INITIATIVES IN THE FIGHT AGAINST CYBER TERRORISM

Kathleen Tolan
Senior Analyst, Electronic Warfare Associates – Canada
55 Metcalfe Street, Suite 1600
Ottawa, Ontario K1P 6L5 Canada
ktolan@ewa-canada.com

Abstract: Cyber terrorism, or a computer-based attack or threat of attack intended to intimidate governments or societies in pursuit of goals that are political, religious, or ideological, has become a real possibility. Shortly after September 11, a Pakistani group hacked into two government web servers, including one at the Department of Defense, and declared a "cyber jihad" against the United States. A second series of attacks known as *Moonlight Maze*, was targeted against the Pentagon, Department of Energy, and NASA and allowed the perpetrators to gained access to technical defense research. Although such attacks have not, as of yet, been terribly sophisticated there is growing concern that this could soon change. There is a school of thought that believes that an enemy using effective information warfare tools and techniques will eventually attack the United States. In the fight against terrorism, the number priority is the prevention of another terrorist attack. With this in mind, this paper addresses three questions: How great is threat of cyber terrorism?; What needs to be done to mitigate the threat?; What initiatives have been undertaken in the fight against cyber terrorism?

Keywords: cyber terrorism, President's Commission on Critical Infrastructure Protection, security, best practices, InfraGard, ISACs

1. INTRODUCTION

Cyber terrorism, or a computer-based attack or threat of attack intended to intimidate governments or societies in pursuit of goals that are political, religious, or ideological, has become a real threat. Shortly after September

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35696-9_19

E. Nardelli et al. (eds.), *Certification and Security in E-Services*

11, a Pakistani group hacked into two government web servers, including one at the Department of Defense, and declared a "cyber jihad" against the United States. An earlier series of attacks known as Moonlight Maze, was targeted against the Pentagon, Department of Energy, and NASA and allowed the perpetrators to gain access to technical defense research. Although such attacks have not, as of yet, been terribly sophisticated there is growing concern that this could soon change. There is a school of thought that believes that an enemy using effective information warfare tools and techniques will eventually attack the United States.

In the fight against terrorism, the number one priority is the prevention of another terrorist attack. With this in mind, this paper addresses three questions:

- How great is threat of cyber terrorism?
- What needs to be done to mitigate the threat?
- What initiatives have been undertaken in the fight against cyber terrorism?

2. THE CYBER TERRORISM THREAT

Before examining the cyber terrorism threat, the first step is to define what is meant by the term cyber terrorism. In a paper presented to the Social Sciences Research Council in November 2001, Professor Dorothy Denning, a recognized expert in the field, explained cyber terrorism as follows:

For a computer-based attack to be considered an act of terrorism the attack should be sufficiently destructive or disruptive to generate fear comparable to that from physical acts of terrorism. Attacks that lead to death or bodily injury, extended power outages, plane crashes, water contamination or major economic losses would be examples. Depending on their impact, attacks against critical infrastructures such as electric power or emergency services could be acts of cyber terrorism. Attacks that disrupt non-essential services or that are mainly a costly nuisance would not be considered as an act of terrorism.[68]

When assessing the threat of cyber terrorism two factors must be considered: first is the existence of vulnerable targets; second, there must be the existence of actors with the capability to carry out acts of cyber terrorism and these same actors must have the motivation or intent to carry out such acts. The section to follow will examine each of these factors.

[68] Denning, Dorothy E. *Is Cyber Terrorism Next?* Paper presented to the Social Sciences Research Council, November 1, 2001.

2.1 Targets Vulnerable to Cyber Terrorism

The information age has changed the dynamic with respect to our dependence on critical infrastructures. Presidential Decision Directive 63, issued in May 1998, defines "critical infrastructures" as "those physical and cyber-based systems essential to the minimum operations of the economy and government." These critical infrastructures include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government (operations). In years past, the infrastructures were largely isolated from one another; there was little risk that a problem in one infrastructure would affect the functioning of another. Information technologies and dependence on cyber systems have altered the equation. For while information technologies create dramatic increases in efficiency and productivity, our dependence on them creates new vulnerabilities.[69]

The United States government has taken an undisputed lead in both studying threats to critical infrastructures and taking action to mitigate these threats. This work began in earnest in 1996 when the President's Commission on Critical Infrastructure Protection was formed. The findings in the Report, published in 1997, highlighted increasing dependence on technology for the nation's security, economic health, and social well-being. All critical infrastructures now rely on computers, advanced telecommunications, and to an ever-increasing degree, the Internet, for the control and management of their own systems, for their interaction with other infrastructures, and for communication with their suppliers and their customer base. [70]

For example, electric power grids and natural gas pipelines are controlled by computer systems, and those computers may be linked to each other and to the company headquarters by publicly accessible telecommunications systems and commercially available information technologies to allow efficient management of power generation and smooth delivery to consumers. Billions of shares are traded each day over the telephone or Internet, and the stock exchanges could not function without their vast networks of computers. Banks no longer rely on their ledger books to account for and secure their holdings, but depend on computerized

[69] White Paper – The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, May 22, 1998.

