A Case of Bureaucracy

If you had told someone ten years ago, that it would be possible to feign an outright physical attack on a country through computers, they would have laughed at you and called you a madman. The sad truth is that this form of violence and terrorism, aptly called cyber terrorism, is no more a thing of the past and is very much possible in our technological and computer savvy world of today. The economic growths achieved by many countries due to such technological advancement in fields of computers such as networking. Networking has provided the world with the Internet that has bridged the distances of the world and made it into a global village. People can now use the Internet to share information with each other. Internet can also be used as a communication tool and people sitting in places half way across the globe can communicate with each other with a click of a button. At the same time, the Internet can also be a dangerous place. People share information through their computers and this means that their computers are online in a cyber world. This means that the person's computer is open to threats and risks from anyone who knows how to get inside the computer. People can use the Internet to steal someone else's credit card numbers, and a lot of other personal information. In this paper, we shall examine how people can use the Internet to spread a new form of terrorism, cyber-terrorism.

A person sitting at home using his personal computer can longer feel safe, even in the security of his/her own home, as information security has become one of the prime concerns of everybody, including the government. It is believed that a threat of cyber-terrorism is a very real threat and the government has taken some very cautious measures in order to repeal such an attack. The U.S policy makers have to come up with various ways in which they can predict and thus divert cyber attacks (Hillyard 2002; Metz 2000; Kelly 2001; Rosen 2002). The reason that cyber-terrorism is something that is very real is because of the advancement in information technology and computer related technologies. People might be surprised to hear that the hijacking of the commercial airlines, and their subsequent crash into the World Trade Center on

September 11, 2001, was all done by using the information and the technology of the United States. Imagine if the terrorists had attacked the digital infrastructure of the FAA and fed wrong information to all the planes that were flying at a given moment. That could have been a much bigger tragedy as it would have left so many planes stranded and lost up in the air. This type of terrorism can be defined as cyber-terrorism (Gray 2002).

In the past few decades, our world has become increasingly dependent upon computers. This dependence is not just restricted to the governments and officials but the public has also become very dependent on computers. The Internet is commonplace and almost everybody uses it everyday for various purposes. As the number of people who are logged on to the Internet grows, so does the threat of cyber-terrorists. The growth of the computers is not only because of the number of people that are connected to the Internet but also in terms of the levels by which computers have been integrated into the national infrastructure. The United States is very vulnerable to cyber-attacks because it is very dependent upon technology. The vulnerability of the United States to cyber attacks suggests that the next significant terrorist event in this country may be coupled with some form of cyber-terrorism. Therefore, it is important to understand what cyber-terrorism refers to, what such acts might involve and what the United States is doing to lessen the impact such attacks might produce (Pasley 2003).

It is extremely important to understand that that cyber terrorism does not only refer to the cyber attacks. It can also be physical attacks on the critical infrastructure through the use or collaboration with the Internet and or other networks. This is why it is a very real threat and can be launched upon us at any time. In order to understand exactly how computers and the Internet can be used to attack the United States, we must analyze on what the terrorists intend to achieve through the attacks and what their goals are. Most of the critical infrastructures of the United States are highly interdependent and rely a lot on each other. The problem is that many of the

people concerned with the security issues are not aware of this fact nor are they aware of the fact that it is not the method or mode of terrorism but the motives behind it must be considered in order to effectively deter the attacks. “In various security exercises that have been carried out across the country, it is evident that this concept is not well understood at any level of government. For example, oil or coal may be needed to run an electric utility plant, which may then be what generates the electricity to keep critical financial and communications systems operational. How does one plan for the interruption of any of these infrastructures for a week or more, on a regional basis? No models exist to help answer these questions” (Verton 2004).

The pre-September 11 scenario was that the airline industry was totally in control of its security of information and the people in charge of security did a perfect, adequate, and cost-effective job of screening out the potential dangers. However, we saw that that failed miserably on September 11. Similarly, the corporate America, which controls about eighty-five percent of the critical infrastructure want us to believe that it has adequate protection for these assets. Do we believe them? It is believed that the Al Qaeda has huge databases that list all the potential targets in the United States, including critical economic nodes. This information can easily be downloaded from the Internet as most of the companies have their data on their facilities and systems online. Verton (2004) was able to pull out maps showing nuclear waste storage facilities and diagrams of every major telecommunications network in a matter of hours. Imagine what terrorists could pull out and use the information in order to attack the United States. Verton (2004) writes, “al Qaeda has trained operatives and has access to other skilled people who could initiate a digital attack against a segment of our critical infrastructure”. He notes that it is very possible that such an attack could critically impair a region’s power grid, especially if combined with physical attacks. That would cripple the region’s economy and have significant national implications.

