October 19, 2001

bandwidth

An Online Newsletter of Discovery Institute

Preventing Cyber-Terror

By: Senior Fellow John Wohlstetter

The First 21st Century Pearl Harbor: Cyber-War, Not; Info-War, Yes

The atrocities of September 11 brought home to Americans the vulnerability of a high-technology information society. Collapsing with the twin towers that topped the Manhattan skyline was a veritable Mother-lode of network communications equipment. For want of communications alone the New York Stock Exchange could not have opened that terrible week.

International traffic was most affected: US-UK traffic increased 10-fold; only 10 percent of calls between Taiwan and the US, and between Sweden and the US got through; less than half of calls between the US and Finland succeeded. In the city, key local central office switches and 12 cellular antenna sites were destroyed. On many domestic routes involving New York, phone traffic doubled and cell traffic quadrupled.[1] Major websites were simply swamped and rendered unavailable.[2] Although the global financial clearing system survived the attack, one bank, Bank of New York, suffered an 8-day ATM network outage.[3] Merrill Lynch, encountering repeated fiber-optic cable cuts (5 times in 3 weeks) turned to free-space (wireless) optics, an emerging high-capacity service; the U.S. District Court, 6 blocks from Ground Zero and without fiber access for nearly 12 days, turned to more conventional fixed microwave service.[4]

Figures from Morgan Stanley and Computer Economics yield an estimated cost of more than $24 billion to restore information technology and communications facilities lost in the attack.[5] Data communications were particularly hard hit. One Verizon switching center serving lower Manhattan routes 3.5 million data lines, 20 times the switch's load of 175,000 voice lines.[6] This represented nearly 30 percent of lower Manhattan's traffic -- enough to fully serve Cincinatti.[7] One set of networks minimally affected were paging networks, which send data packets via the Internet.[8]

Jetliner-bombers murdering thousands of innocents and pulverizing landmarks is far more lethal than most information warfare scenarios. No cyber-attack was launched that day, but savage info-war was. The horror of the civilized world—and the jubilation of the uncivilized—was mega-amplified by live television. No one not at the scene saw Japanese planes bombing Pearl Harbor; it was not a big deal in Afghanistan. Terrorism is part political theater—albeit a designedly gruesome form. And media coverage is pure oxygen for its fire.

President Bush's decision to create a Cabinet-level Office of Home Security reflects a seismic shift in public policy priorities. In a war Presidency, security issues take front row center. A modern war economy needs growth as well, but if enemies can disrupt information networks with impunity their economic value will surely be severely impaired. Thus an info-war calamity raises anew the specter of cyber-war mounted by terrorists instead of school-age pranksters.

Cyber-Security: The Feds Made the First Move

Communications networks have long been a target of adversaries, but until the 1960s America's homeland was exempt from all save acts of sabotage that had only nuisance value. This changed when the Soviet Union began deploying its nuclear arsenal. In the aftermath of the Cuban Missile Crisis President Kennedy created the National Communications System, in search of greater assurance of intact communications during a crisis. Packet-switching,

the routing technology of today's Internet, was invented in 1963 to route signals around damaged military network nodes in event of nuclear attack.

But network vulnerability rapidly extended to civilian communications as well. As computer networking spread, so did the phenomenon of hacking. Originally a benign practice of testing rickety systems to discover flaws, in the 1980s a new breed of hacker, more malevolent, appeared on the scene.

The first harbinger of the new era was Robert Tappan Morris, a Cornell University student whose father worked for the National Security Agency. In 1988 Morris created an Internet "worm" [9] as a prank, and promptly caused 6,000 computers to crash, with damages approaching $100 million. Hackers can harm millions of computers on today's global networks, causing billion-dollar losses. A widely-propagated malicious program such as 1999's Melissa "virus" [10] , which shut down numerous corporate networks by generating spurious messages that clogged network capacity, can also induce network administrators to shut down their networks as a defensive measure to avoid possible damage. Such "denial of service" attacks thereby affect networks beyond those actually infected.

