Cyber-Terrorism

Jason S. Hardman

Row #3

April 24, 2006

Dr. Lejk

ITCS3688

Section 002

Escalation of cyber-war activity on the Internet brings to light anew, the concept of stealth attacks.

The proverbial Chinese "Slow-Virus".
A phasic-interfacing multi-injected attack

“Cyberterrorism is 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.”(Cyber Terrorism : The Sum of All Fears)

Cyber-terrorism is a popular topic these days that not many seem to understand. Questions like, “Are we involved in a cyber war?”, “Are we vulnerable to attack?”, and “Why haven’t we felt the effects of such attacks” are generally rumored about and left unanswered. The answer to these questions is that <u>while a true cyber-war does not seem to have taken place, the threat is real and we should prepare ourselves for the impending assaults</u>.

Although the potential for cyber-terrorism is broad, in fact not a single case of cyber-terrorism has yet been documented(Cyber Terrorism : The Sum of All Fears). It seems that the primary use for the Internet thus far has been as a communication medium for propaganda (Terrorist Activities on the Internet). The Latin American terrorist movements seem particularly inclined towards the technological avenue with groups like the Mexico's Zapatista who have used it to rally support since 1994 (Terrorist Activities on the Internet). The threat is serious, however, as reports have shown that viable Transient Electromagnetic Device (T.E.D.). models, described later, can be built on the cheap. Costs run about $300, and with a week for construction one can create a suitcase size unit and around $500; with two weeks for construct gives you a mobile size unit(Radio Frequency Weapons and Proliferation). So who is likely to create such devices?

According to Secretary of State Madeline Albright, five of the top cyber-terrorist organizations are:

> Tupac Amaru Revolutionary Movement; Fuerzas Amadas Revolucionarias de Columbia; Aum Shinrikyo (Aum Supreme Truth); Islamic Resistance Movement (HAMAS); and Hizbullah (The Party of God)(Cyber Terrorism : The Sum of All Fears).

The Department of Justice reported that in 1997, there were forty-eight referrals for the prosecution of international terrorists... (this) remained stable until 2001, when the rate drastically increased to 204 (Savino).Targets of Cyber-Terrorism are diverse and could include corporations, small businesses, Internet service providers, banks, pharmaceutical companies, air lines and air traffic controllers, utility companies, and more (Pollitt).

Cyber-terrorism techniques fall into roughly two categories: both physical and electronic assaults.

Electronic attack methods employ the uses of computer viruses, logic bombs, Trojan horses, and (distributed) denial of service attacks to break software. A relatively new addition to the list is the use of "bot nets". It is estimated that thousands of computers connected to the Internet are infected with remote controlled "bot" software. These computers, otherwise known as "zombies", are used activated only when needed and are used by the cyber terrorist to collectively assault a selected target server (Hacking Exposed).

The physical attacks are focused towards destroying hardware using electronic waves or pulses. These devices effectively "microwave" a circuit board causing temporary or even permanent damage. Leading technologies are listed and defined as:

- T.E.D. (TRANSIENT ELECTROMAGNETIC DEVICE) (Schriner)(Radio Frequency Weapons and Proliferation)

  T.E.D.s are an inexpensive, yet powerful, method of delivering radio frequency (RF) interference into a circuit. T.E.D.s deliver a spiked-pulse of energy, as opposed to the traditional RF device which delivers a fluid sine-wave flow of energy.

- R.F. WEAPON (RADIO FREQUENCY WEAPON) (Schriner)(Radio Frequency Weapons and Proliferation)

  Uses a flowing sine-wave pattern of energy to excite particles. This can be projected by using a parabolic reflection vector. An example might be to modify a microwave by putting a salad bowl around its wave emitter. The salad bowl would project and focus the energy along a particular line.

- R.F. MUNITIONS (RADIO FREQUENCY MUNITIONS) (Cereijo)

  R.F. weapons are also packaged as R.F. Munitions, which use explosives to produce radio-frequency energy. In the hands of skilled Cuban scientists, these munitions come as hand grenades or mortar grounds.

- ELECTROMAGNETIC PULSE (Definition)

  An electromagnetic pulse (EMP) is an intense burst of electromagnetic (EM) energy caused by an abrupt, rapid acceleration of charged particles, usually electrons. An EMP can contain energy components over a large part of the EM spectrum, from very-low-frequency (VLF) radio to ultraviolet (UV) wavelengths. An EMP is found in lightning strikes and high-altitude nuclear explosions, and destroys all electrical circuits within its range.

