Impact of Cyberterrorism in digital world

Prof. Soumen Ganguly,
Professor,
FTMS Global Academy Pte Ltd, Singapore.
e-mail: soumen012003@gmail.com

Abstract— **There are many forms of terrorism on the Internet. Some are not dangerous enough to be deemed a simple spread of information instead of terrorism. They are simple show of skill and are harmless. Acts of cyber-crimes may involve stealing of money, company secrets, or attacking country's infrastructure and causing real damage. Cyber terrorism is an impending threat to the United States, or any other technologically advanced country. Even nations with more primitive technology can be negatively affected by the "ripple effect". With the excess of technology increasing at a tremendous rate, the threat of cyber terrorism will only get worse. This article provides analysis on definition, methodologies, participants and different forms of protection against cyber terrorism.**

Keywords- Cyber Terrorism, Security, Internet, Computer Viruses, Cryptography

I. TERRORISM TO CYBERTERRORISM

The definition of "terrorism" has been well studied, defined, and documented. There is also a degree of understanding of the meanings of CyberTerrorism, either from the popular media, other secondary sources, or personal experience. This paper examines the future of CyberTerrorism - a term the author coined a decade ago, as the indicia of technological dependence and frailty were forming in our New World disOrder. Indeed, that future has come to fruition, today.

The face of terrorism is changing. While the motivations remain the same, we are now facing new and unfamiliar weapons. The intelligence systems, tactics, security procedures and equipment that were once expected to protect people, systems, and nations, are powerless against this new, and very devastating weapon. Moreover, the methods of counter-terrorism that our world's specialists have honed over the years are ineffectual against this enemy. Because, this enemy does not attack us with truckloads of explosives, nor with briefcases of Sarin gas, nor with dynamite strapped to the bodies of fanatics. This enemy attacks us with one's and zero's, at a place we are most vulnerable: the point at which the physical and virtual worlds converge.

Let us first define theses two domains.

The Physical World

The physical world is matter and energy - light, dark, hot and cold, all physical matter - that place in which we live and function.

The Virtual World

The virtual world is symbolic - true, false, binary, metaphoric representations of information - that place in which computer programs function and data moves.

The physical and virtual worlds are inherently disparate worlds. It is now the intersection, the convergence, of these two worlds that forms the vehicle of CyberTerrorism, the new weapon that we face.

A) Cracker or CyberTerrorist?

A great deal of "cracks" are committed for the purposes of anarchy, humor, or as often stated by the perpetrators, "to be annoying." However, is this the mindset of a CyberTerrorist? Does the CyberTerrorist make a garage door go up and down? Does he change an Internet web site to say a country's government is evil? Does he hack into a major corporation's voice mail system to make long distance calls? No - that is not the domain of the CyberTerrorist - that is the domain of the amateur cracker community that exists worldwide.

A CyberTerrorist's mindset is quite different. A CyberTerrorist would not alter a voice mail, or even abuse credit cards.

B) Examples of Cyber-Terrorism

By using the Internet, the terrorist can influence much wider harm or change to a country than one could by killing some people. From immobilizing a countries military

defense to shutting off the power in a large area, the terrorist can have an effect on more people at less danger to him or herself, than through other means.

Cyber terrorism takes many forms; following are some examples of cyber-terrorism in its many forms:

1. Cyber-terrorists often commit acts of terrorism purely for private gain. Such a group, known as the Chaos Computer Club, was exposed in 1997. They had formed an Active X Control for the account. Without difficulty, this could be used to steal money from users all over the world that have the Quicken software installed on their computer. This type of file is only one of thousands of types of viruses that can do everything from simply annoy users, to disable large networks, which can have disastrous, even life and death, results.

2. Cyber-terrorist is interested in gaining publicity in any probable way. For example, information warfare procedures like Trojan horse viruses and network worms are repeatedly used to not only do harm to computing resources, but also as a way for the designer of the viruses to "brag." This is a serious moral issue

because many people are affected by these cases. The viruses can use system resources until networks become ineffective, costing companies lots of time and money. In addition, depending on the type of work done on the affected computers, the damage to the recipients of that work could be lethal; it could have unpredictable effects that could have dreadful consequences.

