Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Can Cyberterrorists Actually Kill People?

Corporate road warriors become an increasing threat as a point of unauthorized access to restricted networks. Crackers probe network defenses and attack undefended systems that have insecure perimeters. Chinese and American hackers hijack web-pages and use them to rattle digital sabres and spread nationalist propaganda. Hacktivists send email bombs that overwhelm servers at organizations they are protesting against. Script kiddies give orders to zombie computers deployed across the internet and order them to attack tar...

Copyright SANS Institute
Author Retains Full Rights

AD

Can cyberterrorists actually kill people?

© SANS Institute 2002, Author retains full rights.

Full Name: **Scott Anthony Newton**

Course/Certification: **Security Essentials / GSEC**
Submission: **Original**
Version of Assignment: **1.2f**
Group I'm taking the certification with: **North Pacific SANS, Vancouver, BC; November 2001**

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Table of Contents

DEFINITIONS, v2.0.0.2	3
INTRODUCTION (SP1)—Obligatory Imaginary Disaster Scenario	3
THE QUESTION—Robust and Scalable	4
THE ANSWER—Design Document	5
MORE ANSWERS—Beta Code	6
EPISODE: Monday TARGET: Medical Records	6
EPISODE: Tuesday TARGET: Trains	7
EPISODE: Wednesday TARGET: Factories	8
EPISODE: Thursday TARGET: Dams	9
EPISODE: Friday TARGET: Air Traffic and Nuclear Power Plants	9
CONCLUSIONS—Don't install it until the first patches are released…	10
Notes/Bibliography	12

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

DEFINITIONS, v2.0.0.2

Instead of trying to gracefully work them into a smooth-flowing narrative, let's just recognize them for what they are and list them right up front:

warfare

"the waging of armed conflict against an enemy"[1]

information warfare

"any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions"[2,3]

terrorism:

"criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes are in any circumstance unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or other nature that may be invoked to justify them"[4]

The above definition is similar to the one offered by the United States FBI, which is often quoted. However, it does not address the inherent violence of terrorist acts like those in Oklahoma City, New York, Washington, Ireland and Israel, to name but a few. The United Nations Office for Drug Control and Prevention borrows a definition by Alex Schmid that expands on the one above by mentioning:

"repeated violent action…whereby…the direct targets of violence are not the main targets. The immediate human victims of violence are generally chosen randomly (targets of opportunity) or selectively (representative or symbolic targets) from a target population, and serve as message generators…"[5]

cyberterrorism:

"…unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives…an attack should result in violence against persons or property, or at least cause enough harm to generate fear…attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss…"[6]

INTRODUCTION (SP1)—Obligatory Imaginary Disaster Scenario

A government emergency response staffer reports to work and spends a very busy couple of days managing the following incidents, looking for patterns, and trying to predict and prevent the spread of death and destruction:

- A U.S. fighter jet crashes mysteriously into the ocean just after midnight
- ATM machines quit counting higher than $20
- A hospital patient dies due to a computer glitch in the operating room
- Computer-controlled prison doors unlock automatically and release hordes of deadly convicts

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- 911 emergency phone service goes dead
- Cities plunge into darkness as power grids fail around the globe
- A Swedish nuclear power plant malfunctions and kills everybody working there
- Another nuclear plant in Seattle threatens to melt down and take out Puget Sound

Is this the sequel to September 11? An Al Qaeda wish list found in a bombed-out house in Kandahar? Predictions by Nostradamus? No, it is (was) *Y2K: The Movie*.[7] In November of 1999, NBC television offered this disaster of a disaster movie to a mass-market audience pondering the threat of a global catastrophe at the hands of a two-digit computer bug.

While many of the scenarios in the movie were unlikely to occur in the real world (at least not all at once), the potential for chaos during Y2K was real. And no doubt such chaos could have looked attractive to a terrorist watching TV from a cave in Afghanistan (or a bunker in Iraq, or a shack in Somalia, North Korea, North Dakota…).

Just imagine—if civilization as we know it could fall into such a panic and possibly spiral out of control over a relatively minor programming error, what would happen if somebody sat down and starting causing these kinds of malfunctions on purpose? Could terrorists or rogue nation soldiers kill people while tapping away in their living rooms, using nothing more than a dial-up internet connection and laptop computer they ordered from an ad in the back of a magazine?