It is very easy for a hacker to bombard a state agency site with millions of requests asking for information and this can cause the site to overload and shutdown. An intruder can also use the Internet to invade a system that has been designed to control a city's water supply or air transportation systems and this can cause a lot of problems. For a long time, security experts have questioned the possibility of a cyber attack. Now, they are asking how soon they can expect one. According to the various researches and reports mentioned in this paper, a cyber attack is currently very probable and can occur any day! Sounds impossible but this statement can be resounded upon the fact that the impossible did happen on the morning of September 11. "If, on the day before that day, I asked you what the odds were that four people were going to hijack four planes. And three of them would hit prominent buildings and that both towers of the World Trade Center would collapse--you would have said such a risk is minimal," says Scott Charney, the chief security strategist for Microsoft. "After Sept. 11, that very afternoon, in fact," he says, "you would have said there was a 100 percent chance that something like the attacks of that morning could occur". This change in perception occurred because what was considered highly improbable did actually happen (Boulard 2003).

This is why the information systems of the United States are considered very vulnerable and the security officers are being urged to keep this as a necessary and a regular part of their security measures. Many experts believe that cyber-attacks can cripple communications in heavily populated areas and lead to social chaos, as well as death. "Until we secure our cyber infrastructure, a few keystrokes and an Internet connection is all one needs to disable the economy and endanger lives," said Congressman Lamar Smith of Pennsylvania when the Cyber Security Enhancement Act was passed last year. Then he added an unforgettable thought: "A mouse can be just as dangerous as a bullet or a bomb" (Boulard 2003).

There are some people, however, who consider that there is no such thing as cyber-terrorism. One of them includes Dorothy Denning who says, "I thought the talk about the cyber

threats were being overstated. I just didn't subscribe to the 'sky-is-falling' scenarios." She points out that what other critics have long emphasized-even though there have been thousands of documented cases of cyber intrusions, "there hasn't been one instance of a cyber terrorist attack." It has been the hackers, she says, who have been breaking into systems, sometimes just to show they can do it and other times to steal access to money. Such intrusions, Denning admits, "of course, cost money and have to be regarded seriously. But they are not cyber terrorism" (Boulard 2003). Similarly, Washington Monthly magazine explored the sometimes alarmist talk about the advent of cyber terrorism, and noted, "There is no such thing as cyber terrorism --no instance of anyone ever having been killed by a terrorist or anyone else using a computer." (Boulard 2003).

These same experts, however, agree that the real threat of cyber-terrorism is to the information that virtually every government department or agency carries. "Take a department that issues benefits to people," says Charney of Microsoft. "That is an agency that is going to have a large amount of personally identifiable information. Protecting that information is critical because otherwise you are going to be facing a huge risk with things like identity theft" (Boulard 2003). And because most of the government agencies are interconnected to each other, the potential for invading one system through another has never been greater. "This makes it essential, says Dave Morrow, a deputy director of privacy services at EDS, that state and local governments conduct what he calls an "enterprise-wide assessment of their security needs. That is the only way that you can satisfy or protect the data elements you have that are sensitive" (Boulard 2003). If a hacker can access one part of a secure system, it can get into various other networks through there since all these networks are connected to each other. The White House has also become very concerned with this issue and it has released a report that is encouraging industry, government agencies and citizens to reduce cyberspace risks wherever practical and gives advice on how to do it.

The National Strategy to Secure Cyberspace is part of President Bush's larger National Strategy for Homeland Security. This strategy outlines five major national priorities: to create a cyberspace security response system, to establish a threat and vulnerability reduction program, to improve security training and awareness, to secure the government's own systems, and to work internationally to solve security issues. “The plan depends on coordinated and cooperative efforts from federal, state and local governments, businesses and citizens. Unlike the previous draft version that mandated businesses to adopt certain measures, the new strategy encourages state and local governments and the private businesses to reduce threats and vulnerabilities incrementally with a number of recommendations” (Boulard 2003).

