Cyber-Terrorism: Reality or Paranoia?

Sam Berner

The new millennium – if there ever was one in any scientific meaning of the term – has been ushered amid a media circus of a Y2K scare and predictions of total world paralysis. It didn't happen, and we were all relieved for a while, short as it was, until something far more dark and sinister in the shape of two airplanes hit the World Trade Centre. The amount of vital data and information lost in that attack has brought home a new threat to haunt those responsible for information security: cyber-terrorism. Increasingly, the world depends on computers. The systems residing on them control power delivery, communications, aviation, and financial services. They are used to store vital information, from medical records to business plans to criminal records. These computers are vulnerable - to the effects of poor design and insufficient quality control, to accident, and perhaps most alarmingly, to deliberate attack. The modern thief can steal more with a computer than with a gun. Does it follow, though, that tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb?

Terrorism is a much used term, with many definitions. The US Department of State defines it as "premeditated, politically motivated violence perpetrated against noncombatant targets by sub-national groups or clandestine agents." If we combine this definition with the term "cyber", we end up with a working definition of cyber-terrorism: "The premeditated, politically motivated attack **against information, computer systems, computer programs, and data** which result in violence against noncombatant targets by sub-national groups or clandestine agents. (Politt, 1998)." For the term "cyber-terrorism" to have any meaning, we must be able to differentiate it from other kinds of computer abuse such as computer crime, economic espionage, or information warfare. Using this definition, a number of things often miss-associated with cyber-terrorism can be eliminated. For instance non-politically motivated computer crimes, like the 16-year-old hacker's 1994 crashes of 100 U.S. defense systems, or the creation, and release of the Nimda worm (or any other worm for that matter) were not acts of cyber-terrorism, although both were serious incidents, with the potential for great harm. They lacked the essential ingredients that would allow for the term "terrorism". Unlike a virus or computer attack that simply causes a prevention or delay of service, a cyber-terrorist attack leads to physical violence of some sort or extreme financial harm. Thus, possible cyber-terrorism targets include the banking industry, military installations, power plants, air traffic control centers, and water systems. Cyber-terrorists are not merely individuals seeking to cause harm or damage wherever they can. They are people, or groups with political agendas.

The term "cyber-terrorism" in itself well predates September 11th. It was coined in 1980s by Barry Collin, senior research fellow at the Institute for Security and Intelligence (*www.counterterrorism.org*) in Palo Alto, USA. Much earlier, in 1991, the US National Research Council commissioned a book on computer security, "Computers At Risk", but although terrorist use and abuse of computer networks was discussed, the Council limited

itself to the ambiguous "computer crime". In 1996, the US government in the person of the then President Clinton, created the Commission of Critical Infrastructure Protection (PCCIP) which has identified eight critical areas in need of protection: information and communications, electrical power systems, gas and oil (production, transportation and storage), banking and finance, transportation, water supply systems, emergency services and government services (Angelica, 1998). The resources to launch a cyber attack are commonplace in the world; a computer and a connection to the Internet are all that is really needed to wreak havoc. The CIA created the Information Warfare Center, staffed with 1,000 people and a 24-hour response team, and not much to show the tax-payer for it. The FBI investigates hackers and similar cases, as well as pursues banking, fraud and wiretapping cases (Wasserman, 1998). The Air Force created its own group, Electronic Security Engineering Teams, ESETs.

In December 1998, the U.N. General Assembly adopted a resolution related to cybercrime, cyberterrorism, and cyberwarfare. Resolution 53/70, Developments in the Field of Information and Telecommunications in the Context of International Security, invites member states to inform the Secretary-General of their views and assessments on (a) the issues of information security, (b) definition of basic notions related to information security, and advisability of developing international principles that would enhance the global information and telecommunications systems and help combat information terrorism and criminality (UN, 1998).

The media has further "hyped" the concept of cyber-terrorism. According to the press, one is lead to believe that all of the functions controlled by individual computers will all converge into a singular system. Further support for this scenario is the increase in "connectivity". Many people conclude that the entire world will soon be controlled by a single computer system. Technology is feared from two perspectives. First, it is by definition arcane. It is complex, abstract and indirect in its impact on individuals. Because computers do things that used to be done by humans, there is a natural fear related to a loss of control. The mantra of the late 20th century is that information is power. This has become a reality. The possession of accurate, timely information is the key to competitive advantage. This is true regardless if you are a superpower government or a small business person. Computers have created new risks (and rewards) concerning the discovery of information which it originator wished to remain confidential. There is an inevitable trade-off between availability and privacy. These same risks apply to computers designed for the control of processes. In effect, anything that can happen to information can happen to processes controlled by computers.

