

MANAGING THE UNBOUNDED RISK: INFORMATION TECHNOLOGY & HOMELAND SECURITY

Briefing Book

©Copyright 2003, by GSPP/BRIE

A Note About our Sponsors:

ITHS is a joint project of the Goldman School of Public Policy (**GSPP**), the Berkeley Roundtable on the International Economy (**BRIE**), and the **School of Journalism**. “**Managing the Unbounded Risk: Information Technology and Homeland Security**” is the inaugural event of ITHS, and is underwritten by the **Lawrence Livermore National Laboratory** in a grant to the BRIE, with additional funding from the **Larry L. Hillblom Foundation** and the Institute of Governmental Studies (**IGS**) at UC Berkeley. ITHS was founded with a generous grant from John Gage and Linda Schacht to GSPP and the UC Berkeley School of Journalism. Administrative support for the conference is provided by BRIE, the **Haas School of Business**, and GSPP.

Conference Briefing Book

**MANAGING THE UNBOUNDED RISK:
INFORMATION TECHNOLOGY & HOMELAND SECURITY***

September 2003

©Copyright 2003, by GSPP/BRIE

The transition from the Cold War to the War on Terror paints a stark contrast as the primary security risk we now face is poorly understood and appears to be largely out of our control. It would not be an exaggeration to call the risk unbounded, as a terrorist could strike an infinite number of targets with an infinite array of attacks, many of which remain completely unimaginable until actually executed. The attacks of September 11th demonstrated the ability of terrorists to use our advanced technologies and openness against us, so although the terrorist threat to homeland security is immense, our labors will be focused on the highly important issue areas existing in the nexus between homeland security and information technology. Thus, in discussing the terrorist threat in session one, our special attention will be devoted to the threat of cyber terrorism. While there exists innumerable domestic targets vulnerable to a terrorist attack, protecting our nation's critical infrastructures (water, power, transportation, communication, etc.) is an obvious priority. Protecting every potential target is simply impossible, and formulating a meaningful defensive strategy requires a more sophisticated understanding of the risk at hand. This is the task of session two as we consider the political economy of risk assessment and mitigation as it relates to homeland security. Sessions three and four will be devoted to case studies of critical infrastructures. These two cases share an underlying logic and suggest, first, that individual solutions will not suffice absent system wide rules and, second, that effective homeland security begins far beyond the confines of U.S. borders raising questions as to the degree to which the U.S. is able to assure its own security without international cooperation. Session three will explore these problems and others in regard to financial cyber security while session four will look at protecting our nation's ports. A single-minded focus on these issues and a reallocation of resources are likely to go far in enabling the U.S. to combat the terrorist threat, yet we must be careful to maintain a balanced perspective and consider the unintended consequences that result from efforts

* Prepared by Matthew Kroenig for "Managing the Unbounded Risk: Information Technology and Homeland Security," a GSPP-BRIE conference, Sept. 18-19, 2003."

intended to improve homeland security. In session five, we will study the implications of homeland security for privacy, civil liberties, and for security itself.

PROPOSITION ONE- The Threat of Cyberterrorism is real, although widely misunderstood. While the threat posed by cyber terrorism is real, the most dire predictions of an “electronic Pearl Harbor” are likely exaggerated. We must not, however, be blinded by studying the effects of cyber terrorism in isolation. A cyber attack would be most devastating in combination with a complimentary physical attack. But perhaps the greatest danger presented to homeland security by information technologies is not their capacity to be manipulated in a cyber attack against critical infrastructures, but the network type of organization that they facilitate and the difficulty hierarchically organized states face in their interactions with networked terrorist organizations.

PROPOSITION TWO- The distribution of risk is uneven, thus the response becomes a political choice. In the new era of terrorist threats to homeland security, certain zones of the country and types of targets are more likely to be selected for terrorist strikes. This asymmetry of security need makes homeland security a case of redistributive politics. Political representatives may be unwilling to vote for increases in spending for security that disproportionately aids constituents in other districts. When assessments of risk have such important political ramifications, the tools used to assess risk will themselves become the object of political debate.

