

Cyber Terrorism and its Link and Impact to the Facilities Environment

J. Keith Flannigan, CAS

IDRC@att.net www.goIDRC.com

Synopsis

Facility Management provides the underpinning for any well ran organization. However, if it is not properly managed, it may also become the weakest link in a physical security program. For example, the overriding of a facilities elevator controls or the changing of a fire control system could have catastrophic effects on a facility as well as the personnel occupying that facility.

This presentation will address the above issues as well as giving the attendee information on the various types of Cyber Attacks, from the remote detonation of Biological & Chemical Devices to the building and use of Electro Magnetic Pulse Generators. You will be made aware of such weaponry as Radio Frequency Weapons, RF munitions, Transient Electromagnetic Device (TED), TEMPEST monitoring devices, electromagnetic bombs, computer viruses and other harmful computer programs.

About the Author(s)

Keith Flannigan directs Crisis Management Operations specializing in Counter Terrorism, Communication and Information security.

Mr. Flannigan has 28 years of experience in the Law Enforcement and Intelligence Fields. He has written and instructed Law Enforcement curriculum on Technical Surveillance, Crisis Response, Cyber Terrorism, Responding to a Terrorist Incident, and Managing a Bio Chemical Incident. Mr. Flannigan was named Counter Terrorism Professional of the Year in 1998 by the Counter Terrorism EXPO. Mr. Flannigan has completed 4 State and Federal academies, minored in Criminal Justice and holds a PhD in Political Science.

He has been a member of the Standing Committee on Computer Security since 1997. He Chairs the Advisory Council of the International Terrorism Response Institute. He is on the advisory board of the International Society for Anti-Terrorism Professionals and is co-authoring the training modules for the Certified Anti Terrorism Specialist designation for the Anti Terrorism Accreditation Board.

Cyber Terrorism and its Link and Impact to the Facilities Environment

It's 7:30 am and you are just beginning your shift. You receive a call from the Director's office that their air conditioning is out, the call waiting clicks in and the hospital calls and tells you that for some reason all of their life support systems just went down on the North wing. While you're speaking with the facilities supervisor about the power, a person in the East parking lot aims a hand held satellite dish at your communications center, releases a billion watt energy spike and your phone goes dead. You quickly realize that this is not going to be a normal shift.

In a news report released on September 9th 2002 it outlines several intentions of the Al-Qaeda Terrorist Group. They made the statement in a tape located last month that "*We will hit America's shopping malls, stadiums and kindergartens*". In the article it stated that they were looking for disenchanted Americans who might be eager to become suicide bombers. Universities coffee houses and religious facilities are being scoured by Al-Qaeda recruiters the perfect hunting grounds for disenchanted Americans and easily motivated foreign students.

With so many of the known terrorists using student visa's to enter the United States and with the knowledge that most people commit crimes in an area that they are familiar, it becomes apparent that the University environment is a prime location for many types of incidents.

The above scenario is not so far fetched and could be easily accomplished with a minimal amount of expertise. With the Al-Qaeda openly announcing that they are going to make all attempts to disrupt the American life style and with the known fact that they have been using Cyber Terrorism for several years, we must develop a defense against this type of attack or at a minimum be able to recognize and respond to an incident such as this.

Coordinated computer terrorism goes way beyond malicious hackers; these attacks do not only crash your computers but can disrupt entire cities as well as causing death and serious bodily injury.

Cyberterrorism gives the terrorist a much wider area of operations and no longer limits them to geographical areas. The more high-technology systems we put in place, the more systems there are to exploit and attack.

Cyberterrorists could attempt to cripple crucial systems at any time, for any reason and from practically any location. The threat is real enough that taxpayer money is being spent to assess (and prevent) attacks on the nation's infrastructure.

- There have been many news reports of cyber terrorist doing everything from destroying and changing web sites to the actual overt acts to damage pipelines and infrastructure.
- Ten thousand Internet activists calling themselves the Electronic Disturbance Theater launched a denial-of-service attack on the Pentagon, Frankfurt Stock Exchange and Mexico presidential Web servers in support of Zapatista rebels in Chiapas, Mexico.

- A Tamil guerrilla group calling itself Internet Black Tigers launched a denial-of-service attack last year on Sri Lankan embassy computers throughout Europe, North America and Asia for two weeks, paralyzing the network.
- Irish Republican Army members reportedly intend to acquire powerful radio frequency weapons for use against the London financial system. Swedish authorities claim RF weapons have been used against their financial institutions, retired U.S. Army General Robert L. Schweitzer said in congressional testimony in June of 1998.