3. In one of its more remarkable forms, cyber-terrorism can be used for a murder. In one case, a mafia boss was shot but survived the shooting. That night while he was in the hospital, the assassins hacked into the hospital computer and altered his medicine so that he would be given a lethal injection. He died a few hours later. Then they changed the prescription order back to its accurate form, after it had been incorrectly dispensed, to cover their tracks so that the nurse would be blamed for the "accident".

4. Terrorism can also come in the shape of misinformation. Terrorists can repeatedly say what they please without fear of retaliation from authorities or of answerability for what they say. The rumor that a group of people was stealing people's kidneys for sale was spread via the Internet. The report unnerved thousands of people.

5. Small strikes come in the form of "data diddling", where information in the computer is distorted. This may involve altering medical or financial account or stealing of passwords. Hackers may even prevent users who should have access from gaining access to the machine help because the computer would not allow the necessary access for the doctor to save his or her life.

C) Potential CyberTerrorist Acts

Let us examine some example CyberTerrorist acts. Based on the definitions of terrorism, a determination can be made if they in fact constitute terrorism:

• A CyberTerrorist will remotely access the processing control systems of a cereal manufacturer, change the levels of iron supplement, and sicken and kill the children of a nation enjoying their food. That CyberTerrorist will then perform similar remote alterations at a processor of infant formula. The key: the CyberTerrorist does not have to be at the factory to execute these acts.

• A CyberTerrorist will place a number of computerized bombs around a city, all simultaneously transmitting unique numeric patterns, each bomb receiving each other's pattern. If bomb one stops transmitting, all the bombs detonate simultaneously. The keys: 1) the CyberTerrorist does not have to be strapped to any of these bombs; 2) no large truck is required; 3) the number of bombs and urban dispersion are extensive; 4) the encrypted patterns cannot be predicted and matched through alternate transmission; and 5) the number of bombs prevents disarming them all simultaneously. The bombs will detonate.

• A CyberTerrorist will disrupt the banks, the international financial transactions, the stock exchanges. The key: the people of a country will lose all confidence in the economic system. Would a CyberTerrorist attempt to gain entry to the Federal Reserve building or equivalent? Unlikely, since arrest would be immediate. Furthermore, a large truck pulling along side the building would be noticed. However, in the case of the CyberTerrorist, the perpetrator is sitting on another continent while a nation's economic systems grind to a halt. Destabilization will be achieved.

• A CyberTerrorist will attack the next generation of air traffic control systems, and collide two large civilian aircraft. This is a realistic scenario, since the CyberTerrorist will also crack the aircraft's in-cockpit sensors. Much of the same can be done to the rail lines.

• A CyberTerrorist will remotely alter the formulas of medication at pharmaceutical manufacturers. The potential loss of life is unfathomable.

• The CyberTerrorist may then decide to remotely change the pressure in the gas lines, causing a valve failure, and a block of a sleepy suburb detonates and burns. Likewise, the electrical grid is becoming steadily more vulnerable.

In effect, the CyberTerrorist will make certain that the population of a nation will not be able to eat, to drink, to move, or to live. In addition, the people charged with the protection of their nation will not have warning, and will not be able to shut down the terrorist, since that CyberTerrorist is most likely on the other side of the world.

Sadly, these examples are not science fiction. All of these scenarios can be executed today. As you may know, some of these incidents already have occurred in various nations. More of such acts will take place tomorrow. Are you prepared?

D) CyberTerrorists: Who, Where, and Why?

The purpose of this paper is to help you understand the threats that exist, and hopefully, to help you prevent these types of atrocities. But know this - there are people out there with very different goals, who are our real threats, and who are, or will be, attacking us. Make no mistake, the threats are real, today.

