LA-UR- 98-1348

Approved for public release; distribution is unlimited.

Title: The Internet Information Infrastructure: Terroist Tool or Architecture for Information Defense?

CONF-980489--

Author(s): Steve Kadner, Aquila Technologies Group, Albuquerque NM
Elizabeth Turpen, Aquila Technologies
Brian Rees, ESH-1

Submitted to: Eigth Annual International Arms Control Conference, April 3-5, 1998, Albuquerque NM.

Los Alamos
NATIONAL LABORATORY

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

THE INTERNET INFORMATION INFRASTRUCTURE: TERRORIST TOOL OR ARCHITECTURE FOR INFORMATION DEFENSE?

Steve Kadner, Brian Rees and Elizabeth Turpen

Technology defines the positive prospects as well as the dangers that shape our daily lives. As evidenced in the half century after splitting of the atom, any specific technological advance can have peaceful purposes or destructive potential. Under current circumstances, the rapid changes in technology often make clear distinction between potential threat and positive improvement contingent on the ultimate objective for which they are implemented. Moreover, some argue that the rapid evolution (or "revolution") and implementation of information technologies is transforming society itself. Rather than these technologies merely allowing for incremental increases in productivity and augmenting convenience, the transformation they impel makes information the "talisman for a new kind of society, a society in which reason and consensus set the tone rather than raw power and materialism."[1]

Postindustrial society is an information society. Knowledge and innovation are to the postindustrial society as capital and labor were to the industrial society. Assuming this is true, then power is a factor of ones access to knowledge and innovative capacity. Put simply, information becomes the commodity and the means to power, both in hard and soft terms.[2] Although it is not assumed at this point that information superiority will supersede raw material power in all cases, the variables that constitute power are changing. As such, how we think about threats to international security and how we formulate solutions must also shift from industrial to postindustrial or "information age" paradigms.

[1] William J. Martin, *The Global Information Society* (Brookfield, VT: Gower, 1995), 1.

[2] In a classical sense, power has been equated with military or economic might. However, in a more accurate assessment of the components of power, Joseph Nye distinguishes between "hard" (military) and

The Internet, as a culmination of information age technologies and an agent of change, exemplifies this transformation. As with any infrastructure, our dependency upon the so-called global information infrastructure creates vulnerabilities. Moreover, unlike physical infrastructures, the Internet is a multi-use technology. While information technologies, such as the Internet, can be utilized as a tool of terror, these same technologies can facilitate the implementation of solutions to mitigate the threat. In this vein, this paper analyzes the multifaceted nature of the Internet information infrastructure and argues that policymakers should concentrate on the solutions it provides rather than the vulnerabilities it creates. Minimizing risks and realizing possibilities in the information age will require institutional activities that translate, exploit and convert information technologies into positive solutions.

What follows is a discussion of the Internet information infrastructure as it relates to increasing vulnerabilities and positive potential. The following four applications of the Internet will be addressed:

- as the infrastructure for information competence;
- as a terrorist tool;
- as the terrorist's target, and;
- as an architecture for rapid response.

Information Competence

The so-called "information revolution" is rapidly transforming human interactions and transactions, both public and private. This revolution is not a surface or temporary minor transition of the manner in which we conduct our lives. These changes embody an economic upheaval analogous to the industrial revolution in their capacity to transform our lives. According to one view, the Internet is "the new railroad to American life, and,

"soft" (co-optive, ideological) power. See Joseph S. Nye, Jr., in *Bound to Lead: The Changing Nature of American Power* (New York: Basic Books, 1990), 173-201.

like the railroad...(it) will transform first our lives, and then the life of the world. As the railroad created a new network of cities and an urban, industrial society, so this new network that we are laying will replace the urban, industrial world with a new city, a new gathering place for...life: Byte City."[3] Byte City is not a location, but rather a metaphor for a change that is wholly immaterial. More importantly, it is not the technology that is important, except in its role as the agent of change. It is how technology changes us that matters.