THE QUESTION—Robust and Scalable

The official definitions (and the popular notions) of information warfare and cyberterrorism assume the use of computers or networked systems to disrupt infrastructure. It should also be assumed that modern warfare relies heavily on information technology to gather intelligence, plan attacks, and deliver ballistic weapons to their targets. In addition, defending armies should be expected to prevent their foes from delivering those weapons by jamming enemy systems or camouflaging suspected targets with false signals.

Allied forces sorting through the rubble of Afghanistan (and various cybercafes and home computers around the world) have shown without a doubt that Osama bin Laden's terrorist organization used information technology to gather and disseminate information, train attackers, plan their attacks, finance their operations, gloat over their successes and receive real-time guidance in overcoming mission obstacles[8]. But in the end, the terrorists accomplished their goals of killing and terrorizing citizens by blowing things up.[9] In return, while the Allied forces relied heavily on networked systems to unleash their military assault on Taliban and Al Qaeda forces, again the end result was to blow things up with conventional bombs and bullets.

Yet discussions of digital confrontations have increasingly adopted the language of their more traditional, ballistics-based counterparts: Corporate road warriors become an increasing threat as a point of unauthorized access to restricted networks. Crackers probe network defenses and attack undefended systems that have insecure perimeters. Chinese and American hackers hijack web-pages and use them to rattle digital sabres and spread nationalist propaganda. Hacktivists send email bombs that overwhelm servers at organizations they are protesting against. Script kiddies give orders to zombie computers deployed across the internet and order them to attack targets. Network administrators capture packet traffic so they can analyze it and gain intelligence

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

on how to defend against the attack. And there is a debate as to whether those network admins should launch retaliatory strikes or other types of digital counterattacks.

But instead of simply causing annoying service disruptions, catastrophic data loss, or even the fall of a technology-dependent society, could cyberterrorists and information warriors use computers to actually kill people directly?

THE ANSWER—Design Document

The use of information technology to kill people directly, rather than merely facilitate that killing, remains mostly in the realm of science fiction movies and books like *Tron*, *The Matrix*, and *Neuromancer*. But in the real world of 2002, plenty of opportunities exist for cyberterrorists and information warriors to use computers as genuine killing machines. Whether or not they would do so is another matter.

Let's take a look at the possible sequel to *Y2K: The Movie*, called *CyberTerrorWar: The Mini-series*. In this week-long sweeps opus, a different form of cyberterror threatens our cyberheroes, and the physical population each night.

- On Monday, random people die around the world as they receive the wrong medications, thanks to terrorists who have compromised patient databases with Trojan code that prescribes lethal drug combinations.
- Tuesday finds the terrorists attacking the world's railway switching networks, causing trains to collide, derail, and spew toxic chemicals into the surrounding communities.
- Come Wednesday, the terrorists release more toxic chemicals into more towns and cities by compromising storage facility and manufacturing control networks in factories and raw material processing plants.
- By Thursday, the terrorists are gearing up for their grand finale. They have hacked their way into the computer networks of numerous regional hydroelectric companies, opened the waterways, and started drowning everybody who lives below the reservoirs.
- Finally, on Friday night, everybody's two greatest fears culminate in a sure-fire ratings winner: the terrorists seize control of the computer networks that maintain the world's air traffic control and nuclear power plants. Hundreds of passenger airliners collide or simply fall from the sky, while nuclear power plants erupt in fiery balls of radioactive annihilation, killing hundreds of thousands of civilians instantly, while planting the seeds of future cancer epidemics within millions more people.