Enter the Public: Revenge of the Nerds

The advent of public mass market Internet access transformed network security by adding to the user population vast numbers of users, and commensurately increased the economic and social value of network connectivity. The Internet that Morris attacked had fewer than 200,000 host computers.[11] Three years later (1992) Internet hosts topped 1 million, and as of January 2001 stood at 109.6 million.[12] And what was a purely research and educational network when Morris struck in 1988 is now predominantly commercial, with 75.9 percent of registered domain names sporting the .com suffix.[13]

Public access immensely complicates the task of securing networks. The administrator of a private network has authority to control the behavior of users. Tools include requiring frequent password changes, limiting access to portions of the network and restricting access to work-related sites. Workers who surf for birthday-suit images of their favorite celebrities, or empty Land's End of their hottest merchandise, do so at their own risk. Kids at home are also subject to parental control, but such is more theoretical than real—whereas network administrators know more than their user populations at home the situation is famously the reverse.

In truth, just as a secret is as safe as the biggest blabbermouth that knows it, a network is as secure as its most careless user: And so public networks are endemically vulnerable to hostile entry.

The nation's public-switched telecommunications networks are, in reality, a web of linked computers, with terminals (computers, phones or faxes) attached at the customer's premises. Voice networks share the vulnerabilities of their datanet cousins. Hardware and software each pose special challenges.

Hardware: The Achilles Heel of Physical Concentration

Hardware vulnerability arises primarily out of physical proximity. The forest of communications gear on top the World Trade Center re-created on a massive scale what happened in the Chicago suburb of Hinsdale, Illinois in May 1988, when destruction of a single facility took down facilities of multiple carriers and Chicago's O'Hare Airport.[14] The lesson for communications reliability is clear: One cannot build a smart network with dumb buildings. Fresh evidence of this reality surfaced September 11: a single central office in Lower Manhattan supplied 80 percent of the New York Stock Exchange's communications capacity.[15] Arguably worse, a single switch controlled most phone lines for local offices of the Secret Service, CIA, FBI—including its Joint Terrorist Task Force, Federal Emergency Management Agency and the New York Police Department.[16] Regulatory policies promoting physical sharing (co-location of facilities at central offices and cell tower sites, for example) may reduce the cost of competitive entry, but have the offsetting downside of increasing system vulnerability to disruption.

Indeed, FCC data shows that between 1990 and 1999 the total number of Bell central offices rose 1% to 9,968, but total phone lines they served jumped 34 percent.[17] As for Bell rivals, one study shows that less than 10 percent of competing carriers have facilities fully separate from Bell networks.[18]

Another hardware fix is to expand broadband capacity. Simple voice calling to and from the New York and Washington metropolitan areas was severely curtailed for two days. Indeed, at one point authorities requested users to refrain from non-essential calls, so as to enable emergency crews to use the network capacity. Increasing network bandwidth via the abundance offered by optical technologies (wireline — *i.e.*, fiber, and now wireless as well) would obviate the need to communications triage strategies that push mom's calls to the side so firefighters can get through. Central office switching is another hardware bottleneck, with networks typically engineered to accommodate 10 percent simultaneous use, simply not sufficient during times of extreme crisis.

Software: An Information Age Faustian Bargain

Inherent in software are special vulnerabilities: it is global, programmable, accessible and fragile. Its global reach means that widely separate geographic hardware infrastructure nodes can all crash if controlled by a unitary software superstructure. Its programmable features give network software enormous flexibility to control and reconfigure hardware, but such power is potentially available to all users with the skill to bypass network firewalls, including those not to be confused with Mother Teresa's spiritual disciples. Open access means that hostile users have access to network innards that in earlier times were beyond user reach. And software's fragility makes fixing it a demanding task.

As an illustration, consider the AT&T network crash on Martin Luther King Day, 1990. *A single punctuation mark at the end of a single line of software code* (in a multi-million line code switch) caused AT&T to lose over half of its long distance capacity in 19 minutes—on one of the busiest calling days of the year.[20] AT&T's network signaling software controlled switching hardware dispersed nationwide. Programmed mistakenly, the software altered how the network worked, and not for the better: it crashed. While there was no hostile intent networks operate not on user intent, but on user

instructions, good or bad. And the fragility of software meant that it would take AT&T about two weeks to locate the actual bug, albeit the network was back up in a matter of hours.

In essence, software represents a kind of Info-Age Faustian bargain: hardware controlled by software is vastly more flexible than pure hardware, being reconfigurable in real-time and thus offering users many options. But software's accessibility, global reach and fragility makes for vulnerable systems. It will take consequential advances in software security to break the bargain, no easy task.

