Chapter Five

The Cyberterrorism Threat

Gregory J. Rattray

The last decade of the 20th Century has seen the rising concern over a new form of conflict, usually referred to as information warfare. As the US and other nations race forward into an information age, reliance on advanced information systems and infrastructures has grown significantly. Cyberspace has become a new realm for the exchange of digital information to conduct commerce, provide entertainment, pursue education, and a wide range of other activities. Information systems, in particular computer software and hardware, now serve as both weapons and targets of warfare.[1] The possibility of warfare in cyberspace presents opportunity but also involves significant new security risks. As the world's leading military power and the society most reliant on its information systems and infrastructures, the US may well face adversaries searching to find new weaknesses. These adversaries may include terrorists.

Similar to political assassination and car bombs, cyberterrorism could provide a new set of weapons for the weak to challenge the strong. Rapid technological developments based on the Internet and other information infrastructures through the end of the 20th Century create an attractive environment for groups who can not directly confront the US government, yet are willing to use death, destruction and disruption to achieve their objectives. Increasingly, cyberterrorists can achieve effects in the US from nearly anywhere on the globe. Terrorist groups can access global information infrastructures owned and operated by the governments and corporations they want to target. Digital attackers have a wide variety of means to cause disruption and/or destruction. Response in kind by the US government against sophisticated attackers is near impossible due to the difficulty of pinpointing activity in cyberspace and legal strictures on tracing attackers.

The possibility of cyberterrorism receives much attention. The Director of Central Intelligence, George Tenet, cautions about "a growing cyberthreat, the threat from so-called weapons of mass disruption."[2] Noted terrorism expert Walter Laquer observes "… why assassinate a politician or indiscriminately kill people when an attack on electronic switching will produce far more dramatic and long-lasting results."[3] A RAND study on terrorism produced for the US Air Force outlines the possibilities of "cybotage—acts of disruption and destruction against information infrastructures."[4] Yet, so far the US has suffered very little from cyberterrorism despite continuing conflicts with numerous adversaries, including those who employ terrorist means. Improved understanding of cyberterrorism must address why it has yet to fully emerge as a prevalent terrorist strategy. US policymakers need to understand constraints on its conduct as well as possibilities for its use.

What do we know? Evidence exists that cyberterrorism can occur. Government and commercial web sites are defaced almost daily. Computer systems suffer disruptions from intentional e-mail overloads and eruptions of viruses. Hackers of many stripes continue to prove capable of intruding on and exploiting a wide range of computer networks. These incidents can cause significant disruption and financial costs. However, cyberattacks have so far proved at most a nuisance for the US and its national security.

Looking to the future, we can expect cyberterrorism to become a more significant national security concern. Many assert that the US must expect a growth in the number of adversaries willing to use terrorist means.[5] The effectiveness of digital attack means will increase. So will US vulnerabilities to cyberterrorism. Terrorist organizations that wish to use these means can be expected to become smarter about both technological tools and effective targeting strategies. Limits to hitting back against cyberterrorism will remain a difficult problem.

Yet, cyberterrorists too will face significant challenges. When terrorists will develop requisite capabilities to conduct significant cyberattacks remains highly uncertain. The calculus of how cyberterrorism fits in with other terrorist tools, including conventional weapons, weapons of mass disruption, and other techniques will determine the future significance of cyberterrorism. Cyberterrorism may well become a supplement to other terrorist means similar to how information warfare operations complement conventional military forces.

The US President, Congress and many others have clearly recognized concerns raised by cyberterrorism. The Federal government has initiated planning, assigning responsibility, and begun development of organizations to protect the US from cyberattack. However, these efforts are in early stages and must surmount considerable hurdles. The speculative hype combined with lack of real experience with this emerging phenomenon compounds the difficulty. A sound US policy to combat cyberterrorism and investment decisions must emerge from a balanced understanding of the potential threat and its limits.

Cyberterrorism—What Is It and Who Does It?

In general, terrorism proves a difficult topic to set boundaries around. One common approach to defining cyberterrorism is broad inclusiveness in addressing the actors, means and goals involved. My approach endeavors to delineate the threat in terms of factors relevant to evaluating US policy and organizational responses. Definitions and boundaries prove critical in establishing policy, defining organizational responsibilities and addressing resource allocation. So while arguably an artificial exercise, we will begin by answering two key questions—"What types of acts constitute cyberterrorism?" and "Who conducts cyberterrorism?"

This analysis of cyberterrorism centers on the activities of organized, non-state actors pursuing political or systematic objectives against the US[6] The activities of states conducting hostile activities in cyberspace against the US fall outside the realm of cyberterrorism into areas which can be labeled information warfare, espionage, or public diplomacy. However, we will consider the possibility that states may be associated with non-state actors in the furtherance of cyberterrorism. I also do not consider activities of individuals in the furtherance of personal objectives. However, because even individuals can cause disruption and destruction in cyberspace, the possibility of cyberterrorists cooperating with individuals must be addressed. Also, while cyberespionage and cybercrime should not be lumped in with cyberterrorism, both types of activity could be used to support cyberterrorism.

Taking a stab at what acts constitute "cyberterrorism" involves addressing even fuzzier boundaries. From the traditional perspective, consideration of terrorism focuses on acts or threats of violence calculated to create an atmosphere of fear or alarm. For example, cyberattacks could cause train accidents with large death counts through tampering with digital signaling systems. Additionally, cyberspace presents myriad opportunities to commit acts that cause significant disruption to society without direct loss of life, injury, or harm to material objects. For example, digital attacks might cause stock market disruptions by denying service to computer and communications systems.[7] This analysis of cyberterrorism includes both acts that involve physical violence and those causing significant social disruption based on attacking information systems and infrastructures.

Additionally, cyberterrorists could conduct attacks with the goal of corrupting key information within a system that requires high confidence for its use. Corrupting information about blood types within a hospital data base or strike prices within the stock trade settlement systems would involve much more recovery time and effort than a simple denial of service attack on the same target. Such an attack would inflict direct economic costs from system downtime, checking and correcting data and settling disputes. Successful cyberterrorist attacks of this sort may also degrade user confidence in provision of services of fundamental importance to society.

Activities labeled as cyberterrorism must include recognition of both destructive and disruptive components. An open question is whether the potential for "mass disruption" created by reliance on information systems in the US will hold even greater appeal than attacks of "mass destruction" through the use of chemical, biological, and nuclear means.[8] Terrorists may prefer cyberattacks capable of causing widespread, observable impact but not involving death and physical disruption rather than use of WMD or even conventional attacks in terms of limiting moral outrage and managing public opinion. Alternatively, "mass disruption" inflicted via cyberterrorism may prove too ephemeral to achieve desired effects. Governments and societies subject to cyber-based "mass disruption" may quickly learn to react and respond to such attacks, potentially even building up psychological resistance to such attacks.

Delineating the scope of activities that constitute cyberterrorism is difficult. The information age may well provide terrorist groups new ways to discredit governments and disrupt society to achieve their objectives. Therefore, cyberterrorism should be analyzed in light of the objectives sought.

Motives and Accountability

The nature of cyberterrorist campaigns, the means used, and the targets attacked will all depend on the motives of those groups considering the use of cyberterror means. Traditional analysis of terrorism has concentrated on groups with well-defined purposes for using violence as a means of political coercion.[9] Many terrorist groups such as the Weathermen within the US or the Red Brigade in Italy have engaged in efforts to overthrow or substantially change a political regime. Attacks are launched to undermine the legitimacy of the targeted government and garner support among a disaffected populace. Secessionist groups seeking the creation of new states or political autonomy for an ethnic/religious group also may use terrorist means to publicize their cause. Groups utilizing terrorist means to achieve such objectives include the Popular Front for the Liberation of Palestine and the Provisional IRA. A key feature of terrorism for political coercion is the willingness of groups to take credit for their attacks. The ability to inflict pain provides the principal source of leverage in negotiating with governments to achieve their objectives. Given the desire to secure the support of the general population and possibly to negotiate with governments, such groups may have self-imposed limits in terms of how vigorously and indiscriminately they choose to employ violence.