[70] Critical Foundation – Protection America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection, October 1997, page vii.

accounting systems to manage depositors' accounts. The telecommunications system itself no longer uses operators to manually plug in calls to a switchboard but depends on computerized switching stations to handle the billions of calls placed each day. The government also relies on computers and publicly available communications systems to conduct the nation's business. Public and private networks and databases use the same technology, and vulnerabilities that affect one affect the other.

The price for this reliance on new technologies is a new vulnerability to those who would cause harm. While these new technologies make it easier for companies to communicate and control their businesses, they also make it easier for malicious actors to cause harm. The new vulnerability stems in part from the fact that the Internet and modern telecommunications systems are inherently open and accessible. This means that, with a certain amount of technical skill, one can use these communications media to get inside a company's or a government agency's computer system without ever physically penetrating the four walls. This was the case during Moonlight Maze.[71] In addition, the increased centralization of command and control systems afforded by the new technologies also means that, once inside that system, someone seeking to cause harm can use those same technologies to damage a much broader area than they could have hoped for using physical weapons such as a bomb. These are referred to as "cascading effects" and pose a serious threat to national security.

During the past five years three factors exacerbating this vulnerability have been highlighted. First, most of our infrastructures rely on commercially available, off-the shelf technology. This means that vulnerability in hardware or software is not limited to one company, but it is likely to be widespread, affecting every entity that uses the same equipment. An individual or group with knowledge of this one vulnerability can therefore attack multiple victims across the country, with just a few strokes on the keyboard.

Second, our infrastructures are increasingly interdependent and interconnected with one another. For example, the banking system depends on the availability and reliability of the telecommunication system and the Internet, which in turn rely on electrical power. Our transportation system depends on the availability of gas and oil supplies, which in turn are controlled through the use of new information technologies. The infrastructures are increasingly interdependent, so much so that it is difficult to predict the cascading effects that the disruptions of one infrastructure would have on others.

[71] Moonlight Maze refers to the case of sophisticated and widespread hacks into the Department of Defense (DoD) computer networks by personnel at a Russian Academy of Science. This case received considerable media attention in 1999.

Third, our telecommunications infrastructure is now truly global. Satellite communications, the Internet, and foreign ownership of telecommunications carriers in the United States have all combined to undermine the notion of a "National" Information Infrastructure. This means that geographic isolation no longer acts as a barrier to fend off foreign adversaries. Instead it is now as easy to break into an infrastructure network from anywhere in Europe as right next door to a target. A personal computer and a telephone connection to an Internet Service Provider anywhere in the world are enough to conduct an attack.

From the above it is clear that systems are vulnerable to cyber-attacks. In order to determine the threat of cyber terrorism, the next question that must be answered is: are there actors with the capability and motivation to carry out such attacks?

2.2 Terrorist Group Capabilities and Intent

The opinion of experts on the capability and intent of terrorist groups to conduct acts of cyber terrorism has changed considerably during the past three years. In November 1999, the Center for the Study of Terrorism and Irregular Warfare at the Naval Postgraduate School in Monterey, California issued a report entitled Cyber Prospects and Implications. The report found that a good indicator of a terrorist group's potential for cyber attack is likely to be the degree to which the group is knowledgeable and uses the Internet for communications, management, and intelligence gathering of its own. Equally important are the group's own organizational dynamics. For example, is it a young or old group? Is the group healthy or in decline? Is the group state sponsored? Is the group considered to be innovative or is it staid in its approach? The goal of the study was to assess the prospects of terrorist groups pursuing cyber terrorism. The group concluded that the barrier to entry for anything beyond annoying hacks is quite high, and that terrorists generally lack the wherewithal and human capital needed to mount a meaningful operation. Cyber terrorism, they argued was a thing of the future, although it might be pursued as an ancillary tool.[72]

The Institute of Security Technology Studies (ISTS) released a paper on September 22, 2001 entitled Cyber Attacks During the War on Terrorism: A Predictive Analysis. The ISTS stated that it was unclear whether Osama bin Laden's international al Qaeda organization or other terrorist groups have developed cyber warfare capabilities, or how extensive these capabilities may be. To date few terrorist groups have used cyber attacks as a weapon.