PROPOSITION THREE- Financial Cyber security is a collective action problem. Financial cyber security is complicated by interdependent risk. The risk of a catastrophic event faced by one firm is determined in part by the behavior of others. Thus each firm will be unwilling to devote adequate resources to increased security, unless it is guaranteed that other firms will do likewise. A number of possible solutions, both private and public, exist to solve this coordination problem, including industry collaboration, government regulation, and standard setting through the creation of insurance markets.

PROPOSITION FOUR- Port Security is not about protecting the port. Of far greater consequence than economic or military loss due to the destruction of a port is the prospect of a dangerous container passing unnoticed through the port security system delivering a major WMD attack to an American city. Thus, port security is not principally about protecting the port itself, but about deploying promising new technologies to improve supply chain management and creating a point at which

dangerous containers are identified and interdicted before they can bring serious damage.

PROPOSITION FIVE- The protection of privacy and civil liberties is not an obstacle to securing the homeland, but its prerequisite. It would obviously be an absurd consequence to have to destroy our society in order to save it. Yet, the protection of civil liberties is not only valuable in its own right, but is essential in the enterprise of security provision itself. The cooperation of the average citizen will be necessary for the effective implementation of new policies and technologies intended to bolster our civil defenses. If citizens feel that their basic rights are being disregarded, they will likely resist government efforts, slowing defensive measures and rendering our society more vulnerable to attack.

The Propositions Elaborated

PROPOSITION ONE-

The Threat of Cyberterrorism is real, although widely misunderstood.

Over the past decade the operation of a vast array of the United States' civil and military infrastructure has become dependent on information technology. The gains in terms of both efficiency and cost are overwhelming, yet these benefits come at the expense of increased vulnerability. Technologies such as the internet were not designed with security in mind and both state and non-state actors hostile to the United States have begun to develop the tools and expertise that will allow them to exploit the Achilles' heel in the dominant power. The number of reported hackings has increased exponentially in recent years. The Department of Defense alone faced 40,000 attempted hacks in 2001.¹ While we must be careful not to underestimate the disruption that such actions can generate, we should note that these attacks rarely result in severe breaches of national security and the source is often not hostile political forces, but bored teenagers.

More threatening to US national security is Cyberterrorism. Cyberterrorism is distinct from mere hacking as it is the politically motivated use of computer systems to inflict large scale physical and/ or economic destruction. Imagined Cyberterror attacks include electronically hijacking an air traffic control system causing the collision of large commercial airliners, shutting down the information technology-dependent financial markets grinding the economy to a halt, or hacking into an electric power grid to black out an entire city. The threat of a cyber terror attack on the United States is real and will increase with time as more of our critical infrastructures (transportation, communication, water, power, governmental services, etc.) become dependent on computer systems and as members of terrorist organizations, like populations the world over, become more tech savvy.²

While the threat posed by cyber terrorism is real, it is not so great that it cannot be overstated. The most dire predictions of an "electronic Pearl Harbor" in which a computer attack strikes untold levels of mayhem and destruction across the country completely incapacitating the United States government are likely exaggerated. There are a number of factors that would render a hypothetical cyber attack difficult to execute and less attractive to an adversary than alternative measures. First, our nation's critical infrastructures are composed of sometimes thousands of redundant sub-systems

operating on separate control mechanisms requiring terrorists to simultaneously exploit vulnerabilities in multiple systems to achieve a large-scale effect. For example the US operates on 54,064 separate water systems.³ Second, critical infrastructures are highly resilient systems used to routine failure and capable of rapid recovery. German industrial production actually increased under Allied bombing in World War II. Blacking out large portions of the mid-western and north eastern United States and parts of Canada would be an ambitious goal for a cyber terrorist, yet the 2003 blackout due to system failure resulted in only minor economic losses, and no serious threat to national security. Third, substantial human agency intervenes between cyber attack and the final outcome mitigating against the worst catastrophes. For example, pilots are capable of landing planes even after the computers of an air traffic control system are disabled. Fourth, in spite of real vulnerabilities in our computer systems, terrorists may simply prefer to use other methods. It is doubtful whether cyber attacks provide the kind of shock value that terrorists desire and can more easily achieve through conventional means such as explosions.