Taking a broader perspective on the issue of objectives, the use of terrorism by groups with millennial or anarchical objectives has become a source of increasing concern.[10] Rather than pursuing a specific political agenda, such groups may use indiscriminate violence to create a general environment of fear and chaos prior to a general overthrow of Western political order or may even simply seek anarchy as a goal. The Aum Shinrikyo cult took no credit for the use of sarin gas by the in Tokyo subways. Laquer has highlighted the potential for such groups to view "superviolence" as an appropriate means to undermine the world political system in seeking their goals.[11]

A new thread in the analysis of terrorist motivations has received the label "war paradigm."[12] This paradigm holds that certain terrorist groups without the ability to confront opponents directly will take a strategic approach to conducting terrorist acts without making specific demands on the opponent. For example, Ramsey Yousef and others who executed the World Trade Center bombing had no known intent to acknowledge their role. The goal of such groups is to inflict damage and wear down opponents as part of an eventual victory in a long-term struggle. The focus of these analyses has been on groups motivated by Muslim fundamentalism, especially those associated with the Saudi jihadist Osama bin Laden. The attacks seen during the second half of 1990s on US military forces at Khobar Towers and embassies in Nairobi and Dar-es-Saalam may constitute such a campaign. Terrorists waging such campaigns may also see little constraint on inflicting damage or destruction against opponents.

Organization

Changes in the way terrorist groups organize will also impact their motives and perceptions of accountability. Traditional terrorist groups associated with the PLO and IRA relied heavily on tight central control over acts committed by the organization as part of an orchestrated pressure campaign against adversaries. However, the looser organizational structures of groups such as HAMAS, and Afgan Arabs may be enabled by the pursuit of less controlled, more destructive activities conducted by groups with anarchist or religious objectives. The "networked" organization of terrorist groups financially supported by Osama bin Laden has increasingly become the archetype for describing a new form of terrorist organization with no clear center of control. John Arquilla and David Ronfeldt have strongly touted the strengths of such an organizational form for terrorists. Networked terrorist organizations could establish alliances of convenience with state sponsors, criminal organizations (especially those involved in the drug trade), and potentially with hacker groups.[13]

The utility for terrorist groups to employ the services of hackers as surrogates in the conduct of cyberterrorism has also received growing attention.[14] Hacker groups have demonstrated a willingness to sell their services to outsiders. In the most well known instance, hackers in Hannover, Germany during the late 1980s sold information they obtained through access to computer systems in Departments of Energy and Defense, defense contractors and NASA to the Soviet KGB.[15] These intruders first began to obtain access in 1986. After their initial discovery in 1988, the process of identification and apprehension of the Hannover hackers by the US and German intelligence and law enforcement agencies took over 18 months. During the Persian Gulf War, a group of Dutch hackers who had intruded into Department of Defense systems attempted to sell their services to the Iraqis but were apprehended by Dutch police.[16]

Most analyses of hackers as cybersurrogates for terrorism generally stress the ease and advantages of such activity.[17] It is presumed that terrorist groups will be able to easily contact hackers for hire while keeping their direct involvement hidden through the use of cut-outs and proxies. These hacker groups could then be employed to reconnoiter adversary information systems to identify targets and means of access. If hacker groups can be employed to actually commit acts of cyberterrorism, terrorist groups may improve their ability to avoid culpability or blame.

However, employing cybersurrogates would also involve important risks and disadvantages. Attempting to employ hackers to commit acts of significant disruption that may involve killing people would likely prove much more difficult than buying information for the purposes of intelligence gathering. Contacting and employing hackers would also involve major operational security risks for a terrorist group.[18] At a minimum, the intelligence activities of hackers could be discovered and undermine planned operations. Terrorists without adequate leverage to control cybersurrogates run the risk of hackers being turned into double agents by hostile governments. The costs to a terrorist group of having an operation blown or providing adversaries information regarding their location or the identity of members would weigh heavily against use of such means. Both the German and Dutch hackers were eventually discovered, albeit after fairly long periods of activity and investigation.

The dearth of evidence means the calculus of terrorists considering use of cybersurrogates remains highly speculative at this point. One area for greater consideration is identifying which potential partners terrorist sponsors would consider more trustworthy. Some candidate surrogates, such as ex-security service members, may be considered more adept at maintaining operational security. Former members of the Soviet intelligence services that possess the requisite computer expertise and experience in the black arts of espionage may pose a real concern.[19] Terrorist groups may already have forged links with such potential allies. The subject deserves dedicated intelligence gathering efforts and analysis rather than simple hype.

Hacker Groups and Terrorism

Additionally, one must consider to what degree organized groups of hackers acting on their own accord pose a terrorist threat. For purposes of this analysis, hacker refers to persons or groups who gain access or break into digital systems, particularly networked computer and telecommunications systems. Hackers have a wide range of motivations including thrill seeking, knowledge, recognition, power, and friendship.[20] These individuals have also developed a sophisticated network to communicate ideas and coordinate activity through magazines such as *Phrack* and *2600*, stolen phone services, e-mail distribution lists, Usenet newsgroups, Internet chat rooms and even full-blown conferences such as DEFCON. According to one survey of hackers, over half of those asked said they work in teams, and more than a third indicated they belong to a specialized hacker group. Groups have names such as Legion of Doom, Masters of Destruction, and Cult of the Dead Cow. These groups have been known to wage conflicts on each other using the public telecommunications networks as a battleground and touting their degree of illicit access as the source of bragging rights.[21] Many groups analyze software weakness and provide digital tools to exploit mainstream software applications such as Microsoft Windows operating systems. Additionally, hackers are dominantly males between the age of 15 and 25, often disaffected with the prevailing social and governmental order. This profile parallels those involved in terrorism.[22] The combination of technological skills and disaffection could make a sufficiently motivated and organized hacker group in a considerable cyberterrorist threat.

Numerous hacker groups have expressed deep animosity against the US and other governments over attempts to prosecute hackers, regulate activity on the Internet and other political issues. The hacker magazine *2600* has orchestrated a major campaign, including a fundraising campaign, to get the government to release Kevin Mitnick convicted of numerous violations of US computer crime laws.[23] In December, the group known as the Legion of the Underground (LoU) issued a “declaration of war” against the governments of the People’s Republic of China and Iraq citing these regimes' repressive human rights policies. The LoU declared its intention to disrupt and disable the Internet in the two countries.[24] East Asia has also witnessed an exchange of digital intrusions targeted at defacing Taiwanese and People’s Republic of China government web sites with nationalist symbols and slogans of the hacker’s home state.[25]

Thankfully, however, typical terrorists and hackers also have significant differences. Terrorists are generally conservative regarding use of new technologies to conduct operations.[26] Some groups have even conducted attacks to specifically combat the spread of computer technology. A French group called the Computer Liquidation and Deterrence Committee attacked French and American computer companies during the 1980s because “the computer is the tool of the dominant. It is used to exploit, to put on file, to control, and to repress.”[27]

Conversely, the Internet community has seen the rise of white-hat hacker groups with a range of objectives. Some such as the LoPht Heavy Industries group based in Boston simply seek to provide information on latest hacker tricks and security weakness in products. LoPht has also called for hackers to cease attacks against the US government and testified for the Senate on how to improve computer security efforts.[28] The hacker community has also demonstrated a willingness to impose discipline on its own against disruptive hacking when the potential government backlash may prove too severe. A coalition of hacker groups formally condemned the LoU's declaration of war. *2600* magazine declared "This type of threat, even if made idly, can only serve to further alienate hackers from mainstream society and help spread the misperceptions we're constantly battling."[29] So far, the hacker community has stopped shy of conducting activities constituting a serious cyberterrorist threat.

Means and Targets for Cyberterrorism

The headlong rush of the US and other advanced nations into the information age involves new risks. The information systems central to national security, the conduct of government and commerce have significant weaknesses that can be attacked. Yet, such attacks have achieved only limited impacts as we end the 20th Century. To analyze how cyberterrorists might attack the US, we must consider which groups might employ cyberterrorism and for what reasons.

Means for Digital Attack

Terrorists could attack US information infrastructures using a variety of mechanical, electromagnetic, or digital means. Information systems have long been targets of mechanical methods of disruption. Command and control systems can be bombed, fiber-optic cables cut, microwave antennas broken, and computers smashed or simply turned off. The electronic components and transmissions of information systems and networks are vulnerable to jamming, as well as electromagnetic pulses generated by nuclear explosions and other sorts of directed-energy weapons. The rise of digital means of encoding and transferring information has also created new ways to attack information systems. Impacts of digital attacks can range from total paralysis of networks to intermittent shutdown, random data errors, information theft, and data corruption. The tools and techniques for attacking information systems have received detailed attention as the US government, commercial industry, and outside experts have begun to stress the possibilities of information warfare, digital espionage and computer crime.[30] The analysis below focuses on digital means as the new dimension of the equation appropriately labeled cyberterrorism. The possibility of synergistically employing all three types of attack also requires additional analysis beyond the scope of this chapter.