Who are the CyberTerrorists? There a great many poor movies and too many works of fiction about the hacker and cracker communities. In the popular media, there recently was the Kevin Mitnick incident, where one cracker broke into another cracker's systems. This spawned endless press and at least two best selling books. While this incident received much attention, the events amounted to meaningless children's games.

By and large, the cracker community, based primarily in the United States, Europe, the Middle East, Asia, and in the nations of the former Soviet Union, is composed of individuals who see the cracking process merely as a challenge, a brain teaser, a puzzle. They view themselves as not only being innocent of any crime, but perhaps even doing something righteous, something to counter the dark monoliths of the corporate and government worlds. They believe they are being persecuted. These individuals believe that what they are doing is not doing any true damage. At its least harmful, these crackers just look at information. However, privacy issues and military secrecy can render such infiltrations acts of terror.

Sometimes crackers make minor changes, just for fun, to be annoying, or to make a statement. The potential for damage here is enormous.

E) Why do they use cyber attacks?

Cyber terrorist prefer using the cyber attack methods because of many advantages for it.

- It is Cheaper than traditional methods.
- The action is very Difficult to be tracked.
- They can hide their personalities and location.
- There are no physical barriers or check points to cross.
- They can do it remotely from anywhere in the world.
- They can use this method to attack a big number of targets.
- They can affect a large number of people.

F) What can they do?

On Oct. 21, 2002, a distributed denial of service (DDOS) attack struck the 13 root servers that provide the primary road-map for all internet communications. Nine servers out of these thirteen were jammed. The problem was taken care of in a short period of time.

According to Kevin Coleman (Oct. 10, 2003) the internet being down for just one day could disrupt nearly $6.5 billion worth of transactions. At Worcester, Mass, in 1997, a hacker disabled the computer system of the airport control tower.

In the same year a hacker from Sweden jammed the 911 emergency telephone system in the west-central Florida. This indicates that an attck could be launched from anywhere in the world.In 1998 attacks were launched against the NASA, the Navy, and the Department of Defense computer systems. In 2000, someone hacked into Maroochy Shire, Australia waste management control system and released millions of gallons of raw sewage on the town. In Russia In the year 2000, a hacker was able to control the computer system that govern the flow of natural gas through the pipelines.

Financial institutions have been subject to daily attacks or attack attempts. They are the most preferable targets for cyber criminals.

The Israeli cyber warfare professionals targeted human rights and anti-war activists across the U.S.A in late July and August 2002 disrupting communications, harassing hundreds of computer users, and annoying thousands more.

G) The danger of cyber terrorism:

General John Gordon, the White House Homeland Security Advisor, speaking at the RSA security conference in San Francisco, CA Feb. 25, 2004 indicated that whether someone detonates a bomb that cause bodily harm to innocent people or hacked into a web-based IT system in a way that could, for instance, take a power grid offline and result in blackout, the result is ostensibly the same. He also stated that the potential for a terrorist cyber attack is real.

In their paper, Jimmy Sproles and Will Byars said: "By the use of the internet the terrorist can affect much wider damage or change to a country than one could by killing some people. From disabling a countries military defenses to shutting off the power in a large area, the terrorist can affect more people at less risk, than through other means".

Cyber terrorists can destroy the economy of the country by attcking the critical infrastructure in the big towns such as electric power and water supply, still the blackout of the North Western states in the US in Aug. 15, 2003 is unknown whether it was a cterrorist act or not, or by attckig the banks and financial institutions and play with their computer systems.

Senator Jon Kyl, chairman of the senate judiciary subcommittee on terrorism, technology and homeland security mentioned that members of al-Qaeda have tried to target the electric power grids, transportation systems, and financial institutions.

In England the National High-Tech Crime Unit (NHTCU) survey showed that 97% of the UK companies were victims to cyber crime during the period from June 2002 to June 2003. Cyber terrorists can endanger the security of the nation by targeting the sensitive and secret information (by stealing, disclosing, or destroying).