[72] Cyberterror: Prospects and Implications, Center for the Study of Terrorism and Irregular Warfare, Monterey, Ca., Prepared for the Defense Intelligence Agency, November 1999.

However, terrorists are known to be using information technology and the Internet to formulate plans, raise funds, spread propaganda, and communicate securely. For instance the convicted terrorist, Ramzi Yousef, who was responsible for planning the first World Trade Center bombing in 1993, had details of future terrorist plots stored on encrypted files in his laptop computer. At the same time, the September 11, 2001 attacks on the World Trade Center and Pentagon demonstrates an increasing desire by terrorist groups to attack critical infrastructure targets. The World Trade Center attacks not only took lives and property but also closed markets and affected a significant component of the financial information infrastructure in New York City. Thus trends seem to clearly point to the possibility of terrorists using information technology as a weapon against critical infrastructure targets. [73]

While there has been no indication terrorist groups have actually employed cyber tools as weapons to use against critical infrastructures, their reliance on information technology and acquisition of computer expertise are clear warning signs. Up to one year ago, the threat of cyber terrorism was considered to be unclear by some and a thing of the future by others. Prior to September 11, officials said Osama bin Laden's operatives have nothing like the proficiency in information war of the most sophisticated nations. But al Qaeda is now judged to be considerably more capable than analysts believed a year ago. And its intentions are unrelentingly aimed at inflicting catastrophic harm.

One catalyst for this revised view of the capability of terrorist groups was well captured in a Washington Post article published June 27, 2002. This article described the vulnerability of specialized digital devices known as Distributed Control Systems (DCS) and Supervisory Control and Data Acquisition (SCADA) systems that are used to monitor our critical infrastructures. Many companies that control water and energy supplies use standard operating systems such as Windows and Solaris to run their web sites. A malicious user could exploit known vulnerabilities in these operating systems to hack into the utility's server, and then gain access to unprotected SCADA system within its network. This vulnerability caught the attention of officials within the U.S. National Security Community earlier this year. What sparked the interest was that one al Qaeda laptop found in Afghanistan was determined to have made multiple visits to a French site run by the "Societe Anonyme". The site offers a two volume online "Sabotage Handbook" with sections on tools of the trade, planning a hit, switch gear instrumentation, anti-surveillance methods and advanced techniques. In

[73] Institute for Security Technology Studies at Dartmouth University, *Cyber Attacks During the War on Terrorism: A Predictive Analysis,* September 22, 2001, Page 12.

Islamic chat rooms other computers linked to al Qaeda had access to "cracking" tools used to search out networked computers, scan for security flaws and exploit them to gain entry – or full command.[74]

The article went to describe that US investigators found evidence in the logs that mark a browser's path through the Internet that al Qaeda operators spent time on sites that offer software programming instructions for the digital switches that run power, water, transportation and communications grids. In some interrogations, al Qaeda prisoners have described intentions, in general terms, to use those tools. The Chief of Staff of the President's Critical Infrastructure Protection Board stated recently "the US had underestimated the amount of attention that al Qaeda was paying to the Internet. Now we see it as a potential attack vehicle. Al Qaeda spent more time mapping our vulnerabilities then we previously thought. An attack is a question of when, not if." Similarly, in February 2002, the CIA issued a revised Directorate of Intelligence Memorandum. According to officials who read it, the new memo said al Qaeda had "far more interest" in cyber terrorism than previously believed and contemplated the use of hackers for hire to speed the acquisition capabilities.[75]

2.3 Summary

In preparing the above section, the literature reviewed to define the threat of cyber terrorism as well as the capability and intent of terrorist groups to employ such techniques span a very short period of five years. The start point that was used was the publication of the President's Commission on Critical Infrastructure Protection that highlighted the threats to US critical infrastructures and recommended steps that the government should take to eliminate these threats. The capability and intent of terrorist groups to employ cyber terrorism in attacks against the United States has gone from " a thing of the future" in 1999, to something that was unclear in 2001, to a potential attack vehicle in 2002. In short, the vulnerabilities exist, the capability is there and growing, and evidence of intent has surfaced. With that, it is clear that the threat of cyber terrorism is real. The next question that must be addressed is what needs to be done to mitigate the threat.

[74] Gellman, Barton, Washington Post, Thursday, June 27, 2002, Page A1.

[75] *Ibid,* page 3.

