April 25, 2003

bandwidth

An Online Newsletter of Discovery Institute

Cyber-Safe Meets Fail-Safe: The Bush Strategy

By: Senior Fellow John Wohlstetter

This February the Bush Administration released *The National Strategy to Secure Cyberspace*, a long-awaited document spelling out the nation's cyber-security strategy, a crucial element falling into the homeland security portfolio.[1] Heightening cyber-fears is the military's concern about battlefield e-mails sent home, which travel through the public networks at the end of their cyber-journey; the military has its own Secret Internet Protocol Network for war messages.[2] At the same time the White House also released a new critical infrastructure security strategy document, *The Physical Protection of Critical Infrastructures and Key Assets*.[3] Together the documents outline a broad strategy for homeland security in both the physical and virtual realms, based upon an extensive array of partnerships between the public and private sectors. Highlights follow.

Cyberspace Security: Keys to the City?

First the good news: the report finds that it requires considerable technical sophistication to inflict "debilitating disruption" on critical infrastructure, national security or the economy.[4] The bad news, of course: It IS possible. While pre-eminence is ceded to the private sector, government involvement is necessary in special cases. High transaction costs prevented airlines from making needed investments in air security; expensive software remediation could erect similar financial hurdles for cyber-security. Antitrust laws erect legal barriers to private coordination—one man's coordination is another's unlawful conspiracy. Then there is the incentive problem known as the so-called "tragedy of the commons": users have no individual incentive to act responsibly, and the ensuing result is disastrous for all; thus, no single user of antenna space on top of the World Trade Center towers had an incentive to provide full security. Finally, there are certain traditional areas for government action, such as military communications.[5]

The report sets five "critical" priorities, each with multiple actions and initiatives:

- Create a public/private partnership to develop a national cyberspace security response system;
- Apply law enforcement and technology tools to implement a broad national cyberspace security threat and vulnerability reduction program;
- Promote for business and residential populations a national cyberspace security awareness and training program;
- Improve networks and systems to secure governments' cyberspace;
- Work with industry and international organizations to foster national security and international cyberspace security cooperation.[6]

The need for new measures is evidenced by the latest cyber-attack metrics. Identified flaws in software security quadrupled between 2000 and 2002; despite 90 percent of network users having anti-viral software, 89 percent having software firewalls and 60 percent intrusion detection systems, 90 percent reported security breaches, 85 percent had suffered damage to their systems and 40 percent reported outsider penetration of their networks.[7] In the past four years, costs to the domestic economy from computer attacks quadrupled.[8] Amazingly, the top ten known software vulnerabilities were exploited in a majority of cyber-attacks.[9]

The report embraces the governing principle of "subsidiarity": addressing problems at the "lowest common denominator" level—private, then local government, then state government and finally, federal involvement.[10] Federal agencies involved in coordination include the White House Office of Science & Technology Policy, Office of Management & Budget, Department of State, CIA, FBI and Department of Justice.[11]

Certain special vulnerabilities raise immediate concerns: (1) Internet assets—*i.e.*, nodes, protocols domain names, routers, etc.; (2) digital control systems and supervisory control and data acquisition (SCADA) systems; (3) software/hardware remediation; (4) physical infrastructure/interdependency.[12] SCADA systems are identified as a national priority. Via computer networks, SCADA systems control such vital infrastructure assets as water, transportation, chemicals, energy and manufacturing. The problem with SCADA is that typically they are small systems with a limited, self-contained power supply, but often must operate in real-time. Key White House proposals include developing extremely low-latency link encryptors/authenticators, key management and network status/state-of-the-art health monitoring.[13]

Other points of note: Infrastructure cross-dependencies are another problem. In one instance, a campfire in New Mexico damaged a gas pipeline, which shut down IT-production in Silicon Valley.[14] Federal employees will increasingly face multi-layer authentication processes—biometric smart cards, smart tokens, strong passwords—to access buildings and computers.[15] Internationally, the US plans a "Safe Cyber Zone" with Canada and Mexico, plus initiatives for the G8, APEC (Asia) and OECD; a global information network for cyber-security is also on tap.[16]

The most worrisome weak spots may well be SCADA systems. In mid-2002 a teenager gained control of the gates of a dam in New Mexico. Having more of a conscience than your typical al-Qai'da member, he did not open the dam. The potential for loss of life and property damage from such an event makes a denial-of-service attack on networks seem positively tame by comparison. SCADA must be provided with multiple layers of protection: dedicated private networks for mission-critical functions; highly reliable authentication to prevent insider manipulation; and multiple authorization of key actions, so no one actor can cause a disaster.

