


January 8, 2002



bandwidth

An Online Newsletter of Discovery Institute



**Techno-Terror and the
Information Society's
Homeland Defense:
Reflections Upon the
New Year**

By: Senior Fellow John Wohlstetter

September 11, 2001 will, in American history, “live in infamy” as surely as did December 7, 1941. And our response to the challenge posed by the atrocities of September 11 must match—in effectiveness, not scale (post-industrial war involves highly specialized human and material resources)—that of the “Greatest Generation” in response to the slaughter of December 7. It has been said that America and its allies face a new kind of challenge, and in some sense this is indeed true. Never before could sub-national groups so plausibly threaten the hideous harm that bio-weapons, let alone nuclear devices, can inflict. Yet sub-nationals—especially, the most dangerous groups—are generally supported by states, and in this more fundamental sense the challenge is not new.

The dilemma facing us was best captured nearly half a century ago by one of the 20th century’s greatest political philosophers, the late Frenchman Raymond Aron. He assessed the twin threats of nuclear and guerilla warfare—for today’s context terrorism may fairly be substituted for guerilla warfare, despite technical differences between the two. Wrote Aron:

Let us have the courage to admit that the fear of war is often the tyrant’s opportunity, that the absence of war, that is of open conflict between legally organized political units, is not enough to exclude violence between individuals and groups. Perhaps we shall look back with nostalgia to the days of “conventional” wars when, faced with the horror of guerilla warfare and the atomic holocaust, the peoples of the world submit to a detestable world order provided it dispels the agonies of individual insecurity and collective suicide.¹

The credible prospect of collective suicide was dissipated because the United States and the alliance it led for nearly half a century triumphed in the Cold War when the former Soviet Union crumbled in 1991. It was, even then, understood widely among national security specialists that terrorism would become a major, if not the primary, threat the United States would confront in the future.

Mapping terrorism to Aron’s statement of the challenge civilization confronts, i.e., substituting terrorism for guerilla warfare as noted above, terrorists aim to exploit the agony of “individual insecurity.” A government that cannot dispel such agony faces de-legitimation, for failure to discharge its twin bedrock functions: provide for the common defense and preserve domestic tranquility.

What Insecurities Must We Dispel?

Modern, free civil society requires certain levels of confidence to function: foremost is an acceptable level of safety—including protection from terrorist acts. Social and economic intercourse is ultimately paralyzed absent security. Free societies require an added kind of security: that essential liberties are preserved and protected. But liberties cannot survive without order: in times of anarchy people will turn to Thomas Hobbes, not John Locke, for guidance.

Information technology (IT) can help reconcile the security/liberty dilemma that perpetually bedevils free societies. What strategies might best defeat our terrorist adversaries and, in particular, what role can IT play in helping win the war to which the world’s civilized peoples have been so brutally summoned? IT can play a potentially decisive role in determining the outcome of the conflict.

Homeland Security: The Exposed Frontier

Today's terrorist adversaries have already inflicted the most grievous mainland casualties the US has seen since the Civil War. The risk of far worse—in the form of nuclear, biological or chemical strikes—means that even a small probability must be taken seriously, with counter-measures implemented as soon as possible. Consider the magnitude of the task: Every day in the US truckers alone carry 770,000 shipments of hazardous materials. In all, there are 80 million trucks in the US. Add 130 million automobiles and 5,000 aircraft.² Throw in 2,800 power plants, 190,000 miles of natural gas pipelines, nearly 600,000 bridges, 463 skyscrapers, and 20,000 miles of borders.³ Our borders are crossed—daily—by 1.3 million people, more than 50,000 trucks and containers, 2,660 aircraft, 348,000 vehicles and 520 vessels.⁴ For icing on the cake, top off the list with several hundred thousand office buildings.⁵

Shipping vulnerabilities are particularly vexing. In 1999 more than 2 billion tons of goods entered American ports.⁶ In 2000, America's more than 100 seaports handled more than 33 million containers in 2000 (up from only 8 million in 1980); according to one expert, checking every container reaching American ports would entail clearing a box every 20 seconds.⁷ Rendering the task even more nightmarish is that international shipping cargoes typically travel through many insecure ports from origin to final destination. Worse, ship owners whose vessels face official inquiry change flags of convenience—"flag hopping" to a new registry.⁸ British and American officials are now hunting for 20 ships comprising bin Laden's terrorist fleet; one suspect ship was seized December 21.⁹

And what resources do we have to watch all this, besides traditional federal and state law enforcement? The Immigration and Naturalization Service has 2,000 agents to police 303 official points of entry and 95,000 miles of shoreline; the Postal Service has 1,900 inspectors to watch 680 million pieces of mail daily.¹⁰ The Coast Guard has approximately 35,000 personnel to watch 11,900 miles of waterways.¹¹ Do not envy them their task. But, fortunately, help is on the way.

Homeland Security: The Info-Tech Ace in the Hole

As it happens there are technologies of vast promise just coming to fruition as economically viable products that can help detect dangerous materials, and do so in a minimally intrusive way. In a recent edition of his newsletter, technology maven Peter Huber, senior fellow at the Manhattan Institute, described one: millimeter waves, embedded in specialized microprocessors (called MMICs—Monolithic Microwave Integrated Circuits), can significantly improve homeland security in ways minimally intrusive of personal privacy and civil liberties. He stated: "The MMIC will emerge, alongside the microprocessor IC, as one of two critical technologies that will rebalance the asymmetries of conflict in the high-tech versus low-tech clashes of the twenty-first century."¹² Huber elaborated on this theme in a brilliant address to the Gilder/Forbes Telecom V conference in November, identifying functions MMIC-enabled devices would need to perform, with surveillance and sensing foremost among them, in the context of homeland security. The war against terror could, in Huber's tart phrase, become one pitting "our silicon versus their sons."¹³

Other techno-aids are blossoming. A company called Ancore has three surveillance products, already on the market, that use neutron scanning technology to detect contraband based upon its chemical composition, and without human operator intervention.¹⁴ Emerging “bar code on a chip” technology will enable authentication of every package that enters the stream of commerce. Packages without proper authentication can then be rejected.¹⁵ Face recognition technology is promising as a way to survey public places, and is already being tested in several airports.¹⁶

The ultimate security device may be the “Verichip” just unveiled by Applied Digital Solutions, an implanted identification chip that can transmit personal data to monitoring stations for medical, security and emergency purposes.¹⁷ Biometric implants will not likely win mass-market acceptance, given (legitimate) privacy concerns. But how about conditioning release of terrorists convicted of lesser offenses upon their accepting remote police monitoring?

Connecting the Dots: The Next Frontier for Networking

The National Security Agency uses a number of systems—most notably, Echelon, which purportedly can monitor 3 billion calls (voice, various kinds of data calls—fax, e-mail, etc.—and broadcast video), but its capability is not publicly known. As one insider puts it, “anyone who knows about it won’t talk about it, and anyone who talks about it doesn’t really know about it.”¹⁸ But in February 2001 NSA Director Michael Hayden acknowledged on *60 Minutes* that his agency is “behind the curve” on surveying global telecommunications.¹⁹

Networking diverse databases and applying data mining software can yield valuable, timely data. MIT researchers have developed software that monitors emergency room traffic at hospitals, searching for patterns of symptoms that show uncommonly large numbers of patients infected with designated pathogens.²⁰ MIT is also working on an “intelligent city” concept, in which sensors embedded in infrastructure are linked to databases that would direct emergency response per real-time information.²¹ Homeland Security Director Tom Ridge has stated that the Bush Administration will build a health network to link federal, state and local health officials, including a central clearinghouse for public health data.²²

Ridge is not alone. Bush counter-cyber-terror chief Richard Clarke has proposed a separate government network (*GovNet*) to ensure survival of critical functions in the event of a widespread attack on the public networks. The Department of Defense requested private sector proposals for counter-terror technology; by the December 23 deadline the Pentagon had received 12,085 submissions.²³

Such networks will need vast concentrations of processing power, bandwidth and storage—orders of magnitude beyond today’s plant—to gather, transport and analyze voice, data and video, and yield real-time answers. Peter Huber provides an illustration of this: A single automated luggage scanner used in airports today would need a 200 megabit-per-second connection to send data in real-time for analysis.²⁴ This is 4,000 times a typical 56-kilobit dial-up access speed, and over 100 times faster than top-end DSL and cable links today.²⁵ An airport with five machines would need a *gigabit* link for real-time networking. Multiply this by all the facilities noted above, and there goes the “fiber glut.”

Even if all the above techno-measures were adopted, security would still be imperfect and thus penetrable. But vulnerabilities can be significantly reduced by multi-layered protection; multiple lines of defense yield higher reliability than any individual layer alone. It may still take 007 to stop the world's Blofelds, but the vast majority of adversaries are less competent than Ian Fleming's super-Satans.

Security, Privacy, Civil Liberties and Terrorism: Sorting the Wheat from Chaff

We are often warned that the terrorists will have won if we sacrifice our liberties to procure safety. And not without reason: Former CIA chief R. James Woolsey recently offered a chilling cautionary tale of government overreaching, based on his experience defending eight innocent Iraqi clients whom the government sought to deport. Government abuses led to appalling instances of prolonged incarceration: one translator's error left one client in jail for a year; cultural ignorance in parsing Kuwaiti names led prosecutors to wrongly infer another client's intent to hide his identity, for which the man spent three years in jail.²⁶

But while government abuses are serious cause for concern, they do not justify accepting the status quo of defense against terror, which nearly everyone realizes will not suffice. A trade-off between security and liberty will be hard, if not impossible, to avoid in wartime.²⁷ We must ask: Which of our traditional freedoms are truly essential, and thus must be preserved at the end-game?

As one example of a freedom less valuable, Silicon Valley legend Carver Mead stated at Telecom V that he does not regard misrepresenting one's identity as a fundamental right, and that thus biometric smart card authentication of all US residents is a proper step in enhancing homeland security.²⁸ Authentication would have made September 11's attacks less likely. The IRS already knows where to find readers of this e-letter; let terrorists enter the databases as well.

If we wish to maximize freedom from fear—one of FDR's Four Freedoms—we will have to make some compromises. We already have. Those of us of a certain age remember the golden age of flying, the 1960s, when jets began ferrying us at high subsonic speeds and in unprecedented comfort, and when walking through an airport to board a domestic flight entailed no ID, baggage search or security check, no ritual posing of hilariously inane questions, no "wand" passes or pat-downs and no beeping metal detectors. We accept loss of the golden flying years—never to return—as the price of greater flight safety.

Wartime exigency requires enhanced security measures, a matter justly worrisome in free societies. Most infamous was the wholesale internment of Japanese-Americans in World War II, now universally condemned. The most eloquent defense of civil liberties abridgement was offered by Abraham Lincoln, defending to Congress—on Independence Day, 1861, no less—his decision to suspend the writ of *habeas corpus* shortly after commencement of the Civil War: "Are all the laws, but one, to go unexecuted, and the government itself to go to pieces, lest that one be violated?"²⁹ Lincoln even prosecuted antiwar firebrand Clement Vallandigham for encouraging Union soldiers to desert, famously saying in a letter to the New York Tribune defending his action: "Shall I

shoot the simple-minded soldier boy who deserts while I must not touch a hair of a wily agitator who induces him to desert?”³⁰ Could the Civil War restraints be imposed today?

Consider the following horrific hypothetical (may it remain just that): A nuclear device is detonated in a major American city, causing over 100,000 deaths, leveling a mile or two of pricey downtown office space and rendering additional miles of real estate radioactive and therefore uninhabitable for decades. How would the government respond? Bet that martial law—at minimum locally and very possibly nationally—would be declared within 24 hours.

Other free countries accept levels of surveillance we have historically rejected. Today’s visitor to London can expect to be captured in an average of 300 photos per day. Many European countries require national ID cards. And now the US State Department plans to use digital imaging in connection with issuing visas.³¹

No one wants to sacrifice bedrock liberties—e.g., speech, assembly, worship, due process, fair trial, self-defense, etc. Intelligent, pervasive application of IT will require accepting less privacy than before. But better to surrender modest amounts of traditional privacy and non-essential liberties, and thus avoid having to surrender far more freedom later, after a mega-death terrorist catastrophe. A government that goes to heroic lengths to protect the Tooth Cave pseudo-scorpion³² is entitled to do as much to protect innocent *homo sapiens*.

America’s Future: Not Terror-Free, but Fear-Free?

Broadly speaking, from among many possible futures civilized societies face, two may best bound the range of outcomes: England and Israel. Despite security intrusions due to a 30-year terror campaign by the IRA, the English manage to live day-to-day much as they did before, enduring sporadic terrorist acts. England is not free from terror, but fear does not rule their daily lives. Israelis are not so fortunate. Palestinian suicide bombers have made Israel a garrison state under constant siege. Israeli life has been radically disrupted, with security becoming an overwhelming pre-occupation of the entire target population.

America can wind up on the English end of the continuum (and Israel can as well). By deploying ubiquitous, networked information technology the US can take positive steps towards reaching England’s near normalcy. We cannot totally eradicate terrorism in all its forms. But if we destroy the most dangerous actors and contain the rest, we can live free and prosperous lives, with fears of terrorist attacks once again reduced to a probability we regard as remote. Such a collective societal sense of security is vital to sustain our essential liberties.

Information technology has a vital role to play in enhancing homeland security, while minimizing loss of liberty. A “surveillance society” must be safe—and free.

- ¹ Aron, Raymond, *On War*, p. 59 (W. W. Norton & Co. 1958).
- ² The Power of Millimeter Waves, *The Huber Mills Power Report*, p. 3, Vol. 2, Issue 11 (Nov. 2001).
- ³ Tom Ridge, on High Alert, *Washington Post*, p. C1 (Nov. 12, 2001).
- ⁴ The Real Border Problem, *New York Post*, Dec. 26, 2001. Crossings traverse choke points: nearly 70 percent of traffic and over 80 percent of the value of goods transshipped between the US and Canada pass through just 6 points. US and Canada: An Efficient, Secure and Smart Border, Office of Homeland Security, Dec. 12, 2001. < <http://www.whitehouse.gov/news/releases/2001/12/20011212-6.html> >
- ⁵ In the Matter of Implementation of Section 6002(b) of the Omnibus Reconciliation Act of 1993: Annual Report and Analysis of Competitive Market Conditions With respect to Commercial Mobile Services, FOURTH REPORT, Federal Communications Commission (adopted June 10, 1999).
- ⁶ Carr, David, The Futility of 'Homeland Defense', *Atlantic Monthly*, p. 53, (Jan. 2002).
- ⁷ Port of Entry Now Means Port of Anxiety, *New York Times*, p. B1 (Dec. 23, 2001). The 20-second estimate comes from Stephen F. Flynn, an international shipping expert from the Council of Foreign Relations.
- ⁸ How the Armada of Terror Menaces Britain, *Guardian Unlimited*, Dec. 23, 2001. < <http://www.observer.co.uk/waronterrorism/story/0,1373,624278,00.html> >
- ⁹ Hunt for 20 Terror Shops, *Guardian Unlimited*, Dec. 23, 2001. < <http://www.observer.co.uk/international/story/0,6903,624196,00.html> >
- ¹⁰ Carr, David, The Futility of 'Homeland Defense', *Atlantic Monthly*, p. 53, (Jan. 2002).
- ¹¹ <http://www.uscg.mil>
- ¹² *Id.*, p. 1.
- ¹³ Silicon Security, Killer Apps and the Coming Boom, *Gilder/Forbes Telecom V*, Nov. 5, 2001. Huber wrote on this in the Nov. 10 *Forbes*. < http://www.manhattan-institute.org/html/_forbes-the_next.htm >
- ¹⁴ Forbes, Steve, Fact and Comment: Better Security, Faster Security, *Forbes*, p. 28, Dec. 10, 2001. Ancore's technology and three products are described at the company website.
- ¹⁵ Bar Codes on a Chip: Technology Could Transform Product Tracking, *Internet Week*, Nov. 19, 2001.
- ¹⁶ Stikeman, Alexandra, Recognizing the Enemy, *Technology Review*, pp. 48-49, Dec. 2001.
- ¹⁷ Applied Digital Solutions Introduces Verichip, a Miniaturized, Implantable Identification Device With a Variety of Medical, Security and Emergency Applications, *Yahoo Finance*, Dec. 19, 2001, 8:06 AM EST. < http://biz.yahoo.com/bw/011219/190064_1.html >
- ¹⁸ Hoogan, Kevin, Will Spyware Work?, *Technology Review*, pp. 44-45, Dec. 2001.
- ¹⁹ *Id.*, p. 47.
- ²⁰ Talbot, David, Detecting Bioterrorism, *Technology Review*, p. 36 (Dec. 2001). The military used this system to detect a flu outbreak in the vicinity of President Bush's inauguration.
- ²¹ *Id.*, pp. 40-41.
- ²² Ridge Plans Health-Data Network To Defend Against Bioterrorism, *Wall Street Journal*, p. A4 (Nov. 28, 2001).

²³ Suddenly, Uncle Sam Wants to Bankroll You, New York Times, sec. 3, p. 1, Dec. 30, 2001.

²⁴ Huber, Peter, The Vision Thing, Forbes, p. 125 (Jan. 2, 2002).

²⁵ Figure 100 times rated DSL/cable speeds, and more like 300 to 400 times actual online high-speed access transfer rates achieved in today's real-world Internet.

²⁶ Woolsey, R. James, Keep Terror Trials Fair, Wall Street Journal, Dec. 21, 2001.

< <http://www.opinionjournal.com/editorial/feature.html?id=95001632> >

²⁷ A few examples of action by prior Presidents: Lincoln suspended habeas corpus during the Civil War; Wilson jailed war dissenters, including Socialist Presidential candidate Eugene V. Debs; FDR interned 110,000 Japanese-Americans, many of them second generation Americans. Smaller wars have historically not lead to such actions.

²⁸ Neural Networks and National Security, Gilder/Forbes Telecosm V, Nov. 4, 2001.

²⁹ Rehnquist, William H., All the Laws But One: Civil Liberties in Wartime, p. 38 (Alfred A. Knopf 1998). The Chief Justice, a superb storyteller, provides a first-rate survey of American liberty in wartime.

³⁰ Id., p. 73. Vallandigham had been charged with undermining the government's campaign to suppress a rebellion. Could the same charge be sustained today, to protect the campaign against terror? Not likely.

³¹ Digital Images Will Verify Identity of Visitors to US, latimes.com, Jan 2, 2002.

< <http://www.latimes.com/news/nationworld/nation/la-010202secure.story> >

³² As Dave Barry would say: "I am not making this up." Along with other equally exotic species, this protected creature resides exclusively in three caves on the Jollyville Plateau in Travis County, Texas. Greve, Michael S.. National Power, Post 9-11, AEI Federalist Outlook, No. 9, Nov. 2001.

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>