3. ACTIONS REQUIRED TO MITIGATE THE THREAT OF CYBER TERRORISM

Before considering what action need to be taken to mitigate the threat of cyber terrorism, it must be recognized that this everyone's problem and the actions taken to reduce the threat is the collective responsibility of the government, private sector, professional organizations, academia, and citizens. There is a considerable amount of literature that provides recommendations on how to deal with the threat of cyber terrorism. In the section that follows five themes will be highlighted. These are:

- Information sharing;
- Following best practices for computer and physical security;
- Recognizing the need for research and development to improve cyber security;
- Coordination among international partners;
- Being on high cyber alert during the War on Terrorism.

3.1 Information Sharing

Information sharing and coordination are key elements in developing comprehensive and practical approaches to defending against cyber attacks, which could threaten national security. The importance of sharing information and coordinating the response to cyber threats among the various stakeholders has increased as our government and out nations have become ever more reliant on interconnected computer systems to support critical operations and infrastructures, such as telecommunications, power distribution, financial services, national defense, and critical government operations.[76] As The Report of the President's Commission on Critical Infrastructure Protection pointed out protecting America's infrastructure is neither an entirely public nor an entirely private interest. Vulnerabilities pose risks to government's business, and citizens alike. Reducing those risks requires a coordinated effort within and between the private and public sectors. The need for infrastructure protection creates a zone of shared responsibility and potential cooperation for industry and government.[77]

Owners and operators have a responsibility to deliver reliable service. Regardless of whom these owners and operators are primarily accountable

[76] United States General accounting Office, *Information Sharing: Practices That Can Benefit Critical Infrastructure Protection*, GAO-02-24, available at www.fas.org.irp/gao.

[77] Critical Foundations – *Protecting America's Infrastructures,* The Report of the President's Commission on Critical Infrastructure Protection, October 1997. Page 35

to, they adopt the procedures necessary to reduce their own vulnerabilities. Government has role in accomplishing these tasks through law enforcement at local, state and federal levels, and national defense and diplomacy. But there is growing need for a new partnership between government and owners and operators to assure our critical infrastructures. Back in 1997, the Commission found that the need to share information was a foundation on which we could build that partnership. With all the events that have occurred during the past five years, including the horrific actions of September 11, 2001, this need for partnerships and information sharing has grown exponentially.[78]

Infrastructure Assurance is essentially a process of risk management. The process is generally defined to include prevention, mitigation, incident management, and recovery. The many functions associated with information assurance fit into these four categories. Two-way sharing of information is indispensable to infrastructure assurance. While infrastructure owners and operators have the fullest appreciation of vulnerabilities, in many instances they have access only to their own information, or in some case information pertaining to their industry or sector. Consequently there is no comprehensive body of knowledge available for effective analysis of overall infrastructure vulnerabilities and threats. This is especially true of vulnerabilities created by the interdependencies of one infrastructure on another. [79]

Establishing effective information sharing mechanisms will allow the government and private sector to establish and enhance systems to coordinate prevention, response, and sharing data as well as warning information. Particularly as the threat of cyber terrorism grows, it is necessary to quickly establish a communication and coordination system between government and the private sector to handle cyber terrorism.[80]

3.2 Following "Best Practices" for Computer and Physical Security

Effective management of information security risks requires that organizations adopt a wide range of "best practices" for maintaining systems. Such best practices include: regular updating of operating systems and software, enforcement of password policies, locking down of systems,

[78] *Ibid,* page 35.

[79] *Ibid,* page 27.

[80] *Ibid,* page 28.

disabling of unnecessary services, installing and updating anti-virus software, and employing intrusion detection systems and firewalls. These practices help organizations reduce their vulnerability to attacks from both outsiders and insiders.[81]

Included in following "best practices" is the need to implement measures for securing critical systems. This includes checking for characters associated with popular web server exploits, using existing authentication mechanisms in border routers, running only recent and secure software in Domain Name Servers, backing up all vital data and storing it off-site, copying and maintaining log records in a secure location, and explaining all measures in an enforceable security policy. [82]

3.3 The Importance of Research and Development to Improving Cyber Security

Improving cyber security is a multifaceted problem. Part of the solution is to ensure that government agencies charged with warning of and responding to the problem, such as the National Infrastructure Protection Center (NIPC), have adequate resources. This has been a significant and ongoing problem. Part of the task also involves creating market incentives for manufacturers to build security into products from the ground up. This can be done in part through government purchases, but the biggest incentive of all is consumer demand - when consumers demand better security, manufacturers will respond accordingly.

