weapons insofar as their destructive action is due mainly to blast or shock. But nuclear weapons are tremendously more powerful; nuclear explosions can be thousands or millions of times more powerful than the largest conventional detonation. In addition, the temperatures reached in a nuclear explosion are much higher than in a conventional explosion resulting in a large proportion of light and heat, generally referred to as 'thermal radiation.' This is capable of causing skin burns and starting fires at considerable distances. Nuclear explosions also are different in that they are accompanied by highly-penetrating and harmful invisible rays at the time of the blast ('initial nuclear radiation') and afterwards ('residual radioactivity').

Depending on their yield and the height of their burst, nuclear weapons can cause the destruction of large areas and serious damage and contamination of still larger areas. Psychological effects are enormous, and long-term contamination may only be neutralised by the use of huge quantities of decontamination equipment and personnel. Destruction or disruption of infrastructure, military and economic centres and communications (caused by the electro-magnetic pulse—EMP—associated with a nuclear explosion) leads to the erosion of civil control....

Id. See also STERN, *supra* note 8, at 57-60.

Radiological weapons are "basically a nuclear-weapon variant designed to kill through radiation only (as opposed to blast or shock)." CTR. FOR DEF. AND INT'L SECURITY STUDIES, *Devil's Brews in Details: Radiological Weapons*, *at* http://www.cdiss.org/rw.htm (last visited Nov. 4, 2002). Radiological weapons are sometimes referred to as "dirty bombs," since they "would consist of waste by-products from nuclear reactors wrapped in conventional explosives, which upon detonation would spew deadly radioactive particles into the environment." CTR. FOR DEF. INFO., THE TERRORISM PROJECT, *What if the Terrorists Go Nuclear?*, *at* http://cdi.org/terrorism/nuclear.cfm (last modified Oct. 1, 2001). They

could be fabricated for delivery by ballistic or cruise missiles or aircraft-delivered bomb. A weapon containing plutonium could be released in aerosol form. [The Stockholm International Peace Research Institute] states that radiological weapons might consist of bombs or shells packed with radioactive materials and delivered by means of ordinary (non-nuclear) explosives. In addition, radioactive materials could also be delivered in liquid or solid aerosol form by aerial spraying from an aircraft or UAV....

Of the five physical world delivery methods encapsulated by the CBERN acronym, only two have not been used in an effort to inflict terror. Explosives have been used in thousands of terrorist attacks around the world.[13] Anthrax, a biological agent, was recently deployed in the United States, Pakistan and Germany.[14] An additional example of biological terrorism occurred in 1984 when followers of Bhagwan Shree Rajneesh infected a restaurant salad bar with salmonella bacteria in an attempt to influence a local election.[15] On March 20, 1995, the Aum Shinrikyo cult[16] used a chemical agent—sarin gas—in their attack on the

---

CTR. FOR DEF. AND INT'L SECURITY STUDIES, *Radiological Weapons, Devil's Brews in Details*, http://www.cdiss.org/rw.htm.

> The materials used to produce the radiation could be fission products, plutonium and other actinides from civilian nuclear reactors, or artificially produced radioactive nuclides .... [R]adiological weapons could be used to force mass evacuations, create economic chaos, or occupy territory, avoiding the infrastructure damage that would be created with a nuclear explosive ....

Id. See also STERN, *supra* note 8, at 54-57.

13. *See, e.g.*, The INT'L POL'Y INST. FOR COUNTER-TERRORISM, Terror Attack Database, *available at* http://www.ict.org.il/ [hereinafter Terror Attack Database] (last visited Nov. 4, 2002). Search of international terrorist attacks database run on November 11, 2001 yielded 292 bombing incidents between January 1, 1999, and January 1, 2001; the attacks spanned the globe, from Greece to the Philippines, Spain and Bangladesh. *Id.*

14. Kate Connolly et al., *Germany Reports Anthrax Letter*, THE GUARDIAN, Nov. 3, 2001, at 4, *available at* http://www.guardian.co.uk/anthrax/story/0,1520,586923,00.html.

15. *See e.g.*, John Cramer, *Oregon Suffered Largest Bioterrorist Attack in U.S. History, Twenty Years Ago*, THE BULLETIN (Bend, Oregon), Oct. 14, 2001, *available at* http://www.bendbulletin.com/news/story.cfm?story_no=5309.

In "the early 1980's, Tamil separatists in Sri Lanka threatened to infect Sri Lankan rubber and tea plantations with nonindigenous diseases" as part of a biological war strategy intended to cripple the Sinhalese-dominated government. JAMES S. GILMORE, III ET AL., FIRST ANNUAL REPORT TO THE PRESIDENT AND THE CONGRESS OF THE ADVISORY PANEL TO ASSESS DOMESTIC RESPONSE CAPABILITIES FOR TERRORISM INVOLVING WEAPONS OF MASS DESTRUCTION (Dec. 18, 1999), *available at* http://www.infowar.com/class_3/00/class3_tp-terr.shtml. And prior to their experiments with chemical agents, described in the text above, the Aum Shinrikyo cult attempted several

> unsuccessful acts of biological terrorism in Japan between 1990 and 1995. As early as April 1990, the cult had tried to release botulin toxin from a vehicle driving around the Diet and other government buildings in central Tokyo. In early June of 1993, another attempt was made to release botulin toxin, this time in conjunction with the wedding of the crown prince. A vehicle equipped with a spray device was driven around the imperial palace as well as the main government buildings in central Tokyo.
>
> Later that month ... the cult attempted to release anthrax spores from its mid-rise Tokyo office building laboratory .... [P]olice and media reported foul smells, brown steam, some pet deaths, and stains on cars and sidewalks. Then, in March 1995, ... an attempt to spray botulin toxin in the subway at Kasumagaseki Station was preempted by a cult member who opted not to load the improvised briefcase sprayers with actual agent.
>
> No injuries were reported in any of these biological events despite the fact the cult was dealing with very toxic materials. The cult's failures can be attributed to a variety of factors. The cult may not have had the right agents or the right technologic facilities; they could have overcooked the bioagents or not known how to use them ....

Kyle B. Olson, *Aum Shinrikyo: Once and Future Threat?*, EMERGING INFECTIOUS DISEASES, July-August 1999, at 513, *available at* http://www.cdc.gov/ncidod/EID/vol5no4/pdf/olson.pdf.

16. The Aum Shinrikyo group has been designated a terrorist organization by the U.S. Department of State. *See, e.g.*, U.S. DEPT. OF STATE, FOREIGN TERRORIST ORGANIZATIONS DESIGNATIONS BY SECRETARY OF STATE MADELEINE ALBRIGHT 10 (Oct. 8, 1999), *available at* http://usinfo.state.gov/topical/pol/terror/fto1999.htm#04. As to the cult's philosophy,

> Shoko Ashahara is the undisputed head. Ashahara (born Chizuo Matsumoto) had numerous exalted titles, including venerated master, yogi, and holy pope ....

Tokyo subway system.[17] Only radiological and nuclear agents remain mere possibilities in the arsenal of "physical world" delivery methods.

One might wonder why explosives have been, until this point, the almost exclusive "physical world" delivery device used by terrorists. This is especially curious given that four other agents are likely to induce heightened states of terror in the target population due to their insidious, yet generally fatal effects. The primary reason is simply that it is far more difficult to obtain and deploy chemical, biological, radiological, and nuclear agents than conventional explosives.[18] A secondary reason is that it is generally more difficult to calculate and direct the effects of chemical and biological agents than with the other three delivery methods.[19] Aum

---

Millennial visions and apocalyptic scenarios dominate the group's doctrine, evidenced by the prominent role of Nostradamus as a prophet in Aum Shinrikyo teaching. Ashahara has . . . claimed to be the reincarnated Jesus Christ, as well as the first 'enlightened one' since the Buddha. He has frequently preached about a coming Armageddon, which he describes as a global conflict that would, among other things, destroy Japan with nuclear, biological, and chemical weapons. According to Ashahara, only the followers of Aum Shinrikyo will survive this conflagration . . . .

Aum's actions were perfectly logical within the context of their value system. They were a self-legitimized group that . . . felt obliged to confront society . . . . Unable to achieve their objective—political power—through legitimate means, they determined that a preemptive strike was necessary.

Olson, *supra* note 15, at 515.

17. *See, e.g.*, Olson, *supra* note 15.

On the morning of March 20, 1995, packages were placed on five different trains in the Tokyo subway system. The packages consisted of plastic bags filled with a chemical mix and wrapped inside newspapers. Once placed on the floor of the subway car, each bag was punctured with a sharpened umbrella tip, and the material was allowed to spill onto the floor of the subway car. As the liquid spread out and evaporated, vaporous agent spread throughout the car.

Tokyo was experiencing a coordinated, simultaneous, multi-point assault. The attack was carried out at virtually the same moment at five different locations in the world's largest city: five trains, many kilometers apart, all converging on the center of Tokyo. The resulting deaths and injuries were spread throughout central Tokyo. First reports came from the inner suburbs and then, very quickly, cries for help began to flow in from one station after another, forming a rapidly tightening ring around the station at Kasumagaseki . . . . Most of the major ministries, as well as the national police agency, have their headquarters at Kasumagaseki.

By the end of that day, 15 subway stations in the world's busiest subway system had been affected. . . . The number injured in the attacks was just under 3,800. Of those, nearly 1,000 actually required hospitalization—some for no more than a few hours, some for many days . . . . And 12 people were dead.

Id. at 513-14. *See also* THE INT'L POL'Y INST. FOR COUNTER-TERRORISM, Aum Shinrikyo, *at* http://www.ict.org.il/inter_ter/orgdet.cfm?orgid=68 (last visited Nov. 4, 2002).

18. *See, e.g.*, Bowman & Barel, *supra* note 5, at CRS-4. Nuclear and biological agents are the most difficult to obtain. *Id.* The difficulty of obtaining chemical weapons varies with the sophistication of the weapon at issue: "[T]oxic industrial chemicals such as chlorine or phosgene are easily available and do not require great expertise to be adapted into chemical weapons," but "nerve agents are more difficult to produce, and require a synthesis of multiple precursor chemicals." *Id.*

19. *See* Leslie A. Rodrigues, *The Chem/Bio Terrorism Threat,* NATIONAL INTERAGENCY CIVIL-MILITARY INSTITUTE, at 2 (1998), *available at* http://www.nici.org/Research/Pubs/Docs/98_1_info.pdf.

While instructions for making biological and chemical weapons are readily available on the Internet . . . terrorists will still encounter some key technical problems in utilizing CBW. The level of sophistication and lethality of a CBW depends on a number of variables such as agent purity, dispersal method, and favorable climatic conditions . . . . The technical obstacles in manufacturing, storing, and dispersing CBW . . . must not be underestimated.

Id. See also Bowman & Barel, *supra* note 5, at CRS-5.

The Aum Shinrikyo [attack] . . . provides an example of the unpredictable effectiveness of chemical weapons. Although the cult was able to produce the nerve agent sarin and release it in a

Shinrikyo, for example, conducted an unsuccessful sarin gas attack nearly a year before its 1995 assault on the Tokyo subway system. In June 1994, the cult released sarin in Matsumoto, a mountain resort town.[20] The goal was to kill three judges hearing a fraud case against Aum Shinrikyo and thereby delay a ruling in the case.[21] The judges survived because the wind blew the gas in the wrong direction,[22] but seven innocent people died and hundreds became ill.[23] Also in July of 1995, the cult unsuccessfully attempted to disseminate the lethal gas hydrogen cyanide in another Tokyo subway. The attack failed when the chemicals used to create the lethal gas failed to mix.[24]

Radiological and nuclear agents also have the disadvantage of rendering the areas where they are used uninhabitable for long periods of time,[25] a distinct consideration when terrorists target a populace

---

closed environment — the Tokyo subway — the attack resulted only in 12 fatalities and injury to hundreds of others, whereas there were 301 fatalities and 5,000 injured in the conventional bombing of the U.S. embassies in Kenya and Tanzania.

Id. (note omitted).

20. *See* STERN, *supra* note 8, at 63-64.

21. *See, e.g.*, Olson, *supra* note 15.

> [O]n June 27, 1994 . . . in Matsumoto, a city of 300,000 population 322 kilometers northwest of Tokyo, a group of cult members drove a converted refrigerator truck into a nondescript residential neighborhood. Parking in a secluded parking lot behind a stand of trees, they activated a computer-controlled system to release a cloud of sarin. The nerve agent floated toward a cluster of private homes, a mid-rise apartment building, town homes, and a small dormitory.
>
> This neighborhood was targeted for a special reason. The dormitory was the residence of all three judges sitting on a panel hearing a lawsuit over a real-estate dispute in which Aum Shinrikyo was the defendant. Cult lawyers had advised the sect's leadership that the decision was likely to go against them . . . . Aum responded by sending a team to Matsumoto to guarantee that the judges did not hand down an adverse judgment. A light breeze (3 to 5 knots) gently pushed the deadly aerosol cloud of sarin into a courtyard formed by the buildings. The deadly agent affected the inhabitants of many of the buildings, entering through windows and doorways, left open to the warm night air. Within a short time, seven people were dead. Five hundred others were transported to local hospitals, where approximately 200 would require at least one night's hospitalization.

Id. at 513. *See also*, Chronology of Aum Shinrikyo's CBW Activities, Monterey Inst. of Int'l Studies, *at* http://cns.miis.edu/pubs/reports/pdfs/aum_chrn.pdf (last modified Mar. 19, 2002) [hereinafter Chronology].

22. Henry Sokolski, *Looming Security Threats: Rethinking Bio-Chemical Dangers,* 44 ORBIS 207, 213 (2000), *available at* http://www.npec-web.org/published/2-00fpri-full-vers.htm. *See also* STAFF STATEMENT, MATSUMOTO: A DRY RUN FOR TOKYO, GLOBAL PROLIFERATION OF WEAPONS OF MASS DESTRUCTION: A CASE STUDY ON THE AUM SHINRIKYO, U.S. SENATE GOVERNMENT AFFAIRS PERMANENT SUBCOMMITTEE ON INVESTIGATIONS (Oct. 31, 1995) [hereinafter MATSUMOTO], *at* http://www.ict.org.il/inter_ter/ attackdet.cfm?IncidentID=1737. In January 1995, the cult tried and failed to kill the leader of the "Aum's Supreme Truth Victims Group" by spraying him with VX nerve gas; he was hospitalized for several weeks, but survived. Chronology, *supra* note 21, *at* tbl.

23. *See* STERN, *supra* note 8, at 63. *See e.g.*, Chronology, *supra* note 21.

24. The cult left two bags—one containing sulfuric acid, the other containing sodium cyanide—plus a timer and a reaction device in a womens' restroom in the subway. *Id.* The chemicals, which were supposed to combine to create hydrogen cyanide gas, failed to mix. *Id.*

25. Bernard Anet, *And What About Nuclear and Radiological Terrorism?,* THE ASA NEWSLETTER (Applied Science and Analysis, Inc., Aberdeen, Md.), Apr. 18, 2001, at 1, *available at* http://www.asanltr.com/newsletter/01-2/articles/012c.htm; Kevin O'Neill, *The Nuclear Terrorist Threat*, INST. FOR SCI. AND INT'L SECURITY, Aug. 1997, at 6, *available at* http://www.isis-online.org/publications/terrorism/threat.pdf.

situated in a locale they occupy or intend to occupy upon successful completion of their terrorist mission. Finally, terrorists who are pursuing a political agenda are likely to turn away from chemical, biological, radiological, and nuclear agents for fear that their use will cause public condemnation of the group due to the "inhumanity" of the method(s) employed.[26] This, of course, is not true of groups like Al-Qa'ida which pursue transcendental ends.[27]

While conventional explosives are relatively easy to obtain[28] and can be employed with a fair amount of precision, there are disadvantages associated with their use. It may be easy to obtain the explosives themselves,[29] but terrorists still have to assemble the raw ingredients into a bomb. This process can attract attention,[30] not to mention raise a risk of

---

26. Bowman & Barel, *supra* note 5, at CRS-2.

> A number of factors are seen as having constrained terrorist use of WMD [weapons of mass destruction]. Most terrorists [sic] groups possess political goals and have traditional, ethnic, nationalist, or ideological associations. These groups seek to gain politically from attacks and to draw the attention of large audiences without diminishing their basis of support. As expert Brian Jenkins noted years ago, 'terrorists want lots of people watching, not lots of people dead.'

Id.

27. *See* STERN, *supra* note 8, at 8 ("A new breed of terrorists—including ad hoc groups motivated by religious conviction or revenge, violent right-wing extremists, and apocalyptic and millenarian cults—appears more likely than the terrorists of the past to commit acts of extreme violence.").

> The Center for Nonproliferation Studies at the Monterey Institute of International Studies . . . identified six characteristics among the groups involved in chemical/biological weapons (CBW) incidents: charismatic leadership, no external constituency, apocalyptic vision, loner or splinter group, sense of paranoia/grandiosity, and preemptive aggression. The two common characteristics that appeared in all cases of actual CBW use were the lack of outside constituency and a sense of paranoia/grandiosity. Only a limited number of groups were motivated enough to employ CBW, amongst them religious millenarian groups, small terrorist cells, and brutalized groups seeking revenge or facing destruction.

Bowman & Barel, *supra* note 5, at CRS-2.

28. As the bombing of the Oklahoma City federal building illustrates, it can be ridiculously easy to obtain conventional explosives. Timothy McVeigh destroyed the building using a fertilizer bomb, composed of ammonium nitrate mixed with fuel oil and equipped with a detonator. The fuel oil-ammonium nitrate mix is known as ANFO, "a concoction so cheap, powerful and easy to handle that it has largely replaced dynamite in the commercial blasting industry." Scott Kilman, *Fertilizer Used in Oklahoma City Bomb Is Still Sold With No Restrictions*, WALL ST. J., Oct. 3, 2001, at B1. Six years after the Oklahoma City bombing, "on any given day . . . large amounts of ammonium nitrate are being transported on trucks, barges and rail cars. Some lack locks and might sit in a remote location for days." *Id. See also* SIMON REEVE, THE NEW JACKALS: RAMZI YOUSEF, OSAMA BIN LADEN AND THE FUTURE OF TERRORISM 146 (1999) ("The ease with which [Ramzi] Yousef was able to acquire the chemicals for his bomb" apparently encouraged him to try to obtain radioactive waste to include in the device, making it a radiological weapon).

29. There may be logistical difficulties associated with getting the explosives to the scene of the to-be-consummated terrorist event. In 1999, for example, "U.S. border patrol guards caught Ahmed Ressam driving a rented Chrysler across the Canadian border into Washington state. His trunk contained explosive materials and timing devices." Phil Hirschkorn, *Boyhood Friend Fingers Defendant in Y2K Bomb Plot,* CNN.com, http://www.cnn.com/2001/LAW/06/28/millennium.bombing/ (July 2, 2001). The explosives were to be used to plant a bomb at the Los Angeles airport. *See id.*

30. When Ramzi Yousef and his associates were building the bomb that would be used against the World Trade Center in 1993, they rented a locker at a New Jersey storage center and used it to store parts for the bomb. REEVE, *supra* note 28, at 36. The staff at the storage center became suspicious after they saw containers of chemicals, including hydrogen gas tanks, being delivered to the locker rented by Yousef. *Id.* Indeed, they went so far as to tell Yousef he could not store the hydrogen gas tanks in the locker he had rented. *Id.* The staff ultimately became so suspicious they

injury to those involved.[31] Also, since their effectiveness depends on their proximity to the physical target, conventional explosives have to be deployed in an area that is relatively near the target, an endeavor that can attract unwanted attention or otherwise raise the risk of apprehension, failure or death.[32]

---

requested a key to enter the locker to see what it contained; unfortunately, they were not able to do so until after the World Trade Center had been bombed. *Id.* at 37. Learning about the bombing, the storage center staff did enter the locker, observed chemicals, tubes and glassware, and contacted the FBI. *Id.* at 37-38. The FBI confiscated the material in the locker, thereby gaining valuable evidence that would be used against the perpetrators, who were eventually apprehended.

31. In 1993, Ramzi Yousef was staying in Pakistan, a fugitive from the search for the perpetrators of the World Trade Center bombing. REEVE, *supra* note 28, at 46. A local militant Islamist group asked him to assassinate Benazir Bhutto, then a candidate for Pakistani Prime Minister. *Id.* at 50. Yousef agreed, and assembled a remote control bomb that was to be detonated when Bhutto's car drove past the area where the bomb had been placed, killing Bhutto. *Id.* at 52. On their way to plant the bomb, Yousef and his accomplices were stopped by a police patrol; Yousef dropped the bomb into the gutter, telling the police he had dropped his keys there. *Id.* at 53. The police left and Yousef tried to pull the bomb out of the gutter; it exploded in his face as he did so, knocking him unconscious and sending fragments of metal into his face and eye. *Id.* His accomplices were able to obtain medical treatment for him without arousing suspicion, so neither they nor Yousef were apprehended for the attempted assassination. *Id. See also,* Reuven Paz, *The Future of Islamic Terrorism,* THE INT'L POL'Y INST. FOR COUNTER-TERRORISM, Jan. 20, 1999, *at* http://www.ict.org.il/ [hereinafter *The Future of Islamic Terrorism*]. In an interview with retired Egyptian Brigadier-General Tala't Muslim on "the terrorist activity of Hamas, the Palestinian Islamic Jihad, Hizballah and other Islamic groups, against Israel," the General noted that "there were cases where the bomb exploded in the hands of one of the warriors of the Jihad. This is a great loss for two reasons: on one hand it hits a warrior, and on the other it prevents the bomb from exploding on the enemy." *Id.*

32. After Ramzi Yousef had parked the van containing the bomb in the parking garage of the World Trade Center, he climbed into a car driven by his accomplices. *See* REEVE, *supra* note 28, at 9-10. As they drove carefully toward an exit from the garage, and the timer on the bomb was counted down, they found their exit path blocked by another van. *Id.* Yousef and his accomplices waited briefly while the driver of the van moved it, then were able to leave the parking garage and the scene of what would soon be a huge explosion. *Id.* at 10. No one noticed Yousef or his group, so the delay did not markedly advance the apprehension of any of the perpetrators. It is interesting, though, to imagine what might have happened if Yousef and his accomplices had, for example, been involved in a traffic accident on their way to the World Trade Center, before the bomb had been armed. At the very least, such an incident would have raised a distinct possibility of their being apprehended before they were able to plant the bomb.

Things went further awry in the August 7, 1998 bombing of the U.S. Embassy in Nairobi. The bomb was carried in a "yellow Mazda or Mitsubishi Canter pickup" truck, which was driven to the embassy. BODANSKY, *supra* note 1, at 261.