We are finding that since the invasion of Afghanistan and the Al-Qaeda fleeing to other parts of the world that they are becoming more aware of the benefits of using computers to promote their cause. We have also seen that cyber attacks immediately accompany physical attacks.

In a recent research study it was noted that the most potential targets of cyberterrorism:

- Banks, and financial transactions
- Water resources
- Voice communications systems
- Oil and gas
- Air-traffic control systems, resulting in collisions of civilian aircraft.
- Medication formulas at pharmaceutical manufacturers.
- The electrical grid, causing blackouts.

In the Government or University setting you will find that the electrical grid causing blackouts would be your most common problem but with our lives becoming more and more dependent on computers, the problems are as large as the imagination of the students or terrorist. The computer and network equipment at your site could also be co-opted into launching a denial of service attack on another element of your facility or an outside entity.

Facility Infrastructure vulnerabilities

The major problem that we have in America is the dependence we have on automation and our computerized way of life. If we look at all systems that are computerized in an organization environment it becomes apparent how vast our dependence is on our technology systems.

From our police communication systems, fire control systems, hospital support systems, bio research refrigeration systems, climate control, communication and satellite uplinks we find ourselves continuously accessing more and more automated systems.

The *Intelligence Report* from the Centre for Infrastructural Warfare Studies lists more than 30 infrastructure-related incidents worldwide in just the previous two weeks before the article was written.

For example:

- A natural gas explosion cuts service to 1.4 million households in Australia for 14 days at a cost of more than \$750 million.
- A car accident fells an electrical transmission line, blacking out 19,000 homes in Sonoma and Napa counties.
- Attacks on Nigerian oil pipelines block the flow of 130,000 barrels per day of crude oil.

According to CIA director George Tenet in congressional testimony, "We rely more and more on computer networks for the flow of essential information. Potential attackers range from national intelligence and military organizations, terrorists, criminals, industrial competitors, hackers and disgruntled or disloyal insiders."

There are plenty of incentives, he said: "Trillions of dollars in financial transactions and commerce moving over a medium with minimal protection and sporadic law enforcement; increasing quantities of intellectual property residing on networked systems; and the opportunity to disrupt military effectiveness and public safety, with the elements of surprise and anonymity."

Cyber weapons that are in use

The cyber terrorist's traditional weapons such as Trojan horses, worms, computer viruses and logic bombs that wake up on a certain date, cracking, sniffing, social engineering and dumpster diving are not all that they have to use against us.

A new tactic, coordinated large-scale attacks, emerged about 3 years ago. They reported the details of intrusion attempts involving multiple attackers working together from different IP addresses, many in different countries and continents. The intent apparently was to make the attacks more difficult to detect, increase the "firepower" and acquire more data, he said.

Most commercially available IDS (intrusion detection systems) cannot detect such large-scale attacks. But the Government has systems such as the Navy's SHADOW (Secondary Heuristic Analysis for Defensive Online Warfare) software can detect and track such attacks.

TEMPEST

Another advanced cyber terrorist tool is monitoring computers, fax machines, printers and other devices by picking up their electromagnetic radiation. TEMPEST devices (Transient Electro-Magnetic Pulse Emanation Standard, also called "Van Eck" devices after Wim van Eck who wrote the first paper on the subject in 1985) pick up radiation mainly from monitors and connecting cables. They allow cyber spies to intercept your password, proprietary business plan or embarrassing love letter, clearly displayed on their monitors.

Such monitors can be as far away as 1 kilometer—or further if they have special fast-fourier-transform chips and other classified systems designed by the National Security Agency (or its foreign counterparts or your competitors). And there's no way for you to know you're being monitored.

RF Weapons are real

Radio Frequency (RF) weapons can zap your computer into oblivion from a distance. RF weapons are real, according to top military experts at congressional Joint Economic Committee hearings. RF weapons consist of a power supply, transmitter and antenna. HPM, one type of RF weapon, (high-power microwave), generates gig watts (billions of watts) of short, intense energy pulses focused into a narrow beam capable of silently burning out electronic equipment, according to retired U.S. Army Lieutenant General Robert L. Schweitzer in congressional testimony.

