Defense Horizons
Number 59
A publication of the
Center for Technology and National Security Policy
National Defense University
JANUARY 2008

Strategic Fragility: Infrastructure Protection and National Security in the Information Age

by Robert A. Miller and Irving Lachow

Overview

Modern societies have reached unprecedented levels of prosperity, yet they remain vulnerable to a wide range of possible disruptions. One significant reason for this growing vulnerability is the developed world's reliance on an array of interlinked, interdependent critical infrastructures that span nations and even continents. The advent of these infrastructures over the past few decades has resulted in a tradeoff: the United States has gained greater productivity and prosperity at the risk of greater exposure to widespread systemic collapse. The trends that have led to this growing strategic fragility show no sign of slowing. As a result, the United States faces a new and different kind of threat to national security.

This paper explores the factors that are creating the current situation. It examines the implications of strategic fragility for national security and the range of threats that could exploit this condition. Finally, it describes a variety of response strategies that could help address this issue. The challenges associated with strategic fragility are complex and not easily resolved. However, it is evident that policymakers will need to make difficult choices soon; delaying important decisions is itself a choice, and one that could produce disastrous results.

Faustian Bargains

Developed societies around the world face an unexpected paradox: though wealthy beyond the dreams of earlier generations and able to call forth vast resources and project influence across the globe, they face threats and dangers that did not exist a few decades ago. During the past half-century, global integration has accelerated significantly. A growing number of nations and regions have been incorporated into the international economy, which now depends on a set of interconnected critical infrastructures that in many cases extend far beyond national boundaries and are controlled by an increasingly elaborate information grid. Information has become both instantaneous and ubiquitous; it often seems that very little happens anywhere that is not known within a few hours everywhere. In many cases, these critical infrastructures are the keys to our prosperity. We depend on them. But they can break—or be broken.

The development of these linked infrastructures and interdependencies has taken place with astonishing rapidity. They have emerged, seemingly out of nowhere, within the past few decades. The result is revolutionary.

An excellent example of this change is in merchant shipping. For many, the word *seaport* conjures up an image of sailors and longshoremen swarming over cargo-strewn piers, but that world no longer exists. Almost all of the longshoremen are gone, as are most of the merchant sailors. Many once-bustling ports have shrunk, their piers replaced by office buildings, condominiums, entertainment centers, restaurants, parks, and other amenities of the modern city.

The major reason for this transformation has been the advent of containerized shipping.[1] Almost unknown half a century ago, containers are now the primary method for moving finished goods around the world. In a sense, containers have made globalization possible. Not so long ago, the cost of transportation was a significant part of the total cost of any product, which was why so many factories were located near their ultimate customers. Now, the cost of transportation has dropped precipitously and businesses can move their operations far from customers—even across a continent or ocean—and still be competitive with businesses only a few miles from the point of sale.

Within little more than a generation, the old way of handling freight—break-bulk loading of goods stacked on pallets onto small merchant ships by gangs of longshoremen—has become as antiquated

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JAN 2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Defense Horizons. Strategic Fragility: Infrastructure Protection and National Security in the Information Age	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University,Information Resource Management College,Washington,DC,20319**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**6**	

as oxcarts and almost as rare. Approximately 90 percent of the world's trade in non-bulk goods is transported in cargo containers. In the United States, almost half of incoming trade (by value) arrives in containers piled high on very large, specialized ships. Millions of these containers arrive at U.S. seaports each year.[2] To be efficient, though, these new container ships have to operate through large, carefully designed, highly automated, and extremely capital-intensive ports of call.[3] The inevitable result is that a growing percentage of traffic is routed through a few large ports. By 2003, just five U.S. seaports carried 60 percent of America's total container traffic.[4]

Coupled with concomitant improvements in intermodal transportation, end-to-end supply chain operations, and information-based logistics management systems, containerization has brought radical improvements in efficiency. These changes have permitted huge increases in capability and profitability. By putting more eggs into a smaller number of baskets, companies have cut costs across the board. Our just-in-time world hums along more and more efficiently—until one of these baskets breaks or is broken.[5]

Two conspicuous examples of this pattern of concentration and the resulting vulnerability are electric power grids and air traffic control systems. Today's interconnected, continent-wide power grids are much better than their local and regional predecessors at providing cheap and reliable power, and they are significantly less prone to local breakdowns. But when they do crash, the consequences are far greater than those of the more frequent and more localized failures of past decades. Similarly, the highly integrated systems that control air traffic are much safer and more efficient than the disjointed regional systems of half a century ago, but when the system seizes up, the effects are far more immediate and widespread.