As *Y2K: The Movie* prepared to air, several government agencies determined that the show was irresponsible and a possible cause of mass hysteria. As government agencies (and certain software monopolies) are wont to do, they asked the network to withhold any potentially problematic information from the public. At the very least, scientists and government officials felt that NBC should give them equal time after the broadcast to discuss the realities of the Y2K problem.[10] Neither of those things happened, but since *CyberTerrorWar* is even more over the top than *Y2K*, the government officials and academics will probably be given a chance to calm what may or may not be irrational fears after each episode. Viewers watching the post-episode analysis each night might have discovered the following information.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

MORE ANSWERS—Beta Code

EPISODE: Monday
TARGET: Medical Records

The U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA), among other things, calls for the strict protection of patient medical records, whether they be in a paper folder in a country doctor's office or in massive databases owned by national health insurers and their business partners. But HIPAA pays particular attention to network security and the electronic transmission of patient data. The implication is that these electronic records are at risk for compromise (as any network administrator worth his or her salt already knows). In fact, the Australian Institute of Computer Ethics cites altered medical records as one of the many problems caused by hackers.[11]

While HIPAA's overriding concern is protecting the confidentiality of patient records, the more recent USA Patriot Act seeks to strengthen existing anti-terrorism laws by designating "the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals"[12] as an act of terrorism.

While this provision could apply to an act as blunt as shooting a patient in surgery or blowing up a hospital, the legislators added the language to the section titled "Deterrence and Prevention of Cyberterrorism." The placement of this clause again implies that electronic patient records are at risk of compromise, and further suggests that those compromised records could bring harm to people.

The above addition to an existing law looks like a blank check to prepare for an uncertain threat that may or may not materialize. But a U.S. State Department web site for its Pakistan consulate makes the following direct comment in a discussion of cyberterrorism:

> "An example of cyber-terrorism could be hacking into a hospital computer system and changing someone's medicine prescription to a lethal dosage as an act of revenge. It sounds far fetched, but these things can and do happen."[13]

If "these things can and do happen", then terrorists can and might use those tactics to further their cause. However, there are several reasons why terrorists probably won't use this approach.

First, it would simply take too much time and energy. There are far too many types of systems and too many types of databases out there to make such an attack effective in causing widespread panic or terror.

Second, any such operation would require legions of highly skilled hackers and programmers, working in concert with medically knowledgeable colleagues. The resources required to launch these kinds of attacks would, from the terrorists' point of view, have a relatively small payoff.

Finally, medical staff are already highly trained and widely deployed as a defense against these types of operations. Nurses and pharmacists are required to recognize incorrect dosages and combinations of drugs. In fact, even if a doctor (or altered database) prescribed a harmful dosage

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

and the pharmacist filled it, the nurse administering the medication would still be liable for any harm to the patient, because "as nurses, we're trained to know better."[14]

In the end, it would be easier to just send a suicide bomber into the emergency room.

EPISODE: Tuesday
TARGET: Trains

In response to the September 11 attacks, railroads across the United States strengthened physical security around their physical assets, especially railway bridges and hazardous material tankers. But the trains kept running, and in fact Amtrak expanded its passenger service to accommodate stranded air travelers. Near midnight on December 31st, 1999, however, Amtrak planned to stop every train in North America until the date change had occurred,[15] as did rail authorities in Australia[16], Belgium,[17] France,[18] Italy, and other parts of Europe and Asia, as well as commuter rail systems in Chicago and Washington.[19]

In public, railway officials said that even though they were confident all systems would work properly after midnight, they merely wanted to reassure anxious passengers. But an official report from the Federal Railroad Administration was less confident: "... no organizations whose operations depend as heavily on computers and software as the railroad industry can be absolutely sure there will be no date-related glitches that escaped redemption."[20] Such statements allow for the possibility that terrorist-related "glitches" could also cause life-threatening accidents.

The threat is real enough that the RAND National Defense Research Institute cited a rail-related cyberattack in a report prepared for the U.S. Secretary of Defense. As part of the complex threat scenario, a

> new high-speed Metro-Superliner traveling at 300 km/hr slammed into an apparently misrouted freight train near Laurel, Maryland. Maryland State Police estimated that the train wreck had killed over 60 passengers and crew and critically injured another 120 persons. Within three hours, the National Transportation Safety Board (NTSB) chief investigator notified the Secretary of Transportation that there was "clear evidence" that the freight train had been misrouted onto the Metroliner track with "some evidence" pointing to a sophisticated intrusion into the East Coast rail control system.[21]

