



 HAVE DIGITAL MYTHS DIVERTED
ATTENTION FROM TRUE THREATS?

By Robert Lemos, John Borland,
Lisa Bowman and Sandeep Junnarkar
Staff Writers, CNET News.com
August 26, 2002, 4:00 AM PT

Doomsday predictions of a "digital Pearl Harbor" have persisted in the year since the terrorist attacks of Sept. 11.

The specter was a driving force behind controversial new law enforcement measures portrayed as necessary by the government but decried by civil libertarians as an assault on constitutional rights to privacy. Yet security experts, network managers and public safety officials say privately that the threat of cyberterrorism has been overblown and misunderstood--and that physical attacks remain far easier to carry out.

As a result, government officials and industry leaders may have spent needless effort addressing an arguably nonexistent enemy at a time when all resources are needed to guard against more realistic dangers. In this three-day special report, CNET News.com reporters in New York, San Francisco and Washington examine the technological and political realities of this volatile issue.

Editors: Mike Yamamoto, Lara Wright
Art: Pam Dore, Ellen Ng
Production: Mike Markovich, Ben Helm

TABLE OF CONTENTS


Safety: Assessing the risks

Countless urban legends have been circulated about possible cyberterrorism, involving everything from water supplies to power grids. But while security experts agree that risks do exist, they say any digital attack would be measured in loss of data, not life.


Politics: Security vs. liberties

No prosecutions under new security laws have been reported, but critics say aggressive investigations and public overreaction have had a chilling effect on personal freedoms. In an instant, Sept. 11 reversed years-long momentum to protect online privacy.


Lessons: Networks as lifelines

The communications breakdown at Ground Zero revealed the risks of concentrating networks in one place--but, after a century of haphazard growth, the system is impossible to uproot. Manhattan is a case study for cities facing similar problems worldwide.



E-TERRORISM

TABLE OF CONTENTS

DAY 1 SAFETY:
Assessing the risks

DAY 2 POLITICS:
Security vs. liberties

DAY 3 LESSONS:
Networks as lifelines

Safety: Assessing the infrastructure risk

By Robert Lemos
Staff Writer, CNET News.com
August 23, 2002

In 1998, a 12-year-old hacker broke into the computer system that controlled the floodgates of the Theodore Roosevelt Dam in Arizona, according to a June Washington Post report. If the gates had been opened, the article added, walls of water could have flooded the cities of Tempe and Mesa, whose populations total nearly 1 million.

There was just one problem with the account: It wasn't true.

A hacker did break into the computers of an Arizona water facility, the Salt River Project in the Phoenix area. But he was 27, not 12, and the incident occurred in 1994, not 1998. And while clearly trespassing in critical areas, the hacker never could have had control of any dams--leading investigators to conclude that no lives or property were ever threatened.

"It's like the children's game of 'telephone,'" said Gail Thackery, assistant attorney general for Arizona and the prosecutor on the Salt River hacking case. "You get the reality at one end and, at the other end, something completely different."

The misreported incident serves as a metaphor for today's pressing debate over the Internet's vulnerability to attack. While warnings pervade government and the media, doomsday scenarios of cyberterrorism that result in massive deaths or injury remain largely the stuff of Hollywood scripts or conspiracy theory.

Although it is possible for electronic intrusions to damage infrastructure and threaten physical danger, taking control of those systems from the outside is extremely difficult, requires a great deal of specialized knowledge and must overcome non-computerized fail-safe measures. As a result, government and corporate security experts--while careful not to dismiss the gravity of the issue--point to this indisputable fact: It is still easier to bomb a target than to hack a computer.

"If we had so many dollars to spend on a water system, most of it would go to physical security," said Diane VanDe Hei, executive director of the Association of Metropolitan Water Agencies and point person for the Information Sharing and Analysis Center (ISAC) for the water utilities.

In a so-called "digital Pearl Harbor" exercise sponsored by the U.S. Naval War College and Gartner last month, analysts posing as terrorists were able to simulate a large-scale cyberattack on the nation's infrastructure. But to do so they needed \$200 million, high-level intelligence and five years of preparation time. The college concluded that such an offense could cripple communications in a heavily populated area but would not result in deaths or other catastrophic consequences.

Yet the hyperbole about an Internet attack frequently overshadows common sense. On Sept. 11, it took less than 24 hours after four passenger jets were used as weapons of mass destruction for cries of cyberterrorism to emerge as the next great threat, triggering calls for new legislation to broaden the authority of law enforcement agencies.

HARD TARGETS

Fear of cyberterrorism has led to false ideas about the damage that can be inflicted on U.S. infrastructure facilities. Here is a list of some possible--though still improbable--worst-case cyberattacks, followed by more realistic threats.

Electricity Power lines, transmission facilities

Worst-case cyberattack:

An attack on control systems via wireless, modem or Internet access could cause localized brownouts or blackouts.

More realistic threat:

Physical destruction of generating plants or transmission facilities could cause brownouts or blackouts for days.

"All the electric companies are connected to the Web in one way or another, but that doesn't mean that the control systems are."

--Ellen Vancko, representative, North American Electric Reliability Council

Surface transportation Railroads, trucks, barges and buses

Worst-case cyberattack:

An attacker could use the Internet to gain access to one of 500 small railroads' control systems and cause two trains to take the same track and collide.

More realistic threat:

Use of explosives on trains or trucks carrying hazardous materials could cause an environmental disaster.

"We simply know there is room for damage to be done, and we are trying to take steps to plug any holes in the system. Are we taking cyberterrorism more seriously than physical terrorism? No. They are both threats."

--Nancy Wilson, senior assistant vice president, Association of American Railroads

■ Water Reservoirs, canals, dams and water treatment facilities

Worst-case cyberattack:
Water could be contaminated with untreated waste or high levels of chlorine or other chemicals by attacks on control systems via wireless, modem or Internet access.

More realistic threat:
Physically adding a biological or chemical agent to the water could cause people who drink it to become ill. Frequent testing of the water minimizes this risk, however.