In his testimony in September 2001, Michael Vatis, stated that perhaps the most important thing of all in mounting a good defence is the task of researching and developing new technology to secure the information infrastructure against attacks. As Mr. Vatis pointed out, security was never a primary consideration when the Internet was designed. This has resulted in the foundation of our information infrastructure being embedded with vulnerabilities that make it inherently susceptible to attacks. As the Internet grows exponentially, the vulnerability grows, as do the number of people with the capability and intent to exploit these vulnerabilities. The ultimate solution, then, lies in developing technology that builds in security from the ground up. This specifically entails security features that render networks more resistant, robust, and resilient in the face of attacks.

[81] *Fighting Cybercrime: Efforts by Private Business Interests.* Testimony of Dave McCurdy, President of Electronic Industry Alliance before the Subcommittee on Crime of the House Judiciary Committee, June 14, 2001.

[82] Vatis, Michael A. *op cit*

Much work is currently underway in the private sector to develop new virus detection software, firewalls, and the like. But commercial research is largely focused on existing threats and near-term, profit-making developments. There is an ongoing requirement for research that can look at the mid- and long-term threats. Research to develop technologies, for which there may be little commercial incentive, may be vital to protecting the computer networks that underpin our economy and our national security. As the White House Office of Science and Technology Policy (OSTP) emphasized a year ago: "The Federal government and the private sector are now making substantial investments in cyber security technologies. However, neither the private nor public sectors are adequately elucidating the fundamental principles that underlie complex, interconnected infrastructures, or developing key technologies or analytical methodologies crucial to protecting the information infrastructure. Therefore, government becomes the only realistic underwriter to ensure that these technologies are developed." [83]

3.4 International Cooperation

The ability of any nation to assure homeland security clearly relies on the full participation and support of international partners. The I Love You virus, which surfaced in May 2000, provides a good example that a typical cyber investigation can involve victim sites in multiple states and often many countries, and can require tracing a trail of evidence that crosses numerous states and international boundaries. Even intrusions into a country's systems by a perpetrator operating within that country often require international investigative activity because the attack is routed through Internet Service Providers located in another country. When a computer crime is committed against a country by a perpetrator overseas, the victim country must depend on international support to investigate the crime. In a Statement for the Record given by Ronald Dick, Director of the National Infrastructure Protection Center, the special problems posed by international investigations were addressed. First, many countries lack the substantive laws that specifically address computer crimes. This means that those countries often lack the authority not only to investigate or prosecute computer crimes that occur within their borders, but also to assist when evidence might be located in those countries. In addition, the quickly evolving technological aspects of these investigations can exceed the capabilities of local police forces in some countries. Finally, even when countries have the requisite laws and have developed the technical expertise necessary to conduct cyber investigations,

[83] *Ibid*

successful investigation in this arena requires a much faster response than has traditionally been the case in international matters, because electronic evidence is perishable and, if not secured quickly, can be lost forever.[84]

The need for international cooperation was further highlighted in a report published in August. The report cited a series of tests conducted by the NIPC and Pacific Northwest Economic Region called the "Blue Cascades" project. The goal of the project was to assess the preparedness of the region" critical infrastructure systems and how an attack on one sector would impact others. More than 150 representatives from 70 private and public sector organizations – including Bonneville Power Administration, British Columbia Gas, PG&E, the US Navy, Telus, Verizon and Qwest participated. Members of the group formulated scenario where terrorists physically attacked electrical power grids and the region had no electricity for extended periods of time. The findings of the project were that critical infrastructure operators lack key information nor did they have plans to disseminate key information. One of the recommendations that came out of the report was that United States and Canada must increase collaborative efforts to share aid and resources, as well as to develop a North America threat alert system and common technology to respond to incidents.[85]

Despite these obstacles, cyber crimes know no boundaries. Understanding the impediments to international cooperation is the essential first step. These include diplomatic, political, legal, and cultural. Once these issues have become fully understood, mechanisms must be put in place to foster a spirit of international cooperation.

3.5 Being on High Cyber Alert During the War On Terrorism

Fifteen days after the terrorist attacks in Washington and New York last September, Michael Vatis, Director of the Institute for Security Technology Studies made a Statement for the Record before the House Committee on Government Reform Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations. The Statement entitled Cyber Terrorism: The State of US Preparedness made a number of

[84] Statement for the Record of Ronald L. Dick, Director, National Infrastructure Protection Center, Federal Bureau of Investigation on Cyber Terrorism and Critical Infrastructure Protection, before the House Committee on Government Reform, Government Efficiency, Financial Management and Intergovernmental Relations Subcommittee, Washington, D.C. July 24, 2002.