And, in fact, Japanese extremists may have already tried something along these lines. According to the background information in another paper for the National Defense University, Japanese "…groups have attacked the computerized control systems for commuter trains, paralyzing major cities for hours…"[22] Combine that possibility with the cult members who released poison gas into the Tokyo subway system in 1995, and you have a potential for tremendous casualties. While the poison gas might be considered a more conventional, physical attack, shutting down the train system at the time of that attack, via a computer system intrusion, would result in a cyberterrorist operation that could kill thousands.[23]

Now, given the possibility of cyberterrorists attacking regional rail control systems, it's not hard to imagine those same terrorists causing all kinds of collisions and derailments that would spill

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

chlorine, nuclear waste, or a host of other toxic chemicals that travel by rail every day. These accidents would force the evacuations of large neighborhoods, and in some cases, entire towns. And in most cases, the casualties would probably be light, depending on the location of the release and the weather. But if the terrorists wanted to go the extra mile, they could access the national database that lists authorized railways routes for transporting hazardous materials,[24] and cross-reference that with another national registry, this one identifying exactly what chemicals are in what railroad cars at any given time. Mix that information with data from another railway scheduling database, add control of the railway switching operations, and a terrorist could theoretically target trains carrying the most toxic chemicals, causing them to derail and release their cargo in the most populated areas at the deadliest times of day.

It's interesting to note that in the wake of September 11, the railroad industry began to restrict public access to cargo and scheduling information that was once available on the Internet…[25]

EPISODE: Wednesday
TARGET: Factories

In 1984, toxic chemicals spewed out of a Union Carbide pesticide plant in Bhopal, India, causing over a quarter of a million casualties: 3,820 dead, 2,720 permanently disabled, and 230,789 others injured in varying degrees. Another 155,203 reported to area medical facilities for examinations. This catastrophe was caused by the release of too much in water in a manufacturing process.[26]

Now imagine all of the chemicals that millions of people around the world use to clean their kitchens, bathrooms, yards, cars, tools, manufacturing equipment… Next, imagine other manufacturing plants in locations throughout the world, all using manufacturing processes that mix chemicals and other additives to either concentrate or dilute their toxicity. Finally, imagine all those manufacturing processes being controlled by computers. The potential for disaster at the hands of cyberterrorists is huge.

As usual, the internet can help a terrorist decide how to select the most lethal industrial target. Government agencies across the United States and environmental organizations like Greenpeace identify sites containing toxic chemicals, either by regulation or in the name of public awareness. All a terrorist would have to do is select a potential target, get an email account, enter a sample address on a government web form, and wait a few days for the Environmental Protection Agency to email him or her back and identify whether or not that address is at risk of exposure to hazardous materials.[27] Once the target has been selected, it's back to the grunt work of gaining access to the insecure networks and trying to alter manufacturing scripts or databases that could result in an explosion and/or release of poisonous chemicals into the air.

Terrorists have options other then a direct hack when it comes to sabotaging manufacturing plants and killing nearby residents. In Russia, hackers used a gas company employee to plant a Trojan horse which gave them control of the nation's gas pipelines. In Japan, the same Aum Shinrykok cult that gassed the Tokyo subways turned out to be a major government and industry software subcontractor. And the U.S. State Department recently recalled software from some 170 embassies, after realizing that the programs had been written in the former Soviet Union and could contain dangerous code.[28] Software savvy terrorists could just as easily infiltrate software

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

houses that produce manufacturing process software, and with so much coding done off-shore these days, the potential for problems is even more widespread.

EPISODE: Thursday
TARGET: Dams

Most discussions about terrorist attacks upon dams involve ballistic and/or explosive devices, such as a missile or plane crashing into a dam and breaching it, or the poisoning of the nearby water supply. While a physical breaching of these dams could obviously cause catastrophic death and destruction to people living in the valleys below, engineers appear to be confident that their structures can withstand most of these types of attacks. But what about a cyberattack?

In at least one instance, "a hacker known as 'Infomaster' penetrated the Bureau of Land Management network in Portland, then skipped on to Sacramento where (s)he obtained root access to the computers that controlled every dam in northern California."[29] While the tellers of Infomaster's tale suggest that his cyberwanderings could have caused the deaths of tens of thousands of people, a quick survey of contingency plans and interviews with officials from dams and hydroelectric agencies around the United States suggests otherwise.