Cyberterrorists could cause disruption, damage, and destruction through achieving unauthorized access and control over a targeted information system through a vast array of intrusive tools and techniques, commonly referred to as "hacking." Means for successful intrusion range from compromised passwords to sophisticated software for identifying and exploiting known vulnerabilities in operating systems and application software. The difficulty of attaining access and time required to successfully "hack" a system will also depend on the targeted system's defensive measures including proper password and configuration management, patching of known vulnerabilities, and use of firewalls and intrusion detection systems. If control over a targeted computer or network is achieved, cyberterrorists could inflict a wide range of effects. Possibilities range from changing the graphics on a web page to corrupting the delivery schedules for medical supplies or military equipment to denying access to 911 services, air traffic control data, or disrupting telecommunications backbone networks. A principal advantage of intrusion for cyberterrorism is the potential for tight control over the timing, scope and effects of an attack. According to former Director of the Central Intelligence, John Deutch, "the electron is the ultimate precision weapon."[31]

Another well-known potential means for cyberterrorist attack would be the employment of malicious software code, more commonly referred to as viruses and worms. Malicious software can be broadly defined as software designed to make computer systems operate differently than intended. The effects of viruses and other malicious software range from benign messages displayed at system start up to code that can cause hardware failures and wide-area network overloads. Concern over malicious software increased rapidly after the unintentional release of the Internet Worm by a Cornell graduate student in 1988 disrupted most Internet services for a period of days.[32] During the early 1990s, reacting to and mitigating the consequences of viruses was a major computer security focus. Development of anti-virus software capable of periodic updating has helped mitigate the virus threat. However, 1999 saw a series of virulent outbreaks, including the Melissa virus and Worm.ExploreZip that proved capable of disrupting government, commercial, and other private information systems. A major feature of these viruses has been traffic overloads that occur when the viruses propagate vast amounts of e-mail through networked systems. Creators of malicious software determine the intended impact of running their code. However, the degree of disruption and damage caused by viruses and other code which replicates and passes quickly across networked systems can be much more difficult to control. Cyberterrorists using malicious code created by others may have much less certainty regarding the effects of their attack.

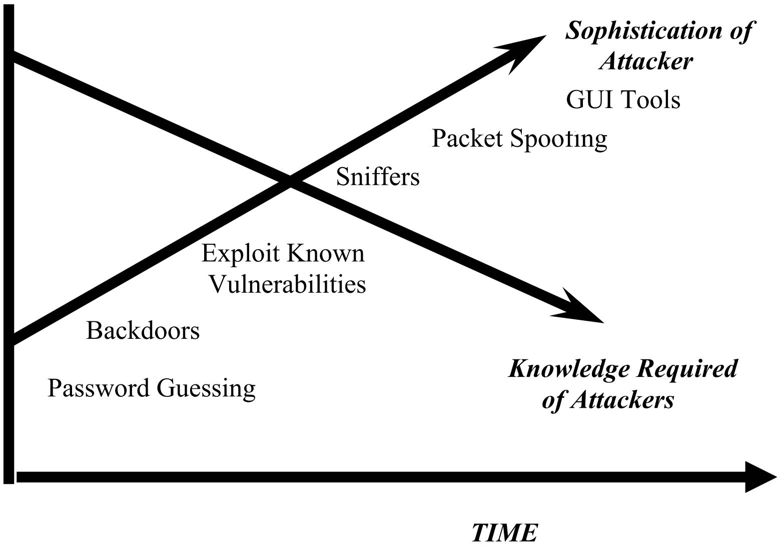
Combining features of both intrusions and malicious code, cyberterrorists could also intentionally corrupt software programs in targeted information systems and infrastructures to cause desired effects. While access to rewrite software code could be achieved through an intrusion, a terrorist group may endeavor to corrupt software in the process of creation or production by emplacing backdoors for access or insert "trojan horses" to cause desired effects at a predetermined time or upon a given command. Software maintenance and updates also present opportunities for such activities. Software code creation and maintenance for systems employed across the globe occur in places like India, Ireland, and Israel. The possibility for insertion of corrupted code as part of the massive effort to update software to fix Year 2000 problems provided a major concern for all sectors of the US government and society.[33] The main protection against such activity would be rigorous quality control over software products used in key systems, but such a process is time-consuming and expensive. As with intrusions, the degree of control possible through corrupted code can allow precision effects. Cyberterrorists could also achieve widespread effects by corrupting code in systems underpinning key information infrastructures. AT&T suffered nation-wide disruption of its telephone network in January 1990 due to a single line of faulty code in an upgrade to its primary switching software.[34] While this error was unintentional, the ability to attack the digital foundations of advanced information infrastructure presents sophisticated cyberterrorists with a significant means of attack.

Cyberterrorists can also disrupt or disable information systems and networks using techniques generically labeled as denial-of-service (DOS) attacks. Common DOS techniques involve overloading targeted e-mail systems by employing automated software and exploiting features of the Internet communications protocol through "smurf" or "SYN flooding" attacks. In recent years, hackers and politically motivated groups have increasingly turned to DOS attacks as a means of responding to specific events and policies by harassing targeted organizations and to draw attention to their complaints. One well-known instance involves a group known as the Electronic Disturbance Theatre (EDT). In October 1998, the EDT targeted the computers of the US military and the Frankfurt Stock Exchange in an effort to overload servers in these networks with the goal of publicizing the cause of the Zapatista rebels in Mexico. Yet, while cyberterrorists can specifically target denial-of-services attacks against known systems connected to network accessible to the attackers, operators of the targeted systems can also modify their systems either preventively or in reaction to the attacks. The Defense Information Technology Center simply reconfigured the targeted computers to refuse to acknowledge the originating Internet addresses in response to the EDT attacks. The EDT computers were overloaded with return messages as a result of employing the automated FloodNet software and forced to reboot.[35] The cat and mouse game of offensive moves and defensive responses will continue to evolve as information technology advances and presents new vulnerabilities to exploit. Cyberterrorism and other types of warfare, espionage, and crime waged in the digital realm will demonstrate this see-saw dynamic.

Another possible approach open to cyberterrorists would be to conduct hoax attacks, publicizing the possibility of intrusive activity and release of viruses. Virus scares can swamp help desks with requests for information. Users and system operators must ensure anti-virus software is up-to-date, creating an additional burden on the networks and wasting time. The Good Times scare in 1994 caused a massive reaction while only infecting a handful of computers.[36] Similarly, the possibility of intrusive activity requires system administrators and computer incident response teams to assume higher states of readiness with an attendant decline in attention to routine operations and maintenance. The US Department of Defense has instituted an Information Operations Condition (INFOCON) system of progressively higher levels to raise the awareness and preparedness of cyberdefenses similar to the THREATCON system use for responding to increased threat of terrorist attack.[37] Attaining the defensive posture called for by higher INFOCON levels would require substantial efforts for those responsible for the DoD information infrastructure and pose constraints on the use of the Department's information resources. Cyberterrorists focused less on high impact events and more on waging a protracted conflict could use hoaxes designed to cause the targeted adversary to waste significant effort without the terrorist having to run the risks of conducting actual attacks. Defensive efforts may suffer over the long-term if multiple hoaxes create a "cry wolf" syndrome regarding calls for increased protection. The impact of hoaxes will be magnified if terrorist groups develop a credible reputation for being able to conduct digital attacks.

Access and Expertise

To use any of the tools and techniques described above, cyberterrorists must have access to the means and the expertise to employ these tools effectively. The prevailing wisdom is that both are readily available. Well-known information warfare pundit, Winn Schwartau states, "Anyone can be an


Sophistication of Attacker
GUI Tools
Packet Spoofing
Sniffers
Exploit Known Vulnerabilities
Backdoors
Password Guessing
Knowledge Required of Attackers
TIME

information warrior…. Potentially, a hundred million information warriors are poised, and honing their skills while they wait."[38] Numerous analyses cite the vast number of web sites on which hacker tools and techniques can be found and downloaded, as well as the presence of Internet chat sites, conventions, catalogues, and publications in which hackers exchange information.[39] In a similar vein, most analyses also hold that the means for attacking information systems have become both more sophisticated and easier to use. The following figure from a 1996 GAO report entitled *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks* depicts the evolution of attack tools and required expertise as time has progressed.[40]

One way terrorists may build their expertise and understanding of the potential for digital attacks is through the use of cyberspace for other activities. Increasingly, terrorist groups including the Provisional IRA, Algerian extremists, HAMAS, and others are using the Internet and cellular phones to orchestrate their activities. Many groups have begun to use encryption technology to protect their digital communications. According to Arquilla,

> Egyptian "Afgan" computer experts have helped devise a communication network that relies on the World Wide Web, e-mail and electronic bulletin boards so that extremists can exchange information without a major risk of being intercepted by counterterrorism officials.[41]

The Provisional IRA uses computer databases to catalogue individuals, installations, and other targets.[42] Terrorists and associated groups have also begun to use the Internet as a mechanism for publicity, fundraising, and recruitment. The Zapatistas have established a major presence through the World-Wide Web supported by activists in the US, Europe, and elsewhere.[43] Drug cartels use the Internet in transactions with banks to launder money, and at least potentially, terrorists could use cybercrime to steal money to support their operations.[44] Terrorists may also use advanced information technology for intelligence gathering. Access to commercial satellite imagery may provide information for targeting physical attacks. Hacker and information warfare websites may provide conceptual approaches and even lists of targets for cyberterrorism. Evidence is clear that terrorist groups increasingly use advanced information technologies and are building an experiential base that could be used for cyberterrorism.