[85] Sirhal, Maureen, *Critical Infrastructure Operators Lack Key Information*, National Journal's Technology Daily, August 13, 2002.

recommendations on actions to follow in the effort to prevent cyber terrorism. The first recommendation was for system administrators and government officials to be on high alert for the warning signs of hostile cyber activity, particularly during periods immediately following military strikes. This recommendation follows an observed trend that cyber attacks often accompany regional and global conflicts, both armed and unarmed and often immediately accompany physical attacks.[86]

It was further recommended that any observed changes in "normal" scanning activity should be considered suspicious and reported to the appropriate authorities. Logging levels should be temporarily raised to trap as many events as possible. Anything suspicious should be reported to enable law enforcement and/or counterintelligence investigations to allow for the issuance of specific warnings by appropriate entities to other potential victims. Systematic and routine risk assessments should be undertaken, and incident management plans should be developed, and law enforcement contact numbers should be readily available in case of an attack.[87]

3.6 Summary

The first section of this paper concluded that the cyber threat is real and growing. The section above sought to address some of the actions that must be taken to mitigate the threat. The focus of this discussion was on five themes. While establishing mechanisms for sharing information, exercising best practices, understanding the need for research and development, international cooperation, and being on high cyber alert are all very important, the requirements do not end here. Just as our understanding of the magnitude of the threat is evolving, all the necessary actions needed to mitigate the threat are still coming to light. During the past five years, much work has been in the fight against cyber terrorism. Some initiatives will be discussed in the section that follows.

[86] Examples of this are quoted in Denning, Dorothy, *Activism, Hacktivism and Cyber Terrorism The Internet as a Tool for Influencing Foreign Policy.* Paper presented at the Information Technology and American Foreign Policy Decision-making Workshop, April 2000.

[87] Statement for the Record of Michael A. Vatis, Director of the Institute for Security Technology Studies at Dartmouth College on *Cyber Terrorism: The State of U.S. Preparedness*, before the House Committee on Government Reform Subcommittee on Government Efficiency, Financial Management ad Intergovernmental Relations, September 26, 2001.

4. ACTIONS TAKEN IN THE FIGHT AGAINST CYBER TERRORISM

Before looking at specific examples of actions taken in the fight against cyber terrorism, it should be noted that this discussion will in no way be all-inclusive. This section will rather highlight some of the progress that has been made and demonstrate that this is a threat that is being taken seriously by the public and private sector, members of the academic community, and concerned citizens.

4.1 Information Sharing Initiatives

The need to share information within the government and between the private and public sector has been discussed at length since The Report of the President's Commission was published. The critical need for information sharing has never been clearer than since September 11. There are many impediments to information sharing not the least of which are legal, cultural, and lack of confidence. Despite these obstacles many successful vehicles have been established to allow for the sharing of information. Where some of the progress has been the greatest in information sharing include the publication of watch and warning products Interagency cooperation within the Federal government, the InfraGard Program, Information Sharing and Analysis Centers Interagency Coordination between the federal government and international partners.

In the section to follow, three initiatives will be discussed. These are the InfraGard Program, Information Sharing and Analysis Centers, and Watch and Warning Programs.

4.2 The InfraGard Program

The InfraGard program is a U.S. nationwide initiative that grew out of a pilot program started at the Cleveland FBI field office in 1996. Nationally, InfraGard has over 5000 members and it is by far the most extensive government-private sector partnership for infrastructure protection in the world. The program particularly benefits small businesses, which have nowhere else to turn for assistance. InfraGard expands direct contacts with the private sector infrastructure owners and operators and shares information about cyber intrusions and vulnerabilities through the formation of local InfraGard chapters within the jurisdiction of each of the 56 FBI Field Offices. InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a cooperative undertaking between the U.S.

Government and an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to increasing the security of United States critical infrastructures. The goal of InfraGard is to enable information flow so that the owners and operators of infrastructure assets can better protect themselves and so that the United States government can better discharge its law enforcement and national security responsibilities.[88]

4.3 Information Sharing and Analysis Centers (ISACs)

Another successful initiative underway in the fight against cyber terrorism are information sharing and analysis centers (ISACS). The creation of ISACS was called for in PDD 63. An ISAC is a one-stop clearinghouse for information on cyber and physical threats, vulnerabilities and solutions. Membership in an ISAC allows a company to better understand the threats and vulnerabilities to their business and anonymously receive near time updates and take advantage of 24/7 incident response consulting fròm leading industry experts. There are currently eleven ISACs operational for the following sectors: electrical power, telecommunications, information technology, water, surface transportation, oil and gas, emergency fire, food, the chemical industry, emergency law enforcement, and interstate.