H) Efforts of combating cyber terrorism

The Interpol, with its 178 member countries, is doing a great job in fighting against cyber terrorism. They are helping all the member countries and training their personnel.

The Council of Europe Convention on Cyber Crime, which is the first international treaty for fighting against computer crime, is the result of 4 years work by experts from the 45 member and non-member countries including Japan, USA, and Canada. This treaty has already enforced after its ratification by Lithuania on 21st of March 2004.

The Association of South East Asia Nations (ASEAN) has set plans for sharing information on computer security. They are going to create a regional cyber-crime unit by the year 2005.

I) Crackers as Facilitators

Individuals with a background in intelligence are aware that a frequent element of case execution is enlisting the indigenous, sometimes called "facilitators," to assist in a campaign. At the convergence of the physical and virtual worlds, the indigenous are the crackers.

There is the incorrect assumption in the cracking community that they, the crackers, are so sophisticated or so knowledgeable as to know when they are being approached for a truly illicit reason (e.g., to be enlisted as a facilitator to commit an act of terrorism). However, despite cracker arrogance, these individuals are easy targets for enlistment.

What about those crackers who actively wish to cross the line, or more basically, need money? To a teenager, a $1,000 U.S. can purchase a good many compact disks, a new modem, and a great deal of libation. Beyond youths, there are professionals in this arena as well.

Historically, individuals engaged in the practice of terror tended not to be people working upon a computer 20 hours per day. Terrorists have not been in the business of tracking the latest holes found in UNIX or an obscure government telnet opportunity. There are people, however, who are in that business - for illicit as well as good cause. As stated, just as indigenous people may be turned into soldiers, so can crackers be turned into CyberTerrorists. Sometimes such a transition may be motivated by money or prestige. Usually, this transition will occur without the cracker's cognizance. The potential threat from such transitions is mind boggling, considering the damage even one mis-directed cracker can cause.

Further, as young, educated people are brought into the folds of terrorist groups, this new generation will have the talent to execute the acts of CyberTerrorism of which we have spoken.

We are going to see increasing levels of in-house expertise, and concomitant exponential increases CyberTerrorism. Unlike other methods of terrorism, CyberTerrorism is safe and profitable, and difficult to counter without the right expertise and understanding of the CyberTerrorist's mind. Combine our increasing vulnerability, with the explosive increases in the level of violence, and increasing expertise available inside terrorist organizations through new blood and outside through facilitators, and we can see that at the point where the physical and virtual worlds converge, the old models of managing terrorism are obsolete.

II. ESTATISTICS ON CYBER - TERRORISM

A) Who is at risk of an attack?

Most feel that military installations, power plants, air traffic control centers, banks and telecommunication networks themselves are the most likely targets. Other targets include police, medical, fire and rescue systems, which could be hurt, along with Wall Street, water systems, etc.

B) Who are the terrorists?

The graphic below shows that amateur hackers are by far the biggest threat on the Internet at the current time. They are responsible for about 90% of all hacking activity.