We must, however, be cautious not to underestimate the value of cyber terrorism. This is especially dangerous when we examine its effects in isolation . Information warfare is almost always implemented as part of a broader campaign. A cyber attack would be most devastating in combination with a complementary physical attack. For example, using the internet to incapacitate a city's emergency response system would amplify the damage caused by a conventional bombing. Or a nation such as China could electronically disrupt US satellite feeds before invading Taiwan presenting the world with a *fait accompli*. Even when not directly complimentary, cyber warfare could be used as a low-cost diversionary tactic while a damaging physical attack is executed. Given the enormous benefits to such a strategy, an increase in the incidents of information warfare may actually signal an impending physical attack.

Networks Vs. Hierarchies

Perhaps the greatest danger presented to homeland security by information technologies is not their capacity to be manipulated in a cyber attack against critical infrastructures, but the network type of organization that they facilitate and the difficulty hierarchically organized states face in their interactions with networked terrorist organizations. Networks require the capacity for continuous and dense flows of information and communication between geographically dispersed nodes. The information revolution generated a myriad of technologies such as cellular telephones, fax machines, and the internet that greatly strengthened the network form of organization. Hierarchical states have a difficult time in adapting their standard operating procedures to conflicts with networks for a number of reasons. First,

networks are composed of functionally equivalent nodes without a strict chain of command and thus lack a head rendering negotiation difficult and making them invulnerable to decapitation. Second, networks tend to operate in the seams of traditional boundaries and jurisdictions making it difficult for states to assign responsibility for them to a single agency. Third, networks defy traditional principles of conflict in favor of tactics better suited to their strengths such as swarming. Swarming is the coordinated attack on a single point from all directions by small agile forces that may be quickly dispersed and then reassembled for a sustained pulsing attack. Empirically, the efficacy of netwar, “the use of network forms of organization, doctrine, strategy, and technology attuned to the information age”, has been demonstrated not only by Al Qaeda, but also by groups diverse as the Zapatistas, the Serbian opposition, and anti-globalization protestors in Seattle.⁴ It takes a network to fight a network, thus the US effort to improve homeland security may be less about technological fixes and more about organizational realignment.

PROPOSITION TWO-

The distribution of risk is uneven, thus the response becomes a political choice.

During the Cold War the risk of a general nuclear war with the Soviet Union was perceived as the same for inhabitants of Manhattan and Omaha. Every dollar of military spending that went towards expanding, modernizing, and maintaining our nuclear triad protected all Americans equally by ensuring our second strike capability, deterring a Soviet attack. In the new era of terrorist threats to homeland security, certain zones of the country and types of targets are more likely to be selected for terrorist strikes. These sites’ higher value is due to a variety of factors including military and economic importance, symbolic status, or simply because they are known by someone planning an attack on the other side of the world. This asymmetry of security need makes homeland security a case of redistributive politics. Political representatives may be unwilling to vote for increases in a military budget that disproportionately aids constituents in other districts.

When assessments of risk have such important political ramifications, the tools used to assess risk will themselves become the object of political debate. The Terrorism Futures Market has encouraged brilliant arguments both in favor and against and raises many interesting questions about the value of such a tool, including; what is the difference between a market and a bookmaking operation? Does the former require

precisely defined outcomes, which runs counter to the inherent unpredictability of a terrorist attack? Does a market create incentives for terrorism?⁵

A realistic understanding of the risk we confront is required not only by those who make policy, but also by the public at large, if society and the economy are to function smoothly and if the general public is to respond to the demands made upon it for increased vigilance in fighting the terrorist threat. At present the general public's assessment of the risk is exaggerated because they are afraid. Such a response is predicted by the literature on the social construction of risk.⁶ People focus more attention on an event the rarer it is, eg September 11th, and tend to fear human generated dangers, such as terrorism, far more than equivalent natural phenomena. For example, people's concerns about the construction of a nearby nuclear power plant tend to outweigh their concerns about naturally occurring radon creeping into their basement, although the latter is objectively far more dangerous. A simple education campaign is likely insufficient to allay the worst fears. In psychological terms, we must understand that people go to great lengths to avoid, not only risks, but even the worry of risk. In economic terms, risk anticipation itself is a social cost.