The best a cyberterrorist could hope to do after taking control of a dam's computers would be to open the floodgates and drain the reservoir into the populated valleys below. However, it would still be a controlled release, not a devastating wall of water that might result from a major breach. True, the towns and cities that are typically far downstream from the dams would eventually end up under water, and in some cases be washed right off the map. But the floodwaters would take hours, and in some cases days, to accumulate. That timetable would leave residents plenty of time to evacuate to higher ground. Even a town like Redding, CA, with 80,000 residents living just ten miles downstream from the nation's second largest concrete dam (Shasta) would have hours to evacuate in the face of a major breach.[30] While the eventual property and psychological damage from an electronically compromised dam would be catastrophic, the loss of life in most instances should be minimal.

EPISODE: Friday
TARGET: Air Traffic and Nuclear Power Plants

We know all too well the death and destruction a terrorist can cause when attacking an aircraft with explosives or a suicidal pilot. But could those suicide attackers be replaced by cyberterrorists who compromise air traffic and flight control systems?

In his 1997 Annual Report to the President and Congress, Secretary of Defense William Cohen mentions in passing the possible use of cyber attacks to create a situation where the "air traffic control system collapses in a cascading effect[31] But in a summary of 41 cybercrimes prosecuted by the government between 1998 and 2001, only one involved a "threat to public health or safety," and that one incident involved a teenager disabling a single FAA control tower.[32] While the hacker did not actually take command of any air traffic control systems, he did disable several pieces of vital communications equipment that managed runway resources and aircraft interaction.[33]

Most aircraft collisions occur when pilots don't maintain sufficient situational awareness; most single aircraft crashes are caused by human error or mechanical failure. One would hope that

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

even if the entire air traffic control system were taken out by a terrorist or military attack, most pilots could rely on their visual flight rules training and get their ships safely to the ground. They may not get them back up for some time, but at least their passengers would be safe.

A potentially more effective form of cyberterrorism that could actually cause planes to crash into each other and fall from the sky would be to follow the example of the previously mentioned industrial saboteurs—infiltrate the contracting and subcontracting corporations that design and manufacture avionics equipment, and try to plant logic bombs and Trojans in the code that will activate at a later date and disable flight controls on the aircraft.

As for nuclear power plants, even the Nuclear Regulatory Commission admits that "increasing vulnerabilities to cyber-terrorism continue as systems become more automated".[34] Just what those vulnerabilities are, however, the NRC declines to say. One might suppose that nuclear power plants would be subject to the same types of vulnerabilities as chemical production plants, dams, and the air traffic control system, but instead of mixing toxic chemicals, terrorists would try to program insufficient cooling of nuclear material to cause a meltdown. However, one would also hope that greater precautions have been taken to make sure that such an attack can't occur, and that if one did, that redundant systems and failsafes would prevent a catastrophe.

But again, sophisticated cyberterrorists could plant their cyber weapons as trap-doors in source code while working as programmers who have infiltrated government agencies and contractors, or more likely, sub-contractors. Indeed, in the wake of extensive Y2K reprogramming, the Government Accounting Office and National Security Council were concerned that malicious code could have been planted in nuclear power plant software.[35] Still, the vast majority of research and discussion in to nuclear terror revolves around explosive-based attacks on power plants or the use of more conventional nuclear weapons (oxymoron intended…)

CONCLUSIONS—Don't install it until the first patches are released…

Well, that's quite a mini-series. And as with many Hollywood offerings, some possibilities deserve more consideration than others. Trains and factories (especially factories) could be vulnerable to deadly cyberterrorist attacks that could kill many people. But while cyberterrorists could access and control the networks controlling dams, air traffic, medical records and nuclear power plants to kill people, it would be more efficient to just use traditional ballistic or explosive weapons against these targets.

Another possibility worth considering is that that few (if any) hackers, and therefore cyberterrorists, would electronically attack an enemy system directly. They would instead be spoofing IP addresses, relaying potentially deadly packets through router after router to cover their tracks, and using zombie computers to do their bidding. Cyberterrorists could in fact use even the most innocent of unsecured home or cooperate computers to carry out deadly terrorist acts.