> At first, the terrorists tried to place the car bomb against the front wall of the embassy. They approached the embassy's front gate, claiming to be carrying sandwiches for the cafeteria. They were refused entry... and sent to the back entrance. The terrorists... drove around the building.... The terrorists tried to get... into the underground parking. The third terrorist got out of the pickup and argued with the embassy's local security guards, but they refused entry. With time running out .... [t]he pickup truck tried to break its way into the embassy, but apparently the driver lost control....

Id. The bomb exploded, but did far less damage than it would have had the terrorists been able to get into the underground parking garage. *See id.* at 262 ("Had the bombers managed to gain entrance to the underground parking garage, it would have devastated the embassy building, killing most of the people inside.").

Ramzi Yousef failed entirely in his 1994 attempt to bomb the Israeli embassy in Thailand. The bomb was loaded into a rented truck; on the way to the embassy the terrorist driving the truck:

> [c]rashed... into a taxi-motorcyclist and another car at a busy intersection... The man panicked and tried to pay off the other drivers with foreign banknotes, but onlookers... crowded around... and police sirens began wailing in the distance. The... terrorist ran off down a side-street....

II. THE ALTERNATIVE: CYBERSPACE

[H]ostile low-risk perpetrators launching a well-coordinated attack with about thirty computer experts strategically placed around the globe and with a budget of approximately 10 million dollars, could bring the United States . . . to its knees.[33]

Cyberspace is an attractive delivery method for terrorists. It suffers from none of the disadvantages associated with the CBERN methods and offers certain other advantages. This article argues that the CBERN acronym should be expanded into CCBERN, with the new "C" standing, of course, for cyberspace, which promises to be a superior terrorism delivery method in many respects.

Access to cyberspace is even easier to obtain than conventional explosives. All one needs is access to a computer that is linked to the Internet. The computer can belong to the terrorist or it can be a "public" computer, e.g., a computer located in a library or a cybercafe.[34] While it is true that an aspiring cyberterrorist also needs a level of computer expertise, the precise type and extent of which will depend upon the nature of the cyberterrorist events. This issue of computer expertise is considered later in the discussion of why cyberterrorism events have so far been exceedingly rare.[35]

A. Cyberspace is Borderless

The permeability of cyberspace facilitates cyberterrorism.[36] Cyberspace differs in this regard from terrestrial borders where people

---

When the Bangkok police arrived, they found the abandoned truck .... The damaged vehicles were pushed to the side of the road and the [truck], with the bomb still undetected inside, was driven to a police depot and impounded.

REEVE, *supra* note 28, at 64. The bomb was discovered a week later, when the truck's owner came to the impound lot to retrieve his vehicle. *Id.* at 64-65.

33. Yonah Alexander, *Terrorism in the Twenty-First Century: Threats and Responses,* 12 DEPAUL BUS. L.J. 59, 86 (1999/2000).

34. Authorities investigating the September 11 attacks believe that at least some of the hijackers used "computers in all-night Kinko's stores and cybercafes ... to coordinate their activities in the weeks before the assaults." Kevin Johnson, *Hijackers' Emails Sifted for Clues,* USA TODAY, Sept. 30, 2001, *available at* http://www.usatoday.com/news/attack/2001/10/01/offlede.htm. The FBI also found "hundreds of e-mail messages in English and Arabic between the alleged hijackers and their associates" stored on public-access computers in libraries. Jim Puzzanghera, *FBI Pursuing Clues to Terrorists on Internet and in E-mail,* SAN JOSE MERCURY NEWS, Sept. 21, 2001, *available at* http://www.s-t.com/daily/09-01/09-21-01/a02wn008.htm. Members of the Lashkar-e-Toiba, an Islamist terrorist group operating in India and Kashmir, may have used a cybercafe to plan their December 2000 attack on the Red Fort monument in New Delhi. *See* Vinay Menon, *Is Lashkar Messaging Via Cyberporn?,* HINDUSTAN TIMES, Feb. 19, 2001, *at* http://www.hindustantimes.com/nonfram/200201/detFRO04.asp (on file with the University of Illinois Journal of Law, Technology & Policy). *See generally* B. Raman, *Lashkar-e-Toiba: Its Past, Present and Future,* The INT'L POL'Y INST. FOR COUNTER-TERRORISM, Dec. 25, 2000, http://www.ict.org.il/articles/articledet.cfm?articleid=149.

35. *See infra* notes 145 - 169 and accompanying text.

36. As to the permeability of boundaries in cyberspace, *see, e.g.,* David R. Johnson & David G. Post, *Law and Borders—The Rise of Law in Cyberspace,* 48 STAN. L. REV. 1367 (1996), *available at* http://www.cli.org/X0025_LBFIN.html.

and goods crossing international boundaries are subject to scrutiny. Immigration officers question aliens entering a country about their credentials and plans, while customs officers inspect imported goods to ensure that they are not contraband and that taxes are paid on lawful goods.[37] Cyberspace can be used to defeat this system and evade inspection.[38] Terrorists in different countries can exchange e-mail with little fear it will be monitored. They can dematerialize many items – books, newspapers, magazines, music, movies, software, games – from their physical formats (hard copy, records, tapes, CD's) into bits and bytes of data and send them to accomplices halfway around the world. No customs authority inspects them; no one monitors their

---

Cyberspace has no territorially-based boundaries, because the cost and speed of message transmission on the Net is almost entirely independent of physical location: Messages can be transmitted from any physical location to any other location without degradation, decay, or substantial delay, and without any physical cues or barriers that might otherwise keep certain geographically remote places and people separate from one another. The Net enables transactions between people who do not know, and in many cases cannot know, the physical location of the other party. Location remains vitally important, but only location within a *virtual* space consisting of the "addresses" of the machines between which messages and information are routed.

The system is indifferent to the *physical* location of those machines, and there is no necessary connection between an Internet address and a physical jurisdiction.

Id. at 1370-71.

37. *See, e.g.*, Stephen E. Flynn, *Drugs, Thugs & Trade: Border Control in an Era of Hemispheric Economic Integration,* Council on Foreign Relations – Globalization and the Future of Border Control (Jan. 2002), *available at* http://www.cfr.org/BorderControl/chapters/chapter3.html (on file with the University of Illinois Journal of Law, Technology, & Policy).

For centuries, states have invested substantial resources into controlling their maritime and terrestrial frontiers. Border control has always been an important part of managing the flows of goods that the host society perceives as threatening, such as weapons and drugs. States traditionally have had a keen interest in regulating who comes and goes across their borders. Passports and visas are closely scrutinized at points of entry. Additionally, public health strategies that aim to manage the spread of disease by people, livestock, and agricultural products generally include border control measures. More recently, safety and environmental threats such as hazardous waste spills and the spread of invasive species caused by ships, planes, and trucks have made the border the locus for regulating the transportation sector. In short, effectively policing national borders lies at the very heart of how states have defined themselves to each other and to their domestic populations.

Id. See also Michael E. Roll, NAT'L LAW CENTER FOR INTER-AMERICAN FREE TRADE, *Customs and E-Commerce*, *at* http://www.natlaw.com/ecommerce/presentations/roll.doc (last modified Oct. 11, 1999).

Historically, importers have filed paperwork (*i.e.*, a customs entry or declaration) with customs authorities and paid duties for the privilege of introducing "merchandise" of foreign origin into their country. "Merchandise" usually was something a customs inspector could see, hear, feel, touch and/or smell, such as a machine, a toy, or food.

Id.

38. Some uses of cyberspace do not, of course, affect the application of traditional border inspection procedures. For example, assume someone in Capetown orders a book from Amazon.com in Seattle. The book may have been ordered in cyberspace but it will travel through terrestrial space, since Amazon.com will send it to South Africa, where it will be inspected by customs officials. *Buying From Outside the U.S. – Customs and Taxes*, Amazon.com, *at* http://www.amazon.com/exec/obidos/tg/browse/-/541262/qid=1007228560/sr=1-2/104-2909125-0627941 (last visited Nov. 5, 2002). The same is true of individual travel. A Buenos Aires businessman flying to Chicago to meet with a client can buy his airline ticket online, but he must still travel in terrestrial space and go through immigration screenings and inspection once he arrives.

transmission.[39] Terrorists can "meet" online using software such as NetMeeting and avoid immigration checkpoints. Such a meeting occurs not in Argentina, Macao, or Yemen, but in cyberspace, where no one monitors cyberspace.[40] Finally, as CIA Director George Tenet noted, cyberspace offers terrorists "greater security and operational flexibility. They can launch an assault from almost anywhere in the world without directly exposing themselves to physical harm."[41]

B. Structured Attacks

Aside from ready access to the delivery agent, cyberspace also offers terrorists the ability to structure attacks that can be implemented with a great deal of precision. A terrorist group might, for example, hack into the New York City subway computer system[42] and systematically strand all the operating trains between stations until none of the original trains were operating and no new trains could be added because all rail lines were blocked.[43] The effects of such an attack would be enhanced if it were implemented, say, beginning at 8:00 a.m. on a Thursday morning, as thousands of commuters were taking — or trying to take — the subway to work. The people in the stalled trains would at first be merely

---

39. The World Customs Organization has considered the issue. *See, e.g.,* WCO Secretary General M. Michael Danet, Address at Regional Conference of Directors General of Customs (Sept. 21 1999), *at* http://www.wcoomd.org//ie/en/past_events/vision_statement.htm.

40. One way to counter this would be to create a "virtual immigration and customs service," a system for inspecting data as it travels across the Internet. Doing this could require modifying the protocols that guide traffic across the Internet; data travels in packets, each with a header that identifies the source address from which the data was sent, the destination address to which it is being sent and the size of the data packet. *How Computers Work* (pt. 1), SMART COMPUTING, Aug. 2001, at 180-187 *at* http://www.smartcomputing.com/editorial/article.asp?article=articles%2Farchive%2Fr0503%2F33r03%2F33r03%2Easp; William S. Cleveland & Donald X. Sun, Bell Labs, *Internet Traffic Data* (paper presented at the University of Michigan on Sept. 21, 2000), *available at* http://www.stat.lsa.umich.edu/~gmichail/stat600-F00/traffic.pdf. Historically, governments have not been able to track data packets because the header information does not give them any way to determine where a packet originated; the FBI cannot, for example, identify Pakistani or Iraqi data packets. In 2000, the Internet Engineering Task Force (IETF), which is responsible for the protocols, was asked to modify them so countries could monitor the packets entering their portion of cyberspace. *See, e.g.,* Declan McCullagh, *Wiretapping the Net: Oh, Brother*, WIRED NEWS, Oct. 12, 1999, *at* http://www.wired.com/news/politics/0,1283,31853,00.html. The IETF declined to do so. *See, e.g.,* Declan McCullagh, *IETF Says "No Way" to Wiretaps*, WIRED NEWS, Nov. 11, 1999, *at* http://www.wired.com/news/politics/0,1283,32455,00.html.

41. GOVERNMENT INFORMATION SECURITY ACT OF 1999, S. REP. NO. 106-259, at 7 (2000), *available at* 2000 WL 369621.

42. In 1997, hackers broke into the computer system that controls the electronic signs which normally flash messages telling commuters to "Watch your step" and "Have a great day." *See, e.g., Hackers Break Into NY Subway Electronic Message Signs*, NANDO TIMES, Nov. 3, 1997, http://www.techserver.com/infotech/11.3.97/tech14.html (on file with the University of Illinois Journal of Law, Technology & Policy). The messages were altered to read "The Hacker Quarterly." *Id.* For a photograph of one of the reprogrammed signs, *see* Jeremy Quittner, *Hacker Psych 101*, TLC, *available at* http://tlc.discovery.com/convergence/hackers/articles/psych.html (last visited Nov. 5, 2002).

43. This scenario has not happened yet, but "in Japan, groups have attacked the computerized control systems for commuter trains, paralyzing major cities for hours." Matthew G. Devost, et al., *Information Terrorism: Can You Trust Your Toaster?*, The Terrorism Research Center, (1996), *at* http://www.terrorism.com/terrorism/itpaper.html.

irritated, and would assume that they were confronting another random instance of glitches in the mass transit system. But as the delay lengthened and they learned — via cell phone calls and radio broadcasts — that they were caught up in an intentional shutdown of the entire system, a shutdown perpetrated by persons whose identities and goals remained unknown, simple irritation would blossom into anger, then fear, and finally panic. While this type of attack would not yield the body count associated with the use of a weapon of mass destruction, people would die. They would die from stress-induced maladies such as heart attacks, miscalculated escape attempts, and panic-driven assaults by their fellow passengers as struggles ensued for perceived avenues of escape or other forms of relief.[44]

Even if the terrorists responsible for the attack did no more than shut down the subway system for half a day, it would still have marked effects on New York and other cities dependent upon subways and similar forms of mass transportation. The most obvious direct effect would be to undermine public confidence in mass transit systems, just as the 9/11 attacks undermined public confidence in air travel.[45] While the subway attack would be neither as dramatic nor as heart-wrenching as the 9/11 attacks, it would produce the loss of public confidence that is an integral component of "terror."

Terrorists, of course, seek to inflict terror upon a target population,[46] but terror is not simply a state of heightened fear of some horrific event. Bizarre as it may seem, human beings can adapt to the prospect of horrific events; British citizens, for example, adapted to the Blitz,[47] sleeping in subways and managing to carry on normal life in the face of almost constant bombardment, destruction, and death.[48] The "terror" that terrorists seek to inflict is a compound state incorporating a physical fear of death or injury plus a state of uncertainty as to who the architects of the possible disaster are, what their motives are, how they will carry out their plans and when the terrorist event will occur.[49] This fused state of fear and uncertainty unravels the fabric of routine that animates everyday life in any stable society. If New Yorkers can no longer assume that subways will travel as scheduled, if this simple yet essential fact of

---

44. After the World Trade Center was bombed in 1993:

> tens of thousands of people had to escape from one of the world's tallest buildings through thick smoke and down blackened stairwells.
>
> Many people were crushed underfoot as panic began to spread. Hysterical men and women punched and kicked their way down the stairs. In a country fed a regular diet of disaster movies, it was almost inevitable that many would think they were facing death.

REEVE, *supra* note 28, at 13. The Sarin gas attack Aum Shinrikyo perpetrated on the Tokyo subway in 1995 caused panic among the passengers trapped in the subway and suffering from the gas. MATSUMOTO, *supra* note 22.

45. *See, e.g.*, 2 OFFICE OF THE UNDERSEC'TY OF DEF. FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS, PROTECTING THE HOMELAND: REP. OF THE DEF. SCI. BOARD TASK FORCE ON DEF. INFORMATION OPERATIONS 85 (Mar. 2001), [hereinafter PROTECTING THE HOMELAND] ("The next Saddam Hussein, or the current one, for that matter, could win a symbolic victory just by tying up Manhattan's traffic control network for a day."), *available at* http://www.acq.osd.mil/dsb/dio.pdf.

urban life can be defeated, and defeated deliberately by persons unknown, then the predictability of routine that gives urban dwellers the sense that there is order and control in their world has been disrupted.[50] This is concededly a different approach to delivering "terror," one that relies less on the resulting casualty count and more on the sense that the basic systems on which people predicate their lives are vulnerable in ways never expected. One could see this type of systemic attack as having consequences that are more profound in their long-term effects than the use of "physical world", CBERN delivery methods. The use of CBERN methods fills us with fear and dread as to the possibility of death

---

46. *See, e.g.,* S. Sanyal, Inst. for Conflict Management, *One Man's Terrorist: Victims' Perspectives on Terrorism*, FAULTLINES, Nov. 20, 2000, *available at* http://www.satp.org/satporgtp/publication/faultlines/volume7/fault7-ssanyal.htm.

> The success of a terrorist act depends on the reaction of the society towards it. As one commentator has remarked, terrorist violence is always 'propaganda of the deed.' Paul Wilkinson notes that 'Political terrorism is thus . . . a weapon of psychological warfare. . ., and the terrorists judge their own 'success' or 'failure' primarily in terms of political, psychological and propaganda impact rather than purely by traditional military criteria of death and damage caused.'

Id. (quoting H.J. Horchem, *Terrorism in Germany: 1985*, *in* CONTEMPORARY RESEARCH ON TERRORISM 144 (P. Wilkinson & A.M. Stewart, eds., 1987) and P. WILKINSON, TERRORISM AND THE LIBERAL STATE 81 (1977)).

47. The Blitz was the Nazi bombing of Britain during World War II. In September and October of 1940,

> Germany tried to bomb Britain into submission, and in an effort to break the will of the people, the capital London was heavily bombed every night for a total of fifty-seven consecutive nights. Thousands of buildings and homes were destroyed, countless thousands died night after night, all services were stretched to the limit often fighting a losing battle.

Royal Air Force Fighter Command, Battle of Britain – 1940, § 6, *at* http://www.battleofbritain.net/contents.html (last visited Nov. 5, 2002).

48. *See,* How We Coped During the Blitz, *at* http://www.battleofbritain.net/section-6/blitz-p08.html (last visited Nov. 5, 2002) ("When the air raids first started, we were concerned if not terrified. But as time wore on and we started to get used to bombs and going down to the shelters we actually got used to it, and it soon became all part and parcel of our way of life."). For another example of coping during an attack, *see* Gerald Steinberg, *The Rewards of Restraint,* Jan. 24, 1991, *available at* http://faculty.biu.ac.il/~steing/ conflict/oped/o91.htm.

> Like most other Israeli citizens, the people on my block are well disciplined in times of national emergency. In between attacks and false alarms, all of us are trying to continue normal lives and to prevent giving Saddam Hussein and his backers the satisfaction of pushing us into panic.
>
> While this would drive any other society mad, we seem to have accepted the absurd and macabre scenes of going to work, visiting our friends and going shopping carrying gas masks.

Id.

49. *See, e.g.,* William Booth & Ceci Connelly, *Terror Attacks Spark a Pervasive Anxiety,* WASH. POST, Sept. 19, 2001, at A23, *available at* http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A52811-2001Sep18.

50. *See, e.g.,* Daniel S. Weiss, *Challenges of Coping with Trauma,* ABCNews.com, *at* http://abcnews.go.com/sections/living/Healthology/trauma_coping.html (Oct. 1, 2001).

> Most of us function with certain assumptions about the world and our surroundings. We assume that our worlds are safe and predictable. Exposure to traumatic stressors like the events of September 11th . . . rudely punctures this psychological bubble of invulnerability. Our normal assumptions are ruptured, and our understanding of the 'rules' of daily living are shocked and upset. The term 'upsetting' is apt, because not only do we experience strong emotions in these times, we actually lose our balance psychologically.

Id.

and destruction, whereas the use of cyber-methods causes us to doubt our ability to pursue ordinary life.[51]

The subway attack described above is a focused, single-target attack. In this regard, it is analogous to the use of many of the CBERN delivery methods, such as the release of a chemical agent or the detonation of a nuclear or conventional explosive. The use of cyberspace also lets terrorists deliver an attack that proceeds in a series of layered, sequenced stages directed at a single geographical target.[52]

C. Sequenced Attacks

A "sequenced" attack is one that is designed to achieve the repetitive infliction of a particular category of "harm," usually physical injury to persons and/or damage to property.[53] Sequential attacks are

---

51. *See, e.g., Cyber Security-How Can We Protect American Computer Networks from Attack, Before House Comm. on Science*, 107th Cong. (2001), (testimony of Robert N. Weaver, N.Y. Elec. Crimes Task Force Assistant Special Agent in Charge), *available at* http://www.house.gov/science/full/oct10/weaver.htm [hereinafter Testimony of Robert N. Weaver].

> Let me relate the Secret Service's mission in fighting cyber crime to the bigger picture of critical infrastructure protection .... [W]e target cyber crime as it may affect the integrity of our nation's financial payment and banking systems. As we all know, the banking and finance sector comprises a very critical infrastructure sector and one which we have historically protected and will continue to protect. In this context, our efforts to combat cyber assaults which target information and communication systems which support the financial sector are part of the larger and more comprehensive critical infrastructure protection scheme. The whole notion of infrastructure protection embodies an assurance and confidence in the delivery of critical functions and services that in today's world are increasingly interdependent and interconnected. To put this all in perspective, the public's confidence is lost if such delivery systems and services are unreliable or unpredictable regardless of the cause of the problem.

Id.

52. The September 11 attacks demonstrate the difficulty of carrying out a sequenced attack using real world methods; even though the architects of the September 11 events spent "years planning their activities," they did not entirely succeed. Press Release, U.S Department of Defense, Statement of the Secretary of Defense (Nov. 1, 2001), *available at* http://www.defenselink.mil/news/Nov2001/b11012001_bt560-01.html. They did achieve one sequenced attack (i.e., the serial plane crashes into the two World Trade Center towers) and may have meant to achieve another (i.e., the crash of a second plane into a target in the Washington, D.C. area). *See, e.g., FBI: Flight 93 Passengers Were in "Fight for Their Lives"*, CNN.com, *at* http://www.cnn.com/2001/US/10/03/inv.pennsylvania.crash/ (Oct. 3, 2001); *White House, Air Force One Possible Targets*, CNN.com, *at* http://www.cnn.com/2001/US/09/12/bush.terrorism/index.html (Sept. 12, 2001). The second sequenced attack failed because the plane intended for the White House or Capitol crashed in rural Pennsylvania. *See, e.g., FBI: Flight 93 Passengers Were in "Fight for Their Lives", supra.*

The sequencing achieved in and contemplated for the September 11 attacks was of a relatively simple type, analogous to delivering two bombs in succession to the same target. The attacks did not encompass the type of complex sequencing and staging discussed above.

53. It is also possible to stage simultaneous attacks, such as the bombings at the East African embassies or the Aum Shinrikyo attacks on the Tokyo subways. *See infra* note 55 (embassy attacks) and *supra* note 17 (subway attacks). *See also* The Terrorism Research Center, MKO, *available at* http://www.terrorism.com/terrorism/MKO.shtml (last visited Nov. 5, 2002) (in 1992, the MKO/MEK "carried out nearly simultaneous attacks on Iranian embassies in 13 different countries in North America, Europe, and the Pacific Rim" which "caused extensive property damage"). Until recently, simultaneous attacks have been unusual. *See, e.g.*, Bruce Hoffman, *Terrorism and Counterterrorism After September 1*, U.S. FOREIGN POL'Y AGENDA, Nov. 2001, at 22-23, *at* http://usinfo.state.gov/journals/itps/1101/ijpe/pj63hoffman.htm.

certainly possible with the CBERN delivery methods. One can, for example, achieve a sequential assault by setting off several bombs in sequence or by sequencing a bomb and a biological or radiological delivery mechanism.[54] Sequential assaults using explosive devices have been carried out in Israel and other parts of the Middle East, though these attacks have generally been limited in scale.[55]

> The significance of the September 11th incidents from a terrorist operational perspective is that simultaneous attacks . . . are relatively uncommon. For reasons not well understood, terrorists typically have not undertaken such coordinated operations. This was doubtless less of a choice than a reflection of the logistical and other organizational hurdles that most terrorist groups are not able to overcome . . . .
>
> During the 1990s, perhaps only one other . . . terrorist incident evidenced those same characteristics of coordination and high lethality: the series of attacks that occurred in Bombay in March 1993, where a dozen or so simultaneous car bombings rocked the city, killing nearly 300 persons and wounding more than 700 others . . . .