The provision of security has long been a defining characteristic of national governments. Change may be underway as security threats are increasingly localized, the responsibility of improving homeland security has begun to fall on state and local authorities. Yet, these governments are in the midst of huge budget shortfalls and are incapable of purchasing expensive technologies that could aid them in the fight against terror. Assistance from the federal government has been requested, but these requests have been met with an obvious reluctance by the federal government to shift funding.

Without effective political leadership in risk mitigation, efforts by private actors to protect their assets may lead to socially sub-optimal outcomes. Since terrorists are thought to substitute away from hardened targets, a sizable increase in security spending by one potential target eg. The Sears Tower, would have the paradoxical result of increasing the risk posed to other similar targets eg. The Empire State Building. This type of incentive structure may propel a security arms race resulting in costly overprotection.

For other types of targets, characterized by interdependent risk, the opposite, but equally undesirable, result of underprotection may occur if private actors engage in uncoordinated self-protection. Security problems are interdependent when a catastrophic risk faced by one firm is determined in part by the behavior of others.⁷ For example, interdependent risk is endemic in the airline industry, where an infallible

screening system is useless when bags are transferred from other airlines that may take less security precautions, and also in computer networks, where a hacker or virus can exploit a single weak link to access and violate the rest of the system. In situations of interdependent risk, firms will be hesitant to increase security spending unless they are assured that all other firms are doing likewise.

Such a coordination problem raises interesting questions of comparative homeland security and how models of risk mitigation may vary across countries. Countries with highly developed institutions for inter-firm coordination, such as Germany, may be better suited to improving homeland security than countries with a more fragmented market economy such as the United States.

PROPOSITION THREE-

Financial Cyber security is primarily a collective action problem.ⁱ

Over the past two decades, information technology has permeated the financial markets to the point that market operations are almost completely dependent upon IT systems. While this technology allows firms and market actors to greatly leverage resources, it also introduces weaknesses into America's "critical" financial markets, which terrorists and hackers have and will seek to exploit. These weaknesses include the communication and technology infrastructure's susceptibility to physical disruption as well as electronic damage done via viruses, denial of service campaigns, or electronic theft.

The early marriage of financial markets with information technology has given this sector a head start in grappling with the problem. In many ways, it may be better prepared and provide examples for industries that are only now awakening to the terrorist threat. Yet, the private and public sector organizations involved in the financial markets have allocated an uneven level of effort and resources towards securing the financial industry from either another physical or a cyber based attack. Financial markets and their computer systems are characterized by the before mentioned problem of interdependent risk, where security shortcomings in one system of operation or firm could disrupt or halt market activities important to the continued functioning of the US economy as a whole.

ⁱ This section written in collaboration with Paul N. Ebner

The incentives toward inadequate security spending typical of industries faced with interdependent risk is further exacerbated by a number of characteristics specific to the financial industry. First, a decentralized market structure makes it difficult to coordinate across firms and enforce a minimum level of security. Second, given the globalized nature of financial markets, a purely domestic solution will not adequately secure the entire network. Rather, substantial international cooperation may be necessary to ensure that coordination transcends state boundaries. Third, the range of firms important to market operations include giant multi-national bank holding companies like Citigroup, investment banks of different sizes such as Goldman Sachs or the smaller Lehman Brothers, to regional clearing banks like Bank of New York, down to the small Inter Dealer Brokers (IDB) like Cantor Fitzgerald. The varying sizes and roles of these firms lead to drastically different security goals, needs, and budgets. Fourth, the inability to quantify the risks of a physical or cyber attack incorporating firms' interdependencies makes it difficult to identify the appropriate level of spending. Fifth, firms are hesitant to reveal their true security levels or breaches for fear of inviting another attack or being punished by investors. Sixth, recent efforts have focused on rapid business recovery following an attack, but technological and financial limitations make the most robust security set ups prohibitively expensive for some firms.