Networking Nostrums: Never Rely on "One" of Anything

What remedies might be proposed for such vulnerabilities? From a hardware standpoint, physical geographic diversity is essential. Technology diversity must complement spatial diversity—wireless and wireline provide mutual redundancy. Regulatory policies should encourage deployment of added network facilities, rather than perpetuate dependence upon existing plant.

Turning to software, diversity is valuable here as well. The 1990 AT&T network crash showed that single-point software failures can be as devastating as any hardware failure. Today's commercial software is riddled with security holes, including "backdoors" unknown to most users but exploited by hackers. One private group that studies computer security, the Computer Emergency Response Team, urges that security functions be built into the core design of next-generation software.[21] In the longer term, simplifying network equipment so it is less dependent upon mammoth software code would reduce fragility. A sacrifice in flexibility can be accepted if specialized hardware can be cheaply deployed.

Above all, network resiliency means the ability to rapidly restore connectivity after a disruption—ideally, in milliseconds. Hostile attacks will occur, and stopping them in advance cannot be the primary goal, as doing so is difficult. There are too many points of network entry to secure them all, especially as the user population is spread around the globe. Want to try to control how a hacker in the Philippines accesses American networks?

Better by far to build in added robustness and adaptability into networks, to enable rapid return to normal. It is the equivalent of the Cold War strategy of hardening missile silos so as to withstand a first strike, preserving a retaliatory capability. Telecom networks can be remarkably resilient if built wisely.

Relying on restoration rather than prevention furthers another vital goal: keeping public network access as open as possible. Closing off access to the maximum extent turns our information society into a garrison state, one inconsistent with cherished values. To do so is, from an economic standpoint, to risk killing the goose that laid the golden egg.

But Does Saddam Know Software?

Fortunately, Saddam Hussein does not appear to have software on his mind (he prefers nuclear, chemical, or bio-weapons, so not to cheer too loudly). But other villains are more tech-savvy. Cyber-terrorism has already been tried. In May 1988 Israeli computer scientists at Hebrew University detected what was dubbed the "PLO virus," designed to activate on the 40th anniversary of Israel's birth (May 14 of that year). The virus was thwarted just in time.

Some security experts believe that the "Nimda" worm ("Nimda" is "admin"—IT slang for network administrator—spelled backwards), unleashed 8:50 AM, just one week plus two minutes after the first World Trade Center tower was hit, was an "echo" cyber-strike; a hacker group named "the Dispatchers" claimed credit. Nimda slowed the Internet global traffic index, which measures speed on a 100-point scale, to around 20 in North America by noon that day (any figure below 50 is considered cause for concern). The worm affected 399.000 servers in 3 hours 10 minutes. Its impact was greater than that of the July 2001 "Code Red" worm, which slowed Internet traffic by up to 50 percent.[22] One expert at McAfee, a leading anti-viral software firm, says that Nimda is a "proof-of-concept" attack that may well be prelude to far nastier attacks later.[22] The CERT Coordination Center has tallied 35,000 attacks or probes for the first three quarters of 2001, with 46,000 estimated for the year, more than double the 22,000 recorded last year (and only partly due to Internet Growth in 2001).[23]

More chillingly still, terrorist groups—including bin Laden's—use the Internet to plan strikes, relying on available "public key" encryption schemes that are for practical purposes unbreakable.[24] Worse, only about half of one percent of the 4 trillion e-mails sent annually are encrypted, so as encryption usages increases the task of tracking coded messages will become harder.[25] Often accessing the Internet at public library sites, terrorists use "steganography"—hiding coded messages "in plain sight" among numerous legitimate ones at popular websites—including sports chat rooms, music sites and pornographic ones; much of their traffic is carried over "freeware" available to all on the Net.

This is not sci-fi: A French defense official told ABC News, based upon seizure of a code book from a suspected terrorist accomplice to the unsuccessful plot to bomb the US embassy in Paris, that bin Laden's network embedded messages in music and image files.[26] A sender could hide a building plan in a picture of the Mona Lisa. And the Taliban—proving that Stone Age backwardness and technology sophistication mix just fine—are online as well. Data passed includes candidate targets, maps, and funds transfers.[27] A White House source has said that bin Laden relies on the Internet as "a major mode of communication" and "a good place to hide and communicate in real-time." [28]

So What Do the Feds Have in Mind?