Id. Sequenced or simultaneous attacks can have goals other than the infliction of personal injury or property damage. *See, e.g.*, The Terrorism Research Center, MRTA-Tupac Amaru, *at* http://www.terrorism.com/terrorism/MRTA.shtml (last visited Nov. 5, 2002).

> MRTA has proven itself capable of coordinated, simultaneous attacks on multiple targets. A notable example of this was the February 1987 takeover of six local radio stations, which were then used to broadcast anti-governmental propaganda. The takeover of radio stations by MRTA has since become a trademark of the group, highlighted by the broadcasting of prerecorded messages.

Id.

54. Terrorist groups certainly recognize the advantages of staging these more complex attacks. *See, e.g., The Future of Islamic Terrorism, supra* note 31. This article consists of an interview with retired Egyptian Brigadier-General Tala't Muslim on "the future of the terrorist activity of Hamas, the Palestinian Islamic Jihad, Hizballah and other Islamic groups, against Israel." *Id.* Among other things, the General noted that

> [g]ood planning brings about the concentration of powers in order to act against several targets at the same time and place, and hence to increase the losses of the enemy to such a degree that he will seriously reassess his actions. It is possible to hit specific targets such as electricity network, water supply or an Israeli military camp. Bombing of such vital targets within a short time would not let the enemy recover from the first one before being hit by the next.

Id.

55. *See, e.g.*, Terror Attack Database, *supra* note 13. On November 7, 1999,

> [t]hree pipe bombs exploded at a busy intersection in Netania at 10:30 in the morning. The bombs were placed near a trash can in the center of town and timed to detonate during the morning rush hour. A fourth pipe bomb was apparently intended to explode when rescue workers arrived on the scene. It was defused by police sappers. Twenty-seven people were hospitalized with light to moderate injuries. One woman was seriously injured.

Id. On February 2, 1994, "[s]everal bombs exploded inside railcars" in Baku, Azerbaijan, "killing five persons and injuring several others." *Id.*

The difficulty of implementing a sequential attack of the type described above is perhaps illustrated by the fact that the 1998 bombings of the United States embassies, which involved the coordinated detonation of two bombs at sites in two different countries, were lauded as a highly complex undertaking. *See, e.g.*, REEVE, *supra* note 28, at 200. *See also* BODANSKY, *supra* note 1, at 258. The September 11 attacks on the World Trade Center towers and the Pentagon were sequenced attacks directed at geographically dispersed targets; it is estimated that the consummation of these attacks required years of planning. *See, e.g.*, Daniel McGrory et al., *Key Aide Planned Suicide Attack Hijacks*, THE TIMES (London), Oct. 5, 2001. *See also* Niles Lathem, *Anatomy of an Atrocity*, N.Y. POST, Sept. 16, 2001, at 10 ("The FBI believes planning for Tuesday's attacks began five years ago"). Indeed, the trademarks of Al-Qa'ida's terrorist operations are "meticulous long-term planning, a desire to inflict mass casualties, suicide bombers and multiple simultaneous attacks." *A Nation Challenged; Britain's Bill of Particulars: "Planned and Carried Out the Atrocities,"* N.Y. TIMES, Oct. 5, 2001, at B4 (text of British report identifying Al-Qa'ida as the group responsible for the September 11 attacks).

D. Layered Attacks

A "layered" attack is designed to inflict different categories of "harm" upon a single target populace.[56] As noted earlier, the terrorist's goal is to achieve the psychological state of "terror" in a target population.[57] The different types of "harm" are the implements terrorists use to achieve this goal.[58] The "harms" include, death and physical injury,[59] the fear of death or physical injury,[60] the destruction of or damage to property,[61] the disruption of the routines of normal life,[62] and the dissemination of disinformation or propaganda.[63] By using a layered attack to combine various "harms," terrorists can exacerbate the effects of attacks and the "terror" they produce.

> The attacks of 11 September 2001 are entirely consistent with the scale and sophistication of the planning which went into the attacks on the East African embassies and the U.S.S. Cole . . . .
> Al Qa'ida operatives, in evidence given in the East African embassy bomb trials, have described how the group spends years preparing for an attack. They conduct repeated surveillance, patiently gather materials and identify and vet operatives, who have the skills to participate in the attack and the willingness to die for their cause.

A Nation Challenged; Britain's Bill of Particulars, *supra*. For a description of the lengthy, detailed planning that went into the East African embassy bombings, *see, e.g.*, United States of America v. Usama bin Laden, Indictment, Count One - ¶¶ 10-12, 98 Cr. 1023 (S.D.N.Y. 1998), *available at* http://www.fas.org/irp/news/1998/11/indict1.pdf.

56. A layered attack can also be defined as an attack involving the use of different weapons. *See, e.g.*, Douglas De Bono, *Cyber Wars Part 2*, ImaginationStreet.com, *at* http://imaginationstreet.com/media/blood_covenant/cyberwarsprt2.stm (last visited Nov. 5, 2002) ("Any cyber attack must be massive and layered. A massive attack would attempt to disrupt multiple systems, and a layered attack would vary the weapons."). This definition is, however, more appropriate for use in connection with conventional warfare, which seeks the achievement of particular real-world goals, such as the acquisition or retention of geographical territory. The definition of layered attack presented above is used in this article because its focus is on terrorism, which seeks to achieve very different goals; for terrorists, the infliction of different types of "harm" is the device that is used to impose the psychological state of "terror" on a target population. *See infra* text accompanying note 58. The terrorist's focus is, therefore, on using these "harms" as implements for achieving "terror," not on realizing specific tactical objectives.

Logically, a layered attack can be either a sequenced or a simultaneous attack. The discussion in the text will assume that a layered attack is also a sequenced attack, partly because of the difficulty involved in delivering a simultaneous layered attack but primarily because part of the advantage a layered attack offers a terrorist is the ability to deliver "harms" incrementally, in stages. This incremental delivery compounds the fear and uncertainty resulting from an attack, thereby compounding the "terror" it produces.

57. *See, e.g.*, Diane Myers, *Weapons of Mass Destruction: Mental Health Consequences and Implications for Planning and Training*, Presentation to the Weapons of Mass Destruction/Terrorism Orientation Pilot Program at the Clara Barton Center for Domestic Preparedness (Aug. 15-17, 2001), *available at* http://www.icisf.org/Acrobat%20Documents/TerrorismIncident/WMD_Myers.htm ("Terrorism intends as its primary goal to terrify, to fill or to overpower with intense fear, to intimidate to achieve an end. We do not call terrorist events 'bomb-ism' or 'radiation-ism' or 'poison-ism' or 'disease-ism' or 'murder-ism.' Terrorist phenomena derive their power from their ability to psychologically injure, manipulate, and control the behavior of individuals and populations.").

58. *See* Sanyal, *supra* note 46.

59. *See, e.g., supra* note 8.

60. This "harm" is illustrated by the anthrax letters that were disseminated in the fall of 2001. While only a few people died from the disease, the letters had a significant psychological impact:

> As a weapon of mass destruction, anthrax has so far proved to be less than effective - with just one fatality and a handful of illnesses resulting from the spate of recent cases. But as a form of psychological warfare, it's having a profound impact . . . .
> . . . .

> . . . While not nearly as devastating as the Sept. 11 attacks, the anthrax cases have been arguably more powerful in getting under Americans' skin, creating a sense of fear that has disrupted daily routines.
>
> Newsrooms have been evacuated after receiving letters laced with talcum powder, and jittery Americans across the nation have called authorities to test everything from beach sand to confetti. . . .
>
> . . . .
>
> "This is the kind of thing that terrorists want - they want to put sand in the gears," says Rep. Christopher Shays (R) of Connecticut. "They don't always need to do something dramatic. But this forces us to spend a lot of time and attention on something that's fairly easy to do . . . . Everybody becomes a potential target, at random."
>
> Indeed, it's this sense of randomness, and an innate fear of the unknown, that has managed to deeply unsettle so many Americans.

Liz Marlantes, *Anthrax Impact: Little Harm, But a Lot of Fear,* CHRISTIAN SCIENCE MONITOR, Oct. 17, 2001, at 1, *available at* http://www.csmonitor.com/2001/1017/p1s2-ussc.html.

61. The destruction of property can contribute to the cultivation of "terror" in at least two ways. The most obvious effect is that the population whose property is damaged or destroyed by a terrorist attack suffers dislocation, inconvenience and possible physical suffering due to the loss of that property. After the World Trade Center bombing, for example, police sealed off

> a 30-block area . . .embracing Wall Street, city hall, state and federal courthouses and government office buildings and some of the city's busiest subway stations. It is also home to 9,000 people in the new high-rises of Battery Park City, thousands more in TriBeCa lofts and prewar office buildings converted to apartments. Most of those people were still homeless by the end of the week, leaving behind belongings buried beneath an inch-thick layer of gritty dust.

Jerry Adler, *Ground Zero,* NEWSWEEK, Sept. 24, 2001, at 72, 74, *available at* http://www.msnbc.com/news/629543.asp.

The destruction of property can also have psychological effects that transcend its immediate, personal value as "property." This is evidenced by the after-effects of the destruction of the Twin Towers of the World Trade Center, which were important symbols for New Yorkers and others:

> [T]he targeting of the World Trade Center, the Pentagon and possibly the White House reveal a keen understanding on the part of the terrorists of the importance civic landmarks play in the collective conscience of a people.
>
> The destruction of the twin towers, in particular, seems to have tapped into deeper emotions. In part, that may be because they embody an essential element of the American Dream: an unshakable faith in the future. Like the disaster site itself, that faith has been severely damaged. Both will have to be carefully reconstructed. And once that process begins, architecture will become a critical part of the healing process.
>
> . . . .
>
> . . . [T]he World Trade Center's psychological impact on the city was indisputable . . . . [I]t was more than a blunt symbol of the triumph of capitalism. Its massive forms provided a reassuring image of stability amid New York's congested, sometimes chaotic urban landscape . . . . [I]t was the city's emotional anchor.
>
> The horrific image of Tuesday's events has dealt a shattering blow to that sense of shared urban identity. When the second tower fell, . . . the implosion demonstrated that even the most enduring architectural monuments can disappear in an instant.

Nicolai Ouroussoff, *Towering Symbols of Faith,* L.A. TIMES, Sept. 13, 2001, at A32, *available at* http://www.latimes.com/news/nationworld/nation/la-091301arch.story. *See also* Michael Barkun, *Defending Against the Apocalypse: The Limits of Homeland Security, in* CAMPBELL PUBLIC AFFAIRS INST., GOVERNANCE & PUBLIC SECURITY 17, *available at* http://webdev.maxwell.syr.edu/campbell/Governance_Symposium/barkun.pdf.

> The September 11 attacks were not simply destructive of lives and buildings. They inflicted profound psychic damage . . . . The inner psychological trauma of 9/11 was initially linked to shocking images, planes crashing into buildings, occupants jumping to their deaths, and landmark structures collapsing as panicked crowds sought to outrun clouds of debris.
>
> Much of this was seen in real time by immense television audiences . . . . They instantly became . . . vicarious victims. The effect of mass communications in this case, as in the assassination of John Kennedy nearly four decades earlier, was to transform spectators into survivors.

Id.

62. *See, e.g.,* David Gates, *Living a New Normal,* NEWSWEEK, Oct. 8, 2001, at 64, *available at* http://www.msnbc.com/news/635919.asp.

A layered attack could begin, for example, with shutting down the New York subway system, the scenario described above. The next step could be to shut down telephone service to essential emergency services, such as police departments, fire departments, and hospitals,[64] cutting off

---

63. Disinformation is "[d]eliberately misleading information announced publicly or leaked by a government or especially by an intelligence agency in order to influence public opinion or the government in another nation." AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE 519 (4th ed. 2000), *available at* http://www.bartleby.com/61/23/D0272300.html. Propaganda, on the other hand, is the "systematic propagation of a doctrine or cause or of information reflecting the views and interests of those advocating such a doctrine or cause", and includes the information disseminated by the advocates of the doctrine or cause. *Id.* at 1320. Disinformation is necessarily false; propaganda may or may not be false. Both are components of what is known as

> psychological operations, or PsyOps . . . . PsyOps is the manipulation of the psyche of an adversary or target population with information, misinformation, disinformation and propaganda. It involves perception management, or controlling what a group of people think and believe is the goal.

Winn Schwartau, *PsyOps and Network Security*, NETWORK WORLD FUSION, Nov. 19, 2001, *at* http://www.nwfusion.com/columnists/2001/1119schwartau.html.

> An episode from several years ago illustrates how easy it is to disseminate disinformation in an age of technology:
>
> In the summer of 1997, a group of senior Pentagon officers and military reporters gathered for a retreat . . . . [T]alk turned to psychological operations, disinformation and public affairs.
>
> One of the guest speakers . . . showed how video images could be created and/or altered electronically, and without detection, unless the creator inserted an electronic watermark to indicate it was a fabrication. But if the creator's intent was to misinform, the presenter said, then there would be no watermark, and the doctored image would be indistinguishable from reality.
>
> With the Pentagon's fleet of EC-130 'Commando Solo' aircraft—capable of inserting radio and TV programming into national broadcast systems—the implications of such electronic wizardry were obvious. First, journalists monitoring local media in a war zone would need to question constantly whether what they were receiving was U.S. military disinformation. Assuming they asked, would the military take the reporters into its confidence to spare them from spreading the disinformation? The officers at the retreat responded that they would not.

Maud S. Beelman, *The Dangers of Disinformation in the War on Terrorism*, NIEMAN REPORTS MAGAZINE, Winter 2001, at 17, *available at* http://www.nieman.harvard.edu/reports/01-4NRwinter/NRwinter01.pdf. At one point, the Pentagon was considering the use of disinformation in the war on terrorism:

> As part of George Bush's war on terrorism, the military is thinking of planting propaganda and misleading stories in the international media.
>
> . . . .
>
> The options range from the standard public relations stuff . . . to more underhand tactics such as e-mailing journalists and community leaders abroad with information that undermines governments hostile to the United States.These e-mails would come from a .com return address rather than .mil to hide the Pentagon's role. The most controversial suggestion is the covert planting of disinformation in foreign media, a process known as black propaganda.

Tom Carver, *Pentagon Plans Propaganda War*, BBC News, *at* http://news.bbc.co.uk/hi/english/world/americas/newsid_1830000/1830500.stm (Feb. 20, 2002). The idea was subsequently abandoned. *See, e.g., Pentagon to Close Information Office*, MSNBC News, *at* http://www.msnbc.com/news/711387.asp (Feb. 26, 2002) (file on copy with the University of Illinois Journal of Law, Technology & Policy).

64. Such an attack is far from unprecedented. *See, e.g.*, Dorothy E. Denning, *Cyberterrorism* (Aug. 24, 2000) (prepublication version of an article appearing in GLOBAL DIALOGUE, Autumn 2000), *at* http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc.

> In March 1997, one teenage hacker penetrated and disabled a telephone company computer that serviced the Worcester Airport in Massachusetts. As a result, telephone service to the Federal Aviation Administration control tower, the airport fire department, airport security, the weather service, and various private airfreight companies was cut off for six hours. Later in the day, the juvenile disabled another telephone company computer, this time causing an outage in the Rutland area. The lost service caused financial damages and threatened public health and public safety.

access to those in positions to help. Then, to make things interesting, the terrorists might email bomb threats to a randomly-selected set of schools and other agencies, perhaps even courts. The anxiety induced by these threats could be enhanced by falsifying the name of the sender to make it appear that the threat originated within the school or court that is the object of that threat.[65] This effect, in turn, could be further enhanced by incorporating facts specific to the target school/court in the emailed threat; such facts could no doubt be gathered by scrutinizing the target entity's Web site and other public sources of information.[66] The net result of all this, so far, would be the death, injury and disruption resulting from the subway shut-down, the erosion of security produced by denying phone access to sources of emergency assistance, and the overlay of impending violence and destruction generated by the bomb threats, most of which would target children, the most vulnerable members of the target populace.[67] Even if there were no actual bombs,

---

Id. See also Paul Festa, *DOJ Charges Youth in Hack Attacks,* CNet.com, *at* http://news.cnet.com/news/0,10000,0-1005-200-327551,00.html (Mar.18, 1998).

> [T]he federal government this week charged a juvenile with computer crimes, including bringing down an airport control tower and emergency services for several hours.
>
> The youth, who was not identified, quickly accepted a plea bargain negotiated with the U.S. Attorney for the District of Massachusetts . . . .
>
> He pleaded guilty to disabling a Worcester, Massachusetts, airport control tower and other airport facilities for six hours and disrupting telephone service in Rutland, Massachusetts, on March 10, 1997.
>
> . . . .
>
> In the airport and telephone service attacks, the youth temporarily disabled a loop carrier system, which combines multiple phone lines for transmission over a single fiber-optic cable.
>
> By targeting the loop carrier system, the confessed hacker wiped out telephone access to the airport's control tower, fire department, airport security, and weather service, as well as private airfreight firms for six hours. The attack also downed the airport's main radio transmitter and the circuit that lets incoming aircraft switch on runway lights.

Id.

65. In 1999, Christian Hunold, a Missouri man confined to a wheelchair, used the Internet to terrorize a Massachusetts middle school. "Hunold began his campaign by monitoring and participating in Internet chat rooms visited by Hawthorne eighth-graders. He was able to learn enough about some students and the school to create the impression he was in the community and capable of violence." Tom Mashberg, *"Internet Terrorist" To Be Sentenced Today,* BOSTONHERALD, June 5, 2001, at 5, *available at* http://pqasb.pqarchiver.com/bostonherald/. Hunold eventually escalated from chatting with the students to issuing threats. He

> created an Internet site featuring a photo illustration of the... school's main entrance in the crosshairs of a firearm, and a photo of its principal with bloody bullet holes in his head and chest . . . . [A]t one point he posted a list of students' first or last names atop a caption reading "some of you lucky individuals will be going home with more bullet holes than you came with."

Id. His acts terrorized the town, the citizens of which were being threatened by an unknown perpetrator. They believed, however, that the terrorist was local and therefore quite capable of carrying out this threats. *Id. See also* Michele Kurtz, *The "Stalker" Who Stayed at Home: A Town Terrorized Over the Internet,* BOSTON GLOBE, Sept. 2, 2001, at A22; Press Release, Office of the Massachusetts AttorneyGeneral, Alleged Cyber-Terrorist Indicted on Child Pornography and Other Charges In Connection With Internet Threats Against Townsend School Students (Aug. 3, 2000), *available at* http://www.ago.state.ma.us/txt/townsnd2.htm.

66. *See, e.g.,* Kurtz, *supra* note 65, at A27.

67. *Id.* at A22. For a slightly different scenario, *see, e.g.,* SECOND ANNUAL REPORT TO THE PRESIDENT AND THE CONGRESS OF THE ADVISORY PANEL TO ASSESS DOMESTIC RESPONSE CAPABILITIES FOR TERRORISM INVOLVING WEAPONS OF MASS DESTRUCTION: TOWARD A

the threats alone should generate enough anxiety and uncertainty,[68] especially when coupled with the denial of access to sources of help, to traumatize the city for most of that day, and to leave the populace questioning their security for some time thereafter. These effects, in turn, could be compounded if the architects of this terrorist event issued some ominous pronouncements shortly after the event in which they threatened more overtly destructive incidents.

E. Multiple Target Attacks

Cyberspace also allows terrorists to structure sequential attacks that target several geographical targets using the basic scenario described in the paragraph immediately above. Imagine, for example, that at 8:30 a.m. on a January weekday, Des Moines, Iowa is hit by a focused, structured attack: First, the system that controls traffic lights in the city is taken over and all the lights are fixed at green. This produces a traffic gridlock, especially in busier parts of the city. Next, the power grid goes down,[69] depriving citizens of electricity and, consequently, of heat from their furnaces (which, though they are powered by natural gas, require electricity to operate). The next infliction is that local landline telephone service shuts down;[70] at the same time, the computers that control the

---

NATIONAL STRATEGY FOR COMBATING TERRORISM 40 (Dec. 15, 2000), *available at* http://www.terrorism.com/documents/gilmore2.pdf.

> [C]yber attacks inside the United States could have 'mass disruptive' . . . consequences. It is easy to envision a coordinated attack by terrorists, using a conventional or small-scale chemical device, with cyber attacks against law enforcement communications, emergency medical facilities, and other systems critical to a response. Moreover, it is conceivable that terrorists could mount a cyber attack against power or water facilities or industrial plants—for example, a commercial chemical plant that produces a highly toxic substance—to produce casualties in the hundreds or thousands.

Id.

68. *See, e.g.,* House of Commons Debates for 14 December 1999, 341 PARL. DEB. H.C., col. 221 (statement of Mr. Liddington) ("Had the Bishopsgate bomb or the Arndale centre bomb in Manchester gone off with no loss of human life and no injuries, those would still have been acts of terrorism designed to intimidate British people and to force the British Government into action out of fear that, otherwise, further lives would be put at risk or major damage would be done to the normal way of life."), *available at* http://www.parliament.the-stationery-office.co.uk/pa/cm199900/cmhansrd/vo991214/debtext/91214-23.htm.

69. In a 1998 exercise known as "Eligible Receiver," hackers hired by the National Security Agency used "software obtained easily from hacker sites on the Internet" to break into computer networks and gain access "to the systems that control the electrical power grid for the entire country. If they had wanted to, the hackers could have disabled the grid, leaving the United States in the dark." *See* Bill Gertz, *Eligible Receiver,* WASH. TIMES, Apr. 16, 1998, at A1, *available at* http://www-ugrad.cs.colorado.edu/~ife/114/EligibleReceiver.html. *See also* John Christensen, *Bracing for Guerrilla War in Cyberspace,* CNN.com, *at* http://www.cnn.com/TECH/specials/hackers/cyberterror/ (Apr. 6, 1999). Three years later, an obviously inexperienced hacker was able to gain access to "two Web servers at the California Independent System Operator (ISO)—the nonprofit corporation that controls the distribution of 75 percent of the state's power." Robert Lemos, *Humans Opened the Door for Calif. Power Attack,* ZDNet News, *at* http://zdnet.com.com/2100-11-268400.html (June 13, 2001).