However, the utility of user-friendly attack technologies and general computer expertise to any terrorist group depends on the nature of the targeted infrastructure and intended effects. Denial of service attacks against Internet connections may require much less sophistication but achieve less controlled effects than attacks based on successful remote access and control of a targeted information system or network. Additionally, a defender’s ability to assess vulnerabilities and deny access to known digital attack tools and techniques may also increase the level of technological knowledge required for attacking forces. If key information infrastructures are well protected, achieving surprise and inflicting disruption against significant centers of gravity may require cyberterrorists to employ more technological sophistication, time, and effort. The pool of human capital with the ability to develop sophisticated new attack tools or quietly probe strong, attentive defenses is much more limited than the number of individuals capable of running scripted tools or sending multiple e-mail messages to an Internet address. The Center for Infrastructural Studies stated in early 1998, “According to recent studies, most attacks use standard or well-known script exploits. Our research reveals less than 1,000 hackers in the world who have the professional programming skills to create their own attack scripts.”[45]

For cyberterrorists, easily accessible and usable digital attack techniques may equate to more conventional hand grenades and pistols in terms of scale of effects and lack of precision. To develop the digital equivalent of weapons of mass destruction or achieve the precision of sniper rifles may require a much greater degree of technological sophistication and self-reliance on the part of cyberterrorists. Developing collection means and analytical techniques to understand the technological skill and resources of terrorists presents an important challenge for the US intelligence community.

Targets for Cyberterrorist Attacks

Since at least the early 1990s, the US government and outside experts have grown increasingly concerned about the possibility of cyberterrorist attacks as our society has become more reliant on information systems and infrastructure. The 1991 National Research Council *Computers at Risk* report finds, "The modern thief can steal more with a computer than a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than a bomb."[46]

The increasing ability of terrorists and others to attack US critical infrastructures through use of digital attacks has received the most attention.[47] In the wake of the Oklahoma City bombing in 1995, the President set up a Critical Infrastructure Working Group to address both physical and cyber threats. As a result of hacker incidents, Department of Defense exercises and Congressional prodding, the Presidential Commission on Critical Infrastructure Protection was set up to analyze the threat to US infrastructures and policy responses for their protection. The PCCIP's October 1997 report, entitled *Critical Foundations*, provides the most comprehensive analysis of the cyberthreat to US infrastructures "essential to minimum operations of the economy and government."[48] The report stresses how the growing reliance on information systems that underpin a whole range of infrastructures including communications, electric power, transportation, and emergency services creates substantial risks for a wide range of digital attacks, including possible cyberterrorism. While a comprehensive discussion is beyond the scope here, possible targets for cyberterrorism include the Supervisory Control and Data Acquisition (SCADA) systems which govern the distribution of telecommunications, electric power, and other infrastructure-based services. The Global Positioning System (GPS) network of satellites, ground control stations, and signaling systems constitutes an infrastructure target whose role in military and civil navigation as well as broadcasting timing signals in cellular communications and other information networks could prove attractive to cyberterrorists. The disruption caused by the failure of a single PanAmSat communications satellite in May 1998 crippled most US paging services as well as a number of data and media communications feeds for hours and, in some cases, a couple days.

While attacking information systems underpinning critical infrastructures presents cyberterrorists with potentially high impact targets, important questions need to be addressed in order to adequately gauge the potential threat. One area of significant uncertainty is how fast infrastructures will be able to recover from digital attacks. Many analysts focus on how many infrastructures have single points of failure that can cause quickly cascading effects disrupting or disabling effects over a wide area. The Northwest power outage in August 1996 that affected hundreds of thousands of users began by a tree growing into a single power line. Others point to the ability of complex systems to adapt and recover.[49] In the cases of the AT&T switching failure, the Northwest power outage, and the PanAmSat satellite failure, the infrastructure operators were able to recover in a period of hours. What is clearly unknown is how such complex infrastructures would react to orchestrated cyberterrorist attacks instead of unintentional mishaps and accidents.

Another approach would be to attack organizations or institutions with high public visibility. Hackers have proven capable of repeatedly defacing the web pages of corporations such as DuPont and Ford as well as government agencies including the White House, FBI, NASA, and the Air Force. Cyberterrorist attacks may specifically be launched to garner media attention rather than cause physical damage or economic losses. Demonstrated ability to disrupt computerized inventory systems of Wal-Mart or corrupting medical records within a large health management organization would provide prime fodder for media attention. Newspapers have reported that the hacker group, RTMark, has endeavored to depress the stock price of eToys by disrupting the company's web site.[50] Financial institutions have often been listed as a potential target of cyberterrorism. Citigroup admitted in a highly publicized incident that a Russian hacker managed to electronically siphon off $12 million in funds in 1995. While Citigroup actually managed to recover all but $400,000 of this loss, competitors reportedly used the incident to convince commercial clients to switch banks due to the perceived greater insecurity of Citigroup information systems.[51] In 1996, the *London Times* reported that banks, brokerage house, and investment firms paid hundreds of millions of dollars in blackmail to extortionists to avoid cyberattacks whose capabilities had been demonstrated.[52] The high level of media attention to financial markets and the critical role of public confidence in their activities mark them as prime targets.

Terrorist groups could also conduct digital attacks against media outlets themselves. Indonesian media outlets had their computer systems attacked by hacker groups supporting the Timorese rebels.[53] However, cyberterrorism targeted with an eye towards garnering media attention rather than death and destruction may require more sophisticated targeting and digital attack capabilities than generic attacks against any open targets within the US infrastructure. The disruptive effects of such attacks may prove short-lived, but cyberterrorists could endeavor to shake public confidence in core institutions through such attacks.

Terrorist groups could also use digital attacks to support traditional terrorist operations. As monitoring and sensor systems for protecting people and facilities become increasingly reliant on information technology, digital attacks may prove a useful means of creating opportunities for conventional terrorism. In 1998, the *New York Times* reported a design flaw in a security system widely used in airports, prisons, financial institutions, and the US government allowing digital intruders to access secure areas, unlock doors, and erase evidence of changed access records.[54] Emergency 911 systems have been found vulnerable to computer intrusions and could be targeted by cyberterrorists. Paralyzing communications as a means of slowing emergency responses could plausibly enhance effectiveness of conventional or WMD terrorism. As with any potential tool, terrorist groups could employ cyberattacks synergistically along with other means to achieve their objectives.

Cyberterrorists may also endeavor to make use of "insiders." Reasons for assisting terrorists could include personal gain, revenge, or sheer destructiveness. The assistance of individuals knowledgeable of technical characteristics and operational significance of a targeted information and systems would prove of immense value to terrorist groups in launching all types of digital attacks. The threat posed by insiders with authorized access to information resources presents a fundamental information security concern.[55] A network programmer fired by Omega Engineering Corporation in 1996 provides an illustrative case. Upon his departure, the programmer activated a logic bomb that permanently deleted all the company design and production software used to produce high technology measurement and control instruments for the US Navy and NASA. Damage was estimated at $10 million.[56] The 1999 Computer Security Institute/Federal Bureau of Investigation "Computer Crime and Security" survey indicated sixty-five percent of organizations responding had suffered incidents involving insiders.[57] Cyberterrorists intent on causing widespread destruction and damage might use insiders to corrupt SCADA systems or plant viruses. The ability to effectively screen employees, discover attempts at outside recruitment, and identify and mitigate malicious activities quickly will play a role in combating cyberterrorism as part of overall information security efforts

Thinking About Cyberterrorist Campaigns

With a wide range of available tools and potential targets, cyberterrorist groups may use very different types of campaign strategies to pursue objectives. So far, most attention focuses on the possibility of single events causing catastrophic physical effects such as a plane crash or the failure of control systems in a nuclear power plant. The assumed objective of the attack is widespread publicity for the group's cause and negotiating leverage against governments. A potentially more serious threat that receives less attention would involve cyberterrorist groups adopting a protracted war strategy similar to the ones used by Mao Tse Tung and Ho Chi Minh. Instead of striking the most dramatic target, terrorists waging a protracted guerilla campaign of cyberterror could strike targets of opportunity that also minimized the chance of discovery and retaliation. The objectives of such a campaign may well involve media attention but also target the will of an adversary's government and populace over the long-term.