The cyber-terrorist's traditional weapons of choice include computer viruses (such as logic bombs that wake up on a certain date, worms and trojan horses), cracking (accessing computer systems illegally), sniffing (monitoring Net traffic for passwords, credit card numbers and other data), social engineering (fooling people into revealing passwords and other information) and dumpster diving (sorting through the trash). As these and similar tools proliferate, companies such as Semantec and McKaffey make fortunes by writing protective software: firewalls, IDS, filters, etc. Terrorist groups are using the Internet extensively to spread their message and to communicate and coordinate action. However, there have been few if any computer network attacks that meet the criteria for cyber-terrorism. The 1998 e-mail bombing by the Internet Black Tigers against the SRI Lankan

embassies was perhaps the closest thing to cyber-terrorism that has occurred so far. During the Kosovo conflict in 1999, NATO computers were blasted with e-mail bombs and hit with denial-of-service attacks by hacktivists protesting the NATO bombings. In addition, businesses, public organizations, and academic institutes received highly politicized virus-laden e-mails from a range of Eastern European countries, according to reports. Web defacements were also common. After the Chinese Embassy was accidentally bombed in Belgrade, Chinese hacktivists posted messages such as "We won't stop attacking until the war stops!" on U.S. government Web sites.

For a terrorist, cyber-terrorsim would have some advantages over physical methods. It could be conducted remotely and anonymously, it would be cheap, and it would not require the handling of explosives or a suicide mission. It would likely garner extensive media coverage, as journalists and the public alike are fascinated by practically any kind of computer attack. This takes us back to the question postulated earlier: can tomorrow's terrorist do more damage with a keyboard than with a bomb?

Both yes and no. Yes, because vulnerabilities in computing systems can be exploited by terrorist elements. No, because although the exploitation can directly impact the public, it is rarely serious or fatal. However, after having read all the frightful scenarios available so freely online (see, for example, Brenner, 1998) one main thing remains to remember. Computers don't exert control by themselves – there are humans involved in the information chain. Whether or not we chose to consider humans more fallible than the computerized systems they have created is a related issue. After all, cyber-error can be as devastating as cyber-terror. However, as long as there are humans involved, controlling and monitoring the system, then terrorist attacks in cyberspace can be offset. The world does not yet face a compelling threat from terrorists using information warfare techniques to disrupt critical infrastructure. They lack either the motivation, capabilities, or skills to pull off a cyber-attack at this time. Although a physical attack against the infrastructure cannot be ruled out, such a threat is neither new nor matured by the developed world's reliance on technology [Church, 1997]. Because systems are complex, it may be harder to control an attack and achieve a desired level of damage. Unless people are injured, there is also less drama and emotional appeal. Further, terrorists may be disinclined to try new methods unless they see their old ones as inadequate.

Given that there are no instances of cyberterrorism, it is not possible to assess the impact of acts that have taken place. It is equally difficult to assess potential impact, in part because it is hard to predict how a major computer network attack, inflicted for the purpose of affecting national or international policy, would unfold. So why is cyber-terrorism suddenly basking in lime-light, from government agencies, to "specialists" to the hubris of the media? There are multiple reasons, and more of these political than informational. One close look at the proposed remedies, especially those put in place after the WTC attacks, will show that fighting "cyber-terrorism" can become a heaven-sent excuse for governments to place more control on the evasive cyber-space. How this affects such issues as democracy, privacy, freedom of expression, and copyright, will be discussed in the forthcoming issue.

RELATED WEBSITES: (not exclusive)
http://www.pccip.gov

http://cybercrimes.net
http://www.ciao.gov/
http://www.ists.dartmouth.edu/
http://www.cert.org

BOOKSHELF:

Arquilla, J. & Ronfeldt, D. (eds.) (2001) **Networks and Netwars: The Future of Terror, Crime, and Militancy**. Rand Corporation: Santa Monica CA

Schwartau, W. (1996) **Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age.** Thunder's Mouth Press: NY
Sofaer, A. & Cuellar, M. (eds.) (2001) **The Transnational Dimension of Cyber Crime and Terrorism (Hoover National Security Forum Series).** Hoover Institute Press: Stanford CA

Webster, W. et al (1998) **Cybercrime Cyberterrorism Cyberwarfare: Averting an Electronic Waterloo (Csis Task Force Report).** Center for Strategic and International Studies: Washington DC

REFERENCES:

Angelica, A. (1998) "The New Face of War." *Techweek*, (02/11).

Brenner, S. & Overholt, M. (1998) Introduction to Cyber-terrorism. [Online] Available WWW: http://cybercrimes.net/Terrorism/overview/page1.html

Church, W. (1997) Information Warfare Threat Analysis for the United States of America, Part Two: How Many Terrorists Fit on a Computer Keyboard? Journal of Infrastructural Warfare, (Summer).

Collin, B. (1996) The Future of CyberTerrorism. Proceedings of 11th Annual International Symposium on Criminal Justice Issues. The University of Illinois at Chicago. [Online] Available WWW: http://www.acsp.uic.edu/OICJ/CONFS/terror02.htm

Pollit, M. (1997) Cyberterrorism – Fact or Fancy? Proceedings of the 20th National Information Systems Security Conference [Online] Available WWW: http://www.cs.georgetown.edu/~denning/infosec/pollitt.html

UN (1998) G.A. Res. 53/70, U.N. GAOR, 53rd Sess., U.N. Doc. A/RES/53/70 [Online] Available   WWW: http://disarmament.un.org/vote.nsf/91a5e1195dc97a630525656f005b8adf/0e4088ff35d55 05d0525681200673c74?OpenDocument&ExpandSection=4

Wasserman, E. (1998) "Feds take steps against threat of cyber terrorism". [Online] Available WWW: http://www.idg.net/go.cgi?id=13818