70. *See, e.g.,* Simon Romero, *Attacks at Hubs Could Disrupt Phone Lines,* N.Y. TIMES, Nov. 23, 2001, at B4 ("Public safety experts . . . are increasingly concerned about the possibility of . . . . cyberattacks that could shut down parts of the public telephone system"), *available at* http://www.nytimes.com/2001/11/23/technology/23PHON.html?todaysheadlines. In February 2001,

emergency service system, the 911 phone system, are hacked into and sabotaged, so that system becomes dysfunctional.[71] The collapse of the landline telephone system effectively shuts off communication with local hospitals. At the same time, the hospital computer systems are compromised by a virus that begins erasing data files. Simultaneously, another computer virus infects the emergency alert system, causing emergency sirens to sound every fifteen minutes, further heightening the anxiety of the populace. Now, imagine that two hours after the Des Moines attack began another, almost identical attack hits Columbus, Ohio; and another two hours after the Columbus attack has been consummated another similar attack hits Phoenix. Imagine the effect such a calculated, layered attack on cities in the American heartland would have on the American public. There is no sanctuary remaining when a faceless entity can strike any city in America, crippling essential services and causing death, especially among the vulnerable elderly, poor, and young. The less vulnerable upper-middle class populace of each city are inconvenienced, traumatized, and angry; their sense of security has been violated, and they have no idea how it can be restored, but they want it to be restored. An attack such as this would have consequences far exceeding the tragic events of September 11 because its sequential, seemingly random structure strikes at America's very core, at the places we have always believed to be impregnable.

"two major wireless telecommunications service providers" informed the New York Electronic Crimes Task Force that

> they had identified two hackers in different remote sites who were attacking their systems. These hackers were manipulating the systems to obtain free long distance service, re-route numbers, add calling features, forward telephone numbers, and install software that would ensure their continued unauthorized access.
>
> The level of access obtained by the hackers was virtually unlimited, and had they chosen to do so, they could have shut down telephone service over a large geographic area, including '911' systems, as well as service to government installations and other critical infrastructure components.

Testimony of Robert N. Weaver, *supra* note 51. The Secret Service investigated and arrested both suspects, who were charged under state and federal laws. *See id.*

Cell phones would be a temporary alternative at best since, as September 11 showed, cell phone and pager networks can quickly become overloaded. *See, e.g.,* Jonathan Krim and Cynthia L. Webb, *Region's Phone System Buckles Under Surge of Calls,* WASH. POST, Sept. 11, 2001, at A7 ("Cell phone and pager networks were overwhelmed . . . in New York and Washington . . . as the East Coast's communication infrastructure strained to handle Americans' need to talk to each other about today's multiple terrorist attacks"), *available at* http://a188.g.akamaitech.net/f/188/920/45m/www.washingtonpost.com/wp-srv/nation/articles/telecom091101.html.

71. A few years ago, a Swedish hacker cut off 911 service in Florida for periods ranging up to four hours. *See, e.g.,* Critical Infrastructure Assurance Office, *Critical Infrastructure Event Timeline, at* http://www.ciao.gov/CIAO_Document_Library/cip_timeline.htm (on file with the University of Illinois Journal of Law, Technology & Policy); Bob Sullivan, *Cyberwar: The Threat of Chaos,* MSNBC.com, *at* http://www.msnbc.com/news/295227.asp (Aug. 6, 2000) (on file with the University of Illinois Journal of Law, Technology & Policy). It took months for the FBI to identify the perpetrator. *See* Critical Infrastructure Assurance Office, *supra.*

F. Risk Reduction

Another advantage of using cyberspace as a delivery method is that it frees terrorists from many of the risks they confront when using CBERN agents. A terrorist mounting a cyberterror attack runs no risk of contamination by chemical, biological or radiological agents and no risk that an explosive device will detonate prematurely. Furthermore, a terrorist can mount a cyberterror attack from a remote location with little, if any, fear of apprehension.

Even if a terrorist uses a computer in physical proximity to the scene of the terrorist event, the terrorist still does not have to be present. This eliminates the possibility that the terrorist will be identified and/or apprehended while initiating the event or, like Timothy McVeigh, be apprehended while fleeing the scene.[72] And while terrorists of the Al-Qa'ida stripe are certainly willing to die for their cause, the use of cyberspace can eliminate the necessity of sacrificing senior, expert terrorists such as Mohammed Atta to carry out one terrorist event.[73]

G. Increased Scale

Cyberspace offers another significant advantage for those would be terrorists: the use of computer technology can give terrorists the ability to inflict harm on a scale they could never achieve in the physical world. A terrorist using CBERN methods might be able to shut down the power grid or the phone system in one city. Doing even this would be a daunting task, since it would require coordinated attacks using conventional or nuclear explosives directed at critical nodes in one of the two systems.

---

72. Even if the computer used to commit an attack is identified, it may not be possible to link the computer to the terrorist(s) who used it since. Terrorists have used "public" computers, e.g., computers located in libraries, cybercafes and businesses that rent computers for use by the hour. *See, e.g.,* Johnson, *supra* note 34; Puzzanghera, *supra* note 34. *See also* Menon, *supra* note 34. And even if the computers were traced to the terrorists and the latter were identified, this does not guarantee their apprehension; the state harboring them might refuse to hand them over because of inadequate extradition laws and/or for political reasons. The Phillipines inability to extradite the "Love Bug" suspect illustrates the first obstacle; the United States' efforts to persuade the Taliban to hand over Bin Laden after the 9/11 bombing illustrates the latter difficulty. *See, e.g.,* Lynn Burke, *Love Bug Case Dead in Manila*, WIRED NEWS, Aug. 21, 2000, *available at* http://www.wired.com/news/print/0,1294,38342,00.html; *Taliban Won't Turn Over Bin Laden,* CBSnews.com, *available at* http://www.cbsnews.com/stories/2001/09/11/world/main310852.shtml (Sept. 21, 2001).

73. It can also mean that the perpetrators of a cyberterrorist attack can remain anonymous, if they like, and therefore immune to retaliation. *See, e.g.*, Rod Stark, *Cyber Terrorism: Rethinking New Technology*, *available at* http://www.infowar.com/mil_c4i/stark/Cyber_Terrorism-Rethinking_New_Technology1.html (last visited Nov. 6, 2002).

Even if a terrorist group could accomplish such an attack, it would be exceedingly difficult to carry out similar, temporally proximate attacks in other cities. Apart from the logistics involved in identifying the physical points in each city at which the explosives would need to be directed, the terrorists would have to confront the problems of delivering the necessary explosives to each target, and doing so without detection. The difficulty of delivering the explosives and avoiding detection would escalate markedly once the initial attack had been consummated because other cities would presumably be in a heightened state of alert.

H. "Terror Multiplier"

The use of computer technology to carry out acts of terror also has a collateral effect, one that is more subjective in nature. Military and law enforcement personnel use the term "force multiplier" to denote factors which enhance the effectiveness of troops or weapons.[74] The use of cyberspace to carry out terrorist events can be regarded as a "terror multiplier" to the extent it allows the perpetrator of the event to remain unknown. In both World Trade Center bombings and the Oklahoma City bombing, the respective perpetrators were quickly identified. Moreover, the perpetrators of the 1993 World Trade Center bombing and the Oklahoma City bombing were brought to trial, convicted, and punished. While it was not possible to bring the perpetrators of the 9/11 attacks to trial, they were identified and their motivations were explicated.

Identification of the architects of a terror event assists in reducing the psychological effects of the event on the surviving members of the targeted populace. Explaining a terrorist event helps the affected populace to deal with it and move on. An explained event is knowable, categorizable, and therefore less threatening. Perhaps the most unnerving aspect of a cyberterrorist event could be its unknowing quality.[75] The faceless perpetrators with their unarticulated, unidentified motives could persist in troubling the targeted population for months, if not years.

---

74. *See, e.g.*, EDWARD LUTTWAK & STUART L. KOEHL, A DICTIONARY OF MODERN WAR 226 (1991) ("Force Multiplier: U.S. term for new tactics or equipment which are meant to increase a unit's combat effectiveness in a manner equivalent to an increase in its size."(*quoted in* Tim Hoyt, *Malicious Support: Diplomacy's Ultimate Force Multiplier*, DIPLOMACY WORLD http://ourworld.compuserve.com/homepages/DiplomacyWorld/support.htm (last modified Feb. 1, 1998)).

75. While the perpetrators of a cyberterrorist attack presumably can remain anonymous, they may choose not to do so. Terrorists may want to take credit for what they have done; choosing to publicize their names and their objectives, possibly with the intention of inducing even more fear in the targeted population. And they can announce that they were responsible for a cyberattack without surrendering any of the other advantages described above.

III. CYBERTERRORISM SCENARIOS

At some future time, the United States will be attacked, not by hackers, but by a sophisticated adversary using an effective array of information warfare tools and techniques.[76]

Essentially, a cyberterrorist attack is launched from one computer and directed at another computer or computer system.[77] Attacks on computer systems can be divided into three types: physical attacks, syntactic attacks, and semantic attacks.[78]

A. Physical Attacks

Physical attacks are irrelevant for the purposes of this discussion because they do not involve the use of cyberspace; a physical attack is simply a physical assault on a computer or a computer system.[79] Using an explosive device to destroy a computer system is an example of a physical attack. Since it involves the use of a "physical world" delivery method, such an attack should be analyzed under the CBERN typology.

B. Syntactic Attacks

Syntactic attacks are directed at a computer's operating system, and/or at the software level that controls its functions.[80] A syntactic attack "consists of modifying the logic of the [computer operating] system in order to introduce delays or to make the system unpredictable."[81] A majority of the attacks experienced in the recent years have been syntactic attacks.[82] Worms, viruses, Trojan Horses and denial of service attacks are examples of syntactic attacks.[83]

---

76. PROTECTING THE HOMELAND, *supra* note 45.

77. *See, e.g., Cyberterrorism: Testimony Before the Special Oversight Panel on Terrorism Committee on Armed Services,* U.S. H.R., 105th Cong. (May 23, 2000) (testimony of Dorothy E. Denning, Professor, Georgetown University) *available at* http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html [hereinafter Testimony of Denning].

> Cyberterrorism . . . . is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives . . . . [T]o qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear . . . .

Id. See also Rod Stark, *supra* note 73 ("cyber-terrorism is any attack against an information function, regardless of the means").

78. *See, e.g.,* Martin Libicki, *The Mesh and the Net: Speculations on Armed Conflict in an Age of Free Silicon,* McNair Paper 28, March 1994, at 110, *available at* http://www.ndu.edu/inss/macnair/mcnair28/m028cont.html.

79. *Id.*

80. *Id.* at 111.

81. Patrick Galley, *Computer Terrorism: What Are the Risks?*, Swiss Federal Institute of Technology, *at* http://homer.span.ch/~spaw1165/infosec/sts_en/index.html (May 30, 1996).

82. *See, e.g.,* Bruce Schneier, *The Third Wave of Network Attacks*, ZDNet News, *at*

Syntactic attacks are capable of inflicting widespread damage. The Love Bug virus,[84] for example, raced around the world in two hours, affecting forty-five million users in more than twenty countries causing between $2 billion and $10 billion in damage.[85] The Love Bug was neither designed to be, nor disseminated as, the instrument used to carry out a terrorist event; indeed, it may have been released accidentally.[86] How might a worm designed for terrorist purposes and decimated to this end be designed? It could be engineered merely to delete files on any infected machines or it could be a Trojan Horse, designed to insinuate itself into the operating system of infected machines and then let terrorist controllers take over and direct the infected machines toward some concerted end.[87]

A terrorist-designed worm/virus previously might have features rendering it far more destructive than any previously encountered worm/virus. One factor mitigating the damage inflicted by the worms and viruses that have emerged, to date, is the computer security

---

http://zdnet.com.com/2100-11-524330.html?legacy=zdnn (Oct. 2, 2000).

83. *See id.*

84. Technically, the "Love Bug" was both a virus and a worm:

> Once you've clicked open that fatal attachment and activated its deadly code, the virus either erases or moves a wide range of data files . . . and . . . replaces them with identical copies of itself. Then, if it finds the Microsoft Outlook Express e-mail program on your computer, it raids the program's address book and sends copies of itself to everyone on that list . . . . [T]his two-pronged approach makes the Love Bug both a virus and a worm; it's a virus because it breeds on a host computer's hard drive and a worm because it also reproduces over a network.

Lev Grossman, *Attack of the Love Bug*, TIME EUROPE, May 15, 2000, *at* http://www.time.com/time/europe/magazine/2000/0515/cover.html. For more on computer viruses and worms, *see, e.g.*, Jeffrey O. Kephart, et al., *Fighting Computer Viruses*, SCI. AM., Nov. 1997, at 88-93, *at* http://www.sciam.com/1197issue/1197kephart.html (on file with the University of Illinois Journal of Law, Technology & Policy); Bob Page, *A Report on the Internet Worm* (Nov. 7, 1988), *at* ftp://coast.cs.purdue.edu/pub/doc/morris_worm/worm.paper; Computer Abuse: Worms, Viruses, Trojan Horses, *at* http://www.eos.ncsu.edu/eos/info/computer_ethics/abuse/wvt/ (last visited Nov. 7, 2002).

85. *See* Grossman, *supra* note 84; *Philippine Investigators Detain Man in Search for "Love Bug" Creator,* CNN.com, *at* http://www.cnn.com/2000/TECH/computing/05/08/ilove.you.02/ (May 8, 2000); *Love Bug Suspect Suggests It Was "Accidental,"*, apbnews.com, *at* http://www.apbnews.com/newscenter/internetcrime/2000/05/11/lovebug0511_01.html (May 11, 2000) (on file with the University of Illinois Journal of Law, Technology & Policy); John Leydon, *Love Bug Author Says But Created in Cyber Gang War*, THE REGISTER (London), May 2, 2001 *at* http://www.theregister.co.uk/content/6/16657.html.

86. *See, e.g., Love Bug Author Tracked*, PAKISTAN PRESS INT'L, May 17, 2000, LEXIS, Nexis Library, Nationwide International News file.

87. In 1998, a hacker group known as the Cult of the Dead Cow released Back Orifice, a Windows remote administration tool that let a hacker completely control an infected computer from a remote location. *See, e.g.,* Robert Lemos, *"Back Orifice," A Hacker App, Wows Crowd at DEF CON,* ZDNet News, *at* http://www.zdnet.com/eweek/news/0803/03mdef.html (Aug. 3, 1998) (on file with the University of Illinois Journal of Law, Technology & Policy).

> The application, once installed on a target PC, effectively takes control of the computer, letting the "administrator" use any multimedia or data file on it, generate error messages, browse the Internet as if from the co-opted machine or even shut down the remote computer.
>
> All of this can go on without the PC's legitimate user ever having a clue.

Id. The Cult of the Dead Cow released an improved version of Back Orifice in 1999. *See* Cult of the Dead Cow, *Tools*, http://www.cultdeadcow.com/tools/; *see also* Scott Ard, *Back Orifice 2000 Makes Its Debut,* C|Net.com, *at* http://news.cnet.com/news/0-1003-200-344651.html (July 10, 1999).

community's ability to respond with countermeasures, often very quickly. When the Code Red worm appeared in July 2001, anti-virus companies quickly produced software that could find and remove it from infected machines, and Microsoft distributed a patch that closed the loophole the worm exploited.[88] There is speculation that some worms—known as "flash worms" or "Warhol worms"—could be created that would, upon being released, race around the world, infecting millions of computers within a few minutes.[89] The destructive payload of such a worm could be triggered and have finished its work long before anyone would have a chance to develop countermeasures.[90]

As to denial of service attacks, terrorists hardly need to improve on existing technology; it is already difficult to defend against a properly mounted denial of service attack, which can take either of two forms. In a simple denial of service attack, the attacker shuts a Web site down "by flooding it with large amounts of traffic, similar to . . . repeatedly dialing a telephone number to keep it busy and unavailable."[91] In the more

---

88. *See, e.g., Code Red Keeps World Guessing*, BBC News, *at* http://news.bbc.co.uk/hi/english/sci/tech/newsid_1466000/1466588.stm (Aug. 1, 2001); *see also* Duncan Martell & Bernhard Warner, *Nimda Infections May Be Peaking*, TechTV, *at* http://www.techtv.com/news/internet/story/0,24195,3348549,00.htm (Sept. 19, 2001) (major anti-virus companies quickly responded to September outbreak of the Nimda virus).

89. *See, e.g.*, Stuart Staniford et al., *Flash Worms: Thirty Seconds to Infect the Internet*, SiliconDefense.com (arguing that a worm could be developed that "could result in all vulnerable servers on the Internet being infected in less than thirty seconds"), *at* http://www.silicondefense.com/flash/ (Aug.16, 2001); Nicholas C. Weaver, *Warhol Worms: The Potential for Very Fast Internet Plagues* (Aug.15, 2001) (positing the creation of a "Warhol worm" that could infect the Internet in 15 minutes; the name comes from Andy Warhol's comment that "in the future everybody will have 15 minutes of fame"), *at* http://www.cs.berkeley.edu/~nweaver/warhol.html.

In 1998, there were reports that a "Blitzkrieg virus" had been developed which was "an undetectable and unstoppable cyber weapon" that was "the equivalent of the deadly human Ebola virus, capable of infiltrating and systematically devouring information networks." Rod Stark, *supra* note 73.

90. We are already seeing the emergence of more destructive viruses and worms:

> Computer security experts . . . have begun seeing . . . increasingly potent attacks by hackers . . . . Attackers have also employed new "worms" like the recent Nimda, which transmits destructive activity from computer to computer with greater efficiency and power than ever before by combining several kinds of attacks. Increasingly, these programs are being aimed at routers, which direct traffic throughout the Internet. The effects of these denial of service attacks "are causing greater collateral damage," warned Kevin J. Houle, a researcher at the [CERT Coordination Center at Carnegie Mellon University].
>
> No computer on the Internet is immune from denial of service attacks, said Paul A. Vixie, a security expert . . . , not even crucial machines that direct Web surfers to sites, including the 13 "root" servers and the 10 top-level domain servers. "The only thing that keeps a given server on the air on any particular day is that no teenager with a $300 computer is angry enough at that server's operators to feel like punishing them," he said in an e-mail interview.

Id. See also, John Schwartz , *Cyberspace Seen as Potential Battleground*, N.Y. TIMES, Nov. 23, 2001, at B5, *available at* http://www.nytimes.com/2001/11/23/technology/23CYBE.html?todaysheadlines.

91. Internet Sec. Systems, Denial of Service FAQ, *at* http://www.iss.net/news/denialfaq.php#1.1 (last visited Nov. 7, 2002); *see also,* CENTER FOR DEMOCRACY & TECHNOLOGY, *Denial of Service Attacks* ("A hacker can flood a computer with so many requests for data that it ceases to function and cannot provide information to legitimate requestors. This is called a 'denial of service' attack because it effectively shuts down the affected computer."), *at* http://www.cdt.org/security/dos/ (last visited Nov. 7, 2002).

sophisticated distributed denial of service attack, the attacker takes over hundreds or thousands of computers and uses them to bombard the target site.[92] In February 2000, Yahoo!, Amazon.com, and CNN, among others, were shut down for hours as a result of a denial of service attack attributed to a fifteen-year old boy that was estimated to have caused $1.2 billion in damage.[93] In 1998, in what is generally described as the first cyberterrorist event, Sri Lankan terrorists effectively carried out a denial of service attack against servers in Sri Lankan embassies in three countries.[94] And on September 18, 2001, the FBI's National Infrastructure Protection Center issued a warning that distributed denial of service attacks were possible "as a digital continuation of the terrorist attacks against targets in New York and near Washington, D.C. last week."[95] Denial of service attacks offer terrorists at least three advantages: they can be launched from remote locations (as the Sri Lankan incident illustrates); they do not require that the attacker

---

In February of 2000, for example, the National Discount Brokers Group was shut down for over an hour by a denial of service attack which "prevented 200,000 National Discount customers from placing stock orders through the firm's Web site." Chet Dembeck, *Latest Hacker Attack Cripples Online Brokerage,* E-COMMERCE TIMES, Feb. 25, 2000, *at* http://www.ecommercetimes.com/perl/story/2587.html.

92. *See* Mo Krochmal, *Distributed Denial of Service Threat Grows,* TechWeb, *at* http://content.techweb.com/wire/story/TWB20000208S0016 (Feb. 8, 2000). A distributed denial of service attack works by creating a network of "zombie" computers, e.g., computers the attacker has taken over by hacking into them and installing software that lets him control them from a remote location. *Id.*

> Once the DDoS attack has been launched, it's hard to stop. Packets arriving at your firewall may be blocked there, but they may just as easily overwhelm the incoming side of your Internet connection. If the source addresses of these packets have not been spoofed, you can try to find and then contact the responsible parties (for what may be hundreds of computers around the world) and ask them to stop the agents. If the addresses are spoofed, you will have no way of knowing if they reflect the true source of the attack until you track down some of the alleged sources . . . .
>
> . . . .
>
> . . . Imagine what it would be like to be a victim of hundreds of simultaneous attackers. Are you ready to try to contact hundreds of people around the world (anyone at your office speak Russian or Tagalog?), even as the attackers switch to another set of agents?

Rik Farrow, *Distributed Denial of Service Attacks,* NETWORK MAG., Mar. 1, 2000, *at* http://www.networkmagazine.com/article/NMG20000512S0041/2.

93. *See, e.g.,* James Evans, *"Mafiaboy" Will be Sentenced in April,* NETWORK WORLD FUSION, Jan. 22, 2001, *at* http://www.nwfusion.com/news/2001/0122sentence.html; Rivka Tadger, *Detect, Deflect, Destroy,* INTERNET WEEK, Nov. 13, 2000, *at* http://www.internetweek.com/indepth/indepth111300.htm.

94. *See, e.g.,* Julie L.C. Thomas, *What is Hacktivism?,* SANS INSTITUTE, Jan. 12, 2001, http://www.sans.org/infosecFAQ/hackers/hacktivism2.htm; *see also* Dorothy E. Denning, *Hacktivism: An Emerging Threat to Diplomacy,* FOREIGN SERV. J., Sept. 2000, *available at* http://www.afsa.org/fsj/sept00/Denning.html.

> In what some U.S. intelligence authorities characterized as the first known attack by terrorists against a country's computer systems, ethnic Tamil guerrillas were said to have swamped Sri Lankan embassies with thousands of electronic mail messages in 1998. The messages read 'We are the Internet Black Tigers and we're doing this to disrupt your communications.'
>
> . . . .
>
> The e-mail bombing consisted of about 800 e-mails a day for about two weeks.

Id.