Those possibilities are just one more reason for corporations and individuals to secure their own machines, no matter how innocuous their function might be. If we don't, we might find terrorists using our own infrastructure against us, as they did against the United States on September 11.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Indeed, as physical security continues to tighten around likely targets, while processing power and network knowledge becomes cheaper, we can probably expect some of the suicide bombers to start spreading their terror with the click of a mouse instead of a detonator…

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Notes

All links verified
23 January 2002

[1] Princeton University. *WordNet*. http://www.cogsci.princeton.edu/cgi-bin/webwn1.7.1?stage=1&word=warfare
[2] Fogleman, Ronald R., General, USAF Chief of Staff & Widnall, Sheila E., Secretary of the Air Force. *Cornerstones of Information Warfare/* (no date given). http://www.af.mil/lib/corner.html.
[3] The Air Force definition also includes the bombing of information-related facilities as a component of information warfare.
[4] United Nations General Assembly. *Resolution 51/210: Measures to eliminate international terrorism*, (paragraph 2 of section I). (16 January 1997): page 2. http://www.un.org/law/terrorism/english/a51_210e.pdf
[5] http://www.undcp.org/terrorism_definitions.html
[6] Dorothy E. Denning, Director of the Georgetown Institute for Information Assurance, Georgetown University. *Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives.* (23 May 2000). http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html
[7] Hayes, David and Bullers, Finn. "Don't Bother with 'Y2K: The Movie'". *Kansas City Star,* 12 November 1999. http://www.kcstar.com/item/pages/business.pat,business/37740144.b12,.html
[8] In reference to the so-called "shoe-bomber," Richard Reid, who emailed his superiors in Pakistan to ask what he should do after he was detained for questioning by Paris airport officials and missed the plane he was assigned to blow up. *(*CNN. "Authorities track e-mails sent by alleged shoe bomber". (22 January 2002). http://www.cnn.com/2002/WORLD/europe/01/21/inv.reid.emails/index.html)
[9] Of course, other terrorists have resorted to less explosive methods, such as the Bhagwan Shree Rajneesh disciples who sprayed salmonella on restaurant salad bars throughout The Dalles, Oregon in 1984, the doomsday cultists who unleashed poison gas in Tokyo subways in 1995, and the recent anthrax attacks in the United States.
[10] Hayes, David and Bullers, Finn. "Don't Bother with 'Y2K: The Movie'". *Kansas City Star.* (12 November 1999). http://www.kcstar.com/item/pages/business.pat,business/37740144.b12,.html
[11] Warren, M.J. and Furnell, S.M.. "Cyber-Terrorism – The Political Evolution of the Computer Hacker", *Australian Institute of Computer Ethics Conference.* (July, 1999): page 3. http://www.aice.swin.edu.au/events/AICEC99/papers1/WAR99024.pdf
[12] 107th Congress of the United States of America. *H.R. 3162 (USA Patriot Act of 2001).* SEC. 814(a)(4)(B)(ii). (03 January 2001): page 158. http://www.ins.usdoj.gov/graphics/lawsregs/patriot.pdf
[13] Public Affairs Office of the U.S. Consulate Lahore, Pakistan. "Special Issue on Terrorism". *Lahore IRC Alert,* (January 2002). http://usembassy.state.gov/lahore/wwwhircaterror.html
[14] Atkinson, Jennifer, R.N.. *Personal Interview.*(09 December 2001).
[15] Johnson, Glen, Associated Press. "Amtrak docks trains for Y2K". *Madison County Journal.* (23 January 1999). http://www.onlinemadison.com/19991223/amtrak.html
[16] Bennetts, David. "Y2K Fears to Stop Cityrail Trains". (27 July 1999). http://www.railpage.org.au/ausrail/99july/msg01907.html