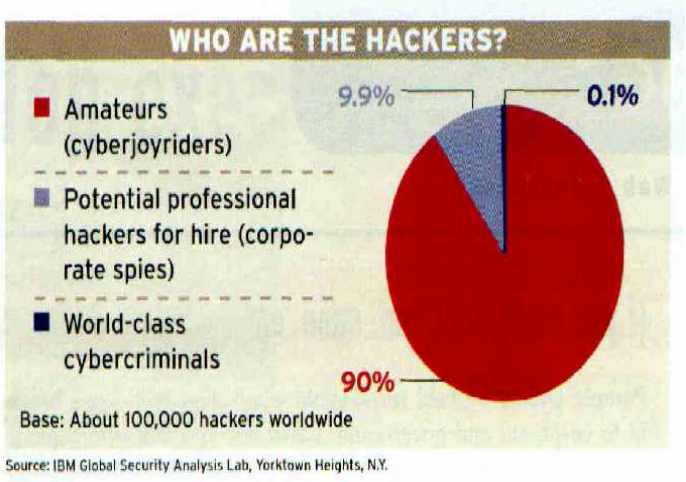

Figure 1: Source from IBM Global – Security Analysis

Cyber terrorism does not have to come from the average hacker or even online terrorists. The Govt. carried out a series of its own attacks on itself, in order to test its own defenses against online-based attacks. The Defense Information Security Agency (DISA) found that 88% of the 3000 defense computer systems that were attacked were "easily penetrable". Of the systems that were illegally entered, 96% of the entries were not detected. Of the 4% that were detected, only 5% of them were reported or investigated.

C) How common is unauthorized system entry?

A survey conducted by the Science Applications International Corp. in 1996 found that 40 major corporations reported losing over $800 million to computer break-ins. An FBI survey of 428 government, corporate and university sites found that over 40% reported having been broken into at least once in the last year. One third said that they had been broken into over the Internet. Another survey found that the Pentagon's systems that contain sensitive, but unclassified information, had been accessed via networks illegally 250,000 times and only 150 of the intrusions were detected. The FBI estimates that U.S. businesses loose $138 million every year to hackers. According to the CIA in the past three years government systems have been illegally entered 250,000.

D) Costs of cyber-terrorism

According to a source in Great Britain, terrorists have gained at least up to 400 million pounds from 1993 to 1995 by threatening institutions. Over the three years, there were 40 reported threats made to banks in the U.S. and Britain. In January of 1993, three separate incidents took place in London. During the sixth, a brokerage house paid out 10 million pounds after receiving a threat and one of their machines crashed. On the fourteenth incident, a blue-chip bank paid blackmailers 12.5 million pounds after receiving threats. Another brokerage house paid out 10 million pounds on the twenty-ninth incident. Some terrorists just take money, rather than resorting to blackmail. A Russian hacker, for example, tapped into Citibank's funds transfer system and took $10 million.

E) Methods of Protection: No Easy Answers

We must consider the following elements when building a counter-CyberTerrorist program:

- We must accept that while the theories of terrorism stand true, the way in which we approach counter-terrorism, in this case, counter-CyberTerrorism, must change.
- We must cooperate and share intelligence in ways we have never have before.
- We must enlist the assistance of those individuals who understand the weapons we are facing and have experienced fighting these wars.
- We must learn the new rules, the new technologies, and the new players.

Unfortunately, one cannot learn how to fight this very unconventional warfare from someone who hasn't been there, nor from someone whose experience is in the old ways and old technologies. The old data processing, auditing, and computer security models in use today are obsolete. On this battlefield, against this weapon, the terrorist is already far ahead. The building of a counter-CyberTerrorist team must be real-time and dynamic, as the weapons will continually change, to morph, in an attempt to beat you, your systems, and your people. There is no re-machining, and unlike other terrorists, if the CyberTerrorist loses today, he does not die - he learns what did not work, and will use that information against you tomorrow.

F) Tools of cyber terror:

1) Hacking
2) Trojans
3) Computer Viruses
4) Computer Worms
5) Email Related Crime
6) Denial of Service Attacks
7) Cryptography

III. TOP 8 COMPUTER SECURITY METHODS

Computer security has never been more important. Our national critical infrastructure, our work and our private lives depend on a smoothly running digital environment.

This is why it's so important that small businesses and home based networks, as well as large organizations, establish good computer security practices. Luckily, many of these practices also serve as good advice to follow in order to limit the effects of disasters, accidents and cybercrimes other than terrorism.

1. Have a Plan

Prepare actionable steps for yourself and other users of your network to follow if your network is attacked or appears to have been. Unlike attacks on physical property, cyber attacks sources can sometimes be difficult to identify. Response plans, therefore, should go into effect as soon as a system appears to have been compromised, and then the source of the problem – whether accidental or malicious—can be sought.