It is very important to consider the actual meaning of terrorism and how it relates to the computers and information technology in order to fully understand the threats to our national security. The study of terrorism usually defines terrorism as “assassinations, bombings, hijackings and kidnappings, these events account for a relatively small portion of what occurs within the rubric of the terrorism experience and are meaningless if they are not understood in terms of their overall consequences. The same is true with respect to cyber terrorism. The rapidly emerging cyber environment brings many concerns and uncertainties” (Flemming et al 2001). The terrorists of today have many opportunities by which they can pursue their campaigns of violence against those whose infrastructure relies heavily on computers and the Internet. However, for this to happen, the terrorists must be proficient in the use of computers and computer-related technologies. For the most part, computer technology plays a major role in providing a wider range of options for terrorist growth potential.

Even though this is not what cyber terrorism is, this line of thought does have critical implications for the future of both conventional and cyber terrorism. “The “real” cyber terrorism has yet to evolve beyond the nuisance stage. While the potential for serious cyber attacks that physically destroy national infrastructures should not be treated lightly, the destructive nature of

this form of violence must be kept in context. First, there are no compelling reasons to believe that cyber attacks will be any more deadly than conventional ones. Second, terrorist desires to escalate current levels of violence are as much dependent on who the groups are and what they hope to achieve, as upon the weapons they have at hand" (Flemming et al 2001). People have always theorized about doomsday and other haunting scenarios that involve weapons of mass destruction. This is not something new only now people have started to relate such scenarios to cyber terrorism.

It can be true that the political actors might be exploiting these fears of the people in order to spread the notions about cyber-terrorism etc for their own personal benefits. So, it would be a very intelligent move for us not just to "prepare ourselves for such purposes by examining not only the doomsday scenarios in our darkest imaginations and the vulnerabilities which lead to them but also the probabilities of exploitation and how to protect against such actions" (Flemming et al 2001). Cyber terrorism should not just be equated with the amount of terrorist violence but studies should be made about how the cyber environment both facilitates and encourages terrorist behavior beyond conventional standards and how it affects the ability of states and the private sector to gather information and create technical as well as political countermeasures. If the fundamentals of terrorism remain the same, the quest to understand cyber terrorism is as much about comprehending the past, as it is about predicting the future (Flemming et al 2001).

Work Cited

1. Boulard, Garry. “Cyber Terrorism: No Longer Fiction; the Threat of Cyber Terrorism Became Much More Real after Sept. 11. Here’s How States Are Trying to Reduce the Risks”. *State Legislatures,* 29, (5), 2003

2. “Cyber Attacks During the War on Terrorism: A Predictive Analysis.” *Institute for Security Technology Studies* at Dartmouth College, 2001.

3. Denning, Dorothy, *Defining, Information Warfare and Security.* Boston: Addison-Wesley 1999.

4. Flemming, Peter, and Michael Stohl, “Myths and Realities of Cyberterrorism,” *Countering Terrorism Through International Cooperation,* Alex P. Schmid (ed.), ISPAC(International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Program), Vienna, 2001, pp: 70-105.

5. Gray, Colin, “Thinking Asymmetrically in terms of Terror,” *Parameters* (Spring) 2002, 32: 5-14.

6. Hillyard, Michael, “Organizing for Homeland Security,” *Parameters* (Spring) 2002, 32: 75-85

7. Kelly, Terrence. “An Organizational Framework For Homeland Defense,” *Parameters* (Autumn) 2001, 31: 105-116

8. Metz, Steven. *Armed Conflict in the 21st Century: The Information Revolution and Post-Modern Warfare.* Carlisle Barracks, PA: U.S. Army War College, Strategic Studies Institute, 2000.

9. Pasley, James F. “United States Homeland Security in the Information Age: Dealing with the Threat of Cyberterrorism”. *White House Studies,* 3 (4), 2003, 403+.

10. Rosen, Stephen P. “The Future of War and the American Military,” *Harvard Magazine*, (May/June) 2002, 104: 29-31;

11. Verton, Dan, *Black Ice: The Invisible Threat of Cyber-Terrorism*, Osborne/McGraw-Hill, 2004.