Perhaps most disappointing is the failure to recognize that existing regulatory incentives will impede deployment of advanced cyber-infrastructure. The White House seems to presume that the proper incentives are in place. Readers of this newsletter have been bombarded at great length as to why such is not the case—policies requiring Bell companies to rent their networks to rivals at below-cost prices, inadequate depreciation schedules, obstructing vertical mergers, etc. FCC telecom regulatory policy thus works at odds with the goals of this White House report. The two are policy ships passing silently in the night.

Critical Infrastructure Protection: Can Vast Vulnerability Be Closed?

The companion report issued by the WH covers broader physical infrastructure concerns pertinent to "national security, governance, public health and safety, economy and public confidence."[17] Protecting 50 states, four territories and 87,000 local jurisdictions is a tall order.[18] Threats include direct attacks on critical nodes, indirect (collateral) damage—*i.e.,* financial impact of infrastructure damage; and exploitation of infrastructure assets to damage another target.[19] The September 11 attacks combined all three elements: direct—the buildings destroyed; indirect—the financial harm that resulted; and exploitation of key assets to damage others—commandeering commercial jetliners to attack key targets.[20]

"Critical infrastructures" are defined 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."[21] The WH

strategy covers 13 critical infrastructure sectors: agriculture and food; water; public health; emergency services; defense industrial base; telecommunications; energy; transportation; banking and finance; chemicals and hazardous materials; postal and shipping. Other key categories are national monument/icons, nuclear power plants, dams, government facilities and commercial key assets.[22] Among the staggering number of assets needing protection are nearly 2 million farms; 1,800 water reservoirs and 1,600 water treatment plants; 5,800 registered hospitals; 250,000 defense firms; 2 billion miles of telecom cable; 2,800 electric power plants and 104 commercial nuclear power plants; 300,000 oil/natural gas production sites; 5,000 public airports; 120,000 railroad track miles; 590,000 bridges; 2 million miles of pipelines, 500 major urban mass transit systems; 66,000 chemical plants; 5,800 historic buildings; 80,000 dams (the report estimates that 10 percent of these, in event of failure, would cause "significant property damage or have public health/safety consequences[23]); 3,000 government-owned buildings; 460 skyscrapers.[24] An estimated 85 percent of infrastructure assets are held by the private sector.[25]

Five cross-sector priorities were identified: (1) planning and resource allocation; (2) information sharing and indications/warnings; (3) personnel surety - i.e., guaranteeing trustworthiness of insiders , building human capital and awareness; (4) technology and R&D; (5) modeling, simulation and analysis.[26] For telecommunications, the Federal Communications Commission is relegated to a supporting role under Homeland Security, as are several executive branch bodies long tasked with telecom security issues.[27] One noteworthy shortfall cited in the report is the lack of communications inter-operability among various emergency services (police, fire, etc.).[28] This became painfully apparent on September 11 (and was covered in an earlier issue of Bandwidth[29]).

Information technology tools will play a prominent role. Computer modeling, simulation and analysis will be applied to identify and assess risks associated with cross-sector dependencies. Risk management and resource allocation will be guided by analysis of threat and vulnerability information. A prime focus will be "interactions between physical and cyber systems."[30]

Modeling complex phenomena is a task that carries with it the risk that computer types call GIGO: Garbage In, Garbage Out. Ascertaining risks for a single infrastructure is a highly subjective exercise at best; factoring in cross-dependencies would seem to multiply exponentially the possible permutations as variables increase arithmetically. The potential payoff of a successful terror attack, however, is so great that a modest investment in such tools may yield surprise benefits.

The sheer number of valued assets augurs for vulnerability into the distant future. Surveillance cameras will play a big role—more than 40 percent of an estimated 26 million worldwide are in the US—but video monitoring represents just one percent of surveillance.[31] The White House knows this, but has wisely started a process of inquiry that may assist not only reducing key vulnerabilities, but aiding rapid restoration. Thus it is an effort very much worth making.