4.4 Watch and Warning Products

One of the most effective ways to mitigate threats is to provide early warning. Assessments, advisories, and alerts are provided to keep members of both the public and private sectors aware of any threats and vulnerabilities. These products are published by a number of sources including the National Infrastructure Protection Center, FedCIRC, the National Communications System, and the Computer Emergency Response Team Coordination Center at Carnegie Mellon University.

4.5 Best Practices

There are many initiatives underway to promote and encourage the best practices for computer and information technology security. The one that will be highlighted is the release earlier this month of the Organization for Economic Co-operation and Development (OECD) Guidelines for the

[88] Statement for the Record of Ronald Dick Statement for the Record of Ronald L. Dick, Director, National Infrastructure Protection Center Federal Bureau of Investigation before the Senate Committee on Governmental Affairs on Critical Infrastructure Information Sharing, May 8, 2002.

Security of Information Systems and Network. This represents the first time in 10 years that the 30 member inter-governmental group has updated its cyber-security guidelines. The new principles seek to recognize the growing reliance on information networks and the increasing number of threats against the security of those networks. The guidelines call for a culture of security to be developed in all aspects of information systems, from designing and planning through everyday use, and among all participants, from governments down through business and consumers.[89]

4.6 Efforts in Research and Development

In his Statement for the Record last September, Michael Vatis spoke of the importance of developing a national research and development and the value that this would provide to the United States. While there are currently numerous research activities underway on cyber security in academia, industry, and the government, there has, to date, been no comprehensive agenda developed, based on the input of all the relevant experts, to assign priority to the principle requirements. The need for such an agenda has been emphasized by numerous government and private sector organizations that have studied the problem, including the OSTP, the National Security Council, the President's Commission on Critical Infrastructure Protection, and the Partnership for Critical Infrastructure Security.

While there is no unified national approach, there are a number of research and development initiatives in progress. Two of these initiatives will be highlighted. On May 14, 2002, George Mason University's law school, along with James Madison University, announced they have teamed up to launch the Critical Infrastructure Protection Project. The major task of this group will be to coordinate the government agencies that are tracking cyber terrorism threats, then coordinate them with private sector entities in the Internet, financial and telecom industries in an effort to assess exactly how the country should protect its mission-critical computer networks. The program is also working with legal experts at George Mason Law School to determine what policies it should recommend to the federal government and business to protect computer infrastructures throughout the country.[90]

[89] Organization for Economic Co-operation and Development, *OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security,* August 2002. http://www.oecd.org/pdf/M00033000/Mooo33182.pdf.

[90] Krady, Martin *Mason, Madison Universities Team to Combat Cyber Terrorist,* Washington Business Journal, May 14, 2002.

Second, the work of the ISTS has had a significant impact. Recognizing that research and development of technology to enhance cyber security and protect the information infrastructure is too large a task for one institution, and that the expertise is located in many places across the country, the ISTS is working on some very interesting partnerships. One major goal of the ISTS is to establish a collaborative community of focused research among numerous universities, private companies, and government agencies nationwide. A significant percentage of ISTS's first-year work has taken place outside of Hanover, New Hampshire, at places like George Mason University in Fairfax, Virginia; Los Alamos National Laboratories and Sandia National Laboratories in New Mexico; Harvard University in Cambridge, Massachusetts; the University of Massachusetts; Columbia University in New York City; the University of California at Santa Barbara; the University of Michigan; the University of Tulsa; and BBN Technologies of Cambridge, Massachusetts. During its second year, the ISTS set a goal of expanding its collaborations by establishing research partnerships with other notable academic centers of excellence in the computer security and counter terrorism field.[91]

Beyond this research, the ISTS is also in the process of establishing a consortium with other academic centers of excellence, which would form a "virtual" institute for information infrastructure protection. This institute, which will be called the Institute for Information Infrastructure Protection (or "I3P"), is based on the recommendations of several expert groups over the last three years including the President's Committee of Advisors on Science and Technology (PCAST). A number of studies published called for a cyber security R&D institute, whose mission would be first to develop a national R&D agenda for information infrastructure protection, which would identify the priority R&D needs; and second, fund research directed at those needs.[92]

4.7 International Coordination

The United States Government is working international partners on several fronts. The first area consists of outreach activities designed to raise awareness about the cyber threat, encourage countries to address the threat through substantive legislation, and provide advice on how to deal with the threat most effectively. Watch connectivity has been established between Canada, the United States, the United Kingdom, Sweden and New Zealand. In addition, Canada and the United Kingdom have each detailed a person on

[91] Michael Vatis, Statement for the Record, *op cit.*

[92] *Ibid*

a full-time basis to the NIPC, and Australia detailed a person for six month in 2001. Finally, there is an initiative underway in the State Department to develop and implement a strategy for information sharing in the critical infrastructure protection arena.