As processing power doubles annually and product cycles are now measured in months, no reversal or even deceleration in the forward pace of technological advances appears likely.[4] Today one cannot assume to clearly decipher precisely how this revolution will change society. However, certain trends in the transformation can be delineated which should be taken into account in how we view global security threats and what means we use to implement a response. Ultimately, the Internet, the dimension of "Byte City," will bring about societal changes, assumed to largely have positive consequences. In short, Byte City's implications for the economy and our personal lives include the following: 1) time and distance play no role in transactions nor do they present barriers; 2) the marketplace will stipulate new standards of value; and 3) the global marketplace will compel openness and transparency in transactions.[5] Each of these will be discussed in turn.

Geopolitical boundaries become anachronistic in Byte City. This dissolution of barriers in our world is happening now. Transactions in real-time from laptop to laptop or ATM to your bank account are already a reality. Rather than the rhythms of the

[3] Michael Vlahos, "The War after Byte City," in: *The Information Revolution and National Security*, ed. Stuart J.D. Schwartzstein (Washington, DC: Center for Strategic and International Studies, 1996), 91. According to Vlahos, this is referred to as "the Infosphere" in industrial lingo; "the global information infrastructure" is an additional term used for the railroad of this information revolution.

[4] For instance, in 1967, the average time span between initial discovery of a technological innovation and its commercialization decreased from 30 years between 1880 and 1919. It was only 16 years from 1919 to 1945, and 9 years from 1945 to 1967. Product cycles for advances technologies, such as computers and software, are usually less than a year. Francis Fukuyama, *The End of History and the Last Man* (New York: The Free Press, 1992), 91-92.

[5] Vlahos, "Byte City," 91-96.

manufacturing society, the information society's "commuting" needs will be served via the net. Byte City allows entities the capability to consume, communicate and collaborate in a borderless world. Information technologies and global communications networks expand personal and commercial freedom through the expanded choices and enhanced possibilities they create. The democratization effect of the Internet entails a fundamental shift in power relations, conferring power to individuals in their access to the commodity of information. Whereas late industrial society was largely characterized by top-down hierarchies that controlled information, the systemic change already underway implies a decentralization of information and, therefore, decision making power.

Businesses, as well as private parties, that are adept in their exploitation of the information infrastructure can greatly enhance organization and communication capabilities. In fact, in the information age, survival will be contingent on maximizing exploitation of these technologies to realize economic objectives. New standards of value created by Byte City's marketplace will be defined by those who lead in the acquisition of information, are adept in turning information into knowledge and are innovative in applying it to solving problems or satiating persistent material, entertainment or lifestyle demands.

The last definitive implication is the force towards greater transparency. The impact of global information flows with unattended access is assumed to create an emphasis on openness, at least in increasing "information-intensive exchanges in social political, economic and cultural life."[6] Democratization compels transparency in that control of the most sought-after commodity is no longer regulated or controlled by the dominant power structures. While this constitutes a threat to the status quo, demands for transparency will elevate society to a new ethos in their interactions.[7]

[6] Vlahos, "Byte City," 93.

[7] According to Vlahos, individuals as well as businesses will profit more through truth and openness in the information age, and the risks of deceit will become too great. In this manner Byte City embodies a radically different society than late industrial civilization. Earlier societies, even those that called themselves democratic "encouraged a kind of human tyranny built into (their) very social architecture. A

The Internet is rapidly becoming the backbone of information competence in this new age, and it personifies the myriad threats as well as positive consequences of technological change. Access to information in post-industrial societies will unravel the hierarchical structures of industrial society and bestow power to individuals. In any age, power has destructive, productive and integrative dimensions.[8] Whereas immense possibilities for the productive use of information power exist, it is the destructive and negative integrative dimensions to which the discussion now turns.