95. Sam Costello, *Terrorists May Launch Denial of Service Attacks,* PC WORLD, Sept. 18, 2001, *at* http://www.pcworld.com/news/article/0,aid,62505,00.asp.

penetrate a computer system because the attacks work by overwhelming the system from outside; they are extraordinarily difficult to prevent and to stop once they have begun.

Finally, syntactic attacks can also take the form of hacks – breaking into a computer system and altering its function in more or less subtle ways. Many of the scenarios described in the previous section—the attacks on New York, Des Moines, Columbus and Phoenix – are examples of this type of syntactic attack.[96] The New York scenario, for example, postulates that terrorists hack into the New York subway's computer system and discretely alter its operation, thereby halting trains between stations. In a less dramatic real-life example, an Australian man hacked into a computerized waste management system in Maroochy Shire, Queensland, and "caused millions of litres of raw sewage to spill out into local parks, rivers and even the grounds of a Hyatt Regency hotel."[97]

C. Semantic Attacks

Semantic attacks are very different from syntactic attacks. Syntactic attacks target a computer's operating system; semantic attacks target a computer user's confidence in the accuracy of the data he or she accesses.[98] A semantic attack consists "of modifying information that is entering the system, without the users' knowledge, in order to induce errors."[99] "A system under semantic attack operates and will be

---

96. In May of 2002, it was reported that terrorists have discussed mounting syntactic attacks on the following targets:

> The Centers for Disease Control and Prevention, based in Atlanta. It is charged with developing the nation's response to potential attacks involving biological warfare.
>
> The nation's financial network, which could shut down the flow of banking data. The attack would focus on the FedWire, the money-movement clearing system maintained by the Federal Reserve Board.
>
> Computer systems that operate water-treatment plants, which could contaminate water supplies.
>
> Computer networks that run electrical grids and dams.
>
> As many targets as possible in a major city. Los Angeles and San Francisco have been mentioned by terrorists . . . .
>
> Facilities that control the flow of information over the Internet . . . .
>
> The nation's communications network, including telephone and 911 call centers.
>
> Air traffic control, rail and public transportation systems.

Tom Squitieri, *Cyberspace Full of Terror Targets,* USA TODAY, May 6, 2002, at 11A, *at* http://www.usatoday.com/life/cyber/tech/2002/05/06/cyber-terror.htm (May 5, 2002).

97. Tony Smith, *Hacker Jailed for Revenge Sewage Attacks,* THE REGISTER (London), Oct. 31, 2001, *at* http://www.theregister.co.uk/content/4/22579.html. "'Marine life died, the creek water turned black and the stench was unbearable for residents' said Janelle Bryant of the Australian Environmental Protection Agency." *Id.* The perpetrator was identified and sentenced to two years in prison for his efforts. *Id.*

In the spring of 2002, hackers broke into a Federal Aviation Administration computer system and downloaded "unpublished information on airport passenger screening activities". Kevin Poulsen, *FAA Hacked by Patriots,* THE REGISTER (London), May 3, 2002, *at* http://www.theregister.co.uk/content/55/25029.html. The hackers also defaced the FAA site and posted information about passenger screeners and their activities, information the FAA insisted was in no way sensitive. *See id.*

98. *See* Libicki, *supra* note 78.

99. Galley, *supra* note 81.

perceived as operating correctly (otherwise the semantic attack is a failure), but it will generate answers at variance with reality."[100]

Semantic attacks are based on the very reasonable premise that computer users implicitly accept the accuracy of certain types of information they access via a computer. Most computer users—and certainly the "reasonable computer user"—are unlikely to accept the content found on particular types of Internet sites, such as those maintained by "hobbyists"[101] or those maintained by groups or individuals who espouse a less-than-mainstream, often proselytizing ideology. They will accept with much less skepticism the accuracy of content on mainstream sites maintained by professional groups or entities, such as FindLaw, CNN, Reuters, and the American Medical Association.[102] One type of semantic attack exploits this trust.

A good example of such a semantic attack occurred in September of 2001: Earlier in the year, Dmitry Sklyarov, a Russian citizen, was arrested and indicted in this country for violating the Digital Millennium Copyright Act [hereinafter DMCA].[103] Sklyarov, who was arrested in California while attending a conference, was charged with creating and disseminating a program that decrypts Adobe's eBook files, letting users freely copy, print, and distribute its contents.[104] His arrest and indictment came under attack from "computer programmers and electronic civil libertarians who argue that the DMCA is an unconstitutional impingement on speech, and interferes with consumers' traditional right to make personal copies of books, movies and music that they've purchased."[105] On August 23, 2001, Yahoo! News published a Reuters story, online, that described a delay in the Sklyarov court proceedings.[106] A hacker broke into the Yahoo! Web site and modified the story so it

---

100. Martin Libicki, *What Is Information Warfare? – Cyberwarfare*, Acis Paper 3, Aug. 1995, at ch.9, *available at* http://www.ndu.edu/inss/actpubs/act003/a003ch09.html.

101. A "hobbyist" is a layperson who has created and is maintaining a Web site dedicated to some topic he or she finds of particular interest. Some hobbyist sites are excellent sources of detailed, accurate information; most are not.

102.

> [S]emantic attacks . . . target the way we, as humans, assign meaning to content. In our society, people tend to believe what they read. How often have you needed the answer to a question and searched for it on the Web? How often have you taken the time to corroborate the veracity of that information, by examining the credentials of the site, finding alternate opinions, and so on? Even if you did, how often do you think writers make things up, blindly accept "facts" from other writers, or make mistakes in translation?

Bruce Schneier, *supra* note 82.

103. *See, e.g.,* Press Release, U.S. Dept. of Justice, First Indictment Under Digital Millennium Copyright Act Returned Against Russian National, Company, in San Jose, California (Aug. 28, 2001), *at* http://www.cybercrime.gov/Sklyarovindictment.htm.

104. *See, e.g.,* Elise Ackerman, *Arrest of Russian Programmer Will Test Copyright Law*, SAN JOSE MERCURY NEWS, July 18, 2001, at 1C, *available at* http://www.siliconvalley.com/docs/news/svtop/arrest071801.htm.

105. Kevin Poulsen, *Yahoo! News Hacked*, SEC. FOCUS, Sept. 18, 2001, *at* http://online.securityfocus.com/news/254.

106. *Id.*

reported, incorrectly, that Skylarov was facing the death penalty.[107] This is a semantic attack; the hacker altered the content of information available on a site to which he did not have legitimate access.

A variation on this type of semantic attack targeted CNN. In October 2001, a man who was "conducting research as to how far and fast misleading information travels on the Web" posted a hoax site that mimicked a CNN.com Web page.[108] The headline on the hoax site, which received 150,000 hits before it was taken down, read "Singer Britney Spears Killed in Car Accident."[109] Ironically, "CNN.com unwittingly helped perpetuate the hoax by directing users to the external bogus report; this made 'Singer Britney Spears Killed in Car Accident' the 'Most Popular' story credited to CNN.com, without it ever actually residing on the news site's pages."[110] This hoax site, one of many, illustrates how easy it is to disseminate misinformation over the Web.[111]

A terrorist could use a variation on this type of semantic attack to enhance the terror and disruption caused by a CBERN-style terrorist attack. Imagine, for example, what could have ensued had this scenario played itself out beginning around 9:30 a.m. EDT on September 11: As the planes crashed into the World Trade Center and the Pentagon,

---

107. *Id.*

> The modified story warned sardonically that Sklyarov's work raised the haunting specter of inner-city minorities with unrestricted access to literature, and through literature, hope.
>
> The text went on to report that Attorney General John Ashcroft held a press conference about the case before "cheering hordes," and incorrectly quoted Ashcroft as saying, "They shall not overcome. Whoever told them that the truth shall set them free was obviously and grossly unfamiliar with federal law."

Id.

108. *Britney Spears Hacked Into CNN.com,* Internetnews.com, *at* http://www.internetnews.com/dev-news/article/0,,10_900811,00.html (Oct. 10, 2001).

109. *Id.*

110. *Id.* The creator of the hoax site, Tim Fries,

> . . . used a mock-up of a CNN.com Web page at an external site and exploited a peculiarity in how Web browsers handle URLs. Fries launched the Spears death hoax by distributing a specially crafted URL to three users of AOL's Instant Messenger chat software.
>
> The URL began with the characters http://www.cnn.com , followed by '@' and the IP address of his Web site. Because browsers ignore the characters to the left of the '@' in the Web address, users were taken directly to the phony article when they clicked on it.
>
> When readers clicked on the 'E-mail This' link on the phony Web story to send it to others, CNN.com's systems were triggered, distributing a message with CNN.com's logo and a link to the bogus news piece. The news site's systems added each 'Email This' click to its 'Most Popular' stories total.

Id. See also fnord, *When Semantics Attack,* ICANNWatch, *at* http://www.icannwatch.org/article.php?sid=423 (Oct. 21, 2001).

111. *Id.* (Fries "sent a specially crafted URL to only *three* people via AOL's IM Chat pointing to an apparent CNN.com story that Ms. Spears had been killed in a car accident. Within twelve hours the bogus news had been read by at least *150,000* people and became CNN's *Most Popular Story*").

Posting bogus sites became much easier in November, 2001, when a group of Internet activists known as the Yes Men created and distributed software called "YesIWill" which would allow "technically savvy users to spoof virtually any Web site in a matter of minutes." David McGuire, *Mirror Software Makes It Easier to Spoof Famous Sites,* NEWSBYTES, Nov. 20, 2001, *available at* LEXIS, News & Business, News, Newsgroup File. *See also* Reamweaver Home Page (site offering YesIWill software for download, along with a gallery of spoofed sites), *at* http://www.reamweaver.com/ (last visited Nov. 7, 2002).

millions of Americans watched the events unfold on televisions and many of those millions turned to the Internet to try to find out more about what was happening. The CNN site, http://www.cnn.com, was hit very heavily that day by people trying to learn as much as they could about what had happened and about what might happen. What if, instead of finding accurate, CNN-generated content, these visitors had encountered a Web page that announced—in appropriately terrifying graphics — "World at War - Nuclear Bombs Falling in Europe, Japan Devastated by Chemical Attack, Nuclear Holocaust in Australia"? Since this would have happened in 2001, not in 1939, an Orson Welles "War of the Worlds" reaction [112] would be unlikely; people obtain their news from several types of media and from various sources within each media type. But the posting of such a falsified page—the product of a semantic attack—would undoubtedly have acted as a terror multiplier, significantly enhancing the unnerving effects of the day's "physical world" terrorist events.

A more insidious type of semantic attack could seek to exploit the philosophical, cultural, and racial heterogeneity of American society by turning black against white, Christian against Jew, neo-fascist against everyone else. Unlike the other types of terrorist events discussed in this article, a semantic attack of this type would have to be subtle and sustained, designed to erode not only the respect, but the tolerance the members of one group have for members of another. An attack of this type would not be a simple, single-event endeavor, though it might well commence with a single, calculated bit of misinformation.

If the goal were, as it might well be, to discredit Israel and foment antipathy toward Jews here and abroad,[113] the semantic campaign might start with a theory that has gained great credence in some parts of the world: that the 9/11 attacks were a Mossad plot, a deception designed to turn the United States against the Muslim world.[114] The theory could be

---

112.

In the 1930s, the story 'War of the Worlds' was read on public radio. While neither a deception nor disinformation operation, it produced sheer panic in many parts of the country. The broadcast merely exploited the prism and logic of the average citizen through which information was processed, and the means through which he or she received reliable information (radio). It was an unintentional manipulation of the rational thought of the populace.

Timothy L. Thomas, *The Age of the New Persuaders,* MILITARY REV., May-June 1997, *at* http://call.army.mil/fmso/fmsopubs/issues/maninfo.htm.

113. A semantic campaign such as this attempts to exploit underlying resentments and offers an excuse for abandoning what will no doubt be a difficult war on terrorism.

114. *See, e.g.,* Arieh O'Sullivan, *Syrian Defense Minister Blames WTC, Pentagon Attacks on Israel,* THE JERUSALEM POST, Oct. 19, 2001, *available at* http://www.jpost.com/Editions/2001/10/19/News/News.36550.html.

Syrian Defense Minister Mustafa Tlass has blamed the September 11 attacks on the World Trade Center on Israel.

At a meeting in Damascus last week with a delegation from the British Royal College of Defense Studies, Tlass said the Mossad planned the ramming of two hijacked airliners into the WTC's towers as part of a Jewish conspiracy.

He also told the British visitors that the Mossad had given thousands of Jewish employees of the WTC advance warning not to go to work that day.

fleshed out with "facts" proving that the attacks were, indeed, a Mossad production. One fact already cited as supporting this theory in certain parts of the world is that there were no Jews in the World Trade Center or the Pentagon on September 11. Further "facts" of this type could be created and disseminated: the goal being to sew seeds of distrust and eventually turn many, if not most, Americans against Jews and Israel.

What might be the ultimate purpose of a semantic disinformation campaign such as this? Obviously, a group like Al-Qa'ida would like to ignite an internal race ideological religious war in the United States, the type of firestorm envisioned in *The Turner Diaries*, the "Bible of the racist right."[115] While one hopes this outcome is exceedingly unlikely, it might be possible that a semantic campaign of this type could produce enough dissension to cause the country to falter in its efforts to eradicate terrorism. A divided country could even attempt a misguided return to

---

> The Jewish-conspiracy theory started circulating in the Middle East shortly after the terrorist outrages in New York, Washington, and Pennsylvania. The 'rationale' was that Israel wanted to provoke US retaliation against the Arab world.
>
> ....
>
> In Iran, the hard-line Resalat newspaper last week quoted "experts" as saying the attacks were so complicated they had to have been carried out by the Israeli government and the Mossad. In Kuwait, ... some people have even added embellishments, saying Jews were advised by New York rabbis to sell their holdings in the stock market the day before the attack and did so.

Id. *See also* David Stern, *Who Attacked the USA?*, Vaikuttava, http://www.vaikuttava.net/article.php?sid=1112 (Sept. 18, 2001).

> A US military intelligence source revealed details of an internal intelligence memo that points to the Israeli Mossad intelligence service having links to the World Trade Center and Pentagon attacks. The intelligence source, who requested his name be withheld, confirmed the internal US intelligence memo circulated four weeks ago described information that pointed to the threat of a covert Israeli operation on US soil to turn mass public opinion against Palestinian Arabs via an apparent terrorist attack on US interests that would give Israel the green light to implement a large scale military onslaught against the Palestinian Arab population.
>
> The 11 September attack has been described experts as being too sophisticated for a lone terrorist group to execute ....

Id. For an Egyptian perspective, *see* Amil Khan, *Terror Attack Fuels Slew of Conspiracy Theories in Egypt,* MIDDLE EAST TIMES, Sept. 18, 2001, *available at* http://www.metimes.com/2K1/issue2001-39/eg/terror_attack_fuels.htm.

> Emails have been circulating around Cairo reiterating the view that Israel had the most to gain from such an attack. One email argues that Israel had become exasperated with the continuing bad press it had received due to the Palestinian uprising and decided to show American and world opinion what it was like to face a suicide bombing.
>
> ....
>
> The Egyptian theories seem to reflect the view of many Egyptians that the Americans have been vilifying Osama Bin Laden and are ready to kill civilians to reach him on weak evidence that might turn out to be inaccurate. The Oklahoma City bombing is continually referred to, when U.S. investigators announced that they were looking for a 'man of Middle Eastern appearance' when the culprit turned out to be American Timothy McVeigh, who was executed for the crime three months ago.

Id. For a very different theory, *see The World Trade Center Demolition and the So-Called War on Terrorism*, Serendipity, *at* http://serendipity.magnet.ch/wtc.html (last modified Sept. 11, 2002) (the attacks on the World Trade Center and the Pentagon were carried out by the Federal Bureau of Investigation, which is also responsible for the 1993 World Trade Center bombing and the bombing of the Oklahoma City Federal building).

115. Written by William Pierce (a/k/a "Andrew Macdonald"), *The Turner Diaries* describes an "all-out race war" fought by "Whites" against Jews and "Blacks" in the United States. ANDREW MACDONALD, THE TURNER DIARIES, AN EPILOGUE, *available at* http://www.angelfire.com/hi/themadmoose/td.html (last visited Nov. 7, 2002).

the state of isolation that its citizens believed existed until September 11, 2001. One wonders what would happen if a relentless, calculated campaign of this sort were mounted at a time when the war on terrorism was not going well. The notoriously impatient American public may well find this type of conspiracy theory useful as an excuse to abandon the fighting.

At the very least, the semantic campaign sketched above illustrates how an attack of this type can be structured. Its basic structure differs little from similar efforts that have been undertaken in the past,[116] usually in an attempt to generate a Fifth Column[117] in the populace of a wartime adversary. The delivery method would differentiate a semantic attack of the type hypothesized above from prior efforts. Those responsible for mounting such an attack could use web sites and email to disseminate their insidious falsehoods. The Web sites could offer bogus information and fictitious "documentation" consisting of textual records, photographs, videos and sound clips. All of these mediums could be easily fabricated. The latter three exploit humankind's well-known susceptibility to "first-hand information" or, perhaps more accurately, to what we choose to believe is "first-hand information."[118]

Disinformation can also be used to attack the economy. For example, Internet Wire, one of the service companies use to distribute news releases to the public and the media, received an August 25, 2000, email that apparently came from Emulex Corporation, a network equipment maker.[119] The email, which was forged, announced the

116. For a description of one such effort, *see* GEORGES LEFEBVRE, THE GREAT FEAR OF 1789 122-33, 143-47, 211 (1970) (describing panic generated in Revolutionary France by rumors that "brigands" were spreading across the countryside, killing and pillaging; the revolutionaries, at least, believed the rumors were deliberately spread by the aristocracy, as part of an effort to avert revolution).

117. The term denotes a "clandestine group or faction of subversive agents" operating inside a country who attempt to undermine its "solidarity by any means at their disposal." "Fifth Column," ENCYCLOPEDIA BRITTANICA, *at* http://www.britannica.com/eb/article?eu=34839 (last visited Nov. 4, 2002). It was apparently coined during the Spanish Civil War.

> In October 1936, ... the fascist General Emilio Mola Vidal, commanding four columns marching on Madrid, was asked by foreign journalists which of the columns would take the capital. According to historian Hugh Thomas, Mola responded that it would be the 'fifth column,' a cadre of secret Nationalist supporters already in the city.

Martin Peretz, *When America-Haters Become Americans,* THE NEW REPUBLIC, Oct. 5, 2001, at 20, *available at* http://www.thenewrepublic.com/101501/peretz101501.html.

118. *See* Libicki, *supra* note 78.

> Technology will also make it impossible to distinguish among real and fake photographs, video, or recordings. Anyone ... could create for broadcast a video of an opponent counseling acquiescence to his people. This image would look and sound like the real thing, being indistinguishable in both grammar, nuance, and gesture ....
>
> People tend to believe what they want to believe (or what others they fear or respect want them to believe) ....

Id.

119. *FBI Pursued Emulex Release as Online Fraud,* C|Net News, *at* http://www.zdnet.com/zdnn/stories/news/0,4586,2620888,00.html (Aug. 28, 2000).

resignation of the company's Chief Executive Officer and restated its earnings.[120]

> Internet Wire posted the press release .... Several financial news services and Web sites further distributed the false information, and the stock dropped 61 percent (from $113 to $43) before the hoax was exposed.
>
> ... Despite its amateurish execution (the alleged perpetrator ...was caught in less than 24 hours), $2.54 billion in market capitalization disappeared, only to reappear hours later. With better planning, a similar attack could do more damage and be more difficult to detect.[121]

A few years ago, hackers apparently planned to cause the New York Stock Exchange's computer system to crash and delete its files;[122] the scenario now seems highly unlikely in view of the system's increased security, including an elaborate backing up and off-site storage systems.[123] While a denial of service attack is clearly possible,[124] a semantic attack seems the most likely to succeed. Stock exchanges and other financial entities can exert a good deal of control over the information they generate and disseminate. They can take steps to protect their computer systems from outside intrusion. However, there is little, if anything, they can do to control the ebb and flow of information in the global marketplace. As the Emulex incident illustrates, it is quite possible for terrorists to introduce disinformation into the marketplace, disinformation that can affect stock prices and the functioning of the market.[125] If the terrorists work subtly by carefully selecting the type of disinformation to distribute and slowly disseminating it, their efforts might well go undiscovered long enough to cause a major disruption in the market.

---

120. *Id.*

121. Bruce Schneier, *supra* note 82. The alleged perpetrator, a former employee of Internet Wire, made almost $240,000 from the hoax before being arrested and indicted for the attempted stock manipulation. *See, e.g.,* U.S. Dept. of Justice, Emulex Hoaxer Indicted for Using Bogus Press Release and Internet Service to Drive Down Price of Stock (Sept. 28, 2000), *at* http://www.usdoj.gov/criminal/cybercrime/emulex.htm.

122. M.J. Zuckerman, *U.S. Networks Most Vulnerable of Any Nation,* USA TODAY, Feb. 28, 1999, *available at* http://www.usatoday.com/life/cyber/tech/ct033.htm.

> Two years ago, information from a German hacker led officials of the [National Security Information Exchange] to plug a security hole that could have been exploited to wipe out the New York Stock Exchange's computerized trading records.
>
> The hacker discovered how to access the environmental systems in buildings housing the exchange's computer systems. By overheating those buildings they could have crashed the computer.

Id.

123. *Technology Lost In Attacks May Cost US $3.2bn,* TAIPEI TIMES, Sept. 17, 2001 (describing New York Stock Exchange maintains offsite backup data center), *available at* http://www.taipeitimes.com/news/2001/09/17/story/0000103401. The New York Stock Exchange was shut down for ninety minutes on June 8, 2001, because of a flaw in a software upgrade. *Downtime Dangers: Stock Market Outages Highlight Software Availability Issues,* THE PAYNE REPORT (Cigital Labs), July/August 2001, *at* http://www.cigital.com/paynereport/archive/jul-aug2001.html.

124. For one scenario, *see Global Terror, Area-x.co.uk - Conspiracy World, at*

Semantic attacks can take other forms, as well. One example that is often given involves nuclear plants. Nuclear plants have sensors that detect seismic activity within an area; upon sensing seismic activity they transmit that information to a system which shuts down the nuclear

---

http://www.cowan70.freeserve.co.uk/miscellaneous/global_terror.htm (last visited Nov. 7, 2002).