4.8 Summary

The examples provided above are by no means an exhaustive list of initiatives that are currently underway. The programs and initiatives outlined were chosen in order to demonstrate that this is a problem that is being taken extremely seriously. During the second half of the 1990s actions that needed to be taken to protect our critical infrastructures were very well defined. During the first twenty months of this century actions to mitigate the threat have been undertaken by the public sector, the private sector, academia and international organizations. Everyone is making an effort to understand the threat and reduce the vulnerability.

5. CONCLUSION

Three questions were posed at the outset of this paper: The first asked how great is the threat of cyber terrorism? The conclusion that was reached is that the threat is real and growing, the vulnerability exists, the capability of those who would do us harm is present and evidence of intent is surfacing.

The second question posed was what needs to be done to mitigate the threat. The themes that emerged during this section were that the threat posed by cyber terrorism is shared among the public sector, the private sector, the international community, academia, and individual citizens. Similarly, the actions that must be taken to mitigate this threat are shared among these entities. In order to reduce the threat, education and outreach are essential, forming collaborative relationships, developing the mechanisms to share the information, and using best practices are essential.

In the introduction the point was made that the number one priority in the fight against terrorism is the prevention of another terrorist attack. Since 1997 tremendous progress has been made in defining the threat, understanding the magnitude, identifying required actions, and putting into place the necessary programs. The consequences of cyber terrorism would impact all individuals at all levels. Through many of the initiatives that have been undertaken by all those who are concerned, the awareness has been raised and efforts to mitigate the threat are well underway.

REFERENCES

Crude, Martin Mason, Madison Universities Team to Combat Cyber Terrorist, Washington Business Journal, May 14, 2002.

Defense Intelligence Agency, Cyberterror: Prospects and Implications, Center for the Study of Terrorism and Irregular Warfare, Monterey, Ca., November 1999.

Denning, Dorothy E. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. Paper presented at the Information Technology and American Foreign Policy Decision Making Workshop, April 2, 2000. http://www.com/class_2/00/class2_020400b_i.shtml.

Denning, Dorothy E. Is Cyber terrorism Next? Paper presented to the Social Sciences Research Council, November 1, 2001

Gellman, Barton, Washington Post, Thursday, June 27, 2002, Page A1.

Institute for Security Technology Studies at Dartmouth University, Cyber Attacks During the War on Terrorism: A Predictive Analysis, September 22, 2001.

Krady, Martin, Mason, Madison Universities Team to Combat Cyber Terrorist, Washington Business Journal, May 14, 2002.

Organization for Economic Development, OECD Guidelines for the Security of Information Systems and Networks, August 2002

Report of the President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Critical Infrastructures, October 1997.

Sirhal, Maureen, Critical Infrastructure Operators Lack Key Information, National Journal's Technology Daily, August 13, 2002.

Statement for the Record of Michael A. Vatis, Director of the Institute for Security Technology Studies at Dartmouth College on Cyber Terrorism: The State of U.S. Preparedness, before the House Committee on Government Reform Subcommittee on Government Efficiency, Financial Management ad Intergovernmental Relations, September 26, 2001

Statement for the Record of Ronald L. Dick, Director, National Infrastructure Protection Center, Federal Bureau of Investigation on Cyber Terrorism and Critical Infrastructure Protection, before the House Committee on Government Reform, Government Efficiency, Financial Management and Intergovernmental Relations Subcommittee, Washington, D.C. July 24, 2002.

Statement for the Record of Ronald L. Dick, Director, National Infrastructure Protection Center, Federal Bureau of Investigation Before the Senate Committee on Governmental Affairs on Critical Infrastructure Information Sharing, May 8, 2002.

Testimony of Dave McCurdy, President of Electronic Industry Alliance before the Subcommittee on Crime of the House Judiciary Committee, Fighting Cybercrime: Efforts by Private Business Interests. Fighting Cybercrime: Efforts by Private Business Interests. June 14, 2001.

United States General Accounting Office, Information Sharing: Practices That Can Benefit Critical Infrastructure Protection, GAO-02-24, available at www.fas.org.irp/gao.

White Paper – The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, May 22, 1998.