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

[17] Reuters. "Y2K Prompts Belgium to Halt Trains Over New Year". *InfoSec.com.* (28 December 1999). http://www.info-sec.com/y2k/99/y2k_122999g_j.shtml
[18] Reuters. "French Trains to Stop Near Midnight". *ABC News.* (04 October 1999). http://abcnews.go.com/ABC2000/abc2000world/Frenchrail_991004.html
[19] Johnson, Glen, Associated Press. "Amtrak docks trains for Y2K". *Madison County Journal.*(23 December 1999). http://www.onlinemadison.com/19991223/amtrak.html
[20] Stephens, Erica. "Planes, trains, trucks ready as ever for Y2K". *Atlanta Business Chronicle*. (20 December 1999). http://atlanta.bcentral.com/atlanta/stories/1999/12/20/focus6.html
[21] Molander, Roger C., Riddile, Andrew S. and Wilson, Peter A.. *Strategic Information Warfare: A New Face of War.* (1996): page 10. http://www.rand.org/publications/MR/MR661/MR661.pdf
[22]Stark, Rod, Department of Defense & Strategic Studies. "Cyber Terrorism: Rethinking New Technology". (199?): page 15. http://www.infowar.com/MIL_C4I/stark/Cyber_Terrorism-Rethinking_New_Technology1.doc
[23] No author cited. "Cyberterrorism hype", *IWS – The Information Warfare Site*, reproduced from *Jane's Intelligence Review.* (21 October 1999). http://www.iwar.org.uk/cyberterror/resources/janes/jir0525.htm
[24] Federal Motor Carrier Safety Administration. *National Hazardous Materials Route Registry.* http://hazmat.fmcsa.dot.gov/info.html
[25] Johnson, Jeff. "Airline Security 'Like Fort Knox' Compared to Railroads". *CNS News.* (03 October 2001). http://news.crosswalk.com/partner/Article_Display_Page/0,,PTID74088%7CCHID194343%7CCIID899438,00.html
[26] Union Carbide Corporation. "Incident Review" (http://www.bhopal.com/review.htm) and "Chronology" (http://www.bhopal.com/chrono.htm). *Bhopal.* http://www.bhopal.com/index.htm.
[27] Environmental Protection Agency. Vulnerable Zone Indicator System. http://www.epa.gov/ceppo/vzis.htm
[28] Dorothy E. Denning, Director of the Georgetown Institute for Information Assurance, Georgetown University. *Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives*. (23 May 2000). http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html
[29] Marcella, Albert J., Jr.. "Cyber-Terrorism: Is Your Company a Target?", reproduced on *MBDNetwork Services* website. (2001). http://www.mbdnetworkservices.com/news/cyberterror.html. (While this effective paragraph is often quoted on the web, the comprehensive exploits of Infomaster, aka PhantomDialer, aka phantomd, aka a mentally challenged teenager, are detailed in the book *@LARGE:The Strange Case of the World's Biggest Internet Invasion*, by David H. Freedman and Charles C. Mann, Simon & Schuster, 1997-1998).
[30] Breitler, Alex. "Keeping the guard up". *Redding Record Searchlight.* (30 September 2001). http://www.redding.com/top_stories/local/20010930toplo008.shtml
[31] Stark, Rod, Department of Defense & Strategic Studies. "Cyber Terrorism: Rethinking New Technology". 13. 199?): page 13. http://www.infowar.com/MIL_C4I/stark/Cyber_Terrorism-Rethinking_New_Technology1.doc
[32] Computer Crime and Intellectual Property Section. "Computer Intrusion Cases". *U.S. Department of Justice* website. (14 January 2002). http://www.usdoj.gov/criminal/cybercrime/cccases.html
[33] Computer Crime and Intellectual Property Selection. "Juvenile computer hacker cuts off FAA tower at regional airport". *Press Release*. (18 March 1998). http://www.usdoj.gov/criminal/cybercrime/juvenilepld.htm
[34] U.S. Nuclear Regulatory Commission Staff. "Strategic Plan: Appendix, Fiscal Year 2000 - Fiscal Year 2005". *NUREG-1614, Vol. 2, Part 2.* http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1614/v2/part2/index.html#_1_2
[35] Landers, Jim. "Y2K Lessons Help Feds Head Off Cyber-Terror". *Dallas Morning News*. 3(0 November 1999). http://www.infowar.com/class_3/99/class3_113099d_j.shtml

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 23rd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced