


November 13, 2002



bandwidth

An Online Newsletter of Discovery Institute



9-11 Plus One: Have Lessons Been Learned?

By: Senior Fellow John Wohlstetter

The year since “the world changed” has been marked by many changes in American life. By solid margins, both houses of Congress have just voted to authorize the President to use pre-emptive force against an adversary, based upon apprehension of a threat of mass terror whose imminence is the subject of sharp disagreement. Federal and state law enforcement agencies have rounded up dozens of suspects on evidence probably insufficient for the typical criminal prosecution; some are being held solely as material witnesses. Citizens are reporting jokes as signs of suspicious activity. America’s elderly are being frisked in airports as if they were suspects chased into a back alley; passengers have surrendered nail clippers as the price of being permitted to board aircraft.

All these actions would simply have been unthinkable prior to that terrifying September morning one year ago. What is equally difficult to imagine is that, in the aftermath of the worst attack on the homeland in 60 years, the government shows little apparent urgency on improving communications and information networks. This is especially worrisome because these systems’ reliability, robustness and security are vital for daily life, and their weaknesses are well known.

Technology issues nonetheless have been central concerns of policymakers from the outset of our national awakening to terrorism. It is therefore appropriate, at this juncture, to assess progress made since 9/11, both in terms of communications and information networks. A full assessment would run Russian-novel length. The focus here will be on the federal government’s new cyber-security initiative, plus some lessons from the experience of the police and fire departments in New York City on 9/11. Other items will cover the FBI’s info-readiness, and information network-relevant developments of interest in airport and border security.

In a nutshell, progress in cyber-and info-network security has been halting at best. At the end of this collection of highlights are some thoughts on why progress has been slow and what might be done to speed it up.

Cyber-Security: On the Slow Track

Reported security breaches skyrocketed in early 2002, with companies and organizations recording 26,829 attacks in the first quarter, more than half of 2001’s yearly total of 52,658 and more than the 21,756 for all of 2000. Reported software vulnerabilities continue to increase, from 171 in 1995 to 2,437 in 2001 and 1,065 in 2002’s first quarter. Average damage per attack has risen from \$500,000 in 1997 to \$2 million this year.¹

On September 18 the President’s Critical Infrastructure Protection Board released its draft of a national cyber-protection strategy.² The report offers some valuable metrics that illustrate the dimension of the problem of defending info-network assets. Highlights from the draft report follow.

Cyber attacks in 2001 inflicted an estimated \$13 billion in damage.³ To illustrate existing vulnerabilities, consider these examples of *actual attacks already launched*: cyber-terrorists announce they will shut down electric power to the Pacific Northwest for six hours; hackers crash the New York City air traffic control system; hundreds of thousands of credit card numbers are stolen, disrupting online verification for a week.⁴ The Computer Security Institute recently conducted a poll showing that 90 percent of respondents had anti-viral software,⁵ yet 85 percent had been penetrated by a virus.⁵ A security inflection point was reached in 1999, when reported vulnerabilities and incidents handled both jumped; between 1999 and 2001 reported vulnerabilities increased roughly fourfold and incidents handled increased

some fivefold.⁶ Enterprise networks are especially vulnerable to attacks mounted with the aid of insiders; an estimated 70 percent of attacks against enterprises enlist insider assistance.⁷

Much of the problem lies in the private sector, which has some 85 percent of the nation's critical infrastructure.⁸ The draft report offers five "guiding principles" to govern improving cyber-security: (1) embrace private-public partnerships; (2) avoid regulation; (3) safeguard civil liberties and privacy; (4) coordinate with Congress; (5) cooperate with state and local governments (a daunting task, given that there are over 87,000 jurisdictions in the USA). The designated lead agency for telecom and information network security is to be the new Department of Homeland Security.⁹

A key problem is authentication, where there are three basic types: (1) what the user knows—password, etc.; (2) what the user has—such as a smart card; and (3) what the user is—immutable characteristic such as pattern of iris.¹⁰

In terms of strategy, the draft report reaches one critical, correct conclusion: perimeter defense aiming to keep intruders out is unrealistic. Thus a layered defense is needed.¹¹ Many of the recommendations focus on raising awareness of users in the various communities—residential/small business, large business, government, nationwide and global. Much of the advice is common sense and commonplace in security circles, but one item is curious: users are warned to "use caution" when opening e-mail from strangers.¹² "Caution" does not suffice: users should NEVER open mail from unknown senders.

The draft report suggests engaging international agencies and foreign countries in a joint effort to address cyber-vulnerabilities.¹³ That this can be accomplished is a planted axiom, which the history of global bodies argues against. The dog that did not bark is the lack of urgent proactive steps, as if all threats are remote.

The WTC Crisis Management Effort: Grace Under Pressure

New York City Mayor Michael Bloomberg recently released McKinsey & Company reports on fire department (FDNY)¹⁴ and police department (NYPD)¹⁵ performance during the attacks of September 11. Central to both reports is evaluations of communications and information management. Representing independent outside review of events and actions taken in response, they offer lessons for future emergencies on the anniversary of the attacks. The upside is that despite flaws—inevitable during highly stressful situations—the performance of both agencies stands in stark contrast to the serial imbecilities of airport security. The downside is that significant vulnerabilities will persist for years.

Fire and police departments spearheaded the response to the attack on the Twin Towers. Both agencies encountered serious communication problems: radios that did not work and lack of coordination between various departments, forcing them to rely on cellular phones with mixed results. The Fire Department had actually purchased UHF radios in 1999 but failed to deploy them; a planned operations center never got off the ground. The lack of high-speed repeaters in high-rises¹⁶ was a major factor in failures to communicate during the two hours from first impact to the collapse of the second tower. Perhaps worse, the one citywide radio channel dedicated to Fire Dept. use was shared between command and tactical users, severely impeding command communications. Existing command boards are magnetic, rather than PC-based electronic boards.

System procedures failed, too. Specific acknowledgement of message receipt was not required, causing confusion. Fire officials inside the towers lacked outside information, including the video feed from an airborne police helicopter that could

have aided damage assessment. *A recall order for off-duty firemen was poorly implemented; the system had not been activated for 30 years.*

Thus, many firemen went directly to the towers, bypassing staging areas that would have facilitated coordination of rescue efforts. Units assignment records kept in WTC2 were destroyed, and there was no off-site reserve to restore data at a remote site. Communications protocols failed to identify incidents and create radio ID names needed by commanders.

NYPD had many of the same problems. Police radio technology failed 15 percent of the time, but “clutter” disrupted 42 percent of traffic in the early hours. Cellphones rarely worked due to traffic congestion and physical network damage; this was critical, as 65 percent of communications outside of police radio were made via cellphone. Landline communications at police headquarters failed. Clearinghouse coordination was lacking. But some things worked well: 911 call volume jumped 75 percent without disrupting operations, thanks to back-up.

FBI: Flying Blind Informationally?

In July 2002, the FBI e-mailed electronic copies of testimony to the Senate. No big deal? Three months earlier—that is, eight months since September 11—the FBI had been unable to do so, and had instead to supply the Senate staff with ...disks. *What more than half of Americans had been doing—swapping messages via e-mail—the nation’s leading federal law enforcement agency could not do until recently. Indeed, on September 11, no less, FBI computers could not even be operated using a mouse.* Thus, the FBI had to send photos of the 19 September 11 hijackers by snail mail (overnight—*i.e.*, accelerated snail-speed). The agency has recently submitted a technology upgrade plan to Congress.¹⁷

Airport Security: Keystone Cops Do Additional Aerials

Airport security has flunked another test—this time, conducted by CBS News.¹⁸ Lead-lined film bags, which block X-rays, were carried by CBS personnel and let through without a search 70 percent of the time. At several airports, screeners batted .500—and on some trips failed to search even a single bag. An Israeli air security expert said of airport security in America: “The United States does not have a security system; it has a system for bothering people.”¹⁹ NASA thinks it has a better idea: use brain-monitoring devices—“non-invasive neuro-electric sensors—to match physiological data to myriad data banks.”²⁰

Somewhat more prosaic is the TSA’s proposed upgrade to the existing air traveler profiling system, CAPPS (Computer Assisted Passenger Prescreening System). The program, CAPPS II, would use artificial intelligence akin to that used by casinos to spot suspect customers, including associational data and data drawn from databases on suspects, plus behavioral profiling.²¹ Congress set an April 9, 2003 deadline for domestic airliners to be fit with secure doors, with the federal government picking up \$100 million of the \$250 million tab.²²

Border Security: A Passport Upgrade

The Enhanced Border Security Act, passed this year, requires that all passports and visas incorporate biometric data by April 2003, and that biometric readers be installed at every land, sea and air border checkpoint over three years.²³ US Customs reports that in 2001 over 20 million shipping units entered the US, with 52.8 percent carried by truck, 28.4 percent by ship, 11.2 percent by rail and only 4.8 percent by air; special searches were carried out on only 18,000 units

in a recent 10-month period, triple the rate of the prior year—.09% of the total entering the US. Customs has entered into monitoring upgrade agreements with some 400 major firms; over 60 percent of shipping is carried by the top 1,000 importers.²⁴

Shipping continues to present the most daunting challenge, with two-thirds of sea trade involving the US shipped via the world's 240 million shipping containers. US Customs estimates, however, that 68 percent of the 5.7 million containers that reached US ports in 2001 came through just 20 major ports, which have been asked by the US to allow US Customs inspection of departing shipments, as Canada has already done. Rotterdam, Antwerp, Le Havre, Bremerhaven and Hamburg have signed up. But port crime complicates the task: one Senate report found that 15 percent of stevedores and 36 percent of checkers who work in Montreal's port have criminal records.²⁵

Conclusion

One year after 9/11, not much has changed in terms of info-network security. The government's draft cyber-security report offers no accelerated programs to push development of counter-terror measures. Cyberspace is probably no safer than one year ago. There is a silver lining in the cloud of government ineptitude in cyberspace and computers: mouse-illiterate agencies like the FBI are at least less vulnerable to cyber-attack. Then again, their backward state makes impossible the rapid deployment of sophisticated information networking tools to accelerate identification of and response to terrorist threats.

Why this lackluster performance in a country whose population spent the entire past decade gravitating to online usage, with subscribership in overdrive after *Windows95* and Netscape *Navigator* made their twin August 1995 debuts? Surely these bureaucrats observed their children net-surfing? Surely the hundreds of magazine covers

trumpeting the Internet Age must have been on to something (the *dot-com* financial asset value crash notwithstanding)?

Bureaucracies, it seems, are governed by the usual set of laws: Newton's, Parkinson's and Murphy's. An object at rest tends to stay at rest (inertia); work expands to fill the time allotted for its completion; and as for Murphy, O'Toole's commentary on Murphy's famous law (Murphy, by the way, was a test pilot) assures us that the fellow was...an *optimist*. It took a seismic shock—the murder of 3,000 innocent people, mostly American, the collapse of the world's most iconic commercial buildings, and the nation's capital under siege—to give the public sector leviathan the proverbial wake-up call.

President Bush believes that centralizing 170,000 bureaucrats in a Department of Homeland Security will coordinate and focus counter-terror efforts. The author has come around to the view that this is an idea superficially appealing in theory, but bound to fail in practice. Large bureaucracies lack the creativity and agility that fighting this war calls for. Better by far to place in all affected agencies centers of excellence—little DARPAs, so to speak—who can move quickly and interact with each other without being entombed in a mega-department. This will have the added benefit of preserving diverse agency cultures (albeit, within many specific agencies, cultural reform may well be needed), rather than creating a single homeland security bureaucratic culture. In strategic and tactical diversity there is strength. There may also be benefits from combining a few of the smaller agencies, but only if the advantages of scale do not impede celerity.

Air, border and port security offer abundant opportunities to use information technology effectively. The high concentration of traffic in major airport hubs, ground crossings and ports

offers high payoff for early upgrade. Ultimately, comprehensive coverage is essential, as terrorists need only find *one* entry point. The cliché that terrorists need only succeed once with a nuclear device while defenders must succeed all the time is, sadly, true. This does not mean that their success is inevitable, but does lengthen the odds against successful defense and put a concomitant premium on pre-emptive measures against mega-death terror.

Cyberwar will be fought on the run, with swift attacks and adaptation to defenses. The dispiriting news recounted above can serve as impetus for change, but a sense of urgency seems to be missing in Washington. That is not good news for those increasingly dependent upon a safe cyber-world. We may take some consolation that our enemies are not highly cyber-savvy, but they can *learn*.

Meantime, we can start with a prosaic step: it is a national scandal that police and fire departments lack essential radio spectrum. Give them what they need.

-
- ¹ “Cybersecurity’s Leaky Dikes,” BusinessWeek Online, July 2, 2002.
< http://www.businessweek.com/technology/content/jul2002/tc2002072_9216.htm >
- ² *The National Strategy to Secure Cyberspace*, The President’s Infrastructure Protection Board, Sept. 2002. < <http://www.whitehouse.gov/pcipb/> >
- ³ *Id.*, p. 3.
- ⁴ *Id.*, p. 4.
- ⁵ *Id.*
- ⁶ Round figures: vulnerabilities from 400 to 2,400; incidents from 10,000 to 50,000. *Id.*, p. 5.
- ⁷ *Id.*, p. 21.
- ⁸ *Id.*, p. 8. “Critical infrastructure” is defined by the USA Patriot Act of 2001 as: “systems and assets, whether physical or virtual, so vital to the United states that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” *Id.*, p. 7.
- ⁹ *Id.*, p. 8.
- ¹⁰ *Id.*, p. 24.
- ¹¹ *Id.*, p. 9.
- ¹² *Id.*, p. 17.
- ¹³ *Id.*, pp. 49-52.
- ¹⁴ *Increasing FDNY’s Preparedness*, Aug. 2002 (FDNY Report).
< http://www.nyc.gov/html/fdny/html/mck_report/index.html >
- ¹⁵ *Improving NYPD Emergency Preparedness and Response*, Aug. 19, 2002 (NYPD Report).
< <http://www.nyc.gov/html/nypd/pdf/nypdemergency.pdf> >
- ¹⁶ The FDNY Report defines high-rise as a building with at least 7 stories; NYC has 2,000.
- ¹⁷ “Mouse-less FBI,” National Review Online, Oct. 8, 2002. Don’t even ask about the IRS.
< <http://www.nationalreview.com/comment/comment-schatz100802.asp> >
- ¹⁸ “Airport Security Gets Another ‘F’”, CBSnews.com, Sept. 4, 2002.
< <http://www.cbsnews.com/stories/2002/09/03/eveningnews/main520612.shtml> >
- ¹⁹ “Sidelights,” *The American Enterprise*, p. 6 (Sept. 2002).

[ET CETERA]

Competition: Chinese Style. Think competition is tough in America? Try competing with someone cutting your lines, as is commonplace today in China.²⁶

The DVD Hits Warp-Speed. The DVD has become the fastest penetrating consumer product of all time. After five years it is in 30 million of the nation's 110 million households, with 25 percent having more than one DVD player; by year-end estimates are that 40 percent of households will sport at least one DVD (counting PCs that play DVD, over 50 percent of households will be DVD-capable). Introduced at \$600 - \$700 in 1997, they are down to \$150, with \$79 Christmas specials in the works. DVD sales lead rentals, the reverse of VCR tapes. In 2001 DVD sales crossed VCR tapes; of \$10.3 billion spent domestically to buy films, 5.4 million (52 percent) went to DVD. Media Research estimates that for 2002 DVD will take \$8.1 billion, which will be 65 percent of the forecast \$12.4 billion film sale market. DVD rentals more than doubled (up 110 percent) in 2001, while VCR rentals declined 22 percent (VCR rentals still lead DVD). Finally, buying volume is much higher with DVD: the typical home buys about 15 DVDs annually, versus 5 for VCR tapes. Some experts see the VCR tapes vanishing from shelves within five years.²⁷

To see just how economically significant the DVD boom is for Hollywood, consider: *DVD sales and rentals account for more revenue than box office sales*, which are only 25 percent of the take on movies released today. VCRs are still in three times as many households—90 million versus 30 million; but coming to market in the not-too-distant future will be the HDDVD—High Definition DVD.²⁸

The DVD is the quintessential example of a “bandwagon product” (discussed at length in an earlier *Bandwidth* issue²⁹) meeting consumer desires by offering large advantages over a predecessor, in this case, the VCR. It introduces to video the same random access capability, custom programming, longer playing time, superior fidelity and com-

pact size that the CD brought to audio, and thus the VCR will soon go the way of the LP record. Another kicker aiding DVD diffusion: there was no significant litigation launched (as Hollywood did with the VCR) to stop distribution of the product. *Less regulation; more market choice.*

“Beam Me Up, Scotty!” NASA wants to develop ways to read brain waves of air travelers to divine who might be a terrorist—we are NOT making this up.³⁰

Welcome to Insane Airlines... Airport security never ceases to amaze, from sky marshals waving guns at terrified passengers to searching the most improbable suspects. The latest is a passenger who faces a possible twenty-year prison sentence for...*shaving*. It seems a pair of Sikhs, delayed September 10 on their way to a convention in Las Vegas, boarded a Northwest Airlines flight on September 11. Their luggage had gone ahead with the Minneapolis connection they missed the day before, and all they carried were shaving kits apparently given them by the airline. They took a Memphis flight and boarded with a Hispanic, the sight of three swarthy males apparently causing concern among the flight crew. The Sikhs did not sit in their assigned seats. Then one of them asked a flight attendant if he could use the washroom. She consented, and he went in to shave. He insisted on finishing the task, despite repeated calls from the attendant to return to his seat. The captain landed the plane in Arkansas and the two Sikhs, plus the unfortunate Hispanic who boarded with them, were detained. The clean-shaven Sikh has already paid a \$500 civil fine, but now the Justice Department is threatening to prosecute him for “assaulting or intimidating a...flight attendant and [interfering] with the performance of the duties of the ...attendant.”³¹ Earth to Justice Department: come home, please.

China Watch: Next Cyber-Crime Capital? As if snipped phone lines are not enough hassle (see above), some 84 percent of China's 45 million Internet users have been hit with a computer virus, with half suffering damage as a result.³²

- ²⁰ “NASA Plans to Read Minds at Airports,” washtimes.com, Aug. 17, 2002.
< <http://www.washtimes.com/national/20020817-704732.htm> >
- ²¹ “Air Security Focusing on Flier Screening,” *Washington Post*, p. A1, Sept. 4, 2002.
- ²² “How Experts Grade Homeland Security,” *Washington Post*, p. A20, Sept. 10, 2002.
- ²³ “A Growing Body of Biometric Tech,” BusinessWeek Online, July 2, 2002.
< http://www.businessweek.com/technology/content/jul2002/tc2002072_916.htm >
- ²⁴ “For US Customs, Trade and Security Clash on the Docks,” *Wall Street Journal*, p. A1, Sept. 12, 2002. Figures: 20.12 million total units, with 11.19 million by truck, 5.71 million by ship, 2.26 million by rail and 960,000 by air.
- ²⁵ “A Broad Security Measure: US Customs Officers Check Containers for Concealed Terror,” *Washington Times*, p. A1, Sept. 1, 2002.
- ²⁶ “Crossed Lines,” washingtonpost.com, Aug. 17, 2002.
- ²⁷ “In Revolt in the Den, DVD Has the VCR Headed to the Attic,” *New York Times*, p. A1, Aug. 26, 2002.
- ²⁸ “Hollywood Sees the Big Picture with DVDs,” washingtonpost.com, Oct. 7, 2002.
< <http://www.washingtonpost.com/wp-dyn/articles/A51962-2002Oct6.html> >
- ²⁹ “The Broadband Bandwagon: Faster to 10, Slower to 50?” *Bandwidth*, Feb. 22, 2002.
< http://www.discovery.org/bandwidth/issues/2002-02-22_460k.pdf >
- ³⁰ “NASA Plans to Read Terrorists’ Minds at Airports,” washingtontimes.com, Aug. 17, 2002.
- ³¹ “Twenty Years for Shaving?” *Washington Post*, p. A18, Sept. 23, 2002.
- ³² “China Says Viruses Infect 80 Percent of Computers,” reuters.com, Oct. 10, 2002. The story was in Beijing’s official daily.
< http://www.reuters.com/news_article.jhtml?type=internetnews&StoryID=1557133 >

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>