Possible solutions do exist however. A number of broad options for overcoming the security risks of linked systems are visible and include both industry self-regulation and government regulation.⁸ The first, involves collaborative actions by industry itself. A trade association can generate cooperation by demanding that members abide by certain rules and regulations, including the implementation of security measures. Such a solution would only be successful if all networked firms are association members, or if the associated members sever relationships with those firms existing outside of the stipulated regulatory framework. The outline of increased financial industry cooperation may be developing. Several organizations such as the National Association of Securities Dealers (NASD), Financial Services Roundtable, Bond Market Association (BMA) and Securities Industry Association (SIA) exist to help transcend the numerous actors and facilitate coordination. However, in most cases none of these organizations is able to issue specific directives requiring firms to modify their behavior. For instance, the SIA's Business Continuity Practices Committee has compiled a "lessons learned document" and has produced a Best Practices Guideline but none of these recommendations is required.⁹ Achieving increased and sustained collaboration will not be easy and may only be possible under the threat of government intervention.

Government action to achieve improved security is a second possible approach, which could take both direct and indirect forms. The government could legislate and enforce strict industry-wide financial security regulations. Increased security could also be encouraged indirectly through taxes on firms that fail to invest in protection and subsidies for those wishing to take protective measures. The latter option may be less attractive given current political circumstances.

A third possible solution is the assignment of liability for breaches in security and the development of insurance markets to set industry wide security standards.¹⁰ If, in the event of an attack, the party responsible bore some liability for damage to third parties, it would have a strong incentive to make its own networks more secure. At present, liability for computer security is diffuse and must be more clearly assigned to actors that can do the best job of managing risk. Once a party is liable for any damage caused from its own systems, it will then seek to buy insurance against this risk. Insurance is a logical way to encourage security because it rewards those who adopt protective measures by decreasing insurance premiums reflecting a reduced likelihood of attack. Insurance companies also have an incentive to improve the insured's security practices and will likely engage in education on risk management practices and hire third-party inspectors to evaluate the safety and security of those firms seeking coverage.

While attractive for its reliance on market signals and its proven success in other industries, this approach faces some obstacles. First, in practice, determining liability may be difficult. Following a nationwide cyber attack that crashes the financial market's computer systems, discovering the attacker's point of entry and thus the responsible party could be quite difficult. Second, the development of a new domain for insurance coverage will be a long slow process. At present, insurers have yet to develop expertise in risk management for computer security and offer little in the way of protection.

PROPOSITION FOUR-

Port Security is not about protecting the port.ⁱⁱ

Maritime trade is the backbone of global commerce, and shipping containers the very hallmark of this vast, networked, international economy. A full 90% of the world's general cargo moves by container.¹¹ The shipping container has not, however provided

ⁱⁱ This section written in collaboration with Jed Harris.

a secure means of transporting goods. Containers have long aroused the concern of policy officials who see a prime opportunity for WMD terrorism. Coming from halfway around the world, and going through the hands of some twenty to thirty different parties, sea containers are perfectly anonymous terrorist conveyances. A WMD container incident at a port may take fewer lives than, say, a terrorist event at a mall, but the economic toll would be significant. The port itself would be lost, ships would queue up, food, fuel, industrial supplies, consumables, and other imports could not enter the country. Fearing a coordinated attack on other ports, officials would likely close all U.S. ports until confidence in port security procedures had been restored temporarily shutting down the international shipping industry. Ports are also critical infrastructure from a military planning perspective. Major deployments of troops and supplies often depart from U.S. ports on U.S.-flag vessels. The loss of a port near a major base or weapons depot could impact an American military campaign in another part of the world.

Of far greater consequence than economic or military damage is the prospect of a dangerous container passing unnoticed through the port security system delivering a major WMD attack to an American city. Thus, port security is not principally about protecting the port itself, but about improved supply chain management and creating a point at which dangerous containers are identified and interdicted before they can bring serious damage.

The key element in improving supply chain management is of course that much must be done abroad before the container arrives at a U.S. port, indeed before the container is loaded on a ship. This means backing up the major security question to the point at which the container is loaded. To be completely confident that a given container transaction is safe, one must have a range of technical and organizational/procedural information including: the unique supply chain history of all the goods in that container; where it was sealed, by whom, with what lock, and whether it was ever opened after original sealing; and whether anomalous shipping patterns warrant inspection.

A number of promising new technologies exist that would help to ensure security first at the container's point of origin and then verify the integrity of this container throughout its shipment life-to increase the transparency of the supply chain. For example, more sophisticated algorithms could isolate many different patterns of suspicious behavior from the noise of generally normal behavior. To some extent this practice is being done already. The now notorious "2%" of containers that are physically opened up have been targeted ahead of time with this AI capability. Customs

thus claims to inspect much more than 2 % of all *dangerous* containers, although more could be done in this area.

“Smart Containers” with GPS (Global Positioning System) or GLS (Global Locator System) tracking systems would allow the government and/or industry to know the exact location of containers. These smart containers, and the ports themselves, could then be outfitted with other technologies including more numerous, more effective, and less expensive detection technologies. These detectors could passively detect nuclear, biological, or chemical elements and communicate this information to appropriate authorities in real-time. Detection technology is tricky however in that it is an inherent cat and mouse game whose cost structure clearly favors the terrorists. A nuclear bomb could easily avoid radiation detection technologies if enclosed within a lead case. Deploying lead detectors at ports would be a useful response, but only until the next round of terrorist innovation.

Other promising technologies include electronic container seals that communicate real-time information about break ins including the time and place of the violation. Lastly, integrated databases could be used to fuse all manner of export, transportation, and import party information, and merge this data with selected intelligence.

Despite the promise that many of these technologies hold, significant limitations to their real-world effectiveness remain. The primary agencies charged with securing the shipping industry, such as Customs, and the Transportation Security Administration, are notoriously underfunded, and their inadequate resources will limit the rate of technology adoption.

Private actors also lack the resources and proper incentives to self invest in new technology. Government could solve the collective action problem through legislation, but this could be tricky in that mandating a technological standard would raise a number of competitive issues concerning what products, manufactured by which firms, in what countries satisfy the legal requirements.

Another major impediment to technological implementation is the political nature of oversight, funding, and enforcement. Maritime oversight has and will continue to provoke a wide range of jurisdictional competition, as many different agencies-each with different mandates-will seek to impose their own regulatory influence on the problem. Funding for Customs initiatives will also depend on the considerably political federal appropriations process. The majority of Congresspeople who represent non-port,

middle-America districts are unlikely to devote generous funding to container security endeavors.

Despite these serious obstacles to technology implementation, at least some of the costs of improved security can be partially offset by spillover benefits into other arenas. Specifically for shippers, a smart, secure system would likely afford a number of economic benefits including: fewer lost and stolen containers and greater recovery from lost and stolen containers; greater knowledge of whereabouts of cargo; a more visible supply chain in general, facilitating communication between dependent players and improving responsiveness overall; identification of underused containers, underutilized routing capabilities, and hence more efficient logistical arrangements. The value of the increased speed and volume such technologies would afford in this high volume, low margin industry is significant.

Government actors would also receive positive externalities from improved port security. Customs revenues would likely increase as shippers are held to higher declaration standards due to a more accurate and timely reporting of cargo's real value. Container seals and detection technologies might also go far to reduce arms and drug trafficking. As drug and arms traffic are often the stock-in-trade of terrorist organizations, efforts that interdicts this contraband could also aid in the war against terror.

PROPOSITION FIVE-

The protection of privacy and civil liberties is not an obstacle to securing the homeland, but its prerequisite.

Passed in the immediate aftermath of September 11th, the USA Patriot act grants domestic law enforcement and foreign intelligence agencies with sweeping new surveillance powers to use in their fight against the terrorist threat. As an example, the now notorious "sneak and peak" provision allows investigators to enter a home, examine and remove items without immediately, if ever, presenting owners with a warrant detailing what they were authorized to do and where. The imprisonment of "unlawful combatants" in Guantanamo Bay, Cuba and the arrest and detention of Muslim Americans in the wake of September 11th are two other cases where the U.S. government broke with conventional procedures in attempts to more effectively secure the homeland from potential threats.