2. Back up Critical Information

Everyone, from the largest corporation to individual users, should have a system for backing up their critical information and databases. This is so crucial it's worth saying again: everyone should have a back up system in place!

And yet, it is rarely necessary to back up an entire system. Instead, individuals and small business will want to select what to back up in case of an attack or disaster.

3. Authenticate Network Users

Make sure your user authentication system is appropriate for your system. If you are a private or home networked user, make sure you change your passwords at least every 90 days. If you run a small organization, make sure that you know who goes in and out of your workplace, virtually and physically. In larger organizations, it is recommended that passwords be combined with physical hardware and well-implemented biometric systems to ensure that computers are accessible only to authorized users.

4. Create Mechanisms for Reporting Problems in the Workplace.

Developers, researchers and employees may hesitate to report system problems in environments where they know they will be held responsible for failing to fix them. Both formal reporting mechanisms and an atmosphere of support for full reporting will save companies potentially critical and costly losses.

5. Reduce the System's Vulnerability in an Attack Situation

The object of an attack plan must be to reduce the system's vulnerability. As the Computer Science and Telecommunications Board has noted, "making systems do less" is the primary way to make them less vulnerable: Reduce the number of users, run less software and limit communication between systems. All of these actions close off possible places where the system has been or can be breached further.

6. Make Sure that Everyone Knows What to Do and Expect

The day of an apparent attack should not be the first time system operators, managers, and employees see instructions on how to respond. Response plans need to be practiced and made part of an overall prevention strategy. Staging mock attacks or "red teaming" is an excellent way to identify weaknesses and areas to be strengthened in existing response strategies, while reinforcing proper response methods.

7. Prevent Public Relations Crises by Preparing Communications Strategies

CSTB has noted that attacks need to be public: "Researchers, developers, and operators need this information to redesign systems and procedures to avoid future incidents, and national security and law enforcement agencies need it to defend the nation ...." Fearing for their reputations, many organizations keep attacks under wraps. This is detrimental to the safety of all. Instead, a well planned communications strategy can both ensure future safety and protect organizations' reputations.

8. Report Attacks to Government Authorities

If you suspect that a terrorist attack is the source of a slowdown or disruption in your system, it should be reported to the United States Computer Emergency Readiness Team (US-CERT). Reports can be made via telephone at 1-888-282-0870 or through their Internet Incident Reporting System. For the purposes of reporting to the government, an incident is defined as "the act of violating an explicit or implied security policy."

Conclusion

If a computer security advisor states that you, your organization, and your country are safe behind firewalls, behind a system put into place by people who have never fought cyberbattles, behind audit trails, passwords, and encryption, then a great and dangerous fallacy (or fantasy) is being perpetrated upon you. The only solution is the quick deployment of a counter-CyberTerrorist - someone who knows what you are up against today, someone who lives in the world of the people who are, and will be, attacking - someone who can train the people who must fight the battles.

Additionally, a well-designed technical solution can circumvent some of the cultural problems inherent in cross-sector information sharing, by eliminating the need for the actual data to do the correlation. Some technologies have been developed which would appear to lend themselves particularly well to this sort of implementation, but practical tests are required before any conclusion can be reached (Legion, 2002).

Aside from the role of computers in defense, we must attempt to re-educate policy makers, defusing the latent danger of vertical ‘cyberterrorism’ defenses and replacing them with a well-rounded, integrated approach to a problem that is extremely broad. From a corporate and governmental perspective this requires a careful examination of the ‘messaging’ that is broadcast. How do we portray the fusion of computers with terrorism? Can the messaging be made more productive so that we can shape the mindset of our audience to one that is synergistic with a broad view of cyberterrorism?

Finally, it is impossible to neglect to mention the fact that the rapid increase in connectivity and the ultimate frailty of our national IT infrastructure coupled with the astonishing homogeneity of our computing base is a matter of grave concern. Continued focus must be put on increasing the public demand for computer security as well as the corporate awareness of the issue: whereas security flaws in widely used applications were once perceived as personal risks, we must begin to recognize the potentially global consequences of such issues in balance with the more general problems posed by the integration of computing with terrorism.