Terrorist Tool

A fundamental shift in power relations results from the rapid evolution of access to information. The information age, as embodied in the Internet, amplifies the individual's capacity for destruction. This transformation in the power relationship has three dimensions: 1) worldwide connectivity enables an individual, or small group, to distribute a message to an international audience on a broad scale; 2) interconnectivity and reliance on remotely controlled infrastructure systems allows persons to achieve access to realms of information that were previously controlled by large corporations or the state; and 3) the Internet also opens the possibility for individuals, assuming a sufficient degree of know-how and coordination, to exploit the vulnerabilities of the system and wreak havoc through disruption of critical systems. While the third dimension will be handled in the next section, the first two point to the very real possibility that "terrorists" will leverage information technology in the same way that a corporation or a technologically sophisticated armed forces might.

While this explosion of information technologies has enabled the attainment of more efficiency and bestowed greater power to almost every aspect of life, it creates ever more complex security problems as well. Just as the Internet is the railroad of the

world of tightly refined, top-down hierarchies specialized in controlling information; and information-control equaled people-control." Ibid., 95.

[8] Kenneth E. Boulding, *Three Faces of Power* (London: Sage, 1989).

information age for legitimate purposes, it creates an additional tool for undetected communication, coordination and consummation of destructive acts, both physical and cyber.[9] The ability for the ill-motivated Internet user to wield these instruments for achieving large-scale destruction is one side of the coin; the other side is the potential for "customized propaganda" to multiply the range and number of actors that pose a potential threat. In other words, Byte City is potentially also a digitized conference room for visionaries of the Aum Shinrikyo bend.[10] Similarly, it confers on the believers the capability to influence and (mis)inform persons in real-time and across borders.

The fundamental shift in the relationship between the state and individuals is a direct consequence of the information age. Individuals, or small groups, can leverage this power through their own exploitation of communications and information technology. The peaceful or violent use depends on the objectives of the individual user. This multi-use potential of the access to information and communication capabilities can greatly enhance the terrorist's power. The terrorist's use of cyberspace opens up unparalleled opportunities for recruitment efforts, as well as the capacity to formulate, coordinate, and inflict severe damage. While the myriad avenues for manipulation of this information infrastructure are, as yet, unknown, they encompass the potential vulnerability of any information system that is a part of it or can be accessed through it. Increased democratization, increased power, "affords the opportunity for willful, hostile actors,

[9] Others distinguish between the "virtual world" and the "physical world" in discussing future terrorist attacks. The physical world is "matter and energy...that place in which we live and function," while the "virtual world is symbolic - true, false, binary, metaphoric respresentations of information - that place in which computer programs function and data moves." See Barry C. Collin, "The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge," *11th Annual International Symposium on Criminal ustice Issues Proceedings*, March 27, 1997, http//: www.acsp.uic.edu/O1CJ/CONFS/terror02.html. The metaphor of Byte City, however, implies a convergence of these worlds in that cyberspace is the new market and meeting place.

[10] According to one source, the Aum is, indeed, active on the net through exploitation of on-line forums and bulletin board messages. One forum, "Chemistry Square," featured discussions lasting several days on the chemical structure of sarin. On one particular computer bulletin board there have been "many messages supporting Aum, almost trying to woo the reader to Aum's side." In other instances, cyberspace has become a new front for promoting fundamentalist causes and urging illicite activities. See "Cults and the New Information Society," *The Asia Lutheran*, http://www.jlh.org/asia-lut/june 95/sarin.html.

perhaps standing behind the experimenters, to watch, learn and manipulate."[11] Manipulation in the form of so-called cyberwarfare is the third dimension of this power shift to which the discussion now turns.