RF weapons are also packaged as RF munitions, which use explosives to produce radio-frequency energy. "In the hands of skilled Russian scientists, these munitions come as hand grenades, mortar rounds, or large artillery shells or missiles," Schweitzer said.

"The horse is out of the barn," warned Schweitzer. "We are the most vulnerable nation on earth to electronic warfare. ... Our vulnerability arises from the fact that we are the most advanced nation electronically and the greatest user of electricity in the world."

Schweitzer said potential targets of RF weapons include computers and other electronic devices used in the national telecommunications systems, the national power grid, the national transportation system, mass media, oil and gas control and refining, manufacturing processing, inventory control, shipment and tracking, public works, civil emergency service and finance and banking systems, including a bank's ability to dispense cash.

Ninety percent of our military communications now passes over public networks. If an electromagnetic pulse takes out the telephone systems, we are in deep double trouble because our military and non-military nets are virtually inseparable. It is almost equally impossible to distinguish between the U.S. national telecommunications network and the global one. What this means is that it is finally becoming possible to do what Sun Tzu wrote about 2,000 years ago: to conquer an enemy without fighting.

"The paradigm of war may well be changing. If you can take out the civilian economic infrastructure of a nation, then that nation in addition to not being able to function internally cannot deploy its military by air or sea, or supply them with any real effectiveness—if at all."

Schweitzer also said the former Soviet Union developed RF weapons because they realized they could not match the capability of Western electronics but believed RF weapons "have the potential to be effective against our sophisticated electronics."

With the reduction in military spending, Russia is now offering this advanced weaponry to foreign customers to further its own R&D efforts, he said. Based on proceedings of 20 years of international conferences—many hosted and initiated by the United States.

Transient Electromagnetic Devices (TEDs)

There is a new class of ultra-wide band (UWB) devices, also known as Transient Electromagnetic Devices (TEDs), are easier to construct and use. They may be "the RF weapon of choice to the modern cyber or infrastructure RF warrior," said engineer David Schriener before the congressional Joint Economic Committee.

TEDs generate a blast of spike-like electromagnetic pulse that is only one or two hundred picoseconds (or trillionths of a second) in length at very high peak power. They radiate over a broad band of frequencies, so they can burn out a broad range of devices, with effects on electronics systems that are similar to a lightning strike. They would work well on a hospital floor. TED power supplies are much smaller, less expensive, require less power and are easier to build. They use simple spark-gap switches and can be assembled from automobile ignition, fuel pump and other readily available parts in about a week for about \$300 using unclassified literature.

The compact devices could fit in a briefcase or be "placed in a small van ... or directed at buildings that the van was driven past." With a six-foot backyard satellite TV-dish antenna and more advanced spark-gap unit, terrorists could point them at flying aircraft.

Reducing the risk of RF

So how can you defend against these weapons? For starters, you can harden your critical system computers, networks, cables, printers and other devices to make them more resistant to electromagnetic radiation. This is especially important on critical systems that will not tolerate the time it takes to backup and recover data. A side benefit of hardening is that it helps protect you from TEMPEST snooping.

We must look at ways to defend our systems in this growing threat. The defenses that we have used in the past to protect our infrastructure will be of little use in protecting us from a cyber threat in this new virtual world. Our infrastructures and systems can now be vulnerable to direct strikes by a variety of malicious tools.

Eavesdropping on a computer

TEMPEST (Transient Electro Magnetic Pulse Emanation Standard) systems are commercially available for purchase and are legal to use. You need to be aware that there are many people in this industry that sell products that are not very reliable. You need to also be aware of the counter measures that are needed to detect and then protect your system this type of attack. Antennas are easily disguised inside a van with a plastic panel or even in a dorm room of one of your students.

You can reduce your chance of attack from TEMPEST by adding shielding to your systems and switch to optical fibers, or use "TEMPEST fonts" that decrease radiation from monitors. If you have a security clearance, you can purchase expensive TEMPEST-certified systems. Or you can buy used TEMPEST-shielded computers and other devices without a clearance. For other ideas and some names of firms that are involved in conducting TEMPEST shielding you can email me at the below address.

Disgruntled Employee's

We have recently seen where disgruntled ex employee's have been charged for hacking into an ex employers system. There was also a case in August where an outside computer consultant was arrested for going back in and sabotaging a system because he thought he was owed more money. This will continue to be a problem. Programmers are notorious for building in backdoors to the systems that they design so that they can go back in and make changes as needed. The problem is when they are no longer working for the company, they still have that access.