"If you had so many dollars to spend on water-system security, most of it would go to the physical side."

--Diane VanDe Hei, executive director, Association of Metropolitan Water Agencies

■ Energy Energy trading, energy plant operation, exploration, but not pipelines

Worst-case cyberattack:
Disrupting the parts of the Internet used by the energy trading systems could halt buying and selling and cause a temporary energy shortage.

More realistic threat:
Physical destruction of refineries or pipelines could cause a shortage and an environmental disaster.

"We depend greatly on the Internet. Any interruption in that fabric could cause problems."

--Carl Tianen, chairman, Energy Information Sharing and Analysis Center (ISAC)

■ Financial Infrastructure: Banks, trading houses and other financial firms

Worst-case cyberattack:
A worm that disables key servers and networks could create enough disruption that a financial market would be forced to close.

More realistic threat:
Combining a cyberattack that disables computer networks and a physical attack that destroys key facilities could disrupt multiple markets and significantly lengthen an outage.

"We are so interrelated--the payment systems, the clearing systems and the financial distribution--that an effect on one has an effect on everybody."

--Stash Jarocki, chairman, Financial Services ISAC

■ Information technology Server, computer and network software

Worst-case cyberattack:
Vulnerabilities in flawed software could be used to gain access to specific critical systems to aid a cyberattack on other infrastructure elements or to cause widespread Internet communications problems.

More realistic threat:
Vulnerabilities in flawed software could be used to gain access to specific critical systems to aid a cyberattack on other infrastructure elements.

"To say that you can't see the possibility (of a crippling cyberattack) is blinding yourself and preventing the nation from protecting itself."

--Greg Akers, president, IT-ISAC

combination with several other problems, caused a cascading failure. In 1990, a similar event with an AT&T switch touched off a chain reaction that shut down long-distance communications across the United States.

"The system attacks itself in these cases," Dubiel said.

Making matters worse, more than 80 percent of such critical infrastructure is privately owned, and in many cases the companies have not been sufficiently educated about information security until recently. Security consultants have attested that many utilities have an indirect path to the Internet from their SCADA master terminals.

In November 2001, 49-year-old Vitek Boden was sentenced to two years in prison for using the Internet, a wireless radio and stolen control software to release up to 1 million liters of sewage into the river and coastal waters of Maroochydhore in Queensland,

"Until we secure our cyber infrastructure, a few keystrokes and an Internet connection is all one needs to disable the economy and endanger lives," said Rep. Lamar Smith, R-Texas, in a statement heralding the House's passage of the Cyber Security Enhancement Act last month. His favorite tag line: "A mouse can be just as dangerous as a bullet or a bomb."

That sort of rhetoric is why many dislike the term "cyberterrorism." Ambiguity over its definition--and, therefore, which threats are real and which are not--has confused the public and given rise to countless myths. The phrase has become a catchall buzzword that evokes nightmare images that can be exploited to support political agendas ranging from stronger surveillance authority to tighter immigration controls.

"If you say cyberterrorism, you confuse people," said Richard Clarke, President Bush's special adviser for cybersecurity. "Osama bin Laden is not going to come for you on the Internet."

Cyberattacks come in two forms: one against data, the other on control systems. The first type attempts to steal or corrupt data and deny services. The vast majority of Internet and other computer attacks have fallen into this category, such as credit-card number theft, Web site vandalism and the occasional major denial-of-service assault.

Control-system attacks attempt to disable or take power over operations used to maintain physical infrastructure, such as "distributed control systems" that regulate water supplies, electrical transmission networks and railroads. While remote access to many control systems have previously required an attacker to dial in with a modem, these operations are increasingly using the Internet to transmit data or are connected to a company's local network--a system protected with firewalls that, in some cases, could be penetrated.

Still, Clarke and other security officials say any damage resulting from electronic intrusion would be measured in loss of data, not life.

"It would be relatively easy to conduct a cost-free or risk-free attack given the endemic vulnerabilities in our system," said Michael Vatis, director of the Institute for Security Technology Studies at Dartmouth University and a former director of the National Infrastructure Protection Center, the cybersecurity arm of the FBI. "It would be harder to kill people or have a lasting effect using cyberattacks."

It is true, however, that data attacks could have severe consequences without causing deaths. Many power companies and water utilities are operated with networks of computer-controlled devices, known as supervisory control and data acquisition (SCADA) systems, which could be hacked.

SCADA systems could be attacked by overloading a system that, upon failure, causes other operations to malfunction as well, said John Dubiel, a Gartner consultant who worked on the electrical power attack in last month's war games. Such domino effects have been seen in incidents resulting from natural events.

In 1996, the power along much of the West Coast corridor went out for nine hours after a tree branch fell on some power lines and, in

Australia.

Boden, who had been a consultant on the water project, conducted the attack in March 2000 after he was refused a full-time job with the Maroochy Shire government. He had attempted to gain access to the system 45 times, and his last attempt proved successful, allowing allowed him to release raw sewage into the waterways.

"Marine life died, the creek water turned black and the stench was unbearable for residents," said Janelle Bryant, investigations manager for the Australian Environmental Protection Agency.

“If we had so many dollars to spend on a water system, most of it would go to physical security.”

- Diane VanDe Hei, executive director, the Association of Metropolitan Water Agencies

such access should not always be considered unsafe. "All the electric companies are connected to the Web in one way or another," she said. "But that doesn't mean our control systems are hooked up to the public Net."

Granted, but an Internet connection does provide one more way for an electronic intruder to get into a system. Chris Wysopal, director of research and development for digital security firm @Stake, said he first looks for connections to the Net when called in to analyze the security of an infrastructure network.

"Whenever we see a control system connected to the Internet, that is scary. There is no need for it, except for productivity, and when you are talking about public safety, you should err on the side of security," said Wysopal, whose company has been hired for such audits only since Sept. 11. "We found a power plant where all the control systems had their administrative systems set to the same password."