Everyday life offers many more examples of growing system dependencies and tight linkages. Consider traffic signals. Ubiquitous, unremarkable, and essential to traffic flow in every city, these signals were once controlled individually by mechanical devices. They were almost impossible to reset quickly in response to changing conditions. Now, traffic signals in an increasing number of locales are operated through centralized traffic-management networks. The result is that traffic management is much more flexible, easy to modify when conditions warrant—and vulnerable to widespread disruption if the system is compromised.[6]

The preceding examples illustrate the situation that we call *strategic fragility*. Without fully realizing it or planning it, modern societies have created a world dominated by fewer, more highly concentrated, more efficient, and more ubiquitous networks. These networks now govern our daily lives. Radical improvements in systems, processes, and operations have stimulated significant increases in global productivity by squeezing slack and redundancy out of systems and improving process effectiveness. However, these changes have also reduced local and regional resilience and diminished spare capacity available in an emergency. In some cases, they have increased exposure to potentially catastrophic failures and runaway system collapses.[7]

Robert A. Miller and Irving Lachow are Senior Research Professors in the Information Resource Management College at the National Defense University. The authors can be reached at millerr@ndu.edu and lachowi@ndu.edu, respectively.

Thus, modern societies have made an unintentional Faustian bargain that brings increases in operational efficiency and capability at the cost of greater susceptibility to widespread catastrophic failures. Most people probably would not want to reverse this bargain even if they could. Whatever doubts one may have about the globalized, interconnected planet of the early 21st century, few among us truly yearn for the slower, less efficient, more expensive world of a few decades ago. However, we must recognize that our society faces new kinds of vulnerabilities and risks. The challenge is to decide how to manage those risks in a cost-effective manner.

Critical Infrastructures

The term *infrastructure* originally referred to physical networks that supported cities and included things such as roads, water and sewer utilities, power cables, and telecommunications lines. The contemporary concept of critical infrastructures goes beyond physical structures to interconnections and functions that enable a society to survive and thrive (see table). The working definition used by the U.S. Government defines *critical infrastructures* as "assets, systems, and networks, whether physical or virtual, so vital to the United States that the incapacity or destruction of such assets, systems, or networks would have a debilitating impact on security, national economic security, public health or safety, or any combination of those matters."[8] The term also includes the virtual networks that link information assets together in cyberspace.[9]

Critical Infrastructures Identified by U.S. Government

Agriculture and food	Commercial facilities (including theme parks and stadiums)
Defense industrial base	Dams
Energy	Emergency services
Public health and health care	Commercial nuclear reactors, materials, and waste
National monuments and icons	Information technology
Banking and finance	Telecommunications
Drinking water and water treatment systems	Postal and shipping
Chemicals and hazardous materials	Transportation systems
Government facilities	

Source: U.S. Department of Homeland Security, *National Infrastructure Protection Plan* (Washington, DC: Department of Homeland Security, 2006), 20. It is summarized in U.S. Government Accountability Office, *Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan* (Report GAO–06–672, June 2006), table 1, 9–10. The listing does not represent any attempt to rank infrastructures by importance or vulnerability. Other nations and regions have similar lists. See the *CRN International CIIP Handbook* (Zurich, 2006). T.D. O'Rourke has suggested using a simplified grouping of these infrastructures into six "lifeline systems": electric power, gas and liquid fuels, telecommunications, transportation, waste disposal, and water supply. See O'Rourke, "Critical Infrastructure, Interdependencies, and Resilience," National Academy of Engineering *Publications* 37, no. 1 (Spring 2007), available at <www.nae.edu/nae/bridgecom.nsf/weblinks/CGOZ-6ZQQRH?OpenDocument>.

One of the hallmarks of critical infrastructures is that they are complex, adaptive systems that are far more capable and complicated than the sum of their physical components.[10] They also rely heavily on scale-free networks such as the Internet.[11] As one analyst has noted in summarizing current research on the topic, "while these types of networks are very resilient to random failures, they are very vulnerable to targeted attack. . . . [S]elf-organizing competitive networks are highly efficient, but have the negative externality of systemic vulnerability."[12] In other words, these networks are adept at dealing with scattered outages but susceptible to well-targeted, systematic, repetitive attacks on key nodes.

The interdependencies between infrastructures and their reliance on the information infrastructure as a control mechanism make the consequences of failures in any given area unpredictable and hard to manage. In many cases, economic factors—notably, the capital costs of building facilities on the scale needed to operate and compete in a globalized marketplace—continue to create pressures toward having fewer, larger, and more geographically concentrated infrastructures. While this trend is not new, the push toward consolidation has intensified in recent years. One consequence is that in many economic areas we are seeing a smaller number of larger facilities, each of which commands a larger share of its market. A number of examples of this trend can be found in the United States:[13]

- nearly one-third of waterborne container shipments pass through the twin ports of Los Angeles and Long Beach
- over 36 percent of freight railcars pass through Illinois, primarily around Chicago
- about 25 percent of pharmaceuticals are manufactured in Puerto Rico, mostly in the San Juan area
- over 31 percent of naval shipbuilding and repair facilities are in or near Norfolk, Virginia.

A related trend is that various infrastructures are increasingly dependent on a few key providers of products and services. In the past, most organizations had their own unique sets of internal systems and processes. Increasingly, however, these systems and processes are being outsourced to a few companies that provide third-party logistics and supply-chain management services. In addition, many of the firms that still manage their own logistics processes have come to rely on a limited number of system integrators and application providers for core systems. The result is that many organizations that think of themselves as relatively autonomous are in fact highly reliant on a small number of contractors and suppliers, such as United Parcel Service or Federal Express (FedEx), and on information systems developed and supported by a few large vendors, such as Electronic Data Systems or IBM. As in other areas, this trend has typically brought significant increases in not only operational efficiency but also new kinds of vulnerabilities. If FedEx runs supply-chain operations for 50 firms, multiple operating systems are replaced by a single one. The one may be more effective, and even inherently more secure, than most of the 50 were, but hackers now can concentrate their attacks on one target.

attacks on critical infrastructure and key resources can have both direct and indirect consequences

Looking ahead, it is likely that the next few years will see the emergence of de facto standards for the supervisory control and data acquisition systems that govern many physical infrastructures and operations. This trend is accelerating as individual companies consolidate and infrastructures are knit together firmly. More Faustian bargains are on the way.

Implications

The implications of the growing dependence of modern societies on vulnerable critical infrastructures and just-in-time operations have been recognized and widely discussed for many years. Three features of these critical infrastructures increase the potential consequences of their failure: the increasing reach of individual infrastructures that in many cases span countries and continents; the interdependence of infrastructures (so that, for instance, a failure in the electric power grid will disrupt regional water and sewer infrastructures); and the increasing importance of the cyber infrastructure as a control mechanism for the others.[14] As the Department of Homeland Security has pointed out, attacks on critical infrastructure and key resources can have both direct and indirect consequences. Focused attacks on key assets, systems, and networks can immediately disrupt critical functions. Attacks can also have indirect effects by creating disruptions that cascade through the government, society, and the economy. Infrastructure failures stemming from natural disasters or other causes can have similar impacts.

Role of Public Confidence

Most of the analyses of critical infrastructure failure emphasize (for good reason) the tangible consequences that would ensue if these infrastructures were to fail. However, the intangible factors may be at least as important. Civilized societies depend on public confidence in the stability and durability of social arrangements. There are different ways to characterize this attribute. The simplest is to define it as the general expectation that tomorrow will resemble today and that events are generally predictable and controllable by public authorities. In other words, the working assumption that most people have is that the world will remain relatively stable. If things go wrong, public confidence can be shaken and, eventually, broken. History has made it clear that a breakdown in public confidence can lead to a rapid collapse of law and order, anarchy, and a "war of all against all." Something of this sort occurred in the aftermath of Hurricane Katrina.

The public's growing dependence on mass media for information about what is going on has two consequences. If communications are operational during a crisis, the media will likely *amplify* and *accelerate* the sense of crisis and dislocation (as was seen during Katrina). But what happens when these communications media are put out of commission? Many of the mediating authorities that were on hand in the past to mobilize community actions and dampen fear-mongering are less available and less effective than they once were. If the media become unavailable

because of infrastructure collapse, media-reliant individuals will feel a sense of dislocation and confusion that may leave them susceptible to rumors and misinformation.

