

The Cyber Terrorism Threat

*First Appeared in
The Bandwidth Desk,
November 30, 2001.*

Since the September 11 attacks on the World Trade Center and the Pentagon, there are very real worries that terrorists will strike again and that this time a physical attack may be accompanied by a cyber attack.

Cyberspace remains much of a mystery to most of us, so it is hardly surprising that the mere mention of cyber terrorism raises more than mild concern in today's already tense and uncertain atmosphere.

Cyber terror is not just the defacing of a web site, even a prominent one, or launching a virus that elusively corrupts email, computer programs or files before users are aware of its presence. The cyber terrorist takes his attacks to a deeper level, using sophisticated technical skills to infiltrate computers and communications networks that sustain both our critical infrastructures and basic economic, governmental and social institutions. The cyber terrorist is not a prankster, but a skilled computer and communications technician who understands both information technologies and systems and the infrastructures he intends to attack, and has the resources and motivation to follow through on his intent.

The cyber terrorist may or may not intend the kind of physical destruction and loss of human life that are characteristic of the physical terrorist's attacks. Cyber terrorists may use misinformation, software sabotage, denial of communications or information services and other techniques to cause an airplane crash, impede emergency service operations or put military men and women in harm's way, or they

may intend massive disruption of services that can incite panic and melee and undermine public confidence and trust.

Captain Bill Evans, U.S. Navy (Retired), an early proponent of infrastructure protection and the need to counter cyber terrorism, emphasizes its insidious effects.

"Cyber terrorism is a cheap, effective and controllable tool of terrorism in its purest form," he says, "anonymous, fast and wide-ranging, with highly cascading results that are particularly damaging in a democracy." A cyber terrorist can spread doubt and disinformation more quickly and easily than it can be countered, Evans says, and can impact national policy more subtly than physical attacks.

Our banks and financial institutions; air, sea, rail and highway transportation systems; telecommunications; electric power grids; oil and natural gas supply lines—all are operated, controlled and facilitated by advanced computers, networks and software. Typically, the control centers and major nodes in these systems are more vulnerable to cyber than physical attack, presenting considerable opportunity for cyber terrorists.

Fred Cohen, an internationally renowned cyber terrorism expert, who has written extensively and testified on this subject for years and currently, with the University of New Haven, offers a course on cyber terrorism, states that every one of these critical information networks, key hubs or essential communications links is a potential target if a terrorist sees it as vulnerable and has the knowledge, capabilities and determination to go after it. If that seems rather disconcerting, Cohen quickly



**TELECOMMUNICATIONS
& TECHNOLOGIES
INTERNATIONAL, INC.**

RICHARD THAYER, PH.D.
President & CEO

7018 Beechwood Drive
Chevy Chase, MD 20815

T: 301.913.2883
F: 301.913.2884

Email: info.tti@verizon.net
<http://www.ttinetwork.com>

underscores that there are redundant facilities in place for the basic elements of virtually all of our fundamental information and communication systems—those essential for government and emergency services and the economy, such as air traffic control and electric power supply—the likely prime terrorist targets.

Even prior to relying on such fallback facilities, sophisticated sensing, tracking and firewall technologies are now available that raise the bar considerably for attackers, making it more difficult for them to penetrate security gates and virtually impossible to get to information at fully protected levels. “Technical hardening and safeguarding of communications and information systems, infrastructures and networks is something that we can do well,” says Evans.

Still, other informed people voice a concern that increasingly advanced and sophisticated information and communications technologies not only provide better monitoring and control capabilities for management of critical infrastructures and social institutions, but also afford opportunities for cyber terrorists to wreak new and more extensive havoc than they could previously. Just as the architects and engineers who helped

build the World Trade Center and U.S. federal intelligence agencies were caught completely off-guard by the kind of attack that occurred in September, some informed people think we are no better protected from an equally well-orchestrated cyber attack that might disrupt both telecommunications and the Internet. An article in *The New York Times* last week, for example, cites recent Congressional testimony of Frank J. Cilluffo, a recognized terrorism expert at the Center for Strategic and International Studies in Washington, DC, who describes cyber security as a “gaping hole” in U.S. infrastructure defense. Added security comes at a cost that, until now, many organizations have been unwilling to accept and it remains to be seen whether managers and others may now have seen things differently. Surely we all need to be better educated on the subject.

A need for better coordination and use of intelligence in preventing physical or cyber attacks seems obvious as well. The lack of coordination within the federal government has been noted in study after study over a number of years and became tragically evident on September 11. President Bush has now appointed

former Pennsylvania Governor Tom Ridge to head a new Office of Homeland Security, and Richard Clarke, who directed a counter-terrorism office during the Clinton administration, as a special advisor on cyber security. But, even in the context of the recent attacks, 50 or more federal agencies will not find it easy to share information on a timely basis. If we expect the federal government to act on information more quickly than it has in the past, we too will need to be more attentive and better informed.

Lack of vigilance on terrorism, cyber or physical, presents another serious danger to our society, arising from our own government's resort to measures that compromise individual freedom and due process of law. Holding people in custody for extended periods of time without preferring charges against them or substituting military tribunals outside the U.S. for trial by jury with constitutional safeguards are examples of such dangers. They are unnecessary and counterproductive measures, undemocratic and unworthy of our nation.

Richard Thayer is President & CEO of Telecommunications & Technologies, International, Inc. www.ttinetwork.com, a telecom and IT consulting firm located in Chevy Chase, MD. Contact by email: rthayer.tti@verizon.net, or phone: 877.913.2883.

*Copyright 2001, Richard Thayer and Scudder Publishing Group, LLC. www.scudderpublishing.com
Reprinted with the permission of the publisher.*