Because firewalls and other internal protections are not always adequate, risk levels are increased exponentially if networks are connected to the Internet.

"Are we vulnerable? Absolutely. We have the massive bowl of spaghetti between the Internet, phone lines, and extranets, and no one can map it," said Assistant Attorney General Thackery. "We have miles and miles and miles of wire and none of it is secure. And we have all these windows and doors that are open, and they are still open."

She noted that the Net played a major role in a well-publicized incident in 1989, when the Legion of Doom hacker group seized control of much of the infrastructure of Southern Bell's telephone network. During the attack, the hackers could have tapped phone lines and even shut down the 911 system.

BellSouth "had 42 people that I knew of on 24-hour emergency alert to keep control of their network," said Thackery, who was forced to use an encrypted phone in the Secret Service's office in Phoenix because her line had been tapped. "To me, that's one of the scariest scenarios, and these were all college kids. Just pranksters."

Yet even the most notorious incidents have fallen well short of the type of massive destruction envisioned in some of the more imaginative warnings about cyberterrorism. The Queensland incident, for instance, claimed no lives and cost just \$13,000 to clean up, and it was accomplished only with extensive inside knowledge.

Wysopal and many other security experts readily acknowledge that wide-scale infrastructure disruption is no easy feat. Even if an intruder manages to break in, he said, commandeering a system "still requires a fairly sophisticated skill set."

In last month's "Pearl Harbor" exercise, Gartner analysts playing the role of attackers reinforced that observation. "It is very hard to attack something that you don't have a specific knowledge of," said David Fraley, an analyst who simulated an attack on telecommunications networks.

Even in a successful attack on a metropolitan power grid, many critical systems--such as hospitals and prison operations--would continue running because they have independent generators. In addition, utilities and infrastructure operators have elaborate

Attacks of the decade

Several large cyberattacks have threatened the U.S. infrastructure over the past decade or so, but none has resulted in death or mass destruction.

2001:
In September, Nimda virus worms its way into servers and networks Internet-wide, hitting the financial industry especially hard.

2000:
In February, denial-of-service attacks flood Yahoo, eBay, CNN and ZDNet with data, blocking access for many users for two to three hours.

LoveLetter virus strikes companies worldwide in May, flooding e-mail servers as it spreads.

1997:
A technician at a small Virginia ISP updates the company's router with erroneous information. The changes cause a large portion of critical Internet routers to crash.

A teenager disables a key telephone company computer servicing a small airport in Worcester, Mass., in March. The control tower loses critical services for six hours, but airplanes can still get information from radio and other airports in the vicinity.

1994:
A hacker known as Merc manages to dial into a server at the Salt River Project and explores computers used to monitor canals in the Phoenix region.

1990:
A glitch in an AT&T router causes a long-distance outage that lasts nine hours. Many believe falsely that a hacker took down the network.

1989:
The Legion of Doom hacker group "owns" the BellSouth telephone system and is able to tap lines, route calls and pose as technicians.

1988:
Robert Morris releases a worm that infects between 3,000 and 4,000 of the Internet's approximately 60,000 servers.

backup measures to protect the public even if a system is breached.

**THE OFFICIAL DEFINITION OF
CYBERTERRORISM**
n. sī' bər-tēr-ə-rīz'əm

"Terrorist groups are increasingly using new information technology and the Internet to formulate plans, raise funds, spread propaganda and engage in secure communications.

Cyberterrorism--meaning the use of cyber tools to shut down critical national infrastructures (such as energy, transportation or government operations) for the purpose of coercing or intimidating a government or civilian population--is clearly an emerging threat."

--J. T. Caruso, deputy executive assistant director, Counterterrorism/Counterintelligence, FBI in March 21, 2002, testimony before House Subcommittee on National Security, Veterans Affairs and International Relations

For example, if a hacker were to dramatically raise the chlorine levels of a reservoir, the contaminated water would probably never make it to the public because such supplies are typically tested up to five times before entering public pipelines. The Environment Protection Agency requires utilities to look for more than 90 regulated contaminants in these tests. An easier attack, and one that such agencies spend more to prevent, is a terrorist dumping chemicals into a reservoir directly.

Federal authorities are also concerned about computer systems that control the nation's transportation systems, including trains, trucks, buses and barges. The railroad industry's networks alone are massive, with more than 500 small railroads to supervise.

"The railroad industry today is one of the biggest users of computer systems in the country," said Nancy Wilson, senior vice president of the Association of American Railroads and point person on the Surface Transportation ISAC. "We were early users of technology and we are big users of technology. If we lose computer capabilities, we would kind of grind to a halt."

For that reason, most rail companies have extensive safety measures and backup systems. Sensors tell when the track has been tampered with, and security mechanisms provide early warning alerts for possible intrusions.

"We have had our share of little hacker problems, but they have never been serious," Wilson said. "I'm not saying we are perfect, but I am saying that we have come a long, long way toward identifying our vulnerabilities."

Redundant safety measures are also taken in manufacturing companies, many of which use SCADA systems. But that hasn't stopped the proliferation of popular urban legends.

In one such myth, a hacker breaks into a food company's network through a Web connection and manipulates a breakfast cereal recipe to add vastly higher levels of iron, threatening children who have a low tolerance for the mineral. Another rumor had a hacker

gaining entry to a tank-manufacturing company and changing the temperature specifications for armor used in the vehicles, making the metal more brittle and vulnerable. Neither story is true.

Security experts generally agree that the infrastructure most susceptible to hacking alone is the Internet itself. They often point to the Nimda worm, which caused as much as \$3 billion in estimated damages and lost productivity by some estimates.

Some Internet vulnerabilities have been exposed without any attacks. At least one serious weakness was discovered in 1997 when a technician changed two lines of code and nearly brought down the global network for three hours.

The change occurred to one of the hundreds of thousands of routers that form a key part of the Internet infrastructure. Because of the two-line mistake by the technician at the McLean, Va.-based MAI Network Services, one of its routers indicated that it provided the best path to the entire Internet. Other routers then began sending all their data to the ISP's small leased line, crashing MAI's network and clogging systems around the world.