[ET CETERA]

Bell Broadband Blow-Up? Verizon's chairman says it needs 3.5 to 4 million subscribers to make DSL financially viable, roughly twice the company's year-end 2002 total of 1.8 million. Merrill Lynch believes the company will not reach its target until year-end 2005. Meantime, UBS Warburg projects that the Bells will lose another 8 percent of their access lines in 2003. Adding a DSL subscriber typically costs the Bells $150-$200 more than for a new cable modem user.[32] Overall telecom capital spending, over $50 billion in 1998, fell to around $30 billion in 2002; $30 billion was the level of *non-incumbent* carrier investment in 2000, a figure that had by 2002 shrunk over 90 percent.[33] FCC fans, take a bow.

WorldCom Write-Downs: Industry Augury? WorldCom's March announcement that it would write off $45 billion of merger investments in the "goodwill" of acquired firms, plus $34.8 billion of hard assets—to $10 billion from $44.8 billion, a 78 percent loss—presages similar actions, probably at AT&T among others, and imperils tens of billions in inflated capital investment. Earth to FCC….

Fading Fax. Davidson Consulting predicts that global fax sales, nearly 14 million in 2000, will fall below 13 million by 2006. Total fax pages transmitted worldwide, 350 million in 1998, fell more than 50 percent, to 170 million, in 2002. One factor: sales of all-in-one machines (print, copy, fax), 7 million in 2001, are projected by Davidson to reach 8.5 million in 2006. One reason fax will persist: time/date stamping is far more reliable than with e-mail, a critical factor for legal documents.[34] Nice to see the lawyers actually help *preserve* an industry.

United States of Spamerica. Only an estimated 8 percent of Internet traffic in late 2001, spam is now 40 percent, and will hit 50 percent by year-end, according to anti-spam firm Brightmail. Ferris Research pegs the national annual spam bill at $10 billion. Jupiter Research estimates that e-marketing is now a $1.4 billion business. Consider: If one percent of the 24 million small businesses send you a single e-gram per year, your mailbox will get 657 spam messages each *day*. While Congress fiddles, 26 states have passed anti-spam laws.

Spam Slam. A Maryland court has ruled that the state's anti-spam law permits aggrieved users to post name and address information on spammers. The victorious plaintiff posted on his own website a warning to the spammer-defendant, concluding: "Your best option is to crawl back under a rock and suck it up, or move to some state other than the one I live in."[35]

Internet Whiz. A new Internet "speed record" was announced March 7 by the Stanford Linear Accelerator Center: 923 megabits per second over 6,800 miles of optical fiber, effecting transfer between Sunnyvale, California and Amsterdam, the Netherlands, of 6.7 gigabytes of uncompressed data in 58 seconds. Equivalent to a pair of two-hour movies, the transfer was over dedicated bandwidth and with Internet protocols tweaked to enable faster transmission, at 93 percent "efficiency" (presumably, this means 7 percent had to be re-sent to correct errors). The scientists anticipate faster speeds using an *Internet2* connection (*Internet2* is a special research consortium network).[36]

Internet Reaches New Heights. A grandson of the only surviving Sherpa guide from Edmund Hillary's 1953 Mount Everest summit expedi-