> A bell marking the opening of business sounds on the cavernous trading floor of the New York Stock Exchange. It is Feb. 4, 2006 . . . . As traders reach for their phones, all of the computer screens in the Exchange suddenly go blank . . . .
>
> . . . .
>
> In th[is] hypothetical assault . . . the Stock Exchange's computers might be put out of action by an 'electronic-mail bomb.' First the attacker would break into the system of a company, an Internet service provider, that manages the links between the Exchange and the Internet. The attacker would tinker with the service provider's computers so that they routed millions of E-mail messages—which the attacker would generate from his own computer, to the Exchange. If the flood of false E-mail is large enough, the Exchange's Internet connection—and possibly its own computer—would become overloaded and shut itself down . . . .

Id.

Another alternative is a distributed denial of service attack of the type described earlier in the text, above. Instead of routing e-mail messages, the attacker(s) would use hundreds or thousands of zombie computers to bombard the NYSE computers with packets, overwhelming them and ultimately shutting down their ability to interact with the outside world. Similar attacks have occurred, although on a lesser-scale. *See, e.g.*, Steve Macko, *The Cyber Terrorists,* EMERGENCYNET NEWS SERVICE, June 4, 1996 (describing a computer crash that halted trading at a British brokerage firm and the payment of extortion by three other firms that were threatened with similar crashes), *at* http://www.emergency.com/cybrterr.htm. In March of 2000, the New York Electronic Crimes Task Force investigated a denial of service attack directed at a "prominent provider of electronic trading services on Wall Street." Testimony of Robert N. Weaver, *supra* note 51. Between March 9 and March 14, 2000, the company

> received several Internet-based 'denial of service' attacks on its servers. A "denial of service" attack occurs when a perpetrator launches malicious programs, information, codes, or commands to a target or victim computer which causes a degradation of service or shutdown, thereby denying access by legitimate customers to those computers . . . .
>
> While the attacks were still occurring, the company's CEO contacted the New York Electronic Crimes Task Force. The CEO identified a former employee as a suspect, based upon the fact that the attacks preyed on vulnerabilities which would only be known to the former employee. These attacks continued through March 13, 2000, when E. . . agents and task force members identified the attacking computer and arrested the former employee for violating Title 18, USC, Section 1030 (Computer Fraud). In a post-arrest statement, the suspect admitted that he was responsible for the denial of service attacks. As a result of the attacks, the company and its customers lost access to trading systems. Approximately $3.5 million was identified in lost trading fees, commissions, and liability as a result of the customers' inability to conduct any trading.

Id.

125. The Emulex incident was not, of course, the only time this was done, and discovered. In August of 2000, "a hacker broke into a paintball company's Web site and sent out phony financial statements Thursday, forcing the Nasdaq stock market to halt trading in the company's shares for more than two hours." Steve James, *Hacker Cracks Site, Forces Trade Halt,* Yahoo! News, *at* http://www.intellnet.org/news/2001/08/24/6363-1.html (Aug. 23, 2000). And as one commentator noted, the semantic attack against Yahoo! described earlier in the text, above, could have been used to manipulate stock prices:

> SecurityFocus, a security intelligence company, alerted Yahoo . . . that a hacker had easily entered its news pages and inserted phony quotes and wrong information . . . . The hacker said he wanted to show Yahoo that it needed to fix a basic mistake in its network setup. He exploited a flaw that let its corporate network be tricked into thinking it was communicating with an internal computer. He also said he believed other parts of Yahoo's site and other Internet content providers are vulnerable in similar ways, with video archives and stock prices subject to being manipulated.

Arthur Iger, *Commentary*, C|Net.com *at* http://news.cnet.com/investor/brokeragecenter/newsitem-broker/0-9910-1082-7307783-0.html (Sept. 26, 2001),

plant. A terrorist group can mount a semantic attack against a series of nuclear plants, convincing each to shut down because of fabricated seismic activity. [126] This, in turn, can have a notably deleterious effect on power grids, especially in certain states.

Semantic attacks can also be mounted against computers that control water supplies, causing a diminution in or even cessation of the supply. They can be used to degrade or destroy data in essential systems.[127] Semantic attacks can be directed at air traffic control systems. The terrorist attacker can flood the system with fabricated information about the locations and flight paths of non-existent planes.[128] While this might not achieve the Y2K doomsday scenario in which planes fall from the sky, it can cause havoc, namely the crash or collision of some planes, along with a major loss of confidence by the already rattled air-transport-consuming public.

These are only a few examples of semantic attacks. Semantic attacks can no doubt be mounted with a great deal of success for a time, at least, because we are so conditioned to assume the accuracy of the information our computers generate and display. We forget that, unlike the content of the printed page, the content of computer files and Web pages is impermanent and subject to alteration.

D. Blended Attacks

Terrorists can mount complex attacks by combining syntactic and semantic attacks.[129] Imagine that terrorists target Boston, Atlanta, Miami, Chicago, Houston and Los Angeles for an attack which begins with a syntactic assault on computer systems that stops the delivery of state public assistance.[130] General public awareness of the attack will emerge gradually, as successive waves of frustrated welfare recipients file complaints with the appropriate agencies. Eventually, the realization will spread that the distribution of benefits had been deliberately shut down. Once it becomes clear that the funds are not coming, the terrorists can follow up with a semantic attack assigning responsibility for their efforts to carefully-selected right-wing groups whose views are known to carry at least the taint of racial bias. If the terrorists manage to sustain the welfare gridlock, the freezing of the resources upon which thousands

---

126. *See* Libicki, *supra* note 78.

127. *See, e.g.*, Scott Berinato, *The Truth About Cyberterrorism*, CIO MAG., Mar. 15, 2002, *available at* http://www.cio.com/archive/031502/truth.html.

> Parasites—tiny computer programs that live in databases and slowly corrupt the data and its backups—could wreck a crucial database like Social Security. Or a hacker could penetrate a pharmacy chain's network or hospital database, causing fatal medical errors when a patient takes a prescription drug.

Id.

128. For some different scenarios, *see id.* ("If you want to raise hell on airlines, you hack the reservation system . . . . If you want to cyberterrorize airlines, you hack the weights and measures computers that control planes' fuel and payload measurements.")

depend for their survival will produce civil disobedience and localized chaos. National Guardsmen might have to be sent into these cities to maintain order. To make things even more interesting, the terrorists can then direct a syntactic attack at ATM and banking system computers in these cities.[131] Such a shutdown will add to the problem by causing outrage among citizens who do not depend on welfare funds. The cumulative effects of all these efforts will be riots, targeted violence and a National Guard stretched to its limit (which will create an excellent opportunity for the terrorists to stage a CBERN attack in other areas of the country).

Or imagine that it is a heavy travel day, a few days before Christmas. At a selected hub airport – LaGuardia, O'Hare, Atlanta, Los Angeles, Dulles, Denver and Dallas – non-lethal explosions occur in

---

129. Squitieri, *supra* note 96("Officials are most concerned that a cyberattack could be coupled with a conventional terrorist attack, such as those on Sept. 11, and hinder rescue efforts").

130. In states that still issue welfare checks and food stamps, the attack can target the computers that issue the checks and stamps, causing the benefits not to issue. States are moving away from the use of paper checks and food stamps because Federal legislation requires that they implement the electronic delivery of food stamps by October 1, 2002. 7 U.S.C. § 2016(i)(1) (2000). *See also* California Food Policy Advocates, *What Is EBT (Electronic Benefits Transfer) and How Does It Work?*, *at* http://www.cfpa.net/foodstamps/EBT/ebt.htm (last visited Nov. 7, 2002).

> As part of federal welfare reform laws enacted in 1996, Congress required all states to change the way they distribute food stamp benefits. Instead of giving recipients food stamp coupons, all states are required . . . to switch over to an Electronic Benefits Transfer (EBT) system . . . . Essentially, food stamp recipients will use an electronic debit card system instead of paper coupons to purchase food.

Id. See also U.S. Dept. of Agriculture, *FAQ About Electronic Benefits Transfer*, *at* http://www.fns.usda.gov/fsp/ebt/FAQ.HTM (last visited Nov. 7, 2002); Consumers Union, *Electronic Benefit Transfer*, *at* http://www.consumersunion.org/finance/ebtwc401.htm (last modified Mar. 6, 2001). As of October 2000, forty states were using electronic means to distribute food stamps, and most had also shifted to the electronic distribution of cash benefits as well. *Id.* This reliance on electronic transfers makes public assistance systems much more vulnerable to a syntactic attack. *Id.*

States are relying on private corporations to implement the new electronic benefit transfer systems. *See, e.g., Coming Soon To Your Neighborhood: Electronic Benefit Transfer*, Center for Community Change, *at* http://www.communitychange.org/organizing/ebt7.htm (Mar. 1998). This creates an added layer of vulnerability because the issuance of benefits will be in the hands of private parties. While there have as yet been no cyberterrorist attacks on these systems, innocent computer glitches have already delayed the delivery of benefits. *Id.*; *see Glitch Limits Use of Food Stamps*, COLUMBIA DAILY TRIBUNE, Aug. 19, 2001, *available at* http://archive.showmenews.com/2001/Aug/20010819News016.asp. *See also Public Health Must Get Agupa Computer System Operational,* GaumPdn.com, *at* http://www.guampdn.com/news/stories/20001207/opinion/91997.html (Dec. 7, 2000).

> Problems with the Agupa computer system at the Department of Public Health and Social Services means a dismal Christmas for many families that receive public assistance.
>
> Hundreds of people didn't receive welfare checks or food stamps for December because of a system crash two weeks ago. These people are suffering because public health failed to fix long-standing glitches with the problem-plagued system. The agency's lack of action means Guam's less fortunate are worse off than ever, and at the worst possible time of the year.

Id. See also Y2K Problem Delays State Benefits, THE OREGONIAN, Jan. 8, 2000 ("Roughly 10,000 Oregonians who receive child-support payments, food stamps and welfare payments will see a one-day delay in checks and deposits from the state because of a Y2K computer glitch. The delay also will affect as many as 1,400 child-care providers."), *available at* http://www.oregonlive.com/news/00/01/st010802.html.

131. *See, e.g.*, Juliana Liu, *Cambridge Students Find Way to Hack Into Banks,* TechTV, *at* http://www.techtv.com/news/hackingandsecurity/story/0,24195,3359565,00.html (Nov. 9, 2001).

checked baggage, each exploding before the planes take off. An immediate syntactic attack on airport communication systems follows, freezing security and check-in controls. Next comes the release of a flash worm designed to destroy data. The flash worm erases all files in the airport computer systems, thereby immobilizing the recovery of travel information and aborting all travel activity involving these airports. The terrorists then launch a semantic attack, taking credit for the attack and blaming their actions on "the treachery and hypocrisy of American authorities even as to their own people." The terrorists can say they used non-lethal bombs to demonstrate vulnerabilities that still exist in the air security system; vulnerabilities they attribute to the authorities' persistent, callous disregard of citizen safety. They accuse U.S. authorities of concealing prior, successful acts of airline terrorism – including the destruction of TWA flight 800.[132] The American public is outraged by the disruption of their holiday travel and the destruction of their confidence in the air travel system. They are also infuriated by the notion that their leaders had been deceiving them. The media—furious and embarrassed about the possibility that they have been government dupes—joins in, attacking political officials and career bureaucrats. All this produces a political firestorm and extreme volatility in the stock market; the government is besieged and the economy is reeling.

A syntactic-semantic attack scenario can be more nuanced. One such scenario begins with systematic, targeted hacks into governmental and news agency databases to retrieve information about personal and professional "dirty deeds" and "bad acts" attributable to top administration officials and their families.[133] The data is then used in a semantic attack: the terrorists assemble the information into a series of stories and aggressively distribute the ones with the least plausible deniability to domestic and foreign media sources. They do not lay claim to being the source of the stories but attribute them to a millennial Deep Throat.[134] The result would be political, social and media chaos. The

132. On July 17, 1996, TWA flight 800 "plunged into the ocean off Long Island en route from New York's JFK airport to Paris, killing all 230 passengers and crew." REEVE, *supra* note 28, at 238-39. For a persuasive argument that the flight was brought down by a terrorist bomb, *see* BODANSKY, *supra* note 1, at 178-89. *See also TWA Flight 800 Disaster: Cover-up?*, *at* http://www.all-natural.com/twa800.html (excerpting JAMES SANDERS, THE DOWNING OF TWA FLIGHT 800 (1997). *TWA Flight 800*, Serendipity, *at* http://serendipity.magnet.ch/more/twa800.html (last modified Sept. 30, 2002).

133. *See, e.g.*, Skeleton Closet: All the Dirt on the Candidates, *at* http://www.realchange.org (last visited Nov. 7, 2002).

134. *See generally* Stephen T. Hosmer, *The Information Revolution and Psychological Effects, in* ZALMAY KHALILZAD ET AL., STRATEGIC APPRAISAL: THE CHANGING ROLE OF INFORMATION IN WARFARE 217-251 (1999), *available at* http://www.rand.org/publications/MR/MR1016/MR1016.chap8.pdf.

> The Internet is potentially a potent tool for inflammatory rumor, as well as 'black' and 'gray' propaganda, in that the actual affiliation of the provider of information can be masked easily and any visual 'news' materials that are put on the Web can be transformed so as to make faked events appear true.

Id. at 244.

U.S. administration would be consumed by the need to deal with brushfires emanating from the stories; the Clinton-Lewinsky furor would pale in comparison. The national identity and the nation's credibility on the international scene would be severely wounded. Finance, diplomacy and international trade would all be affected.

E. Cyberspace as Support Mechanism

Cyberterrorism scenarios are not limited to syntactic and/or semantic attacks. Other possibilities exist, including using cyber-techniques to fund or support conventional terrorist activities.

It seems clear that Al-Qa'ida, including Mohammed Atta and the other organizers of the 9/11 attacks, used computer technology, such as e-mail, to communicate with each other.[135] There is speculation that they used steganography to send hidden messages to each other.[136] Some evidence shows that other Islamic terrorists used steganography, so this is quite possible.[137] Ramzi Yousef, architect of the 1993 World Trade Center bombing, used a laptop and encrypted his files.[138] More recently, other terrorist groups are using encryption to send undecipherable messages to each other.[139] Terrorists, acting alone or in conjunction with

135. Johnson, *supra* note 34; Puzzanghera, *supra* note 34. *See also Bin Laden Uses Net to Plot Moves,* ZDNet UK, *at* http://news.zdnet.co.uk/story/0,,t269-s2070488,00.html (Jan. 15, 1999) (the "terrorist network of Saudi exile Osama bin Laden is using floppy discs, satellite phone e-mail, and Internet messaging to plan its moves").

136. Daniel Sieberg, *Bin Laden Exploits Technology to Suit His Needs,* CNN.com, *at* http://www.cnn.com/2001/US/09/20/inv.terrorist.search/ (Sept. 21, 2001). Declan McCullagh, *Bin Laden: Steganography Master?,* WIRED NEWS, Feb. 7, 2001, *at* http://www.wired.com/news/politics/0,1283,41658,00.html. Steganography is hiding a secret message or secret data inside an ostensibly innocuous file, such as a photograph or graphic image. *See, e.g.,* Neil F. Johnson, *Steganography, at* http://www.jjtc.com/stegdoc/index2.html (last visited Nov. 13, 2002); *What is Steganography?, at* http://members.tripod.com/steganography/stego.html (last visited Nov. 13, 2002). The file containing the secret information can be sent via email or posted on a web site; the sender can use software, readily available for free on the Internet, to embed the secret information in the file to be sent and the recipient can use the same software to retrieve the embedded information. *Id.*

137. *See* Menon, *supra* note 34.

138. "[C]onvicted terrorist Ramzi Yousef, the mastermind of the [1993] World Trade Center bombing, stored detailed plans to destroy United States airliners on encrypted files on his laptop computer." *Carnivore Diagnostic Tool: Hearing Before the S. Comm. on the Judiciary,* 106th Cong. (Sept. 6, 2001) (statement of Donald M. Kerr, Assistant Director Laboratory Division, Federal Bureau of Investigation), *available at* http://www.fbi.gov/congress/congress00/kerr090600.htm. *See also* Tim Blair, *Online and Out of Reach,* TIME INT'L, Feb. 1, 1999, at 48, *available at* http://www.time.com/time/magazine/intl/article/0,9171,1107990201-20427,00.html; *Bin Laden Uses Net to Plot Moves,* ZDNet UK, *at* http://news.zdnet.co.uk/story/0,,t269-s2070488,00.html (Jan. 15, 1999) (on file with the University of Illinois Journal of Law, Technology & Policy).

139. *See, e.g.,* Sieberg, *supra* note 136 (testifying before Congress in 2000, former FBI Director Louis Freeh said "[u]ncrackable encryption is allowing terrorists—Hamas, Hezbollah, Al Qa'ida and others—to communicate about their criminal intentions without fear of outside intrusion, . . . thwarting the efforts of law enforcement to detect, prevent and investigate illegal activities").

organized crime, are using identity theft, credit card fraud and other cybercrime techniques to fund their terrorist activities.[140]

F. Combined Cyber/CBERN Attacks

Finally, computer technology could play a role in a CBERN-style attack, perhaps as one phase of a layered attack.141 The New York City subway scenario described above could, for example, be only the initial stage of such an attack. Once the subway trains were stalled, terrorists could release poison gas into the subway tunnels á la Aum Shinrikyo, causing deaths from the gas itself and from the ensuing panic of those trapped below. The effects of all this could, in turn, be further enhanced by a computer attack on the emergency telephone system (the 911 system)[142] and/or on the traffic signals that control New York vehicular traffic. As to the latter, the attack could turn all the traffic signals green or make them change rapidly and randomly, causing accidents as confused motorists simultaneously entered intersections from cross streets.[143] This, in turn, would cause gridlock within the city; no

---

140. *Cutting Off the Financial Lifeblood of the Terrorists before the House Committee on Financial Services*, 107th Cong. (Oct. 3, 2001) (statement of Dennis M. Lormel, Chief, Financial Crimes Section, Federal Bureau of Investigation) *available at* http://www.fbi.gov/congress/congress01/lormel100301.htm.

> [T]errorist cells often resort to... fraud schemes to fund their terrorist activities. Prevalent among these are credit card fraud, identity theft, insurance fraud and credit card bust-out schemes. The ease with which these individuals can obtain false identification or assume the identity of someone else, and then open bank accounts and obtain credit cards, make these attractive ways to generate funds. The growing use of the Internet and the relative anonymity it provides make it even easier to open bank accounts and obtain credit cards on-line using an alias.

Id.

141. *See, e.g.,* COUNTERING THE CHANGING THREAT, *supra* note 6, at § 1 ("terrorists are making extensive use of the new information technologies, and a conventional terrorist attack along with a coordinated cyber attack could exponentially compound the damage").

142. The most obvious type of attack would shut down the system. A more creative approach would be to take over the 911 system and use it to mount a semantic attack. Terrorists could, for example, take over the 911 dispatch system and use it to send most of New York City's available police personnel to the Bronx to deal with a fictitious event. This, of course, would leave other parts of the City unprotected and vulnerable to CBERN attacks. Or, the terrorists might send ambulances and fire trucks out on wild goose chases, ensuring that they would not be available to render aid where it was really needed. Finally, terrorists could use their control of the 911 system to list hospitals as being closed to the diversion of patients, even though they were not. This, again, would ensure that help would not be available to those in need.

143. On April 25, 2002, traffic in Santiago de Chile disintegrated into chaos after thieves stole computers and servers from the office that manages traffic flow in the city. *See, e.g.,* Ricardo Sametband, *Crooks Cause Chilean Car Chaos,* WIRED NEWS (Apr. 26, 2002), *at* http://www.wired.com/news/business/0,1367,52114,00.html.

> Without the computer system, the traffic lights continued working but at their own pace, losing all synchronization between one crossroad and the others. Five million citizens were in fear of crossing the streets, whether on foot or by car....
>
> Although police are re-routing vehicles around the city, traffic is far from becoming organized.
>
> Long queues of cars were observed all over Santiago, especially in the wealthy neighborhoods of the southern and western parts of the city, where most of the derelict traffic lights are installed.
>
> Patricio Tambolini, subsecretary of transportation, told the local media that drivers should not expect a normal green light until Monday, when things may be straightened out. About half of the

motorized traffic could move on the ground, and the subways would already be immobilized.[144]

IV. WHY HAS CYBERTERRORISM NOT YET MANIFESTED ITSELF?

This is concededly something of a mystery. There are no reliable answers as to why cyberterrorism remains an as-yet unrealized phenomenon.[145] In considering this issue, it is helpful to break potential cyberterrorists into two categories: foreign terrorists and domestic terrorists.[146] These groups represent the "external threat" and the "internal threat." Each is considered below.

---

800 derelict traffic lights were operational by Thursday evening, thanks to a backup version of the software that controls the lights, but no word on when the job will be completed . . . .

"We thought we had deployed all normal security measures," Tambolini said. "You never know if you've covered all security holes until this kind of thing happens." . . .

In an effort to lower the number of circulating cars and calm down bewildered drivers, the authorities are urging citizens to take public transportation and the subway, even when buses now take three times as long to complete their journey.

Id.

144. An attack could exploit disruption caused by a natural disaster. Federal and state officials developed such a scenario in 2000, as part of an exercise to help officials prepare for a possible terrorist attack during the 2002 Winter Olympics:

The Black Ice scenario takes place on February 14 . . . . A major ice storm topples power lines across seven counties and disrupts microwave communications in the Salt Lake City area. It also damages the high-voltage bulk transmission lines in several states, including transmission lines north and south of Salt Lake City.

The damage to the transmission system isn't extensive, but the ability to import electricity to the seven-county area is hindered significantly. The lack of power generation forces authorities to conduct rolling blackouts.

That's when the Supervisory Control Data Acquisition systems, which control the power grid, are further damaged by a cyber-attack. The source of the disruption is unknown . . . . Regardless, the failure begins to ripple throughout the rest of the regional infrastructure.

"Communications were one of the first things to go," says [Paul] Scalingi[, Director of the Department of Energy's Critical Infrastructure Protection Office]. " . . . [I]f you have a prolonged power outage that goes on for several hours, your infrastructure starts to degrade. Power backup only lasts so long."

And it's not just telecommunications. Water systems rely on electric power, as does the natural gas industry and the natural gas-powered electric utilities in the region. Emergency responders struggle through the chaos that results from Internet outages, cell phone overload and telephone failures . . . .

The ice storm could easily have been replaced with . . . bombs, hijackings or other physical catastrophes . . . Black Ice showed how interdependent are the various infrastructure systems—including telecommunications, utilities and banking—and how major might be the combined effects of cyber- and physical attacks . . . .

Dan Verton, *Utah's "Black Ice": Cyber-attack Scenario,* CNN.com, *at* http://www.cnn.com/2001/TECH/ptech/10/21/black.ice.idg/index.html (Oct. 21, 2001).

145. On November 29, 2001, hackers claiming to be "cyberterrorists" vandalized two web sites operated by agencies of the federal government. *See* Brian McWilliams, *"Mujihadeen" Hackers Take Out US Government Sites*, NEWSBYTES, Nov. 30, 2001, *at* http://www.infowar.com/hacker/01/hack_113001b_j.shtml. The vandalized sites were the NOAA Office of High Performance Computing and Communications' home page and a web server operated by the National Institute of Health's National Human Genome Research Institute. *Id. See also* http://defaced.alldas.de/mirror/2001/11/29/hpcc.fsl.noaa.gov/ (mirror of the defaced NOAA site) (on file with the University of Illinois Journal of Law, Technology & Policy) and http://defaced.alldas.de/mirror/2001/11/30/snoop.nhgri.nih.gov/ (mirror of the defaced NIH site) (on file with the University of Illinois Journal of Law, Technology & Policy). Both defaced sites displayed the flag of Saudi Arabia and a

A. Foreign Terrorists

"[A]nyone who could learn to fly a commercial airliner could probably acquire the expertise to penetrate one of our critical information systems."[147]

As to why there have not been cyber attacks by foreign terrorists,[148] one view — which had some credence at one time but is becoming increasingly dubious — is that terrorist groups lack the computer expertise to mount cyberterrorist attacks. This is the "there aren't

---

sentence in Urdu that translated as "Americans be prepared to die." *See* McWilliams, *supra;* http://defaced.alldas.de/mirror/2001/11/29/hpcc.fsl.noaa.gov/ (mirror of the defaced NOAA site) (on file with the University of Illinois Journal of Law, Technology & Policy); http://defaced.alldas.de/mirror/2001/11/30/snoop.nhgri.nih.gov/ (mirror of the defaced NIH site) (on file with the University of Illinois Journal of Law, Technology & Policy). The defaced NOAA site also included the message "IN THE NEXT DAYS YOU'LL LOOK THE GREATEST CYBERTERRORIST ATTACK AGAINST AMERICAN GOVERNMENT COMPUTER." *See* http://defaced.alldas.de/mirror/2001/11/29/hpcc.fsl.noaa.gov/ (mirror of the defaced NOAA site) (on file with the University of Illinois Journal of Law, Technology & Policy). The defaced NIH site had the message "WE ARE NOT HACKER, WE ARE JUST CYBERTERRORIST!" *See* http://defaced.alldas.de/mirror/2001/11/30/snoop.nhgri.nih.gov/ (mirror of the defaced NIH site) (on file with the University of Illinois Journal of Law, Technology & Policy).

These defacements do not qualify as cyberterrorism; they are simply taunting messages of a type common in "hacker wars." *See, e.g.,* Carmen J. Gentile, *Hacker War Rages in Holy Land,* WIRED NEWS (Nov. 8, 2000), *at* http://www.wired.com/news/politics/0,1283,40030,00.html. Unfortunately, they demonstrate that there are individuals out there who possess at least some ability to hack and have an interest in, if not an inclination toward, cyberterrorism.

146. For the purposes of this discussion, "foreign terrorism" means terrorist acts perpetrated by or at the behest of citizens of other countries. *See, e.g.,* 22 U.S.C. § 2656f(d)(1) (1987) ("'international terrorism' means terrorism involving citizens . . . of more than 1 country"). *See also* FEDERAL BUREAU OF INVESTIGATION, TERRORISM IN THE UNITED STATES: 1999 ii, *available at* http://www.fbi.gov/publications/terror/terror99.pdf [hereinafter TERRORISM IN THE UNITED STATES] . Foreign terrorism involves actions taken to promote ideologies that have their roots outside the United States of America and that are typically antithetical to the United States, its citizens, and the policies and philosophies it espouses. *See, e.g.,* Milan Milosevic, Ljubomir Stajic & Milan V. Petkovic, *Some Aspects of Contemporary Terrorism,* Federation of American Scientists (1998), http://www.fas.org/irp/world/serbia/docs/aspekti_e.html ("transnational terrorism has foreign elements and constitutes an action taken basically by autonomous non-State subjects, regardless of the fact whether they enjoy . . . moral or material support of benevolent governments . . . ."). *See also* TERRORISM IN THE UNITED STATES, *supra. See generally supra* note 8. *See also* WALTER LAQUER, TERRORISM 3-20 (1977). The September 11th attacks and the 1993 bombing of the World Trade Center are examples of foreign terrorism perpetrated on United States soil.

"Domestic terrorism" refers to terrorist acts perpetrated by citizens of the United States who are pursuing, for lack of a better term, "homegrown" ideologies. *See, e.g.,* TERRORISM IN THE UNITED STATES, *supra* note 146.

> Domestic terrorism is the unlawful use, or threatened use, of force or violence by a group or individual based and operating entirely within the United States or its territories without foreign direction committed against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

Id. See also ADL, *Extremism in America,* Introduction, *available at* http://www.adl.org/learn/ext_us/default.asp (hereinafter ADL); Steven Mack Presley, *The Rise of Domestic Terrorism and Its Relation to United States Armed Forces,* Federation of American Scientists, *available at* http://www.fas.org/irp/eprint/presley.htm#N_8. The 1995 bombing of the Oklahoma City federal building is the pre-eminent example of domestic terrorism. *See, e.g.,* ADL, *supra.*

147. Mike Toner, *Cyberterrorism Danger Lurking,* ATLANTA J. AND CONSTITUTION, Nov. 4, 2001, *available at* http://enterprisesecurity.symantec.com/content.cfm?articleid=932 (quoting Professor Seymour Goodman).

148. For the definition of "foreign terrorists" used in this discussion, *see supra* note 146.

enough good terrorist hackers" theory, and there is a certain comfort in subscribing to this view. It allows us to find refuge in the premise that hackers (good ones, anyway) are found only in the technologically sophisticated, technologically superior countries which are for the most part Western (at least in orientation) and therefore are not havens for terrorist groups. The corollary of this premise is, of course, that terrorists are from non-Western, non-technologically superior countries and therefore cannot and do not possess the technical savvy to mount a decent syntactic or semantic attack.

Unfortunately, there are two problems with this view. The first problem is that it ignores the level of technological sophistication one finds in countries in which terrorists operate. Afghanistan may not be such a country, but Pakistan is. Pakistan, home to terrorist training camps that supplied bin Laden with many of his operatives,[149] has already produced such adept hacker groups as G-Force Pakistan and the Pakistan Hackers Club.[150] These Pakistani hackers mount sophisticated attacks on websites they regard as hostile or otherwise intolerable.[151] There is also a high degree of computer expertise in many of the Arab countries,[152] in the Philippines (where Al-Qa'ida associates operate),[153] and in other parts of the Asian and Latin American world.[154] Indeed, the Internet Black Tigers, a special unit of the Sri Lankan Liberation Tigers

149. *See, e.g.*, BODANSKY, *supra* note 1, at 49-51, 94-95; Michael Elliott, *Hate Club: Al-Qaeda's Web of Terror*, TIME.COM (Nov. 12, 2001), *available at* http://www.time.com/time/world/article/0,8599,182746,00.html.

150. *See, e.g.*, Priya Ganapati, *War in Cyberspace*, Rediff.com, *at* http://www.rediff.com/news/2001/jul/10spec.htm (July 10, 2001).

151. *See, e.g., Our New Warriors: A Look at Organized Hackers in Pakistan*, NetXpress, *at* http://www.netxpress.com.pk/archives/articles/cwfb1.shtml (last visited Sept. 25, 2002).

> Since partition in 1947 Pakistan and India have faced three wars and numerous gun battles along their borders .... [A]nother war has erupted between these two, third-world nations; this time it does not involve armies or blood shed. The war in question is not being fought in the mountains of Kashmir, the skies of Punjab, the deserts of Sindh, or along the Coasts of Karachi. This war in being fought in cyberspace and involves civilians who fighting to prove their edge and domination in the field of information technology.

Id. See also Ganapati, *supra* note 150.

152. Kemel Daoudi, for example, has been described as the "computer-and-communications whiz kid" for an Al-Qa'ida group headed by Djamel Beghal, who played "a prominent role" in Al-Qa'ida's European operations. Elliott, *supra* note 149. Daoudi dropped out of a university in Paris, where he was studying computer science, to join the group. *See id.*

153. The Love Bug virus, of course, came from the Phillippines, and Al-Qa'ida has long had strong ties there. *See, e.g.*, Grossman, *supra* note 84. *See also* Elliott, *supra* note 149.

> It was from Manila that Ramzi Yousef, the convicted mastermind behind the first World Trade Center bombing, hatched a plan to blow up 12 American airliners as they flew over the Pacific. In the mid-1990s, Mohammed Jamal Khalifa, married to one of bin Laden's sisters, allegedly funded Islamic schools in the south of the country, where Muslim insurgents have been fighting for years. The Filipino government has long claimed that Abu Sayyaf, the most bloodthirsty of the groups—its specialty is beheadings—has been supported by Al-Qa'ida.

Id.

154. *See, e.g., Hactivism: Civil Disobedience, Cyberterrorism or Silly Posturing*, VIGILANTe.com, *at* http://www.vigilante.com/inetsecurity/hacktivism_1.htm (listing web site defacements, denial of service attacks, and other online protests carried out by hackers from various countries) (last visited Oct. 21, 2002).

of Tamil Eelam, are credited with carrying out what seems to be the first clearly identified cyberterrorism campaign.[155] And, by 1996, Osama bin Laden had equipped his headquarters in the mountains of Afghanistan with computers and access to the Internet.[156] It may well be that there has been no concerted effort to recruit individuals from this pool and turn them toward envisioning, and then realizing, cyberterrorist attacks. It may also be that this recruitment process is underway, or has been underway for some time. If so, we may see the results in the not-too-distant future.[157] What is certain is that it would be foolish to underestimate the talent that exists and that can be recruited to this end.[158]

---

155. *See, e.g., Sri Lanka: Assessment 2000,* South Asia Terrorism Portal - Institute for Conflict Management, *available at* http://www.satp.org/srilanka/Assessment_Sri%20Lanka2000.htm ("The Internet Black Tigers was constituted as an elite arm of the LTTE to specialise in 'e-mail bombings' and carries out an e-mail campaign against Sri Lankan missions around the world"). *See also* Testimony of Denning, *supra* note 77.

> In 1998, ethnic 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.

Id.

156. *See, e.g.,* John Arquilla, David Ronfeldt & Michele Zanini, *Networks, Netwar, and Information-Age Terrorism, in* COUNTERING THE NEW TERRORISM 65 (Ian Lesser, et al., eds., 1999), *available at* http://www.rand.org/publications/MR/MR989/MR989.chap3.pdf.

> Arab Afghans . . . have widely adopted information technology. According to reporters who visited bin Laden's headquarters in a remote mountainous area of Afghanistan, the terrorist financier has computers, communications equipment, and a large number of disks for data storage. Egyptian 'Afghan' computer experts are said to have helped devise a communication network that relies on the World Wide Web, e-mail, and electronic bulletin boards so that the extremists can exchange information without running a major risk of being intercepted by counterterrorism officials.

Id.

See also BODANSKY, *supra* note 1, at 198.

157. *See, e.g.,* Freeh, *supra* note 2.

> Terrorist groups are increasingly using new information technology and the Internet to formulate plans, recruit members, communicate between cells and members, raise funds, and spread propaganda . . . . While these terrorist groups have not employed cyber-tools as a weapon . . . against critical infrastructures, the reliance, accessibility, and expertise of these groups with computer and information technology networks and systems represents a clear warning sign.

158. A recent article suggests the talent is evolving rapidly. *See Computer Lessons For Terrorists,* NEWSWEEK, May 20, 2002, at 4.

> Al Qai'da terrorists interested in computer hacking are just clicks away from a crash course in digital sabotage. A Web site operated by the Muslim Hackers Club offers tutorials in cybermischief: viruses, hacking strategems, network 'phreaking' and secret codes. It also features links to militant Islamic and cyberprankster sites, including U.S. sites that purport to disclose sensitive information like 'code names' and radio frequencies used by the Secret Service.
>
> Bush officials worry that Islamic hackers will . . . graduate from pranks and vandalism to cyberterrorism . . . . Earlier this month the FBI and Defense Intelligence Agency issued a secret warning that the Muslim Hackers Club included experts who had conducted classes on how to mount terror attacks on computer networks. The FBI and the DIA believe the main objective of the club is to develop software tools which can then be used by other Islamic groups to attack Western targets. Some U.S. officials think a serious cyberattack by Islamic militants is inevitable.

See also Evan Kohlmann, *A Web of Terror,* J. OF COUNTERTERRORISM, Spring 2000, *available at* http://law.upenn.edu/~ekohlman/webterror.pdf.

> On March 17, 1997, a British Muslim named Muhammed Sohail posted an advertisement for a group known as 'the Muslim Hackers Club' on an Islamic Internet newsgroup. In the message, Sohail urged religious Muslims with computer skills to improve 'their own expertise/capability -

The other problem with this view is that it ignores the very real possibility that a terrorist group could recruit "hacker mercenaries" who possess the requisite expertise and who are quite willing to implement cyberterrorism attacks for pay.[159] Anecdotal and other evidence indicates that hackers are already offering their services for hire.[160] Since 9/11 attacks, there has been a great deal of concern about the possibility that Al-Qa'ida has recruited nuclear scientists from Pakistan.[161] There has, however, been little, if any, publicly-expressed concern that terrorists might have or might soon recruit Russian or other hackers to implement a cyberterrorist attack strategy.[162] This, however, seems as viable a

---

they may be needed in information warfare (IW) - protect your own side and infect the other side.' Also included were e-mail addresses of contacts for the Muslim Hackers Club and a link to their [Web site] . . . . [T]he site included extensive information on how to make destructive computer viruses, instructions on how to hack into sensitive Pentagon and U.S. Defense Department computer systems, and copies of the Anarchists Cookbook . . . .

Kohlmann quotes Sohail as saying that he works "for two people," one of whom is Osama bin Laden. *See id. See, e.g.,* Muslim Hackers Club, *Why A Muslim Hackers Club?*, *at* http://www.ummah.net/mhc/index.html.

The very first known virus the Pakistani 'Brain' was developed by two brothers from Lahore . . . . So why not a platform for the Muslims to discuss hacking, virus making, etc.? We hope we can somehow help each other by freely debating and learning - insha-Allah!

There are many who believe that hackers, crackers, phreakers and pirates . . . . This isn't all [sic] all true! There's a lot of difference. . . A hacker does not destroy a syste[m] that he/she has hacked . . . . A hacker's aim is just to seek knowledge.

Seeking knowledge may not be destructive. We don't advocate . . . infiltrating or infecting an innocent party's computer systems with a malicious intent designed to destroy valuable data or bring their system to a halt . . . . Be responsible and use the knowledge you may obtain here for your own education. *The programs and information provided on this site can be dangerous if you do not use them properly. They can be a lethal weapon.*

Id.

159. *See, e.g.,* Michael C. Sirak, *Threats to the Net,* AIR FORCE MAG. ONLINE (Oct. 2001), *at* http://www.afa.org/magazine/Oct2001/1001network.html (hacker groups could market themselves as mercenaries hiring out to terrorist groups).

160. *See, e.g.,* Dennis Blank, *Hacker Hit Men for Hire,* BUSINESSWEEK ONLINE (May 3, 2001), *at* http://www.businessweek.com/bwdaily/dnflash/may2001/nf2001053_930.htm.

For a mere $249, the Russian Hacker Assn. promises to destroy your 'Web enemy.' According to its Internet ad, the RHA will configure a robot e-mailer that can bombard your target with tens of thousands of e-mails in a single day, gumming up computer networks and interrupting normal business operations.

This ad is only the latest example of a new threat coming out of cyberspace—the hacker mercenary. It's a tempting proposition for young adults in countries where wages are low, opportunities limited, and computer literacy is high—places like Russia, China, and India. 'These guys are all over the Net with advertising,' says Bill Spernow, a security analyst for technology consultancy Gartner Group . . . .

[T]he party paying for the attack could remain anonymous, meaning that not even the marauding hackers would know who was footing their bill. Even more troubling, contract hackers could find sanctuary in countries where authorities lack the legal teeth, or the inclination, to prosecute.

Id. See also Joshua Dean, *Systems Failure,* GovExec.com, http://www.govexec.com/features/0202/0202s2.htm (Feb. 2, 2002) (freelance hackers "and cyber mercenaries . . . are reputed to be up for hire.")

161. *See, e.g.,* Preston Mendenhall & Robert Windrem, *Pakistan Holds Two Amid U.S. Fears of Nuclear Terrorism,* MSNBC.com, *at* http://www.msnbc.com/news/652309.asp (Nov. 1, 2001).

162. *See, e.g.,* Andrew Rathmell, *Cyberwar: The Coming Threat?*, Infowar.com, *at* http://www.infowar.com/mil_c4i/icsa/icsa2.html-ssi (July, 1997).

Hackers can be divided . . . into . . . amateurs and professionals . . . . [T]he real threat are the professionals, or cyber-mercenaries. This term refers to highly skilled and trained products of government agencies or corporate intelligence branches working on the open market. The Colombian drug cartels hired cyber-mercenaries to install and run a sophisticated secure

possibility as the prospect that Al-Qa'ida recruited Pakistani nuclear scientists.[163]

As to why terrorist groups and especially the very well-funded and sophisticated Al-Qa'ida group[164] have not so far employed cyberspace as a terrorism delivery agent, the answer may simply be that they have so far been concentrating exclusively on physical world delivery methods. One reason why this might be true is that — the 9/11 attacks notwithstanding — many of the terrorist attacks consummated to date have been mounted in parts of the world where a cyberattack would be, if not an exercise in futility, far less effective than an attack with conventional explosives. This is true of the extraterritorial attacks directed at American targets, the Khobar Towers bombing and the 1998 bombing of the U.S. embassies in Kenya and Tanzania, for example.[165] A cyberattack directed at any of these targets would have been little more than a nuisance. This is also true of the many attacks directed at non-American targets, such as the 1997 bombings in India, the bombings attributed to the Basque Homeland and Freedom group and to the Irish

---

communications system while Amsterdam-based gangs used professional hackers to monitor and disrupt the communications and information systems of police surveillance teams.

While amateur hackers have little reason to move around, the professionals can be very mobile. Hence links with foreign organised crime groups are of great interest. The Russian and Eastern bloc governments produced numerous trained hackers . . . .

Id. See also Hackers For Hire, IT-Director.com, *at* http://www.it-director.com/article.php?id=1793 (May 4, 2001).

One . . . hazard is the ever-mushrooming market in 'hackers for hire' . . . . the IT equivalent of the Dogs of War, mercenaries with IT skills. Internet adverts for these are growing and the 'services' that they offer are wide ranging enough to cause every security manager to loose sleep . . . .

Almost every hacking tool known can be found . . . on the web making it increasingly easy for cyber criminals to arm themselves. Added to this is the growth in computer skills in several of the world's poorer countries . . . . There have been many instances where hacking and / or virus creation events can be tracked back to countries such as those in the former Soviet bloc, India and others in South East Asia . . . .

Id.

163. *See, e.g.*, Dorothy Denning, *Is Cyber Terror Next?*, SOCIAL SCIENCE RESEARCH COUNCIL, Nov. 2001, *available at* http://www.ssrc.org/sept11/essays/denning.htm [hereinafter New War].

[I]t is . . . important to look beyond the traditional terrorist groups and to the computer geeks who already possess considerable hacking skills . . . . [S]ome of these folks are aligning themselves with terrorists like bin Laden. While the vast majority of hackers may be disinclined towards violence, it would only take a few to turn cyber terrorism into reality.

Id.

164. Al-Qa'ida is known to have used sophisticated technology in Afghanistan, even after they retreated into mountain caves. *See, e.g.*, Niles Lathen, *Terror.net: Al Qaeda Used Web in High-Tech Caves*, N.Y. POST, Mar. 20, 2002, at 16.

The al Qaeda forces routed in a recent bloody battle were so well organized, they used the Internet and laptop computers to communicate as they dashed from cave to cave.

The ultrasophisticated communications system used by the terrorists was reported by U.S. forces after searches of the cave network abandoned during Operation Anaconda . . . .

[T]he Arab, Chechen and Uzbek forces holed up in the mountain fortresses above the Shah-e-Kot valley connected satellite phones to laptop computers in order to e-mail appeals for reinforcements as U.S. forces began their assault on March 2.

The terrorist fighters also used the Internet to communicate with each other as they moved from cave to cave.

Id.

165. *See, e.g.*, Lucy Walker, *How the US Became A Target*, BBC News, *at* http://news.bbc.co.uk/hi/english/world/americas/newsid_1338000/1338354.stm (May 29, 2001).

Republican Army, and other, similar episodes.[166] Cyberterrorism will not be widely used as long as the terrorists' goal is to inflict as much panic, death and destruction as possible in a circumscribed area and within a limited time frame.[167] It will cease to be true if and when terrorists shift their focus to attacks that are directed at systems — virtual or otherwise – and have the disruption or dismantling of those systems as their primary goal, while the infliction of panic, death, and destruction becomes a desirable but distinctly secondary goal.[168]

Another possible reason why terrorists have not yet moved into cyberterrorism is that the leaders of these groups may still be the products of a different, older world view – one in which the terrorism delivery methods one employs are the CBERN agents, not bits and bytes. If this is a factor, it is a factor that is likely to diminish in importance as terrorist leaders are drawn increasingly from younger recruits, individuals who are more likely to understand how cyberspace can be used to achieve their goals.[169]

---

166. For details on these and other terrorist bombings, *see, e.g.,* South Asia Terrorism Portal, http://www.satp.org/default.asp (last visited Oct. 19, 2002); Terror Attack Database, *supra* note 13. *See also* Bruce Hoffman, *Terrorism: Trends and Prospects*, *in* COUNTERING THE NEW TERRORISM 12-13 (Ian Lesser, et al., eds., 1999), *available at* http://www.rand.org/publications/MR/MR989/MR989.chap2.pdf.

167. Traditional attacks like these focus on achieving the terror moment, i.e., on the instant when the bomb explodes (or the chemical weapon is deployed or the biological agent is disseminated and begins to take effect) and all semblance of normal life is destroyed. A long-term strategy based on this type of attack relies on repeated, unpredictable events to demoralize the target population.

168. James Gilmore, Chairman of the National Advisory Panel To Assess Domestic Response Capabilities for Terrorism of Weapons of Mass Destruction, said in March of 2002 that cyberattacks "are the most likely next attacks" to be mounted by terrorists. *See* Richard W. Walker, *Gilmore Warns of Threat to Information Systems,* GOV'T COMP. NEWS (Mar. 27, 2002), *at* http://www.gcn.com/vol1_no1/daily-updates/18260-1.html.