“ Whenever we see a control system connected to the Internet, that is scary.”

- Chris Wysopal, research and development director, @Stake

"Within minutes you had most of the routers throughout the Internet going down," said Craig Labovitz, director of network architecture and lead border gateway protocol researcher for security firm Arbor Networks. "It was absolutely the most massive Internet outage we've seen."

Here again, however, the consequences were neither disastrous and nor interminable.

"This wasn't a catastrophe. It was a brownout that sporadically hit providers at various strengths," said one network technician to the North American Network Operator's Group following the outage. He noted that at least one network service provider saw a drop of only 15 percent in traffic.

To law enforcement agencies, the Internet's largest threat is simply the ease of international communication and the ability to hide among the seemingly infinite volume of traffic it carries. In an effort to track down terrorists electronically, the FBI has waived several requirements for new recruits who have technical training.

"The worry right now is not so much a cyberterrorism event," said Don Cavender, a special agent and instructor with the FBI's Computer Training Unit at Quantico, Va., "but when the terrorists use the Internet to facilitate the planning of these attacks." ■



E-TERRORISM

TABLE OF CONTENTS

DAY 1 SAFETY:
Assessing the risks

DAY 2 POLITICS:
Security vs. liberties

DAY 3 LESSONS:
Networks as lifelines

NEW VIEW ON CAPITOL HILL

by Declan McCullagh

WASHINGTON--Just over a year ago, a powerful legion of U.S. politicians strove to limit government surveillance of e-mail. Then came Sept. 11.

Politicians endorsing privacy have since become scarce, losing the high ground to their pro-security counterparts, and laws previously unthinkable have been enacted with little dissent.

The abrupt change on Capitol Hill occurred with astonishing rapidity. Two days after jets crashed into the World Trade Center and the Pentagon, a pair of events took place that set the trajectory for the next year of debate over the future of technology, privacy and surveillance.

First, the Senate veered in exactly the opposite direction as the House did one year before. By a unanimous vote, the Senate approved a bill authorizing the FBI to use its Carnivore Net-surveillance system without obtaining a court order. The sponsors of the Combating Terrorism Act argued that it was necessary to thwart future terrorist strikes.

"It is essential that we give our law enforcement authorities every possible tool to search out and bring to justice those individuals who have brought such indiscriminate death," Sen. Orrin Hatch, R-Utah, said during the bill's floor debate.

The second event was a Sept. 13 floor speech by Sen. Judd Gregg, R-N.H., who called for a global prohibition on encryption products without backdoors for

Politics: Weighing security against liberties

By John Borland and Lisa Bowman
Staff Writers, CNET News.com
August 23, 2002

SAN FRANCISCO--Earlier this year, a few California scuba divers found out just how far the long arm of the law can reach since Sept. 11.

Federal agents concerned about scuba-related terrorist plans requested the entire database of the Professional Association of Diving Instructors. Unbeknownst to most of its members, the organization voluntarily handed over a list of more than 100,000 certified divers worldwide, explaining later that it wanted to avoid an FBI subpoena that would have required far more information to be disclosed.

Cindy Cohn, an attorney with the Electronic Frontier Foundation and a diver listed in the database, was livid after learning of the incident. Such concerns resonate with particular volume in this liberal city where the EFF is based, which has a long history of protesting government intrusion.

"You participated in creating an FBI file on me and all the rest of your customers, loyal Americans who have done nothing wrong and who now face the process of increased surveillance by virtue of the fact that we did business with you," Cohn wrote in a letter to the Southern California-based divers association.

Since Sept. 11, databases containing information on tens of thousands of ordinary people have found their way into the hands of federal investigators hungry for any scraps of data that might serve as leads in terrorism investigations. Grocery shopping lists, travel records and information from other, more public databases have all been caught in the government's antiterrorism net.

“What is the greater threat, terrorism or a government run amok? People are generally going to say terrorism.”

- Jonathan Zittrain, co-director, Harvard University Law School's Berkman Center for Internet and Society

In this security-conscious climate, it seems that no activity is off limits to government inspection--and with good cause, many would say. After all, no one predicted that flight school students would bring down the World Trade Center towers, and few would advocate withholding information that could prevent another terrorist attack. Polls show that many people are willing to tolerate increased surveillance, higher encryption standards and other measures for the sake of security.

But civil libertarians worry that the increased investigative powers granted since the attacks, and people's eagerness to comply with them, have needlessly entangled innocent citizens and threaten to undermine constitutional rights to privacy and free speech. Even without explicit limitations, some say that fear of reprisal may have a chilling effect on public behavior.

Either way, those on all sides of the issue agree that the country has undergone changes both psychological and practical, perhaps as subtle as a reluctance to visit an Islamic Web site or as obvious as federal legislation seeking broader online surveillance by law enforcement authorities. While civil libertarians decry the changes, however, their warnings aren't being widely embraced.

"People pretty readily let go of privacy concerns as soon as security is involved," said Jonathan Zittrain, co-director of Harvard University Law School's Berkman Center for Internet and Society. "To the extent that the concern about privacy is a concern about abuse of information by the

government...what is the greater threat, terrorism or a government run amok? People are generally going to say terrorism."

Ironically, despite its libertarian roots, the Internet has arguably hastened that shift. Given the proliferation of log files and massive customer databases, combined with easy access to controversial sites and other information, the Net has accelerated the debate over electronic information and terrorism.

Perhaps most worrisome to Arab Americans and privacy advocates, the FBI has proposed easing 1970s-era restrictions that prevent them from spying on people based solely on political activities. Under the new guidelines, agents would be able to mine publicly available databases even if they aren't conducting a specific investigation, carrying out what civil liberties activists worry would be a digital fishing expedition producing nothing but massive amounts of irrelevant data.