- T.E.M.P.E.S.T. (TRANSIENT ELECTRO MAGNETIC PULSE EMULATION STANDARD) (The Complete, Unofficial TEMPEST Information Page)

  A U.S. government code word that identifies a classified set of standards for limiting electric or electromagnetic radiation emanations from electronic equipment. EM radiation emanations from computers and specifically monitors can be intercepted and used to recreate the images produced by a computer screen.

Prevention of and protection against software attacks on the individual level include well-known techniques such as using firewalls, virus prevention software, secure configurations for software, and common sense.

On a national level, the most viable project in operation seems to be Project Echelon. Though the NSA will neither confirm nor deny the existence of Project Echelon, the limited information available suggests that Echelon may endow the operator with nearly limitless ability to intercept and monitor any kind of electronic communication (…) Furthermore, available data indicates that Echelon is able to monitor signals that originate anywhere on the planet(Cyber terrorism : Combating cyber terrorism).

With the advent of hardware-assault techniques, physical security should also be considered with new regard. Techniques for securing against assault include implementing strict policies to limit physical access to devices and cabling. Establishing card-access to server rooms is an example of a simple yet effective solution. In sensitive projects, Faraday's Cage can be used to protect against the long range signal monitoring techniques outlined in the TEMPEST literature. A Faraday's Cage is effectively a "chicken-wire" mesh that destroys waves moving through it. It is cheap, simple, and effective.

It seems then, that the prospect of full-scale cyber-terrorism is an impending and imminent threat to the public. Though it has not yet been exploited on any large scale, the potentials for damage to various infrastructures is a weakness that we must acknowledge and take measures to secure against. Simple awareness of the potential for attack can help to mitigate the effects of an unforeseen event. We ultimately disagree with the level of secrecy surrounding much of this information, as an educated public is a rationally reacting public. In contrast, however, it is understood that a realization of the fundamental technology doth shed much light on the potential application in events of war and conflict. Thus, we assume that many in the political "know" still do not comprehend the potentials for devastation, were the applications of such technologies developed for war.

Works Cited

Cereijo, Manuel. “The E-Bomb” Viewed March 14, 2006 <http://www.canf.org/ingles/ENSAYOS/2003-nov-11-the%20e-bomb-manuel-cereijo.htm>

“Cyber terrorism : Combating cyber terrorism” Viewed March 14, 2006 <http://ntrg.cs.tcd.ie/undergrad/4ba2.02/infowar/terrorism.html>

“Cyber Terrorism : The Sum of All Fears” Viewed March 14, 2006 <http://www.wws.princeton.edu/ppns/groups/StateSecurity/papers/Cyberterrorism.pdf>

Definition. “Electromagnetic Pulse” Viewed March 14, 2006 <http://whatis.techtarget.com/definition/0,,sid9_gci942666,00.html>

Hacking Exposed 5th Edition: Network Security Secrets and Solutions (p. 488)
Stuart McClure, Joel Scambray, and George Kurtz : Copyright 2005

Pollitt, Mark M. “CYBERTERRORISM - Fact or Fancy?”, FBI Laboratory Viewed March 14, 2006 <http://www.cs.georgetown.edu/~denning/infosec/pollitt.html>

“Radio Frequency Weapons and Proliferation: Potential Impact on the Economy” Joint Economic Committee Hearing Wednesday, February 25, 1998 <http://cryptome.org/rfw-jec.htm>

Savino, Adam. “Cyber Terrorism” <http://cybercrimes.net/Terrorism/ct.html> (Google Cache)

Schriner, David. “Statement of Mr. David Schriner” Hearings before the Joint Economic Committee United States Congress Wednesday, February 25, 1998 : Viewed March 14, 2006 <http://www.house.gov/jec/hearings/radio/schriner.htm>

“The Complete, Unofficial TEMPEST Information Page” Viewed March 14, 2006 <http://www.eskimo.com/~joelm/tempestintro.html#What%20is>

“Terrorist Activities on the Internet” Viewed March 14, 2006 <http://www.adl.org/terror/focus/16_focus_a.asp>