[1] The White House, February 2003. < http://www.whitehouse.gov/pcipb/ >
[2] *U.S. Military Restricts E-Mail From Soldiers and Sailors, Citing Risk of Leaks*, IHT Online, 3/12/03. < http://www.iht.com/articles/89467.html >
[3] White House (February 2003).
[4] *The National Strategy to Secure Cyberspace*, fn. 1 *supra*, p. *viii* (executive summary).
[5] *Id.*, p. *ix* (executive summary).
[6] *Id.*, p. *x* (executive summary).
[7] *Id.*, pp. 8-9.
[8] *Id.*, p. 10. (No dollar loss figure was given in the report.)
[9] *Id.*, p. 33.
[10] *Id.*, p. 15.
[11] *Id.*, p. 17.
[12] *Id.*, p. 29.
[13] *Id.*, p. 32.
[14] Id., *p. 34.*
[15] *Id.*, p. 46.
[16] *Id.*, pp. 51-52.
[17] *The Physical Protection of Critical Infrastructures and Key Assets*, p. vii (executive summary).
[18] *Id.*, p. *x* (executive summary).
[19] *Id.*, p. *viii* (executive summary).
[20] *Id.*, p. 8.
[21] *Id.*, p. 6. (The definition is lifted from the USA Patriot Act.)
[22] *Id.*, p. xii (executive summary).
[23] *Id.*, p. 76.
[24] *Id.*, p. 9.
[25] *Id.*, p. 8.
[26] *Id.*, pp. *xi-xii* (executive summary).
[27] *Id.*, p. 48.
[28] *Id.*, p. 43.
[29] *9-11 Plus One: Have Lessons Been Learned?* < http://www.discovery.org/bandwidth/issues/2002-11-13_330k.pdf >
[30] *Id.*, pp. 33-34.
[31] *Surveillance Nation*, Technology Review, p. 34 (April 2003). Source: I.P. Freeman (1/03).
[32] *How Phone Firms Lost to Cable In Consumer Broadband Battle*, Wall Street Journal, p. A1 (Mar. 13, 2003).
[33] Source: Moody's Investors Service (2002).
[34] *Ease of Paperless E-Mail Sidelines the Forlorn Fax*, New York Times, p. E7 (Mar. 13, 2003.
[35] *Ruling Backs Anti-Spam Activist*, Washington Post, P. E1 (Apr. 7, 2003).
[36] *Scientists: Internet Speed Record Smashed*, CNN, 1:50 PM EST, Mar. 7, 2003. < http://www.cnn.com/2003/TECH/internet/03/07/speed.record/index.html >
[37] *Because It's There: Putting Everest Online*, New York Times, p. E1 (Jan. 23, 2003.
[38] *A Home on the Web: The Afghan Struggle For Internet Domain*, Wall Street Journal, p. A1 (Mar. 10, 2003).
[39] *Storing Movies on DVD Is So Two Weeks Ago: Now it is the HD-DVD*, Wall Street Journal, p. B1 (Mar. 10, 2003).
[40] *Wired and Wireless*, Washington Post, p. E1 (Apr. 3, 2003).
[41] *Six Million Mobile Phones Get the Message*, smh.com.au (4/3/03).

tion aims to set up an Internet café at base camp's nearly 18,000-foot altitude. A $10,000 satellite dish will sit 1,500 feet above base camp, as the camp is on a moving glacier and thus cannot support the dish. Wi-Fi radios will connect the camp and the dish. An ISP in Israel will forward transmissions from the satellite relay. Fees will be assessed each expedition, in the $2,000 to $5,000 flat-rate range. The cyber-cafe set-up will cost an estimated $1,000 monthly during the climbing season. Proceeds from use of the café will support pollution control on the mountain.[37]

Domain Donnybrook. One upside of American victory in Afghanistan: The country now owns the domain locator suffix, *.af*. Seems that the suffix had been owned by a mysterious figure, associated with the Taliban, who had outlawed—yes, outlawed—the Internet in August 2001. But the figure disappeared, and last month, after maneuvering by a dedicated UN worker, Afghanistan joined the Net. Domain name hijackings are, of course, quite common: Bhutan had to persuade British Telecom to surrender the *.bt* suffix in 1999; as BT was not using the suffix, it assented to the transfer.[38]

High-Definition Milestone? In 2002, one in 10 of the 25 million television sets sold in the US was high-definition, and prices for HDTV sets may fall below $1,000 this year. The companion product is, naturally, the HD-DVD, which made its debut in March this year, and crams more data per disc than regular DVDs by using a short-wavelength blue laser instead of a long-wavelength red laser. Uncompressed film runs two terabytes, roughly 1,000 times the two-gigabyte length of a compressed film. Even HD-DVDs need super-compression to carry movies in high-resolution. There are, however, no fewer than three competing standards, and initial prices are way up there—Sony's model runs $3,800.[39]

Wi-Fi Uptake. Starbucks reports that 25,000 of its 22 million customers (.011 percent) use its on-premises Wi-Fi service, which T-Mobile has set up in 60 percent of the company's nationwide outlets. Per-minute rates have been slashed to 10 from 25 cents, with both bucket rates and $30/month flat-rates offered to high volume users. Research firm In-Stat/MDR counts 3,700 Wi-Fi "hot spots" in the US, of which 2,600 are in cafes; the firm projects 10,000 spots by year-end.[40]

Wireless Warning. Responding to the deadly threat of SARS infection, Hong Kong authorities used text messaging to alert 6 million residents to discount an Internet rumor that HK had been declared an "infected city"; it was, the government decided, the fastest way to alert the public.[41]

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 NEW mailing address:
1511 Third Avenue
Suite 808
Seattle, WA 98101

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