Developing a strategy for dealing with single cyberterrorist events may focus on improving warning of attacks and the ability to manage the consequences of disasters. Responses to waging a prolonged conflict with cyberterrorists may be quite different. Fighting such adversaries will require improvement in defensive capabilities and recovery capacity of information infrastructures as well as improving means to track down and incapacitate attackers.

Outlining these two broad strategic approaches and their implications simply provides an illustration of the complex situation facing those responsible for dealing with cyberterrorism. The US government must develop a deeper understanding of how different cyberterrorist groups are most likely to operate, potential objectives and capabilities, the risks posed by attacks, and appropriate responses. This analysis must be based on fact, not speculation.

Cyberterrorism—What We Have Observed

Information infrastructures have long served as targets for adversaries in a conflict. Adversaries have always attempted to intercept messengers. The emergence of electronic communications resulted in cutting telegraph lines and underseas cables during wars. As more communications passed via electromagenetic transmissions, jamming, frequency hopping, and other techniques became a commonplace aspect of military operations known as electronic warfare.

Terrorists have also seen attacks against infrastructures as a means of achieving their traditional objectives. For example, the Provisional IRA in the early and mid-1990s launched major terrorist attacks against transportation and commercial targets in U.K. with the intent of maximizing societal disruption. In April 1993, a bomb detonated in London caused massive commercial disruption by causing the temporary closure of key financial markets.[58] In the 1970s, the Italian Red Brigades specified destruction of computer systems and installations as a way of striking at the state. They conducted numerous attacks against businesses in the elctronics and computer industries.[59] As the functioning of information systems and infrastructures becomes increasingly fundamental to US and other societies, the appeal for terrorists to attack such targets will increase. Lessons learned about what constitutes key features of an adversary's information infrastructure necessary for the conduct of conventional attacks would also prove useful to cyberterrorists considering the use of digital attacks.

Hackers and hacker groups so far have not proven to be significant cyberterrorist actors in terms of conducting digital attacks to create intentional death, destruction, or disruption. While there have been occasional declarations of intent to wage "cyberwar" against the US government, corporations or other entities, these threats have not resulted in serious campaigns to achieve political or even anarchical objectives. However, the dearth of cyberterrorism by hackers so far does not mean they are not capable of inflicting severe damage via digital attacks. Hackers have intentionally disrupted 911 services, launched viruses degrading the information processing of major corporate and government organizations, and gained access to key computer systems such as domain name servers which underpin information infrastructures in such organizations. A good example of the potential for hackers to become cyberterrorists is provided by an incident in March 1997. In this instance, a teenage hacker penetrated and disabled Bell Atlantic telecommunication switches in the Northeastern US One of the disabled switches provided phone and data services to the Worchester, Massachusetts airport control tower, and the incident shut down the airport for many hours.[60] If such an attack were purposely targeted and timed when air traffic control was already difficult due to weather or volume of traffic, the difference between what happened in Worchester and a cyberterrorist attack would only be a matter of intent.

An increasingly common phenomena related to cyberterrorism is hacking by technologically literate groups in support of insurgent, environmental, or other political movements. Hacking into and defacing Web pages has proven a most common means to express discontent. However, the rise of purposeful denial-of-service attacks such as the one by the EDT has also caused increased concern. So far, such activities have proven at most temporary nuisances rather than real problems that might coerce targeted governments to change policies. Yet, reacting to such threats already involves increasing resource commitments by organizations such as the Department of Defense and FBI. Such activity clearly falls within the boundaries of terrorist intent discussed earlier. The real question is when does the level of disruption rise to a standard appropriately labeled as terrorism instead of mischief.

In terms of known terrorist groups using digital attacks for cyberterrorism, we have only begun to see such activity occur. The most well-known case has involved the Internet Black Tigers, an offshoot of the Sri Lankan rebel group Liberation Tigers of Tamil Elam. The Internet Black Tigers swamped the e-mail services of numerous Sri Lankan embassies for a period of approximately two weeks.[61] Yet, such attacks comprised a relatively insignificant aspect of the overall terrorist campaign of these rebels and arguably were principally for publicity rather than disruptive objectives.

A major terrorist campaign waged principally or solely via digital attacks has not occurred. As with other forms of conflict, cyberterrorism will likely evolve as another tool for groups to achieve their objectives rather than springing into life in full bloom. That said, successful cyberterrorist attacks could also provoke a rapid rise in activity once such means are a proven way to achieve terrorist goals. The focus for US policy should be to understand the goals of groups who are most likely to employ such a new approach and potential vulnerabilities arising from possible cyberterrorist attacks.

The US Response

The US national government has recognized the growing threat posed by cyberterrorism. A detailed development of US policy and organizational responses to cyberterrorism is beyond the scope here. The section below presents a brief overview of what has been accomplished and what is yet to be done.

Over the past decade, a confluence of concern with information warfare, terrorism against US targets at home and abroad, and the recognition of the increasing reliance on critical infrastructures all have made dealing with cyberterrorism a higher priority on the national security agenda. A spate of books and articles in the mid-1990s focused on the possibility of a digital Pearl Harbor facing the US The President established a Critical Infrastructure Working Group in 1995 in the wake of the Oklahoma City bombing to address both physical and cyber terrorist threats under the leadership of the Justice Department. Congressional inquires and GAO reports have described the vulnerabilities of our digital infrastructure to hackers and called on the President to details plans to develop cyber defenses. Such threats have been examined through RAND "Day After in Cyberspace…" wargames and DoD exercises such as Eligible Receiver. These evaluations demonstrated significant national and DoD vulnerabilities that would arise from a structured cyberattack.[62]

Growing demands for a comprehensive response have resulted in the US government putting increasing energy behind its response to possible cyberattacks. In the summer of 1996, the President's Commission of Critical

Infrastructure Protection was formed to conduct a comprehensive review and recommend national policy for protecting critical infrastructures against physical and cyber threats. The PCCIP's efforts formed the basis for Presidential Decision Directive 63 "Critical Infrastructure Protection" issued in May 1998. In combination with PDD-62 "Protection Against Unconventional Threats to the Homeland and Americans Overseas," the two directives establish a system of organizations, roles, and responsibilities through which the US will respond to terrorism and protect its critical infrastructures during peace and war.

Since the spring of 1998, national efforts against digital attacks have focused on implementing the construct laid out in PDD-63. The Directive created a National Coordinator for Security, Infrastructure Protection and Counterterrorism on the National Security Council. Departments and agencies within the Federal government have developed sector-specific protection plans across the range of identified critical infrastructures. The Critical Infrastructure Assurance Office (CIAO) in the Commerce Department assists in sectoral planning efforts and their integration into a national plan. The private sector has also started to establish Information Sharing and Analysis Centers (ISACs) as called for in PDD-63. As of late 1999, the first ISAC was established in the banking and finance sector with other ISAC plans under development.[63]

On the operational side, the National Infrastructure Protection Center was established even prior to the issuance of PDD-63 in February 1998.[64] As staffing and resources have increased over the past few years, the NIPC and Federal government agencies have initiated numerous efforts to coordinate activities in response to cyber threats. The NIPC and CIAO are endeavoring to establish linkages with state and local governments as well as the private sector. Yet, the hurdles to improve cyberdefenses are substantial and resources remain limited.

Challenges in Responding to Cyberterrorism

The US intelligence community must play a key role in understanding the threat posed by cyberterrorism. Effective responses require the US both to understand the potential capabilities of cyberterrorist groups and develop advanced warning regarding their intent to use such capabilities. Cyberterrorism presents a very difficult intelligence target. The highly developed imagery and signal intelligence capabilities used to characterize Cold War threats and nation-state military capabilities have limited applicability in providing information to assess whether terrorist groups can effectively employ digital attacks. Also, the skill sets of intelligence analysts required to understand digital communications systems and techniques for exploiting computer weaknesses are not the same as those to characterize capabilities of ballistic missiles and the strength of ground forces. Also, the new skill sets are in high demand in the private sector making them even harder to create and sustain within the US government.[65]

To provide strategic warning of cyberterrorism, the intelligence and defense communities require insight into activities of adversary groups to develop profiles of preparatory steps for digital attacks. In the cyberrealm, distinguishing potential terrorist activity from normal system failures, exploratory hacking, and other threats such as espionage is very difficult. In the spring of 1998, the Department of Defense was initially concerned that hacking activity eventually tracked down to teenagers might have been state-sponsored activity related to US military activities in the Persian Gulf.[66] Conducting counterterrorism involves close coordination between organizations responsible for intelligence, counterintelligence, and combating computer crime. Potential terrorist activity in cyberspace presents particularly acute requirements for such cooperation.