169. An official with the FBI's National Infrastructure Protection Center recently warned that "'[t]he threat of cyberterrorism will grow in the new millennium, as the leadership positions in extremist organizations are increasingly filled with younger, Internet-savvy individuals'". *U.S. Official Warns of Future Attacks on Vital Computer Systems,* NANDO TIMES, Nov. 17, 2001, *available at* http://www.nando.net/technology/story/172635p-1669909c.html. Or, as an expert on terrorism said, "[w]hile bin Laden may have his finger on the trigger, ... his grandson might have his finger on the mouse." John Schwartz , *Cyberspace Seen as Potential Battleground*, N.Y. TIMES, Nov. 23, 2001, at B4, *available at* http://www.nytimes.com/2001/11/23/technology/23CYBE.html?todaysheadlines. *See also* New War, *supra* note 163.

> [T]he next generation of terrorists will grow up in a digital world, with ever more powerful and easy-to-use hacking tools at their disposal. They might see greater potential for cyber terrorism than do the terrorists of today, and their level of knowledge and skill relating to hacking will be greater. Cyber terrorism could also become more attractive as the real and virtual worlds become more closely coupled, with automobiles, appliances, and other devices attached to the Internet. Unless these systems are carefully secured, conducting an operation that physically harms someone may be as easy as penetrating a Web site is today.

Id.

In December, 2001, a "suspected member" of the Al-Qa'ida group claimed, during interrogation by Indian police, that "members of Osama bin Laden's [Al Qa'ida] network, posing as computer programmers, were able to gain employment at Microsoft and attempted to plant 'trojans, trapdoors, and bugs in Windows XP'". Brian McWilliams, *Suspect Claims Al Qaeda Hacked Microsoft-Expert,* NEWSBYTES, Dec. 17, 2001, *available at* http://www.infowar.com/hacker/01/hack_121801a_j.shtml. *See also* GOV'T OF CAN. – OFFICE OF CRITICAL INFRASTRUCTURE PROTECTION AND EMERGENCY

B. Domestic Terrorists[170]

[I]t will not be some foreign speaking terrorist group that's attacking, like Pearl Harbor. . . . This is going to be some kid, or some disaffected adult, some technological Unabomber, that will strike and that will cause more damage than we ever thought possible. [171]

While there has been speculation as to why we have yet to see cyberattacks by foreign terrorists, the possibility of domestic cyberterrorism has received little attention. This is surprising, since domestic extremists seem a likely source of cyberterrorism.[172]

Unlike foreign terrorists, domestic terrorists cannot be dismissed as "lacking in the technological sophistication needed to mount a cyberattack."[173] Because they are citizens or residents of the United States, it is reasonable to assume that the adherents of internal extremist groups have access to the skills and other resources needed to mount a cyberterrorist attack. Indeed, an FBI report pointed out that contemporary domestic extremists, like their foreign counterparts,[174] use computer technology "to exploit the communications potential of the Internet to disseminate propaganda, provide information updates to adherents, recruit new members, and make claims of responsibility for terrorist activities and acts of vandalism."[175] Former FBI Director Louis J. Freeh cautioned that while these groups have not yet used cyberspace as a weapon against critical infrastructures, their access to and familiarity

---

PREPAREDNESS, *Threat Analysis: Al-Qaida Cyber Capability*, *available at* http://www.epc-pcc.gc.ca/emergencies/other/TA01-001_E.html (Nov. 2, 2001).

170. For the definition of "domestic terrorists" used in this discussion, *see supra* note 146. For a review of the history of domestic terrorism in the United States, *see, e.g.*, TERRORISM IN THE UNITED STATES, *supra* note 146, at 28-32.

171. Bill Campbell, Mayor of Atlanta, Georgia, Remarks at Cyberterrorism: Response at the State and Local Level, Institute for Security Technology Studies, (transcript *at* http://iml.dartmouth.edu/ists/transcript.html).

172. The FBI, for one, sees domestic terrorism as a very real threat. *See, e.g.*, Freeh, *supra* note 2. *See also* TERRORISM IN THE UNITED STATES, *supra* note 146, at 32. "[R]ight-wing terrorists . . . continue to represent a formidable challenge to law enforcement agencies". *Id.* The FBI divides domestic terrorist groups into three categories: (1) right-wing extremist groups; (2) left-wing and Puerto Rican extremist groups; (3) and special interest extremists. Freeh, *supra*. For another categorization, *see* SOUTHERN POVERTY LAW CENTER, *Intelligence Project, at* http://www.splcenter.org/intelligenceproject/ip-index.html (listing of "hate groups" and "patriot groups") (last visited Sept. 8, 2002).

173. *See supra* § IV(A).

174. *See supra* § IV(A).

175. TERRORISM IN THE UNITED STATES, *supra* note 146. *See also* New Jersey Attorney General & Commission of Investigation, Computer Crime: a Joint Report 34 (June 2000), *available at* http://www.state.nj.us/sci/computer.pdf.

> Cyberspace permits hate mongers, bigots, racists . . ., Holocaust deniers, . . . anti-Semites and immigrant bashers to reach vast new audiences of potential adherents . . . .
>
> The Internet facilitates mass dissemination of slick propaganda via Web sites accessible to millions . . . . [I]t creates a 'virtual community' of like-minded believers. . .

Id. at 32-34.

with "computer and information technology networks and systems represents a clear warning sign"[176] that this is far more than a possibility.

It is important that the threat of domestic cyberterrorism not be overlooked as the nation concentrates on threats from abroad. Like their foreign counterparts, domestic terrorist groups have so far relied on conventional terrorism delivery methods. Timothy McVeigh, after all, used explosives rather than cyberspace, to wreak his vengeance for what he saw as "crimes" the federal government committed during the Waco siege.[177] It may be that the hypothesis advanced to explain why foreign terrorists have not yet turned to cyberspace also applies to domestic terrorists (i.e. that they have so far been focusing on the gross infliction of physical and property damage as the means for achieving their goals). This will most certainly change once domestic extremists realize the advantages cyberspace can offer with regard to achieving their ends.

V. CONCLUSION

> *So just why is cyber-terrorism such a threat? . . . . The Internet is the digital communications infrastructure. . . . It is the nervous system of the Information Age - just as the airlines are the physical communications infrastructure. . . . With a sufficiently evil perspective, the airlines became a terrorist weapon. The Internet is potentially another such terrorist weapon. You can't crash the Internet into a skyscraper - but you can use the Internet to 'crash' your cyber-terrorist weapon into the millions of PCs, laptops, and servers that connect to it.*[178]

This article is entitled "In Defense of Cyberterrorism" not because we wish to defend terrorism in any guise, but because we want to call attention to the fact that cyberterrorism is a real possibility, if not an imminent probability. In assessing the likelihood of a cyberterrorism event, it is necessary to consider both the threat level of the target and the sophistication of the perpetrator.

As to the former, some targets — which we refer to as "structural" targets – are clearly more attractive to terrorists and consequently are more likely to be attacked. The failure of these systems would have significant impact on society and would threaten human life. The Presidential Commission on Critical Infrastructure Protection recognized the information systems of certain organizations and sectors to be the

176. Freeh, *supra* note 2.

177. *See, e.g.*, Lori Leibovich, *One, Two, Many McVeighs,* SALON (June, 1997), *at* http://www.salon.com/june97/news/news2970610.html.

178. Mark Minasi, *Cyber-terrorism: Take Effective Action While you Still Can,* Previo, *at* http://www.previo.com/perspectives/white.asp.

most necessary to our continued survival.[179] These systems include those responsible for health care, telecommunications, power, financial systems, emergency government services, and national defense. A successful cyberattack against things like power grids, banking transactions, and air traffic control would have the exact type of high impact, high profile, high damage consequences terrorists seek in order to bring attention to their causes.[180]

Because it is likely that these systems will be targeted more frequently and that the damage resulting from a successful attack would have greater social consequences, "structural" targets are protected with resources superior to those guarding "enterprise" targets (i.e. information systems that handle private activities such as the sales of merchandise like books and Beanie Babies).[181] While the financial

---

179. *See* PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION, CRITICAL FOUNDATIONS: PROTECTING AMERICA'S INFRASTRUCTURES ch. 3 (Oct. 1997), *available at* http://www.ciao.gov/resource/pccip/part1.pdf [hereinafter CRITICAL FOUNDATIONS]. *See also Hearing on "Al Qaeda and the Global Reach of Terrorism" Before the House Comm. on Int'l Relations*, 107th Cong., 1st Sess. (Oct. 3, 2001), *available at* http://www.house.gov/international_relations/reve1003.htm (statement of Oliver "Buck" Revell)(hereinafter Revell).

> [T]he . . . threat has been associated with the telecommunications infrastructure and the ability to communicate . . . . But the government is also growing more and more dependent upon the commercial power, transportation, energy, and finance communities, and these communities are also vulnerable to attack. All of these major national infrastructures share a common dependency on computer driven management and control systems . . . .
>
> The continued globalization of the economy, information, and technology will provide significant new opportunities for those seeking to terrorize or intimidate. This is because the interdependencies created by such networking provide a broader base for greater destruction . . . . [O]ur own growing dependency on computer-driven systems in government, within industry, and throughout the Nation's infrastructures of oil and gas, finance, communications, power, and transportation . . . increases our vulnerability. The President's Commission on Infrastructure Protection . . . studied the vulnerabilities of our infrastructure, however it remains to be seen if our society can effectively organize itself to protect these key assets of our nation . . . .
>
> As the government becomes more and more dependent upon commercial-off-the-shelf information technologies, products, and networks, it will become more vulnerable to the infowar threat. This vulnerability will not be limited to potential IW attack on the operation of support infrastructures, but also will include potential 'time bomb' attack via pre-programmed imbedded software in operating systems, much, of which software is written abroad.

Id.

180. *See, e.g.*, Steve Konicki, *Cyberterrorism Czar: Stop Being Sloppy*, INFORMATIONWEEK.COM (Oct. 15, 2001), *at* http://www.informationweek.com/shared/printableArticle?doc_id=IWK20011012S0039:

> *InformationWeek*: What kind of companies are potential targets?
>
> Clarke: We don't have any specific intelligence that indicates a particular company or a particular type of company would be a target.
>
> That having been said, it is clear that the attacks on the World Trade Center were more than attacks on symbolic targets. They were going after our financial systems. They knew what was there. I believe their goal was actually to do more damage than they did. I think they might have thought that the towers would actually fall over sideways and collapse on the financial district.
>
> So I think we need to be aware that this enemy is not out merely to attack us symbolically, but actually to hurt us in ways that hurt our economy as well as our military capability.

Id. (interviewing Richard Clarke, Presidential Advisor on Cyberterrorism and Cybersecurity).

181. Some suggest, therefore, that the private sector is perhaps the most likely target for a cyberterrorism attack. *See, e.g.*, MacDonnell Ulsch, *Security Strategies for E-Companies*, INFO. SEC. (Nov. 2000), *at* http://www.infosecuritymag.com/articles/november00/columns_ec_does_it.shtml ("The U.S. business infrastructure is the nation's Achilles' heel, its soft underbelly").

consequences of a cyberterrorist attack on a company selling books over the Internet could be disastrous for the victim company and its investors, it is highly unlikely anyone will be killed or injured as the result of such an attack. The same cannot be said for successful attacks against the "structural" targets.

Another difference between the two types of targets is access to the various systems. "Enterprise" targets such as online bookstores need to be connected to the Internet to sell books, while the same is not true of "structural" targets. Much of the nation's critical infrastructure operates on private networks that are not directly connected to the Internet, a fact which in and of itself can provide some level of protection.[182] Of course, some "structural" targets, such as financial institutions that allow online banking, are connected to the Internet and they are indeed at risk.[183]

One factor both categories of target have in common is the threat from inside. Indeed, many who argue that the danger of cyberterrorism is exaggerated[184] fail to take the "insider threat" into account. Whatever difficulties a terrorist group might confront in launching a cyber-attack from abroad can be substantially overcome if the group recruits a local accomplice who is familiar with and has access to the system to be attacked. Al-Qa'ida is well known for using sleeper agents.[185] What if a

---

182. Indeed, one of the first measures Richard Clarke proposed after being appointed as President Bush's "Cybersecurity Advisor" was the creation of "GovNet," a protected, ultra-reliable network through which government agencies could share information. Michelle Delio, *GovNet: What Is It Good For?,* WIRED NEWS (Jan. 21, 2002), *at* http://www.wired.com/news/politics/0,1283,49858,00.html.

> Clarke's outline for GovNet called for a massive, completely private Intranet for government agencies and authorized users. The network would have voice and video capabilities; be completely protected from outages, hack attacks and viruses; and be able to carry highly classified data securely.

Id. at http://www.wired.com/news/politics/0,1283,49858-2,00.html.

183. *See, e.g.,* Cyber Security Research and Development Act, H.R. REP. NO. 107-355(I), *reprinted in* 2002 WL 172607 **2-3 (2002).

> The Internet . . . . was not . . . designed to control power systems, connect massive databases of medical records or connect millions of home appliances or automobiles, yet today it serves these functions. It was not designed to run critical safety systems but it now does that as well. We now heavily rely on an open network of networks, so complex that no one person, group or entity can describe it, model its behavior or predict its reaction to adverse events.
>
> The porous fabric of the U.S.'s network infrastructure leaves the Nation open to the constant possibility of cyber attack. Attacks can take several forms, including: defacement of web sites and other electronically stored information in the United States and other countries to spread disinformation and propaganda; distributed denial of service attacks that overwhelm a server with access requests; . . . distribution of destructive worms and viruses throughout the computer network; and unauthorized intrusions and sabotage of systems and networks belonging to the U.S. and allied countries, potentially resulting in critical infrastructure outages and corruption of vital data.

Id.

184. *See* Berinato, *supra* note 127.

185. *See, e.g.,* Dan Eggen & Michael Dobbs, *Danger Persists After Hobbling of Al-Qa'ida,* WASHINGTONPOST.COM (Jan. 14, 2002), *at* http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A40815-2002Jan13&notFound=true.

> Many of the terrorists who took part in the Sept. 11 and other attacks passed through training camps established by bin Laden in Afghanistan after his 1996 expulsion from Sudan. Pakistani intelligence officials estimate that about 20,000 people traveled through Pakistan over the last

member of Al-Qa'ida or an Al-Qa'ida supporter who grew up in some Midwestern city got a job as a programmer at the local power company? What forms of cyberterror could be unleashed from the inside?[186]

In assessing the likelihood of a cyberterrorism attack, it is also necessary to consider the sophistication of those who are likely to perpetrate such an event. As Richard Clarke, the President's Cybersecurity Advisor, said,

> [we] have a system that is fragile, that is vulnerable to sophisticated attacks ... [n]ot to 14-year-olds, but to a sophisticated group, or nation-state, with multiple simultaneous attacks. It could lead to catastrophic damage to the economy, and, if done at a time of national security crisis, it could lead to catastrophic damage to our national defense.[187]

---

decade en route to the camps, with roughly 5,000 completing all stages of training and swearing an oath of allegiance to bin Laden.

Officials fear that as many as half of those loyalists may be living in Middle Eastern, European, Asian and North American cities as sleeper agents, awaiting an opportunity to wage jihad, or holy war.

Id.

186. The scenario outlined above represents what is probably the most difficult type of insider attack because it requires that the terrorist group infiltrate one its own people into the permanent workforce of the targeted system. There are other ways in which a terrorist group can secure the assistance of a "traditional" insider. *See, e.g.,* CRITICAL FOUNDATIONS, *supra* note 179, at 15 ("[M]alefactors may make use of insiders, such as organized crime or a terrorist group suborning a *willing* insider (a disgruntled employee, for example) or making use of an *unwitting* insider (by getting someone authorized network access to insert a disk containing hidden code, for example.")

But this is far from being the only available scenario: Various developments—such as the "increasing trend towards the use of contract or temporary employees," the proliferation of virtual private networks (VPN's) and "trusted networks—can make it much easier to gain 'insider' access to a system". *See IP Security: Building Block for the Trusted Virtual Network,* Intel Internet Data Center White Papers, *at* http://www.intel.com/network/connectivity/resources/doc_library/white_papers/products/ipsecurity/NPD_Whitepaper.pdf/ (on file with the University of Illinois Journal of Law, Technology & Policy). *See also* National Communications System, *The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Internet Communications* (Dec. 2000), *available at* http://www.ncs.gov/ncs/Reports/electronic_intrusion_threat2000_final2.pdf.

The insider threat to NS/EP systems, the Internet, and networks in general is largely misunderstood and underestimated. "Although some security experts estimate that as much as 85 percent of all computer crimes are committed by insiders, media reports have focused primarily on external computer hackers and traditional threat actors." *Id.* at ES3. Furthermore, an insider is no longer simply an employee. "[W]ith the increase in remote access to systems, the insider can encompass employees, former employees, contractors, vendors, business partners, customers, and even competitors." *Id.*

See, e.g., Blank, *supra* note 160.

> [S]ome foreign companies looking to one-up their better-funded Western counterparts have taken surveillance into their own hands by hiring mercenary hackers inside the U.S. .... Alan Brill, who directs Internet-security operations for security firm Kroll Associates .... helped a Silicon Valley software outfit to fend off hacking attacks by a former employee who had been hired by a foreign competitor to access company computers and steal proprietary information. The company watched helplessly as the computer intruder outwitted security measures and continued to download highly secret files.

Id.

187. Shawna McAlearney, *Cyberspace Braces for Escalation and War,* SEC. WIRE (Nov. 29, 2001), *at* http://www.infosecuritymag.com/digest/2001/11-19-01.shtml.

Unfortunately, there are a number of potential candidates for the "sophisticated group" that would launch such an attack. They include a single terrorist organization,[188] a coalition of terrorist organizations, or a coalition combining terrorists with organized criminals.[189]

Because of the bin Laden assets, Al-Qa'ida is unusually well-funded and technologically sophisticated and is, therefore, the primary candidate for launching a single-group attack. Al-Qa'ida's primacy in this regard may also be a function of its organizational structure. A study found that groups like Al-Qa'ida, whose organization is highly decentralized and fluid, are more likely to use information technology, first for decision making and then to carry out their terrorist agenda.[190] There is also evidence that terrorist groups — including Al-Qa'ida — are working with drug traffickers and members of organized crime groups to generate funds that are used to pursue the terrorist agenda.[191] Collaborations such

188. One study divided terrorist groups into four categories—nationalist/ethnic, religious, political and "single issue"—and concluded that the groups falling into all four categories are likely to use cyberspace as a device for advancing their respective agendas. *See* Peter Fleming and Michael Stohl, *Myths and Realities of Cyberterrorism*, OFFICE OF INTERNATIONAL PROGRAMS AND THE CENTER FOR EDUCATION AND RESEARCH IN INFORMATION ASSURANCE AND SECURITY (Sept. 2000), *at* http://www.ippu.purdue.edu/global_studies/gghr/cyberterror6.cfm. The study found that religious and/or political terrorist groups were the most likely to use cyber-tactics to "escalate damage and casualties." *Id.*

For a slightly different categorization of potential attackers, *see* PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION, REPORT ON THREAT AND VULNERABILITY MODEL ON INFORMATION SECURITY 3 (1997), *available at* http://www.ciao.gov/PCCIP/ThreatVulnerabilityModel.pdf (identifying the following "adversaries": "insider," "information warrior," "national intelligence," "terrorist," "organized crime," "industrial espionage" and "hacker"). *See also id.* at Appendix A.

189. The groups identified above are only a sub-set of the possible perpetrators. One study identified thirty-seven possible sources of cyber-attacks. *See* Fred Cohen, *et al., A Preliminary Classification System for Information Threats, Attacks and Defenses: A Cause and Effect Model and Some Analysis Based on That Model* (Nov. 1998), *at* http://www.all.net/journal/ntb/cause-and-effect.html (on file with the University of Illinois Journal of Law, Technology & Policy).

190. *See* Networks in KHALILZAD, *supra* note 7, at 91-98. The authors of this study used the following hypotheses in analyzing Middle Eastern terrorist groups' capacity for cyberterrorism:

> The greater the degree of organizational networking in a terrorist group, the higher the likelihood that information technology is used to support the network's decision making. Recent advances in information technology facilitate networked terrorist organizations because information flows are becoming quicker, cheaper, more secure, and more versatile. As terrorist groups learn to use information technology for decision making and other organizational purposes, they will be likely to use the same technology as an offensive weapon to destroy or disrupt.

Id. at 97-98.

191. *See, e.g.*, Douglas Waller, *The Global Search for Osama bin Laden,* TIME.COM (Nov. 13, 2001), *at* http://www.time.com/time/columnist/waller/article/0,9565,184253,00.html.

> Intelligence agencies and military special operations commandos are increasingly concerned about a nest of terrorists, drug traffickers and assorted organized crime figures who've taken up residence in South America's tri-border area, where Brazil, Argentina and Paraguay meet . . . .
>
> For several years, the CIA has had a team of agents monitoring terrorists from Hezbollah, Hamas, and more recently, bin Laden's [Al-Qa'ida] organization who've poured into tri-border towns like Paraguay's Ciudad del Este to cut deals with Colombian drug traffickers and European and Asian Mafia lieutenants. Counter-terrorism officials believe bin Laden has set up cells to . . . finance operations against the U.S. through international crime syndicates.

Id. See also Hearing Before the Subcomm. on the Western Hemisphere of the House Comm. on International Relations, 107th Cong., 1st Sess. (Oct. 10, 2001), *available at* http://www.ciponline.org/colombia/101001.htm ("In the tri-border area of Argentina, Brazil and

as this could easily take an even darker turn, with terrorists and organized criminals combining forces to perpetrate a cyberterrorist attack.[192]

Paraguay, Middle East terrorist organizations such as Hamas and Hizballah . . . conduct fundraising activities in an area which has a growing population of Middle Eastern and South Asian immigrants. Funds raised in the tri-border area are sent directly to the Middle East to support the operation of these organizations, possibly even the planning and execution of terrorist acts.")

192. Revell, *supra* note 179.

> Whatever tools terrorists select, the fact of increasing cooperation between crime, narcotics and terrorist groups will provide terrorists with new, more creative ways to raise money and a marketplace to shop for weaponry and high tech equipment . . . .
>
> [T]here is growing evidence that drug cartels and other transnational groups—to include some terrorist groups—have recognized the potential for infowar and are developing capabilities. In fact, some groups, like the FARC, ELN, Provisional IRA, and the Sendero Luminoso, already target information infrastructures today for the purposes of collecting intelligence, targeting data, and monitoring of law enforcement and other government activities. In time, with the increasing availability of infowar attack information on the Internet and in other public media, transnational groups will establish some modicum of capability in this arena.

Id.