The lack of understanding of cyberterrorism, and the overall insecurity of America’s networks have allowed a situation to develop which is not in the best interests of the country or computer users. The need to protect computing resources, making the job of a cyberterrorist more difficult is obvious.

However, this can only be accomplished by re-examining commonly held beliefs about the very nature of computer systems and of cyberterrorism itself.

REFERENCES

[1] Crabtree, S. (1996) Cyberspace: a Terrorist Frontier? Insight on the News, 12 (31), 11.

[2] Cyber wars: Logic bombs may soon replace more conventional munitions. (1996). The Economist, 338 (7948), 77-78.

[3] DiDio, L. (1977) Feds Struggle in Race with Hackers. Computer World, 32 (15), 41-42.

[4] Laqueur, W. (1996) Terrorism: Looking to the Future. Current, 386, 9-14.

[5] Laquer, W. (1997) Terrorism via the Internet. The Futurist, 31 (2), 64-65.

[6] Pilant, L. (1997) Fighting Crime in Cyberspace. The Police Chief. , 64 (8), 26-35.

[7] Smith, C. (1997) Get American Troops Ready to March on Cyber Battlefield. Insight on the News, 13 (44), 29-30.

[8] http://afgen.com/terrorism1.html

[9] Collin, Barry C. "The Future of Cyber Terrorism" Proceedings of 11th annual international symposium on criminal justice Issue.

[10] The University of Chicage, IL, 1996 Coleman, Keivin "Cyber Terrorism" www.directionsmap.com/article.php?article.id=432 , Oct. 10, 2003

[11] Gillespie, Michael: "Zionist Israeli Cyber Terrorists Foiled" Sep. 6, 2002, www.sf.indymedia.org/news/2002/09/145461.php and www.cs.etsu-tn.edu/gotterban/stdntppr.htm

[12] Kerr, Kothryn, "Putting cyber terrorism into context

[13] Collin, B., 1997. The Future of Cyberterrorism, Crime and Justice International, March 1997, pp.15-18.

[14] Crenshaw, M . 1999. How Terrorism Ends. US Institute of Peace working group report, May 1999.

[15] Denning, D., “Cyberterrorism”, Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services, US House of Representatives, 23 May 2000.

[16] (http://www.cs.georgetown.edu/~denning/infosec/cyberter ror.html)

[17] DOC, 2002. US Department of Commerce, Export Administration Regulations (EAR), 15 C.F.R. Parts 730-774. Sections 740.13, 740.17 and 742.15 are the principal references for the export of encryption items.

[18] DOD, 2002. Department of Defense Education Activity Internal Physical Security. Department of Defense. DoDEA Regulation 4700.2 DOS, 2002. United States Code. Title 22, Section 2656f.

[19] FBI, 2002. Code of Federal.Regulations. 28 CFR. Section 0.85 on Judicial Administration. July 2001.

[20] Hamblen, M. Clinton commits $1.46B to fight cyberterrorism

[21] http://www.cnn.com/TECH/computing/9901/26/clinton.idg , 26 January 1999.

[22] HLS, 2002. National Strategy for Homeland Security. Office of Homeland Security. July 2002.

[23] Holland, J. 2001. Investigators look into how library computers may have linked terrorists. South Florida Sun-Sentineel. Miami, FL.

[24] Legion, 2002. http://legion.virginia.edu Retrieved from the World Wide Web, August 2002.

[25] Luening, E. 2000. Clinton launches plan to protect IT infrastructure. CNET, 7 January 2000.

[26] McKay, N. 1998. Pentagon Deflects Web Assault. Wired, September 1998.

[27] http://terrorism.about.com/od/beingprepared/tp/ComputerSecurit.htm

[28] http://www.iiuedu.eu/press/journals/sds/SDS_2011/DET_Article2.pdf