You also have many cases of disgruntled employees taking whatever records that they have access to and emailing them out to the people in the business. This has happened several times with pay records being published causing problems with co-employees feeling slighted about their pay.

In the education fields there have been many cases of student grades and or test being posted to bulletin boards. These things can be preempted by having a strong IT security department that reports to the proper person.

Sexual Assaults and Child Abductions

A recent study reports that 32% of child/teen abductions are initiated over the internet. As institutions of higher learning we do not have to worry much about children being taken, but we do have to worry about the abductors using our computers to initiate the assault. We also have the obligation to protect our children from the sexual assaults and from assailants. This will mean that we need to continue to educate our children, faculty and coworkers about the hazards and risk of internet.

Recommendations

Facilities managers must be on high alert during these times of continued acts of Terrorism and with the Countries expanded war on Terror. You must understand that with the Government securing their systems and making them harder to penetrate that cyber terrorist will look for an easier target that will still get him notoriety. They may also target your system to get access to government systems that may be on line with you due to research projects.

You need to be on high alert for warning signs of impending hostile cyber attacks, especially immediately during and following a military strike. Pings by potential attackers is common in network operations, but changes in the normal number of attacks should be noted and considered highly suspicious during these high alert periods. You should notify your IT manager as well as the proper authorities.

They will need the following information.

- Names, location and purpose of the operating system involved
- Names and location of programs accessed
- How intrusion access was obtained

- Highest classification of information stored in the system
- Impact of compromise and amount of loss

To protect evidence and help law enforcement agencies investigate the incident, take the following actions:

- Make backup copies of damaged or altered files and store off site
- Activate all auditing software
- Consider implementing a keystroke monitoring program
- DO NOT contact the suspected perpetrator

Routine risk assessments of your information infrastructures provide important information about the condition of your system and should be a priority. You should also develop an incident management policy and plan and insure that it was in place.

Your best defense from cyber attacks is to insure that:

- Comprehensive password programs should be used.
- Intrusion Detection Systems and firewalls should be in place
- Operating systems and software should be updated regularly
- All unnecessary services should be removed or disabled
- Anti-virus software should be installed and kept up to date
- Systems should be properly maintained with security patches installed in a timely manner.
- IT Security compliance and detection audits should be conducted

With all that is happening around the world with terrorism, we have to remember two things first is that the efforts we used two years ago are not adequate any longer with the increased threat. From a liability side with all of the press and media coverage of terrorism, it will be impossible for you to walk into a court room and try to explain to a jury that you did not know that there was a problem. If you have a dorm full of students die due to the fire control system being shut down, the elevators falling and killing the occupants or the hospital life support systems being burned up the civil suits will be endless.

We must secure our critical assets without financially crippling our budgets. To do this we must set our priorities. We must identify our most critical systems and insure implementation on those systems. You have to implement anti defacement measures for web server exploits.

Authentication mechanisms should be in place on border routers to prevent malicious tampering with router tables. Secure software should be running on Domain name servers to prevent DNS corruption and redirecting of web traffic. Log records need to be copied and kept off site as well as back up data. You need to install ingress and egress filters to limit spoofed ID addresses and un-trusted source addresses.

We know that military attacks are increasingly accompanied by cyber attacks. With this knowledge and the current events, we need to be aware of the probability of having wide spread cyber attacks here in the United States. Most attacks in the past have been nuisance attacks, but with the data that we have at this time, we know that the potential exists for a devastating cyber attack. These attacks could come from inside or outside the United States and if the attack is on the infrastructure networks it could have a large impact on your facility.

Appendix: Resources

<http://www.cert.org>

The Carnegie Mellon Computer Emergency Response Team Coordination Center is a major reporting center for internet security problems that analyzes product vulnerabilities.

<http://www.sans.org>

The System Administration Networking and Security Institute

<http://www.nipc.org>

The National Infrastructure Protection Center

<http://www.ofrac.com>

Office for Regulatory Audit and Compliance

<http://www.GoIDRC.com>

International Dynamics Research Corp. Information Technology compliance department

<http://Incidents.org>

Incidents.org is a community and industry collaboration on security related matters that produces practical technologies.

<http://www.fedcirc.gov>

The Federal Computer Incident Response Center (FedCIRC)

<http://www.goATAB.org>

The Anti-Terrorism Accreditation Board resource materials (ATAB)