Information on exactly what databases have been tapped is scarce, but some instances have come to light:

- An informal poll conducted by the *Boston Globe* and the Privacy Council consultancy found that 64 percent of travel-related and transportation companies had given federal investigators access to customer or employee data after Sept. 11. Only 14 percent of those companies informed customers of their actions.
- Privacy Council CEO Larry Poneman said in a recent interview that an unnamed supermarket chain had given shopping club card records to federal investigators.
- Lexis/Nexis, the massive database containing news articles, legal filings and public records of all kinds, says it is working more closely with law enforcement on several fronts since last September, including "authentication" of individuals' identity.

Civil libertarians complain that federal authorities are giving little to no indication of how this information is being used. A recent attempt by several congressmen to obtain a report on how the new legal tools were being used in investigations was rebuffed by the Justice Department, which asked for more time to answer their detailed questions.

"It's very important that that information be disclosed," said David Sobel, general counsel of the Electronic Privacy Information Center, a group that helped bring the FBI's use of Net monitoring tools to light for the first time with its Freedom of Information Act requests.

EPIC, along with the American Civil Liberties Union and the American Booksellers Foundation for Free Expression, filed on Aug. 21 its own Freedom of Information Act request for details on how Patriot Act powers are being used.

"There aren't yet any answers," Sobel said.

Nor is it clear what online behavior might be considered suspicious--and some believe that Internet service providers, companies and organizations may take unduly severe actions on their own in erring on the side of caution. Overzealous network managers, for example, could arbitrarily restrict certain communication or access to some Web sites, just as they often block pornography or filter e-mail that contains obscenities.

More spying or same as it ever was?

Much of the security-vs.-privacy debate has centered on legislation enacted quickly after the September attacks, the turgidly named "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act."

The American Civil Liberties Union called it a far-reaching law that badly undermined privacy and judicial oversight. Many of the nation's largest newspapers editorialized against the measure as reactionary.

Nine months later, however, many judicial experts are playing down initial fears over the legislation's severity. A law review article scheduled for publication early next year by former Justice Department attorney Orrin Kerr provides one of the first detailed analyses of the so-called Patriot Act that compares it to previous investigative practices.

"The law is a lot more balanced than people thought," Kerr said, adding that it does little to change

government surveillance.

"This is something that we need international cooperation on and we need to have movement on in order to get the information that allows us to anticipate and prevent what occurred in New York and in Washington," Gregg said.

His speech came at a time when privacy and national security, long at odds, had reached an uneasy detente, with privacy gaining ground. In response to business pressure and the reality of encryption embedded into everything from Linux to Internet protocols, the Clinton administration had chopped away most regulations intended to limit crypto dissemination.

As a measure of how suddenly the political winds have shifted from protecting business interests to protecting national security, consider this: Gregg has won 100 percent ratings from the U.S. Chamber of Commerce and the National Federation of Independent Business.

Yet the balance of power has not shifted entirely in favor of law enforcement. Gregg's hope for crypto restrictions--which drew applause from newspaper editorialists and some conservative activists--was defeated by an immediate outcry and mobilization by researchers, businesses and consumer activists.

"What's changed is a massive expansion of authority for the government to engage in all sorts of searches and surveillance, particularly electronic surveillance," says Barry Steinhardt, associate director of the American Civil Liberties Union.

Acts against terror

Law enforcement has sought, and in some cases won, new measures that expand investigative powers in the wake of Sept. 11. Here's a roundup.

What: Cyber Security Enhancement Act
When: July 2002
Status: Passed the House
What it does: Would allow for life sentences for hackers; would allow police to obtain suspects' telephone numbers, IP addresses, URLs or e-mail header information--but not the contents of messages--without a court order in the case of an "ongoing attack" on an Internet-connected computer or "an immediate threat to a national security interest."

What: TIPS program
When: July 2002
Status: Proposed by White House

“The government ended up introducing a law that didn't really take any major steps.”

- Orrin Kerr, former attorney,
Justice Department

the way authorities do their jobs. "The government ended up introducing a law that didn't really take any major steps."

At its core, the Patriot Act explicitly spells out new rules under which authorities can monitor online communications such as e-mail or Web surfing. As was the case with wiretapping or other surveillance, agents must get judicial permission to obtain more information.

Under the law, authorities can obtain information such as where e-mail was sent or originated, and at what time. Roughly analogous to reading an envelope but not the letter inside, this means no court order is needed. If agents want to monitor an Internet service account to determine when messages are sent, they need a judge's permission but with relatively little justification.

If agents seek the contents of a missive, which would include such elements as the body and subject line of an e-mail, they would need a court order requiring a much higher level of justification, legal experts say. Although new, these laws mirror previously secret court decisions on FBI attempts to install high-tech spying equipment, according to Kerr and lawyers representing ISPs.

ISPs are reluctant to discuss surveillance details, citing national security concerns. But they do say that surveillance requests have increased since last September, though their extent is difficult to gauge.

“ In some instances, law enforcement is being aggressive in interpreting USA Patriot to go beyond what was intended.”

- Stewart Baker, attorney, Washington, D.C.

"There has been some upswing, but it's not very significant," said Mike Harrad, a spokesman for Road Runner, Time Warner's cable Net service. "The view here is that the increase in requests has probably more to do with the more vigilant approach taken by enforcement agencies in the post-9/11 world than it has to do with the Patriot Act per se."

Others are more concerned. "In some instances, law enforcement is being

aggressive in interpreting USA Patriot to go beyond what was intended," says Stewart Baker, a Washington attorney who represents ISPs.

Baker and other ISP sources say some law enforcement agents make requests for records of subscribers' past communications--for which no court order is needed--so frequently that it has nearly amounted to real-time information. For instance, agencies might request information about a subscriber several times a day or more, instead of seeking a week's worth of log files.

Authorities hitting the books

Libraries also have concerns about the Patriot Act, particularly provisions that lower the standards for obtaining patron records. Under one portion of the law, federal agents need only a search warrant--which requires immediate release of the records--and no longer have to show that they might find evidence of a crime.