Critics of this intense new focus on domestic threats fear that these measures undermine the values that underlay our society and serve to erode our civil liberties. According to this view, The Patriot Act not only threatens a citizen's right to privacy, but also the American tradition of open and accountable government. Moreover, there are charges that investigators are overstepping their bounds and that these powers passed specifically to combat terrorism are gradually being applied to all types of domestic investigations including cyber crime.

The defenders of civil liberties have reason for concern. Protecting the homeland requires the maintenance of both privacy and civil liberties. It would obviously be an absurd consequence to have to destroy our society in order to save it. Yet, the protection of civil liberties goes beyond the noble objective of preserving personal freedoms. Maintaining individual rights is essential in the enterprise of security provision itself. The cooperation of the average citizen will be necessary for the effective implementation of new policies and technologies intended to bolster our civil defenses. If citizens feel that their basic rights are being disregarded, they will likely resist government efforts, slowing defensive measures and rendering our society more vulnerable to attack.

As demonstrated by our case studies of port and financial market security, promising new technologies do exist to aid us in our efforts to improve homeland security. Overhauling our critical infrastructures with expensive new technologies obviously entails a gigantic economic cost, but such an overhaul could also be interpreted as an opportunity. The political motivation now exists that will allow us, not only to makeover our critical infrastructures with sophisticated new technologies, but also to embed our values into society through them. For example, if privacy is a top priority, designers can create new systems that build in both privacy and security.

In the campaign to redesign our critical infrastructure, we must be cautious however. Generals are often accused of fighting the last war. Likewise, system designers must be cognizant not to overemphasize contemporary concerns in constructing the critical infrastructure upon which we will rely for decades. The system we design today is unlikely to be the system we wish to use tomorrow.

¹D.A. Fulghum and R. Wall, *Aviation Week and Space Technology*, November 5, 2001, 26.

² For a more detailed discussion of many of the arguments presented in this section see Bruce Berkowitz, *The New Face of War: How War Will Be Fought in the 21st Century*. New York: The Free Press, 2003.; Dorothy E. Denning. "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," in John Arquilla and David Ronfeldt eds., *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Rand, 2001.; Dorothy E. Denning. *Is Cyber Terror Next?* Social Science Research Council, November 2001. Available at http://www.ssrc.org/sept11/essays/denning_text_only.htm; James A. Lewis. *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. Washington DC: Center for Strategic and International Studies, 2002, 4.; Peter Rojas. "Online Security Will Benefit Us All," *The Guardian*, April 23, 2003.

³ James A. Lewis. *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. Washington DC: Center for Strategic and International Studies, 2002, 4.

⁴ See John Arquilla, and David Ronfeldt, eds. *Networks and Netwars: The Future of Terror, Crime and Militancy*. Rand 2001.

⁵ For a defense of the terrorist futures market see Hal R. Varian. "A Good Idea With Bad Press," *New York Times*, July 31, 2003.

⁶Michael O'Hare. *Risk Anticipation as a Social Cost*. Cambridge, MA: Lincoln Institute of Land Policy, 1992.

⁷ See Howard Kunreuther, Geoffrey Heal, and Peter R. Orszag. *Interdependent Security: Implications for Homeland Security Policy and Other Areas*. Washington DC: The Brookings Institution Policy Brief # 108, October 2002. Available at www.brookings.edu

⁸ For a discussion of these solutions applied to the airline industry see Kunreuther, Heal, and Orszag.

⁹ Don Kitell. "Recovery and Renewal: Protecting The Capital Markets Against Terrorism Post 9/11," Testimony before the House Financial Services Committee. February 12, 2003.

¹⁰ Hal R. Varian. "Managing Online Security Risks," *New York Times*, June 29, 2000.

¹¹ Hart-Rudmann Report: "America Still Unprepared; America Still in Danger."