Cyber-attacks will be covered in legislation that is before Congress at this writing. The US-based Institute for Technology Security Studies notes that most hacking is mere nuisance. The Institute warns, however, that "[t]he potential exists for much more devastating cyber attacks…[that] could significantly debilitate US and allied information networks."[29] However the final bill reads, enforcement must thus be narrowly targeted to exclude minor acts.

Rep. Stephen Horn (R-CA) presided over a post-attack hearing on cyber-vulnerability. Witnesses identified target areas such as taxpayer records, law enforcement and nationals security databases and benefit programs. Michael Vatis, former Director of the FBI's National Infrastructure Protection Center, called for a Manhattan Project to address cyber-security; he cited the risk of attacks directed at Internet domain name servers, address repositories and routing hardware.[30]

The Bush Administration is building upon work done by its predecessors in enhancing public network security and reliability. Presi-

dent Bush expressed his concern in a March 1 letter to Congress, citing cyber-security among the critical infrastructure vulnerabilities to be addressed; the White House announced in May that it is working with federal agencies to revise the existing National Plan for Cyberspace Security and Critical Infrastructure Protection.[31] The newly-minted Homeland Security Council will have joint suzerainty, in tandem with the National Security Council, over an Office of Cyber Security, whose chief-designate, Richard A. Clarke, warned last December that failure to address cyber-security could lead to America suffering a "digital Pearl Harbor." [32]

America faces major cyber-threats but is not without its own assets, including a vast pool of talented Net nerds. The country that led the Internet revolution will now have to fight a war on the digital frontier as well, aided by cyber-savvy allies like Israel, Britain, Australia, Taiwan and India. President Bush's "war government" will no doubt extend cyber-protections, and not a moment too soon.

---

[1] *New Economy*, New York Times, p. C4 (Sept. 24, 2001). The author is former New York State Public Service Commission Chairman Eli M. Noam.

[2] *Site Operators Regroup*, Internet Week, Sept. 20, 2001. Major news sites, charities, and airline sites were unavailable for hours. The FBI's site was also seriously clogged, with response time slowing to 170 seconds, until 10 PM that first evening.

[3] *Backup Systems Passed Trying Test*, Washington Post, p. E1 (Sept. 27, 2001). The Clearing House Interbank Payment System (CHIPS) clears over $1 trillion daily through 59 world money center banks.

[4] *Lasers, Broadband Wireless Hookups Speed Data Around Lower Manhattan*, WSJ.com, Oct. 3, 2001. In a spooky historical footnote, an early free-space optics trial was conducted 30 years ago--between the twin towers of the WTC.

[5] *IT Scrambles to Restore Order, Internet Week*, Sept. 20, 2001. Breakdown: cost of restoring all IT and communications: $15.8 billion; long-term cost to enterprises, $8.1 billion; cost of replacing hardware destroyed, $500 million; annual IT expenditure at World Trade Center, $826 million.

[6] *Keeping the Lifelines Open*, New York Times, p. F1 (Sept. 20, 2001).

[7] *Exposed Wires: Trade Center Attack Shows Vulnerability of Telecom Network*, Wall Street Journal, p. A1, (Oct. 19, 2001). In all, lower Manhattan had 4.5 million data and 300,000 voice lines, p. A8.

[8] *Id.* Handheld devices such as the Blackberry proved more effective than phones.

[9] A worm is a malicious program that copies itself into host computers and self-activates.

[10] A virus program, unlike a worm, cannot self-activate. It replicates from computer to computer, but the user must invoke the program for harm to be unleashed.

[11] *The Digital Economy Fact Book*, Progress and Freedom Foundation, p. 3 (3rd Ed. 2001). In October 1989 there were 159,000 host computers on the Internet.

[12] Id.

[13] Id., p. 5.

[14] *Carriers Battle to Restore Service*, Internet Week, Sept. 13, 2001, 3:32 PM. The switch belonged to Verizon, one of two it had in the financial district

[15] *After Bunker Proves Vulnerable, Officials Rethink Emergency Response*, New York Times, p. A9 (Sept. 29, 2001). Indeed, New York City's crisis command center, located in one of the smaller World Trade Center buildings, was wiped out; a back-up center had not been constructed due to budget constraints.