What's more, the process is now secret. The court that approves these searches holds closed sessions, and librarians face prosecution if they disclose information about the inquiry to anyone, including the subject of the investigation.

For years, many libraries have had electronic systems that delete checkout records after a few weeks. But information about people who have books checked out and those who owe fines are kept in the database until they return the books or pay the fees.

Of 1,026 libraries surveyed by the American Library Association earlier this year, 85--or 8.3 percent--had received Sept. 11-related requests for records from government agents.

"If you use libraries, whatever you take out is information that could be demanded by the FBI," ALA President Mitch Freedman said. "The library user is just one small person who's been impacted by this dramatic expansion of investigative powers."

The FBI and other law enforcement organizations declined to comment on any details regarding terrorism-related investigations. But comments made by officials in public have heightened concerns among civil liberties groups.

On a recent trip to San Francisco, John Frazzini, a special agent with the Electronic Crimes Branch of the Secret Service, pleaded with companies to cooperate more fully in online investigations and report break-ins. He also warned of new crackdowns on hackers.

What it does: Would create a group of volunteer citizens who would report suspicious activity. Volunteers could come from the ranks of mail carriers and cable technicians. Information may be kept in a database.

What: FBI reorganization
When: May 2002
Status: In the works
What it does: Makes cybercrime a new priority, creates a Cyber Division and devotes more agents to tech-related issues.

What: Loosening regulations on information gathering
When: May 2002
Status: Proposed by Dept. of Justice and FBI
What it does: Would allow agents to frequent public places, such as mosques and libraries, and mine publicly available databases for suspicious activity, even if they're not conducting a specific investigation.

What: USA Patriot Act
When: October 2001
Status: Law
What it does: Gives law enforcement officials expanded powers to monitor suspected terrorists and criminals by, among other things, lowering judicial oversight of monitoring tactics, increasing information sharing among agencies, broadening the definition of a terrorist, and increasing the amount of information agents can seek from ISPs.

"If you're a U.S. citizen and you're breaking into computer networks, not only are you criminal but I think you're unpatriotic," he said.

Although they do not know of any prosecutions based on post-Sept. 11 changes, defense attorneys say they are already seeing their effects in other ways. Jennifer Granick, a defense attorney and director for Stanford University's Center for Internet and Society, said she and her colleagues have noticed that judges and juries are far more wary of hackers than they have been in years and are enforcing existing laws more actively.

"They hear you're a hacker, and in this post-9/11 climate, they just get scared," Granick said, adding that technologists and hackers who point out legitimate security concerns risk getting caught in law enforcement's new web.

She points to a case in Los Angeles, in which a man faced criminal charges after posting information on a Web site that pointed out insecurities in some e-mail software and offered a repair. The man was convicted under a federal computer break-in law and is awaiting sentencing.

"We are dismantling the checks and balances and basically letting government have a free-for-all," Granick said. "It may get uglier before it gets better." ■

“ If you use libraries, whatever you take out is information that could be demanded by the FBI.”

- Mitch Freedman, president,
American Library Association

E-GERARDISM

TABLE OF CONTENTS

DAY 1 SAFETY: Assessing the risks

DAY 2 POLITICS: Security vs. liberties

DAY 3 LESSONS: Networks as lifelines

Working on high alert

Technology experts say Sept. 11 showed that more steps need to be taken to prepare any company or city for an emergency, including both electronic and physical attacks.

"We have initiated a portal that will warn the IT directors of every state about cyberalerts and attacks. A year ago, we didn't do that--nor did we have the capability."
--Matt DeZee, chief information officer, State of South Carolina

"The 9/11 attacks illustrated how fragile and poorly engineered our cellular communications system is. It is incapable of dealing with crisis. (Emergency responders) didn't have a way to communicate with each other since their radio systems are incompatible, and as a result they used cellular phones. But only one in 20 cell phone calls were connected on Sept. 11. In emergency situations, it is not acceptable for them to be relying upon a public system that doesn't give them priority."
--Anthony Townsend, associate professor, New York University

"It is only prudent to expect cyberattacks as well as physical attacks. I hesitate to speak for other people, but I really believe that if your business relies on networking and connectivity, you need to have an extremely resilient infrastructure. That was the one thing people learned: It is not enough to think you've got it, you have to have a process whereby your providers can attest to the fact that you really do have the diversity you need."
--Roger Burkhardt, chief technology officer, NYSE

"You can have the most hardened systems with motor generators, UPS (uninterruptible

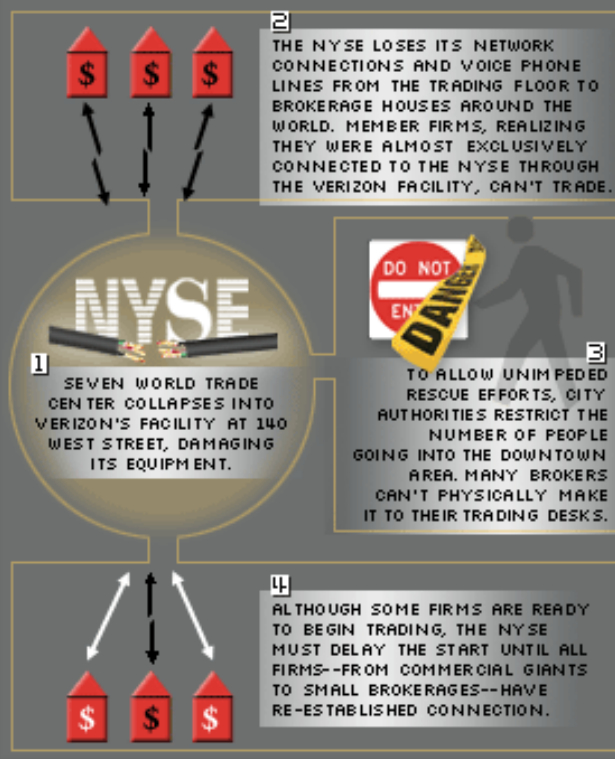
Lessons: Keeping networks alive in New York

By Sandeep Junnarkar
Staff Writer, CNET News.com
August 23, 2002

NEW YORK--As architects submit proposals for rebuilding the World Trade Center, teams of engineers are working deep below the streets of Manhattan to construct a project of their own--one designed to keep the city connected to the rest of the world if disaster strikes again.