Terrorist Target

Second only to the threat of weapons of mass destruction is that of information warfare or so-called cyberterrorism. Warfare in the information age implies additional transformations in the "nature of weapons systems and their targets."[12] Information technology is radically transforming the tactics and potential capabilities for warfare. For example, the application of these technologies for military purposes can provide higher resolution sensors and augment signal or image processing. They can greatly enhance the accuracy of hitting a target, as well as offering myriad possibilities for conflict simulations and virtual reality training functions.[13] Lastly, the military increasingly relies on embedded information systems for all of its so-called C^4I (command, control, communications, computers and intelligence) capabilities.[14] Some analysts already envision "information dominance" and, eventually, "battle omniscience."[15]

Again, however, the changes in military technology brought about through the application of new instruments is less important than the fundamental shift in the nature of conflict. In pursuing the analogy of the Internet today as the railroad of 1870, there is, in fact, good reason to question the military's status quo fixation on industrial age threats

[11] Testimony of Senator Jon Kyl, Chairman, before the Senate Judiciary Committee Technology, Terrorism And Government Information Subcommittee hearing on "Critical Infrastructure Protection," Federal News Service LEXIS/NEXIS (5. November 1997).

[12] John Arquilla and David Ronfeldt, "Information, Power, and Grand Strategy: In Athena's Camp," in: *The Information Revolution and National Security*, 146.

[13] Goodman, S.E., "War, information technologies, and international asymmetries," *Communications of the ACM*, Vol. 39, No. 12 (December 1996): 11.

[14] Jeffrey R. Cooper, "Another View of Information Warfare: Conflict in the Information Age," in: *The Information Revolution and National Security*, Stuart J.D. Schwartzstein, ed. (Washington, D.C.: Center for Strategic and International Studies), 121.

[15] According to Goodman, "IT is central to the war-fighting futures sought by both the big platform advocates, who favor such weapons as tanks, submarines, and bombers, and more radical thinkers who foresee, for example, a battlefield covered with many small, smart, sensors operating under an integrated battle management system that summons brilliant weapons from long distances to surgically destroy their targets." See Goodman, "War, information technologies."

in an information age.[16] Conflict in the information age may entail a transition from utilizing material weapons (ships, tanks, guns) to attack material targets toward using Internet capabilities to attack cyber targets to effect, in metaphorical terms, a black out in Byte City. For instance, increasing concern is being focused on the possibility of destructive acts focused on crippling any number of network grids. Our increasing reliance on the Internet presumably makes these threats all the more menacing.

From the standpoint of international security, the post-Cold War information age is characterized by the increasing confluence of military and civilian, public and private, technological means. This gives rise to a convergence of threats and diffusion of responsibility in mitigating such threats. In recent Senate hearings, the U.S. Deputy Secretary of Defense commented:

> *Our knowledge of the origin of such attacks, and their sponsorship, is likely to be imprecise. State, local and Federal authorities, as well as industry personnel and the general public, are each likely to have only part of the picture. In this context, the boundary between national security and law enforcement is blurred, as is the border between public and private sector responsibility.*[17]

While this statement sounds similar to many descriptions of the difficulties in dealing with the increasing risk of a physical threat to civilians through a terrorist act, the speaker is specifically addressing the problem of cyberterrorism. Neither the potential threats nor

[16] The analogy between the U.S. on the brink of Byte City and France in the industrial revolution is the premise upon which Vlahos' bases his thesis. Namely, France lost in 1871, because it concentrated its efforts on war technologies and combat experience rather than real revolution in warmaking embodied in the railroad. While the French achieved a revolution in weapons modernization (breech-loading rifle, chassepot and needle gun, the "Big Change" in daily life - the railroad as "the tool of Europe's transformation" - created industrial war. Namely, the railroad made "war by mobilization, war by train timetable" a possibility.

