South African Journal
of Information Management
[DoE accredited]

Secure notes Vol.5(1) March 2003

Cyber-terrorism: reality or paranoia?

S. Berner
samalex61@yahoo.com

Information security may be the realm of specialists, but today it touches the lives and safety of millions in the developed world. In this column appears as attempt to sketch short profiles of the most pressing issues.

Cyber-terrorism: reality or paranoia?

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 did not realize, 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, then, that tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb?

New term, old game

Terrorism is a much-used term with many definitions. The US Department of State defines it as 'premeditated, politically motivated violence perpetrated against non-combatant 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 non-combatant 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 that are 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 US defence systems, or the creation and release of the Nimda worm (or any other worm for that matter). These 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. Therefore, 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 11. It was coined in the 1980s by Barry Collin, senior research fellow at the Institute for Security and Intelligence (www.counterterrorism.org) in Palo Alto, USA. In 1991, the US National Research Council commissioned a book on computer security entitled *Computers At Risk*, but although terrorist use and abuse of computer networks were discussed, the council limited itself to the ambiguous 'computer crime'. In 1996, the US government in the person of President Clinton created the Commission of Critical Infrastructure Protection (PCCIP), which 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; 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 1000 people and a 24-hour response team, but not much to show the taxpayer for it. The FBI investigates hackers and similar cases, and pursues banking, fraud and wiretapping cases (Wasserman 1998). The American Air Force created its own group, Electronic Security Engineering Teams, or ESETs.

World prepares itself

In December 1998, the United Nations General Assembly adopted a resolution related to cyber-crime, cyber-terrorism and cyber-warfare. 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 c) 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 led to believe that all of the functions controlled by individual computers will 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 weather you are a superpower government or a small business person. Secondly, computers have created new risks (and rewards) concerning the discovery of information that its 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 traditional weapons of the cyber-terrorist 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 Symantec and McAffee make fortunes by writing protective software such as firewalls, IDS and filters. 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 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 US government Web sites.

Attempts at objectivity

For a terrorist, cyber-terrorism 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?

The answer is both yes and no; yes, because vulnerabilities in computing systems can be exploited by terrorist elements, and 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 on-line (see, for example, Brenner and Overholt 1998), one main thing remains to remember. Computers do not 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 humans control and monitor the system, 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. Terrorists lack the motivation, capabilities and/or skills to pull off a cyber-attack. Although a physical attack against the infrastructure cannot be ruled out, such a threat is neither new nor matured by the reliance of the developed world on technology (Church 1997:23). Because systems are complex, it may be harder to control an attack and achieve a desired level of damage. Unless people are injured, there are 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 cyber-terrorism, 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, with the intent to affect national or international policy, would unfold. So why is cyber-terrorism suddenly basking in the limelight, from government agencies, to 'specialists' to the hubris of the media? There are multiple reasons, and most of these are political rather than informational. One close look at the proposed remedies, especially those put in place after the World Trade Center 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.

References

Angelica, A. 1998. The new face of war. *Techweek* (11 February).

Brenner, S. and Overholt, M. 1998. *Introduction to cyber-terrorism*. [Online]. Available WWW: http://cybercrimes.net/Terrorism/overview/page1.html (Accessed 7 February 2003).

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* (2):23.

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 (Accessed 7 February 2003).

United Nations. 1998. Developments in the field of information and telecommunications in the context of international security. General assembly resolution 53/70, U.N. GAOR, 53rd Session, U.N. Document A/RES/53/70. [Online]. Available WWW: http://disarmament.un.org/vote.nsf/91a5e1195dc97a630525656f005b8adf/0e4088ff35d5505d0525681200673c74?OpenDocument&ExpandSection=4 (Accessed 7 February 2003).

Wasserman, E. 1998. *Feds take steps against threat of cyber terrorism*. [Online]. Available WWW: http://www.idg.net/go.cgi?id=13818 (Accessed 7 February 2003).

Further reading

Networks and netwars: the future of terror, crime, and militancy. 2001. Edited by J. Arquilla and D. Ronfeldt. Santa Monica CA: Rand Corporation.

Schwartau, W. 1996. *Information warfare: cyberterrorism: protecting your personal security in the electronic age*. New York: Thunder's Mouth.

The transnational dimension of cyber crime and terrorism (Hoover national security forum series). 2001. Edited by A. Sofaer and M. Cuellar. Stanford, California: Hoover Institute.

Webster, W. *et al*.1998. *Cybercrime cyberterrorism cyberwarfare: averting an electronic Waterloo (CSIS task force report)*. Washington DC: Center for Strategic and International Studies.

Related Web sites (not exclusive)

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

About the author

Sam Berner (B.Ed., Dipl. LIS, Postgraduate Diploma in Information Management) is a principal of the company ECognus (Brisbane, Australia). She is a knowledge management consultant, assisting SMEs to benefit the most from their intellectual assets. ECognus also provides services in the area of tailored software applications and digitization of business processes.

Disclaimer

necessarily reflect the opinion of the Editor, Board, Publisher, Webmaster or the Rand Afrikaans University. The user hereby waives any claim he/she/they may have or acquire against the publisher, its suppliers, licensees and sub licensees and indemnifies all said persons from any claims, lawsuits, proceedings, costs, special, incidental, consequential or indirect damages, including damages for loss of profits, loss of business or downtime arising out of or relating to the user's use of the Website.

ISSN 1560-683X

Published by InterWord Communications for the Centre for Research in Web-based Applications, Rand Afrikaans University