RIPPLE EFFECT

ALTHOUGH THE NYSE ITSELF REMAINED PHYSICALLY UNHARMED AFTER THE WORLD TRADE CENTERS COLLAPSED, THE DISASTER AFFECTED STRUCTURES, LOGISTICS AND PUBLIC POLICIES--WHICH IN TURN BROUGHT THE EXCHANGE TO A STANDSTILL.



In a subterranean labyrinth of aging pipes and bundled wires stretching for miles in every direction, these engineers are trying to make this city's densely packed communications networks less susceptible to the kind of widespread outages caused by the Sept. 11 attacks.

What they have found, however, is something many had feared all along: New York's concentration of key network interchanges in one place makes its communications exponentially more vulnerable, yet they have no choice but to continue working with it.

"The benefits of connecting all these networks together are so huge that decoupling them would be unrealistic," said Anthony Townsend, an associate professor at New York University's Taub Urban Research Center. As a result, he added: "Failures in one type of infrastructure system are likely to cascade into others because information technology and telecommunications have been linked within individual networks and between different networks like power, telecommunications and transportation."

This unsettling realization is forcing businesses to re-evaluate how to structure computer networks, data backup centers and links to the Internet. Companies, agencies and all manner of organizations

are working on plans to connect their staffs to networks remotely in an emergency, all the while knowing that a single well-placed explosion could render their efforts futile.

If New York's situation seems impossible, that city is hardly alone. The concentration of networks was the product of a century of growth, an evolutionary process that every major metropolis has experienced. As a result, governments and businesses worldwide are observing the city's progress as a case study for ways to reinforce their own systems.

Diversification is key

Manhattan is an island crammed with many of the world's most powerful industries, all of which rely on digital networks to keep their global businesses running, but its systems are representative of

major communications hubs everywhere. Last year's catastrophe exposed just how fragile all communications networks are, from the digital hubs that run American's cities right down to the most basic functions like using a telephone.

Wall Street firms of all sizes were shocked to discover that their well-laid plans for diversified networks and backup systems were little more than theories put to paper. Moreover, following the consolidation of the telecommunications industry, even phone companies did not have such critical information as the exact route of their networks.

The Bank of New York was one of many to learn of all this the hard way. The institution--more like a bank for banks--had multiple backup systems, dual-access in and out of each of its Manhattan buildings, and a resilient state-of-the-art network design known as "ring architecture." It still had a total communications breakdown.

"We had all the redundancies, only to find out that several central offices in the current configuration nationwide were connected to each other," said Donald Monks, senior vice president of the Bank of New York. "As a result of these dual connections, it's not buying you any redundancy from the position of failure of the senior central office. These problems were exposed by 9/11, and in some cases we think they still exist."

Now, major players on Wall Street are demanding that telecommunications carriers guarantee in writing that the network route is well diversified--not just at the central office but throughout the whole infrastructure. Monks suggested that companies pay a fee for such documentation to bind it as a contractual agreement.

Faced with an exodus of companies that could erode its tax base, New York officials are reviewing various diversification proposals to reassure businesses that even if one network is destroyed, alternate systems can pick up the slack. One idea is to convert abandoned underground water pipes into fiber conduits.

“ Failures in one type of infrastructure system are likely to cascade into others...”

- Anthony Townsend, associate professor, New York University

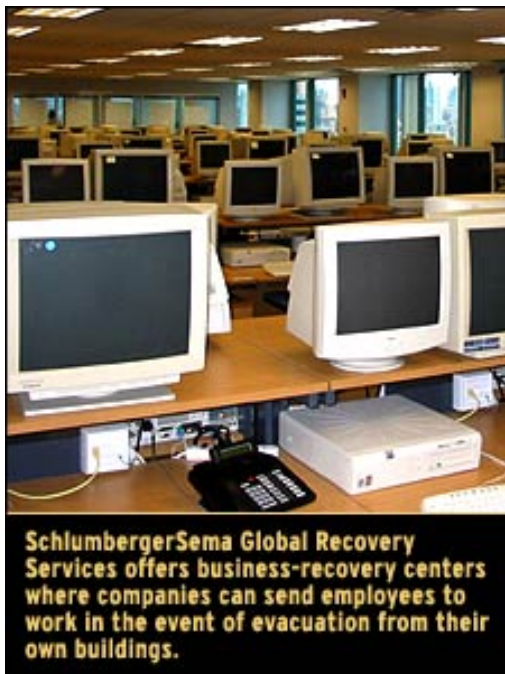
data and cellular communications. The previous mistake was to concentrate major antennas in one location at the World Trade Center: When the twin towers went down, so did all cellular communications in the area. Officials are already negotiating with Ricochet to resume its services from atop 3,000 Manhattan light poles.

Fiber all over the map

Cangemi said the city will also encourage the construction of so-called lateral fiber conduits. At present, shared fiber conduits run north and south under New York's avenues but not east and west along its streets.

"Each time a building on a side street needs a conduit, it costs about \$200,000 to build a new one," Cangemi said. "This initiative is intended to help lower carrier costs associated with getting fiber into the building and to alleviate a reliance on copper connections to a single central office."

Some companies are turning to cutting-edge technologies to strengthen their businesses. The venerable New York Stock Exchange, which lost connections when falling debris severed its digital lines, is building a more resilient infrastructure for its Securities Industries Automation subsidiary.



power supply), all sorts of network redundancies. But what if you can't physically get into the building? What do you do? Do you have a facility outside that area which is prepared with adequate technology where you can send people to work? I think that kind of facility is a value to anybody, whether it is a government office or a corporation."