[16] *Exposed Wires: Trade Center Attack Shows Vulnerability of Telecom Network*, Wall Street Journal, p. A8, (Oct. 19, 2001).

[17] *Id.* The Study was done for Amtrak by the Tanner Group

[18] Wireless optics have arrived. Seattle-based Terabeam provides business customers with networking speeds up to one gigabit per second.

[19] Specifically, AT&T's SS7 adjunct processor components of AT&T's No. 4ESS switches crashed. SS7 is a common channel signaling system that routes network control signals over a dedicated packet-switched signaling network. A software punctuation coding error in an upgrade module created an "and" condition where an "or" condition was called for. The software bug instructed each processor that a traffic overload condition existed, and then issued a contrary instruction that traffic had been cleared, but without removing the first message. As a result of the ensuing message conflict, each SS7 processor crashed and took itself off the network, but not before passing on the mixed signals to the next switch. Every 10 seconds a processor crashed, and in 19 minutes all 114 of AT&T's SS7 adjunct processors had crashed, taking down more than half of AT&T's total network in what net nerds call a global "cascade" failure.

[20] *U.S. Computer Security Called Inadequate*, Newsmax.com Wires, Sept. 27, 2001. The recommendation comes from CERT's Director, Richard Pethia. CERT is affiliated with Carnegie-Mellon University at Pittsburgh.

[21] *Prolific Worm Menaces Internet*, Washington Times, p. C1 (Sept. 19, 2001).

[22] *Inside Track: Focus Shifts to Security: Hackers, Viruses, Failing Hubs - Seldom Have IT Networks Seemed So Vulnerable*, *FT.com*, Oct. 3, 2001.
< http://globalarchive.ft.com/globalarchive/article.html?id=011003001952&query=louise+kehoe >

[23] *Internet Attacks Seen Doubling in 2001*, CNetNews.Com, 1:20 PM PT, Oct. 15, 2001.
< http://news.cnet.com/news/0-1003-200-7532673.html?tag=dd.ne.dht.nl-sty.0 >

[24] Public key cryptography, invented in the mid-1970s, involves use of both published and private keys in combination, with sender and receiver each having two keys, one public and one private. Such systems are considered unbreakable.

[25] *We Hack You: Government Snoops Emulate Cybervandals*, Forbes, p. 48 (Oct. 15 2001).

[26] *A Secret Language: Hijackers May Have Used Secret Internet Messaging Technique*, ABC NEWS.com, Oct. 4, 2001.
< http://abcnews.go.com/sections/primetime/DailyNews/PRIMETIME_011004_steganography.html >

[27] *Terrorists May Have Used Internet to Plot*, Washington Times, p. A3 (Oct. 6, 2001).

[28] *White House Convinced bin Laden Giving Orders Over Internet*, Drudge Report, Oct. 8, 2001.
< http://www.drudgereport.com/matt1.htm >

[29] *Hackers Branded as Terrorists*, BBC News Online, Sept. 28, 2001.
< http://news.bbc.co.uk/hi/english/sci/tech/newsid_1568000/1568302.stm >

[30] *U.S. Computer Security Called Inadequate*, Newsmax.com Wires, Sept. 27, 2001.

[31] *White House Statement on the Review of Critical Infrastructure Protection and Cyber Security*, May 9, 2001.
< http://www.ciao.gov >

[32] *Securing the Lines of a Wired Nation*, New York Times, P. F1, Oct. 4, 2001. Not every expert agrees: Fred Cohen, the computer academic who coined the term "virus," thinks that network components individually are fragile but the network whole is resilient. Commenting on cyber-security, Cohen has said: "It's easy to tear a piece of paper. Try tearing a phone book in half." *Id.*

bandwidth

Is published by Discovery Institute

Discovery Institute is a non-profit, non-partisan, public policy think tank headquartered in Seattle and dealing with national and international affairs. For more information, browse Discovery's Web site at:
http://www.discovery.org

DISCOVERY INSTITUTE

To subscribe or unsubscribe to *bandwidth* or to forward a copy of this issue to a friend visit:
http://www.discovery.org/bandwidth

Discovery Institute's mailing address is:
1402 Third Avenue
Suite 400
Seattle, WA 98101

Questions and comments may be emailed to:
mailto:wohlstetter@discovery.org