PDD-63 and other policy directives have set in place the organizations and responsibilities. At the national level, the NIPC has primary leadership for detecting and responding to digital attacks. The Defense Department established a Joint Task Force - Computer Network Defense to provide centralized capability for the same missions to protect the Defense Information Infrastructure. A program to create a comprehensive Federal Intrusion Detection Network (FIDNet) system under the authority of GSA exists.[67] Other organizations in the public and private sectors have established efforts to achieve similar objectives. In addition to the ISACs, a number of computer security associations and consulting firms strive to improve computer and information security in the private sector. These organizations generally work closely with a community of Computer Emergency/Incident Response Teams known as CERTs or CIRTs established by many organizations in both the government and in the private sector.

Yet, despite the presence of such organizations, those responsible for US cyberdefense at all levels have very limited capability to provide tactical warning of impending attacks or assess attacker motivations and objectives. Defensive tools, primarily in the form of various types of intrusion detection systems, have been developed to help identify presence and intent of malicious digital activity. However, current IDS technology relies on identifying known types of exploits and can not easily identify new types of digital attacks, even those based on modifying previous types of exploits.[68] Adequate attack assessment is even tougher. Owners, operators, and defenders of information systems and infrastructures rarely have an adequate picture of what they are protecting. Defenders not only need to understand physical and logical interconectivity, they also need to understand the operational significance of information and systems which are under attack to properly prioritize their warning, detection, and response efforts.

In specific circumstances, CERT and law enforcement agencies have proven capable of tracking down and punishing attackers. However, the timelines to identify and prosecute responsible individuals in most well-known hacker incidents have been lengthy and the punishments meted out fairly light. The capacity of the NIPC, the JTF-CND, and other organizations to handle big events involving large numbers of sophisticated attackers is unproven. Legal and policy considerations also place constraints on such agencies attempting to precisely identify individuals and organizations responsible for malicious activity in cyberspace. Law enforcement and computer network defense organizations are not allowed to hack back though computer systems to follow the electronic trail of intruders without express permission of system owners or authorized search warrants.[69] Yet, most digital intruders utilize multiple hops through cyberspace before conducting intrusive activity. Also, the CERT and law enforcement communities most closely involved with leading responses to computer intrusions tend to focus on single incidents. Defending against cyberterrorists with long-term objectives and significant attack capabilities will require fighting a campaign, a perspective significantly different than a law enforcement effort focused on building a court case.

Federal government plans also have identified organizations responsible for responding if a cyberterrorist attack caused significant disruption or destruction to mitigate effects and restore capabilities. Under the authority of PDD-63, the Federal Emergency Management Agency (FEMA) would lead consequence management efforts in conjunction with the NIPC, FBI, and state/local authorities. US national-level planning for how to deal with major disruptions to information systems and infrastructures was accelerated due to the requirement to be ready for Year 2000 events. Yet, a continuing consequence management challenge is the lack of detailed knowledge of the network connectivity, information system characteristics, and operational significance of assets that may suffer a cyberterrorist attack. Lack of adequate information infrastructure "mapping" will hamper the prioritization of reconstitution efforts and deployment of available resources. Establishing effective consequence management capabilities also faces difficulties in terms of running operational exercises to simulate large-scale terrorist attacks against complex, interconnected, privately owned and operated information infrastructures. Currently, organizations responsible for responding to cyberterrorism lack understanding of possible modes of system failure and the ability of infrastructures and operating organizations to recover from attacks. Again, those responsible for consequence management efforts should leverage knowledge gleaned from Y2K preparations and experiences with failure and recovery characteristics from Y2K events.[70]

The final step in defending against cyberterrorism is to improve the strength of our information infrastructures against digital attack. The NIPC, in conjunction with sector leads and the ISACs, has the role of identifying critical vulnerabilities and implementing mitigation plans. However, networked information systems and infrastructure at the end of the 20th Century present easy prey for digital intrusion and disruption. The complexity of operating systems such as Windows NT or Linux and applications such as Microsoft Office or SCADA systems combined with the speed of development and new product releases results in foundational pieces of the information infrastructure that have numerous security flaws. These flaws are discovered and disseminated at a rapid pace by the hacker community. As with intrusion detection systems, defensive tools such as firewalls, virus checkers, and network analyzers usually lag development of new attack techniques. Cyberterrorists are among the spectrum of adversaries who can exploit this basic weakness.

The process presently used by many government organizations involves instituting notification and tracking systems to ensure owner/operators of information infrastructures fix known vulnerabilities and update virus defenses to make digital intrusion and disruption more difficult for cyberterrorists and others. For example, the Department of Defense has instituted an Information Assurance Vulnerability Alert system that requires all DoD organizations to patch certain identified vulnerabilities and report compliance within specified timeframes.[71] However, this approach constitutes a rearguard action whose prospects for success are limited. Its success relies heavily on reacting to vulnerabilities after their weakness has already been demonstrated. More fundamentally, the "patching" process means those defending critical US information infrastructures must discover vulnerabilities, notify users, and track the implementation of fixes throughout a extremely diverse infrastructure comprised of and operated by thousands of organizations using thousands of different products implemented and modified by hundreds of thousands of individuals. So far, the procedures and resources employed to reduce infrastructure vulnerabilities to digital attack fall far short of denying access to potential cyberterrorists.

An alternative approach would involve ensuring that key systems and infrastructures were built to make digital attack difficult from the beginning of system concept and design. Such an approach would help mitigate a wide range of threats including cyberterrorism but also address concerns ranging from unintentional problems to cybercrime to information warfare. Yet, US government plans as articulated in PDD-63 and other directives show little desire to pursue such an approach. Huge difficulty faces implementation of a national cyberdefense strategy based on migrating to more stout digital foundations. Fundamentally, the government would have to ensure that owner/operators of key systems and infrastructures employed more secure products. Yet, the forces of technological innovation and competition in the information technology industry have forced commercial producers to move firmly in the direction of deploying products as quickly as possible with a minimum of security and other testing. The booming US economy increasingly relies on this sector as a source of fundamental strength. With the exception of encryption policy, the Clinton Administration avoided any significant moves to interfere with the telecommunications and information technologies industries under the guise of national security.[72] This choice means that the threat from digital attacks will remain significant for the indefinite future.

The US has proactively begun dealing with cyberterrorism as a part of national security. Given that dramatic events have yet to occur to prompt action, such efforts should be lauded. However, while policy directives establish authorities and organizations to provide capabilities to counter cyberterrorism, the US is a long way from having effective defenses against the potential threat. Efforts throughout government and the private sector vary greatly in depth and focus. Human and financial resources are lacking everywhere. Technological and economic considerations limit the government's ability to protect our information systems and infrastructures. The nature of US society and protection of civil liberties also present difficulties for those responsible for protecting US in national security in cyberspace.

Policy Options

Improving US capabilities to deal with cyberterrorism will intertwine with a number of other efforts related to information warfare, critical infrastructure protection, and countering computer crime. This section lays out recommendations designed to make cyberterrorism more difficult and dangerous for perpetrators.

US strategy must include efforts to make information systems and infrastructures more robust. The first step in this process is to improve the basic understanding of the technological underpinnings and operational characteristics of our informational centers of gravity. The US government or private sector organizations can not afford to provide robust protection to any and all information resources. Defenders must catalogue key assets and prioritize the deployment of available resources. Such an undertaking will require significant resource investment in organizations such as the NIPC, by government agencies responsible for specific infrastructure sectors, and in the private sector ISACs to create and sustain knowledge of what ought to be protected and how to most effectively accomplish this task. This type of investment would not only serve to counter cyberterrorism but would improve US defensive information warfare and critical infrastructure protection programs at the same time. The US should incorporate lessons from preparing for and responding to Y2K events.