--Gino Menchini, commissioner of technology, New York City

"You have to worry about insiders damaging your networks. Now when we hire, we look at their tax data and drivers license. We are also re-evaluating our employee exit procedures to make sure their access to the networks is taken away."

--Dan Lohrmann, chief security officer, State of Michigan

Related links

U.S. vulnerable to data sneak attack

<http://news.com.com/2100-1017-949605.html>

Is privacy the next casualty?

<http://news.com.com/2010-1071-948283.html>

National security and the patent squeeze

<http://news.com.com/2010-1071-947508.html>

Is your cable guy a spy?

<http://news.com.com/2100-1023-944555.html>

The tech side of homeland defense

<http://news.com.com/2009-1023-942766.html>

IT pros: U.S. government at cyber risk

<http://news.com.com/2100-1017-939115.html>

Enlisting science in terrorism fight

<http://news.com.com/2100-1001-939084.html>

Want to be a cybercop?

Uncle Sam needs you

<http://news.com.com/2100-1023-937112.html>

FBI digs deeper into the Web

<http://news.com.com/2100-1023-933183.html>

That subsidiary, which provides data processing and communications services for the securities industry, is fortifying its infrastructure with dedicated fiber optic lines it can track. The goal is to create a metropolitan-area network that guarantees geographic diversity of its routes.

Instead of linking to just two of the system's data centers, member firms will connect to the metropolitan network initially at a minimum of four points--two in Manhattan, one in neighboring Westchester County and one in New Jersey. The route between these connection points will consist of interlocking fiber-optic rings; if one part is broken, traffic is routed around the damage. The NYSE hopes to have this infrastructure in place by the end of this year.

The exchange is also pushing an aggressive move to use the Internet because of its greater flexibility and self-healing properties, said Roger Burkhardt, the chief technology officer at the NYSE. "A large part of what we are investing in is a move to modern technologies. We started the move to a common IP-based infrastructure about two years ago so we would have much more flexibility," he said.

Others are investing in early-warning technologies such as embedded chips that could detect anything from leaks along waterways to structural weaknesses at a power facility. Such sensors could also sense explosives or unauthorized entries to a building.

Yet Rae Zimmerman, director of the Institute for Civil Infrastructure Systems at New York University, warns against information overload. Not only can this slow an operation's efficiency, but an elaborate security system can work against itself.

"My biggest problem is, how do you sort through all that information that comes from thousands of data points?" Zimmerman said. "False positives are a huge problem, sending the whole system out of whack. It could be a simple thing like a roach dropping in front of the sensor."

Technology as archeology

In many ways, engineers seeking to update the nation's communications infrastructure are doing battle with history. Most large U.S. cities have grown by building new technologies upon older ones. Because of this haphazard construction, ultramodern digital lines often run precariously beside waterways, sewer pipes and aging telephone lines.

"If you look back to the evolution of the telegraph and telephone, they largely followed existing infrastructure networks like railroads--and like the Interstate highway system followed the railroads," NYU's Townsend said. "These things don't come into being arbitrarily; they are laid down to reinforce existing economic links."

That industrial expediency can have serious consequences, as seen in last year's train derailment and fire in downtown Baltimore. The blaze brought down parts of WorldCom's UUNet network, interrupting Internet access along the Eastern corridor while causing scattered power outages.

Accidental damage to wires and cables by backhoes or other equipment during street work remains one of the most common reasons for floods, power outages and communication disruptions to this day. In addition, any efforts to remedy the situation are often exacerbated by rival companies unwilling or unable to share documentation that shows the exact location of all the wires.

"The level of competition and the tradition of secrecy as well as the fragmentation of the telco sector is a major reason no one has done a comprehensive inventory of telecommunications infrastructure before," Townsend said. "It continues to cause problems and scare people away from looking at it."

“ We had all the redundancies, only to find out that several central offices in the current configuration nationwide were connected to each other.”

- Donald Monks, senior vice president,
Bank of New York

In FBI shift, cybercrime is a priority

<http://news.com.com/2100-1017-927929.html>

Security confab calls for U.S. spending

<http://news.com.com/2100-1001-842795.html>

Patriot Act draws privacy concerns

<http://news.com.com/2100-1023-275026.html>

Privacy vs. safety: Terrorist threat shifts priorities

<http://news.com.com/2009-1023-272972.html>

ISPs aid FBI in terrorist search

<http://news.com.com/2100-1023-272941.html>



SchlumbergerSema, across the river from Manhattan, rents space to New York financial firms to keep backup computer systems. Some companies choose to share space, while others rent spaces they maintain under lock and key.

Not surprisingly, businesses are searching for ways to diversify their physical offices as well as their networks. But because communication lines are so heavily concentrated in Manhattan, they may need to set up auxiliary offices out of the area altogether to ensure their ability to use other networks and remain operational.

Credit Lyonnais, for example, thought it was safely out of reach on Sept. 11, having a branch on a different power grid in midtown Manhattan miles from its other office at Ground Zero. Still, the French bank's operations were disrupted.

"We always thought that we have two locations--one in midtown and one downtown--on separate power grids. We thought that was OK since we were mostly protecting against localized issues like fires or power outages," said George Levitt, the bank's chief information officer. "But after 9/11, you had to adjust your thinking: Maybe one should be a little further away, outside of Manhattan."

The bank is setting up a backup center in SchlumbergerSema Global Recovery Services' facilities about 30 miles from the city.

Others point to a more obvious reason to keep offices farther apart from one another: In any type of disaster, related to terrorism or not, staffs will inevitably face physical obstacles that have nothing to do with the company itself.

"You can have the most hardened systems with motor generators, UPS (uninterruptible power supply), all sorts of network redundancies. But what if you can't physically get into the building?" said Gino Menchini, New York City's commissioner of technology. "Do you have a facility outside that area which is prepared with adequate technology where you can send people to work? I think that kind of facility is a value to anybody, whether it is a government office or a corporation." ■