[17] Statement by the Honorable John J. Hamre, Deputy Secretary of Defense, before the *Senate Judiciary Committee Technology, Terrorism and Government Information Subcommittee*. Hearings on "The Nation at Risk: Report of the President's Commission on Critical Infrastructure Protection" Federal News Service, LEXIS/NEXIS (5 November 1997).

the solutions can be dealt with in isolation due to the intricate web of risks created by advances in technology in conjunction with the blurring of lines between international and domestic, federal and local, public and private sector responsibilities and capabilities. In the information age, this negative potential not only makes distinction between criminal, terrorist, and warlike acts difficult, but it creates responsibilities for entities formerly not involved in coordinating strategies for national security.[18] Moreover, the increasing participation of new actors "shifts the locus from the battlefield and the level of conflict to the strategic plane..." Information age conflict is "part of a dramatic redefinition of the notion of the boundaries of our national security domain in the post-cold war world."[19]

Terrorism: Physical and Cyber Threats

In response to Presidential Decision Directive 39, the Attorney General established a committee to review the vulnerability to terrorism of U.S. government facilities and the U.S. infrastructure. The Critical Infrastructure Working Group, comprised of representatives from the Department of Defense and the intelligence community, identified the following eight critical infrastructures: telecommunications, transportation, emergency services, banking and finance, electrical power systems, water supply systems, gas/oil storage and transportation, and continuity of government. Moreover, the group designated two categories of threat to these infrastructures: physical and cyber.[20]

As computers have become a basic and essential element of every aspect of our infrastructure, the integration of these technologies into society gives rise to cyberterrorist

[18] For instance, unilateral government action cannot assume to address the myriad dangers that arise from this decentralization of power. The information age gives rise to the need for involvement on the part of civil agencies, such as the Department of Justice, Department of Commerce, the Federal Communications Commission, among others. The proliferation of players in cyberspace is by no means limited to state actors. "...the U.S. military has already begun to encounter many of these new players," such as international organizations, NGOs, special interest organization, etc. Cooper, 121.

[19] See Cooper, "Information Warfare," 121.

[20] Louis J. Freeh, Director, Federal Bureau of Investigation before the Senate Appropriations Committee Hearing on Counterterrorism FDCH LEXIS/NEXIS (May 13,1997).

threats to that infrastructure.[21] For instance, the Internet allows transmission of an e-mail message or a computer virus that can, if opened and thereby executed, cause damage to an entire network system. The perpetrator can achieve this objectives from thousands of miles away, across international borders, and, at present, enjoy a high probability of impunity. Deterring or responding to such threats will require collaboration between and among formerly compartmentalized agencies and necessitate increasing cooperation between the international, domestic, corporate and government actors.[22]

In sum, the threat of information warfare or cyberterrorism is commonly perceived as being roughly proportionate to our own increasing dependence on computers and the networks that connect them. This is, however, an inaccurate assessment of the vulnerabilities created by Internet infrastructure. Here the analogy of the Internet as the railroad to the information age breaks down. Unlike the railroad infrastructure, which renders a train wholly reliant on a particular set of physical tracks to arrive at its destination, the Internet is a system of systems. Internet connectivity relies on underlying physical telecommunications facilities. "The Internet can overlay anything from satellite to cable to wireless to dial-the-regular-public-switch network-based lines, anything. It is a hostile overlay network in that it is indifferent to whatever the networks below it are."[23]

Due to the distributed nature of the myriad networks which comprise the Internet, in conjunction with individual, redundant "safety features," only small portions of specific intranets could be vulnerable for short (less than an hour) periods of time. In order for a hostile entity to cause severe damage to the Internet, they would have to make a substantial investment and have considerable expertise. Moreover, the business applications of the Internet lead to financially driven incentives that surpass governmental

[21] Collin defines three potential acts of cyberterrorism: 1) Destruction; 2) Alteration; and 3) Acquisition and retransmission. He also outlines specific instances via such acts as a means to realize terrorist obectives of inflicting damage or causing disruption or destabilization. See Collin, "Cyberterrorism," 3-4.

[22] Comments of Senator Bart Gordon before the Technology Subcommittee of the House Science Committee hearing on Computer Security, FDCH Transcripts LEXIS/NEXIS (6 November 1997).

[23] Brian Kahin, "Thinking about the Information Infrastructure," in: *Information Revolution*, 11.

imperatives for reliability. In short, the Internet's nature and economic imperatives for its robustness mitigate against the damage that could be achieved by cyberterrorism.

However, there already appears to be a threat from sophisticated hackers. For instance, as recent as last month while the U.S. was preparing to mount an attack on Iraq, hackers achieved an electronic assault on 11 U.S. military computer systems. In this instance, there was no evidence that might suggest the intrusions were aimed at disrupting Gulf deployments and no breach in security of classified information occurred. According to one official, the invasion had "the quality of voyeurism or vandalism" and "all the appearances of a game."[24] This is not an uncommon occurrence. To date the objective of hackers appears to be limited to achieving unauthorized access to these systems. This same vulnerability, however, if exploited by coordinated by sophisticated cyberterrorists makes disruption or confusion through a strategic assault on critical systems a possibility.

"Combine our increasing vulnerability, with the explosive increases in the level of violence, and increasing expertise available inside terrorist organizations...(then one) can see that at the point where the physical and virtual worlds converge, the old models of managing terrorism are obsolete."[25] Increasing dependency on the information infrastructure for key aspects of our economy, military competence and personal interactions, including those upon which our lifestyles and survival depend, also creates a highly lucrative target. A well-executed cyberterrorist attack on our critical national information systems presents a risk of the compromise, loss, exploitation, manipulation or denial of the information they carry. The threat of cyberterrorist attacks to strategic information blurs the distinction between government and private sector systems. This interconnectivity greatly complicates the challenges in detecting an information attack

[24] Deputy Defense Secretary John J. Hamre cited by Bradley Graham, in the article "11 U.S. Military Computer Systems Breached by Hackers This Month," *Washington Post*, February 26, 1998, A1.
[25] Collin, "Cyberterrorism," 6.

and in developing defenses against it.[26] As in the case of physical terrorism, it is only through the leveraging of information age technologies and the formulation and implementation of coordination among entities involved that these threats can be effectively addressed.

Real-Time Information and Rapid Response

Parallels to the physical threat of weapons of mass destruction (WMD) surface again in the discussion of solutions to cyberterrorism. However, rather than perceiving these issues as distinct, a more holistic approach would serve to identify the overlap between threats, both physical and virtual, as well as point to possible solutions provided by the technology. A simplified version of policy issues involved in combating terrorism includes the following:

- coordinating various members of response communities in order to integrate the analysis and differentiate between types of potential threats;

- whether response is required by a Federal, local or private sector entity, a critical weakness in current readiness is the capacity to collect and compare information from a variety of sources in order to accurately comprehend its implications;

- more fundamental is the challenge of collecting important information itself, a task that will heavily rely on information sharing between international and domestic, public and private actors. [27]

[26] Testimony of Senator Jon Kyl, Chairman, before the Senate Judiciary Committee Technology, Terrorism And Government Information Subcommittee hearing on "Critical Infrastructure Protection," Federal News Service LEXIS/NEXIS (5. November 1997).

[27] Statement by the Honorable John J. Hamre, Deputy Secretary of Defense, before the Senate Judiciary Committtee "Technology, Terrorism and Government Information Subcommittee." Hearings on "The Nation at Risk: Report of the President's Commission on Critical Infrastructure Protection" Federal News Service, LEXIS/NEXIS (5 November 1997).

It is precisely these activities - collecting, comparing and sharing information - that are greatly facilitated by the existent Internet architecture. Seamless coordination, barring human error, and real-time collaboration are a possibility now. Deterring the threat posed by the Internet, whether as a terrorist tool or target, is contingent on the ability of domestic and international agencies to stay ahead on the learning curve and translate technological advances into solutions. Any strategy to counter the terrorist threat should capitalize on the technological advances in implementing a well-organized and integrated information defense program. While response capability demands achieving clear lines of responsibility among agencies, the efficiency and effectiveness of response can be greatly enhanced through reliance on the Internet infrastructure in devising cost-effective, reliable solutions to information and communication needs.

Response: High-Tech Preparedness

Internet-based applications also provide first-best solutions in coordinating timely and effective responses to physical terrorist threats. Civil defense must be based foremost on timely and accurate information coordination. The Internet architecture provides a foundation for combating terrorism through real-time information collection, exchange, analysis and rapid response. The proper exploitation of the Internet can minimize the probability of success and enhance the response time in the event that an attack occurs.

Example: Radnet

Radnet was designed as a means to monitor radiation detection instruments from a remote location. Radiation detection instruments are placed at various locations in a facility, and readings are needed at various intervals to satisfy operational, regulatory, and safety issues. The Radnet system allows its users the ability to monitor instruments in real-time and make a variety of notifications in the event of an abnormal situation, as well as allowing some capacity for remote control. The key to computerized reporting and data analysis are actualized by the computer's capability to receive data from a wide variety of instruments and to incorporate it into a database with minimal operator action.

Radnet creators conceived of using the Internet to communicate with radiation detection instruments to achieve the following:

- a standard communication protocol that gives manufacturers and users maximal flexibility;
- a flexible protocol to exploit the full use of an instrument's multiple functions but does not burden the computer systems when simpler instruments are used;
- allowing any computer to obtain data from the detection instrument without knowing anything about the instrument, and;
- utility and reliability of the system.

Radnet's implementation at the Los Alamos National Laboratory Plutonium Facility has met these objectives. The Eberline personal contamination monitors (PCM-2s) communicate across an Ethernet Intranet. Personnel can remotely monitor PCM operations through any computer connected to the network and be alerted to problems by messages sent to computers or sent to one or more pagers. Information sent via Radnet communicates through simple e-mail or 80-digit pager messages who used which instrument, what levels the instrument measured, and whether the instrument was working properly. The information gathered is also stored in a database for future use.

Before discussing additional possibilities for implementing a Radnet information structure, several additional advantages of this system should be mentioned. The benefits of Radnet include:

- The Radnet protocol does not require buying another computer, program, or system, and Radnet functions on a variety of platforms (UNIX or IBM).
- The network architecture at an existing location is sufficient. No additional cabling is needed.
- Off-the-shelf hardware can be used to implement the system.
- New and existing instruments can be readily networked.
- Radnet allows any computer to monitor instruments.

- Security can be implemented at several levels. The server can encrypt, select individual computers or subnets to broadcast to and/or require passwords.
- Standard, commercially available wireless networking equipment can be used to communicate, eliminating the need for wiring between instruments and computers.

If one understands the potential applications of Radnet, the immediate possibilities extend far beyond meeting regulatory requirements and increasing efficiency of instrument monitoring for radiation detection devices. Radnet offers one example of the type of systems that could be installed in a subway or ventilation system linked with detection devices to provide real-time information to officials (response agencies) via computer or pager. Information structure systems using a Radnet-type approach would enhance coordination and facilitate efficient and timely response to detected problems.

Radnet detection and response possibilities illustrate that the conversion of information technology into concrete solutions is the first-best approach to mitigating the terrorist threat. While advances in detection instrumentation would be required that eliminate “noise” (false alarms), it is important for persons involved in policy-making and response team coordination to understand the solutions based on exploitation of the Internet. Information technologies should be leveraged at every level to exploit their positive applications. The Internet information architecture allows for enhanced coordination among entities involved in evaluation and analysis of information regarding potential threats. It can also serve as the infrastructure for achieving rapid response in crisis or consequence management of a terrorist attack.

Conclusions

The ultimate form of the information society is still nebulous. Whether Byte City will be a reality for a substantial percentage of the global population is unknown. However, the Internet as the infrastructure for information competence is indisputable. The multifaceted nature of Internet uses, as well as the changes in society it exemplifies, requires careful analysis of the negative and positive potentialities and leveraging technology to reduce the vulnerabilities our dependency creates. Minimizing risks and realizing possibilities in the information age requires first understanding the implications of the decentralization of power, and then taking steps to translate, exploit and convert information technologies into solutions that address the possible threats.