Additionally, identifying key assets and how to effectively protect them must extend beyond the critical infrastructures identified in PDD-63. Most importantly, the US government must find ways to motivate information technology producers to raise the priority of system reliability and security in the production and fielding of new products. Legislative and policy approaches must consider both carrots and sticks. Innovative ideas might include providing the private sector tax breaks for improving protection in key technologies or legislation that establishes liability for losses due to digital intrusions and disruption if companies do not meet proscribed security standards.[73] These efforts would involve economic and social tradeoffs that require thorough evaluation. Yet, despite obstacles, proactively limiting the opportunities presented to terrorists and other digital attackers by building strong information infrastructures will leverage limited resources much more effectively than trying to patch the holes after systems are in place.

The second set of policy initiatives to address cyberterrorism should focus on steps to make it more dangerous for its perpetrators. Cyberterrorism offers opportunities for attackers to remain anonymous or at least unlocated. The US must improve national security, intelligence, counterintelligence, and law enforcement capabilities to track and identify cyberattackers. To achieve this goal, the US must first improve the exchange of information and cooperation across these communities. The NIPC was created to accomplish this task, but long-standing differences in organizational orientations and cultures must be surmounted. Providing these communities with adequate technological tools, organizational capabilities to fuse information, and skilled people to accomplish the mission will prove costly. While discussions of cyberdefense tend to focus on the technological, more difficult will be justifying the resources necessary to recruit and retain sufficient skilled personnel. The defense, intelligence, and law enforcement communities are losing personnel with computer and information security expertise as fast or faster than they can be trained. Establishing effective analytical methodologies for tracking and hunting down cyberterrorists also requires more attention. Finally, the legal context for US government intelligence and law enforcement efforts intended to combat cyberterrorism and other malicious activity requires examination for possible modification. Initiatives could include enabling the courts to issue a single warrant for law enforcement agencies tracking suspects through multiple locations in cyberspace. Cyberterrorists fearful of rapid identification and response by the US government may well have to modify their tactics and strategies substantially.

Finally, the US government must implement a more proactive education and public awareness strategy. At a minimum, such a strategy must stress awareness of individual and organizational responsibilities and liabilities associated with conducting business, recreation, or other activities in cyberspace. Through the PDD-63 system of organizations, the government needs to establish and promulgate best practices for information system and infrastructure security. Going farther, the Federal government should implement a plan to limit confusion and hype in the event of cyberterrorist attacks. The government can potentially play a key role in identifying and limiting the impact of hoaxes. The most important task of the government at all levels if a cyberterrorist adversary was to wage a sustained campaign of disruption might simply be to provide accurate information about events and responses. In our open society, the US will continue to live with risks from cyberterrorism. The government role must focus on effectively mitigating these risks with the least impact on society as possible.

Conclusion

Much of the current hype about cyberterrorism is built on fear of the unknown. We need to move beyond simple speculation to more structured analysis of the threat and appropriate US responses. We do have sufficient reasons to believe cyberterrorism will become a more significant national security concern. The means are available but employing digital attacks to achieve specific terrorist objectives faces multiple obstacles. Within the US government, the challenge presented by the threat has received increasing attention. Plans have been formulated to address cyberterrorism as a part of the national critical infrastructure protection effort. Yet, these efforts are hampered by the narrow scope of defense efforts and inadequate resources. Developing robust defenses will continue to prove difficult. The most effective approaches to protect against cyberterrorism through establishing secure information systems and infrastructures must contend with technological and economic imperatives at the end of the 20th Century that cut in other directions. Improving the ability to track attackers involves issues of civil liberties and the role of government that require extensive public debate. Most clearly, US efforts to mitigate cyberterrorism will have to advance incrementally on a combination of fronts. We have no silver bullets for combating cyberterrorism. Rather, our nation must remain alert, learn, and invest wisely.

[1] The possibility of digital warfare and terrorism became a widespread concern in the early 1990s largely as a result of reports such as National Research Council, Computers at Risk: Safe Computing in the Information Age (Washington, DC: National Academy Press, 1991) and books such as Alvin Toffler and Heidi Toffler, War and Anti-War: Survival at the Dawn of the 21st Century (Boston: Little, Brown and Company, 1993).

[2] Quoted in Michael Evans, "War Planners Warn of Digital Armageddon" *London Times*, 20 November 1999.

[3] Walter Laquer, "Post Modern Terrorism" *Foreign Affairs* Vol. 75, No. 5 (September-October 1996), 35

[4] John Arquilla, David Ronfeldt and Michelle Zaninni, "Networks, Netwar and Information Age Terrorism" in *Countering the New Terrorism* (Washington DC: RAND Corporation, 1998), 71.

[5] See Bruce Hoffman and Caleb Carr, "Terrorism: Who is Fighting Whom?" *World Policy Journal*, Vol. 14, No.1 (Spring 1997), 97-104.

[6] This definition is based on that provided by Ian O. Lesser, "Countering the New Terrorism: Implications for Strategy" in *Countering the New Terrorism* (Washington DC: RAND Corporation, 1998), 85.

[7] As of the end of 1999, there are no publicly known examples of purposeful digital attacks disrupting train services or stock markets. However, computer systems failures in Washington DC disrupted early morning Metro service for a period of hours on 20 September 1999. The different US financial markets have shut down at times for short periods due to loss of necessary computer and information services. Reasons for these shut downs vary from backhoes cutting fiber-optic cables in New Jersey to floods in Chicago.

[8] On the possibility of use of use of weapons of mass destruction by terrorists, see Aston Carter, John Deutch and Phillip Zelikow, "Countering Catastrophic Terrorism" *Foreign Affairs* 77, No. 6 (November/December 1998): 80-94; and Richard Falkenrath, Robert D. Neuman and Bradley Thayer, Chapter 3 "The Threat of Nuclear, Biological, or Chemical Attack by Non-State Actors" in *America's Achilles' Heel* (Cambridge MA: MIT Press, 1998), 167-216.

[9] This perspective is exemplified by the annual State Department Report, *Patterns of Global Terrorism*.

[10] Robert Kaplan "The Coming Anarchy," *Atlantic Monthly* (February 1994), 44-76; and Martin Van Creveld, “What War is Fought For” *The Transformation of War* (New York: The Free Press, 1991), 124-156.

[11] Walter Laquer, *The New Terrorism: Fanaticism and the Arms of Mass Destruction* (Oxford: Oxford University Press, 1999)

[12] Caleb Carr, "Terrorism as Warfare" *World Policy Journal* 13, No. 4 (Winter 1996-1997): 1-12.

[13] On the general concept of netwar, see John Arquilla and David Ronfeldt, *The Advent of Netwar* (Washington DC: RAND Corporation, 1996). As applied to terrorism, see Arquilla, et al, "Networks, Netwar and Information Age Terrorism."

[14] My analysis of the pros and cons of such an approach are fully elaborated in the forthcoming *Strategic Warfare in Cyberspace* (Cambridge MA: MIT Press, 2000).

[15] Clifford Stoll, *The Cuckoo's Egg* (New York: Simon & Schuster, Inc., 1989) contains an extensive description of the activities, discovery, and eventually apprehension of the hackers involved in this incident.

[16] General Accounting Office, *Computer Security: Hackers Penetrate DOD Computer Systems* (Washington, DC: GAO/T-IMTEC-92-5), 20 November 1991.

[17] See for example, Winn Schwartau, *Cyber Terrorism: Protecting Your Personal Security in the Electronic Age* (New York: Thunder Mouth Press, 1996), especially on pp. 543-544.

[18] This challenge is discussed in Andrew Rathmell, Richard Overill, Lorenzo Valeri and John Gearson, "The IW Threat from Sub-State Groups" in *Proceedings of the Third International Symposium on Command and Control Research and Technology* (Washington, DC: National Defense University, June 1997), 170.

[19] See *Cybercrime, Cyberterrorism and Cyberwarfare: Averting an Electronic Waterloo* (Washington DC: The Center for Strategic and International Studies, December 1998).

[20] Bruce Sterling, *The Hacker Crackdown: Law and Order on the Electronic Frontier* (New York: Bantam Books, 1992), 41-145 provides a lucid description of the hacker culture. Also see Dorothy E. Denning, *Information Warfare and Security* (Reading MA: Addison-Wesley, 1999), 46-50, for a concise summary of empirical studies on hacker motivations.

[21] See Michelle Satalla and Joshua Quittner, *Masters of Deception: The Gang That Ruled Cyberspace* (New York: Harper Collins Publishing, 1995) for descriptions of such activities.

[22] See Nicholas Chantler, "Profile of a Computer Hacker," available at http://www.infowar.com.

[23] See information at www.2600.com/home.html.

[24] “Call in the Goon Squad” C/NET Dispatches, 18 January 1999, available at hongkong1.cnet.com/Briefs/ Dispatches/China/990118/ss02.html.

[25] Associate Press release, “Chinese Cyber Battle: Hackers Put Taiwanese Symbols on Internet Sites” 12 August 1999, available at www.freedomforum.org/international/1999/8/12tapei.asp.

[26] See Jessica Stern, *The Ultimate Terrorists* (Cambridge MA: Harvard University Press, 1999), 74-75. Rathmell, et al, 176.

[27] Denning, 160.

[28] US Congress, Senate, Committee on Governmental Affairs, Testimony of Lopht Heavy Industries on Computer Security, 106th Congress, 2nd Session, 19 May 1998.

[29] See previously cited 2600 web site address.

[30] As examples of such studies see National Research Council, *Computers at Risk*; Defense Science Board Task Force, *Information Warfare—Defense* (Washington DC: Department of Defense, November 1996); President’s Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America’s Infrastructures* (Washington DC: President’s Commission on Critical Infrastructure Protection, October 1997); and Statement of Michael A. Vatis, Director, National Infrastructure Protection Center "NIPC Cyber Threat Assessment" to US Senate, Judiciary Committee, Subcommittee on Technology and Terrorism, 6 October 1999.

[31] This quote was provided in Captain (USN) Richard P. O’Neill’s presentation at an Institute for Foreign Policy Analysis conference on “War in the Information Age,” Cambridge, MA, 15 November 1995.

[32] Anne W. Branscomb, *Rogue Computer Programs—Viruses, Worms Trojan Horses and Time Bombs: Pranks, Prowess, Protection or Prosecution* (Cambridge MA: Harvard University, Program on Information Resources Policy, I-89-3, September 1989), 1-5.

[33] A good analysis is provided by Neil Winton, "Y2K Seen As Possible Cover for Cyberwars" Reuters report on WWW at http://www.zdnet.com/intweek/stories/news/, posted 8 October 1999.

[34] Sterling, *The Hacker Crackdown*, 1-39.

[35] "Pentagon Beats Back Internet Attack" *Wired News*, 10 September 1998 and George I Seffers, "Hackers Take Offense at Pentagon Defense," *Defense News*, September 1998, 1.

[36] Information on this incident and other virus hoaxes can be found on the Internet at the Department of Energy Computer Incident Advisory Capability (CIAC) web site, ciac.llnl.gov.

[37] Chairman of the Joint Chiefs of Staff Memo CM-510-99, "Information Operations Condition," 10 Mar 99 provided the initial directive guidance regarding the establishment of a DoD INFOCON system.

[38] Winn Schwartau "An Introduction to Information Warfare" in Robert L. Pfaltzgraff, Jr. and Richard P. Shultz Jr., eds. *War in the Information Age: New Challenges for US Security* (London: Brassey's, 1997), 58.

[39] This assertion is made in a number of authoritative studies including 1996 Defense Science Board study, *Information Warfare—Defense*, 2-16, and the PCCIP, *Critical Foundations*, 19. This conclusion is also prevalent in the author's discussions with representatives of Software Engineering Institute's Network Survivability and Security Program and CERT Coordinating Center, the Defense Information Systems Agency's Automated Systems Security Incident Support Team (ASSIST), the Air Force Information Warfare Center.

[40] General Accounting Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks* (Washington DC: GAO/AMID-96-84, May 1996), 15.

[41] Arquilla, et al, " Networks, Netwar and Information Age Terrorism," 65-66.

[42] Denning, 68.

[43] See Charles Swett, "The Role of the Internet in International Politics" in Robert L. Pfaltzgraff, Jr. and Richard P. Shultz Jr., eds., *War in the Information Age: New Challenges for US Security* (London: Brassey's, 1997), 292-293; and David Ronfeldt, John Arquilla, Graham Fuller and Melissa Fuller, *The Zapatista Social Netwar in Mexico* (Washington DC: Rand Corporation, 1999).

[44] Phil Williams, "Transnational Criminal Organizations and International Security" *Survival*, Vol 36, No. 1 (Spring 1994), 96-113.

[45] CIWARS Intelligence Report, 4 January 1998, vol. 2, no. 1 published by the Centre for Infrastructural Warfare, available on the Internet at WWW site at www.iwars.org, accessed 10 February 1998.

[46] National Research Council, *Computer at Risk*, 7.

[47] History of US efforts to deal with digital warfare and terrorism is discussed in depth in Chapter Five of my *Strategic Warfare in Cyberspace*.

[48] *Critical Foundations*, 2.

[49] See Office of Science and Technology Policy, *Cybernation: The American Infrastructure in the Information Age* (Washington, DC: The White House, April 1997) for an in-depth analysis of the significance of system complexity related to critical infrastructure protection.

[50] "Activist Hackers Target On-Line Toy Company," *Financial Times*, 19 December 1999.

[51] Richard Behar, "Who's Reading Your E-Mail," *Fortune* (3 February 1997): 64.

[52] Denise Shelton, "Banks Appease On-Line Terrorists" at news.cnet.com, posted 3 June 1996.

[53] The Toxyn hacker group published a call for attacks against Indonesian government sites on their web site at toxyn.pt.eu.org beginning in October 1997. The hacker magazine 2600 posted an example of a modified web page at their site at www.2600.com/east_timor/after.html.

[54] John Markoff, "Airports Told of Flaw in Security System" *New York Times,* 8 February 1998.

[55] See extensive discussion in Fredrick B. Cohen, *Protection and Security on the Information Highway* (New York: John Wiley & Sons, 1995), 33-78.

[56] "Fired Programmer Zaps Old Firm," on the Internet at biz.yahoo.com/upi/98/02/17/general _state_and_regional_news/nyzap_1.htm, accessed 10 March 1998.

[57] Computer Security Institute/Federal Bureau of Investigation, *Computer Crime and Security Survey* (San Francisco: Computer Security Institute, 1999), 4.

[58] Rathmell, 174-5.

[59] Denning, 69.

[60] Statement of Michael Vatis to Senate Judiciary Committee, 6 October 1999.

[61] William Church, *CIWARS Intelligence Report*, 10 May 1998.

[62] The history of US efforts to develop a national response to the threat of digital attacks is detailed in Chapter Five of this author's forthcoming *Strategic Warfare in Cyberspace*.

[63] This information was provided by the National Coordinator for Security, Infrastructure and Counterterrorism, Richard Clarke, at the "Preparing for Cyberwar" Conference, Arlington VA, 5 October 1999.

[64] National Infrastructure Protection Center Fact Sheet, 1999.

[65] The problems confronted by the US government in keeping skilled computer security personnel are illuminated by an article by Elizabeth Shogren, "U.S. Tries to Plug Computer Worker Drain," *Los Angeles Times*, 23 November 1999, 1.

[66] For descriptions of the incident, see Bradley Graham, "11 US Military Computer Systems Breached This Month," *Washington Post*, 26 February 1998, A01; James Glave, "DOD-Cracking Team Used Common Bug," on *Wired Internet* at www.wired.com, accessed 10 May 1998; and James Glave, "Pentagon Hacker Speaks Out," on *Wired Internet* at www.wired.com, accessed 10 May 1998.

[67] See Declan McCullagh, "Surveillance Network Draws Fire" from Wired News Online, 29 July 1999 at www.wired.com/news/news/politics/story/20994.html.

[68] Software Engineering Institute, *Detecting Signs of Intrusion* (Pittsburgh PA: Carnegie Mellon University, August 1997).

[69] See Office of the Staff Judge Advocate, AF Office of Special Investigations, "Computer Crime Investigator's Handbook" (Andrews AFB MD: AF Office of Special Investigations, May 1999) for detailed explanation of these constraints.

[70] This case is strongly stated in the Government Accounting Office study, *Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences* (Washington DC: GAO/AIMD-00-01, 1999). The US Air

Force and the National Research Council have instituted a joint effort to conduct a study along these lines.

[71] Specifics on the IAVA system are provided by Lt. Beth A Evans, Technical Analysis Division Chief, DoD CERT, "DoD's IAVA Process" *IAnewsletter* 3, No. 1 (Summer 1999): 8-9.

[72] A detailed analysis of this tension is provided in Chapter 5 of *Strategic Warfare in Cyberspace*. The debates within the US over encryption policy are fully addressed in Susan Landau and Whitfield Diffie, *Privacy on the Line: The Politics of Wire Tapping and Encryption*, (Cambridge MA: MIT Press, 1998).

[73] An analysis of such approaches in provided in Stephen J. Lusiak, *Public and Private Roles in the Protection of Critical Information-Dependent Infrastructures* (Palo Alto, CA: Stanford University, Center for International Security and Arms Control, March 1997).