This fact of life in the information age makes public confidence, human perceptions, and the media prime targets for hostile attack. Attempts to manipulate an enemy's morale and political support are not new, but the growing importance of the media in shaping public perceptions means that information operations have become potent strategic weapons. When combined with directed attacks on other critical infrastructures, these operations can become even more powerful.

Threat

Threats to critical infrastructure and key resources (CI/KR) fall into three general categories: natural disasters, "normal accidents,"[15] and deliberate attacks. The first two are fairly common and infrastructures are generally resilient from their effects, though not always to catastrophic events such as Katrina. Deliberate attacks, while less frequent, are potentially more worrisome for two reasons. First, adversaries can study CI/KR to identify critical nodes. This is important because much of American CI/KR exhibit the attributes of scale-free networks: resilient to random attacks but susceptible to targeted attacks against key nodes. That is one reason why natural disasters and normal accidents do not usually cause long-term strategic damage to CI/KR; unless they happen to randomly take down a key node, the system as a whole will be able to recover quickly. Humans can change that. If they can identify key nodes in a given infrastructure network (the ease of which depends on the characteristics of the infrastructure in question and the capabilities, resources, and motives of the attackers), adversaries might be able to take down the whole thing in one fell swoop.

by focusing on the threat from manmade attacks, the government has diverted attention from the risks posed by both natural disasters and industrial accidents

Another key factor that we can affect is the duration and/or frequency of an outage. A single incident is not likely to cause long-term damage. Infrastructures are generally built to be resilient to all but the most catastrophic events. Even if a major failure occurs, the system will likely return to operating capacity in relatively short order. However, one significant difference between natural disasters and deliberate attacks is that the former tend be one-off events—they are unlikely to occur multiple times in a short period. In contrast, human attackers may choose to mount sustained attacks against key nodes (in one or more infrastructures) that could cause lasting damage to the Nation. The good news is that such sustained attacks are not easy to carry out. They take extensive planning and intelligence-gathering, large numbers of highly skilled people who can keep their activities secret for months or years, significant financial resources, and access to advanced test beds for rehearsal and experimentation with attack methodologies. The bad news is that the number of groups (or countries) that could undertake such operations is growing, and the trends (technological, demographic, and economic) do not bode well for defenders of CI/KR.

Exactly what kinds of attacks are adversaries likely to perpetrate against CI/KR? The answer to that question is the typical analyst's response to any query on a complex topic: it depends. To gain some insights into the problem, we need to look at both means and ends. To begin with the latter: what exactly are the attackers trying to accomplish? Do they wish to create a sense of horror and panic among a civilian population? If so, they will likely want to destroy things or kill people in a violent and spectacular way. This is best accomplished through high explosives or weapons of mass destruction. An examination of the long list of terrorist activities planned or executed since 9/11 reveals exactly such a pattern of attacks. It is not difficult to imagine a scenario where terrorists attack an infrastructure with explosives to cause massive casualties.[16] In fact, such scenarios are both easy to devise and difficult to prevent; they clearly deserve attention. The downside of such attacks is that they will undoubtedly cause a massive response on the part of the attacked nation. In some cases, such a response may be an intended outcome; in others, it may not. Either way, a direct attack on a nation's infrastructure will likely be interpreted as an act of war, with all of the attendant consequences.

Some attackers may have different goals in mind. They may want to disrupt a nation's infrastructures without causing mass casualties or creating conditions likely to provoke a massive response. The most common scenario fitting this description is one where an adversary disrupts U.S. logistics and transportation infrastructures in order to slow a possible American response to an attack on a third party.[17] Because the goal in such scenarios is disruption rather than destruction, and because these attackers may not wish to be identified, the use of cyber attacks is much more likely in these cases. Cyber attacks can be conducted in ways that make attribution difficult. For example, commonly available hacker tools and techniques could be used either to deny the availability of critical infrastructures or create uncertainty in the minds of decisionmakers about the reliability and dependability of the infrastructures.

Finally, it is important to point out that the attack mode is not "either/or." An adversary could certainly use both physical and cyber attacks to achieve desired ends. The most likely goal in such a scenario would be to use cyber methods to enhance the effect of physical attacks. For example, someone could attempt to disrupt the computer or communications systems of first responders just after a large explosion in an urban area. This strategy would probably be used when the goal is massive destruction or disruption. Because physical attacks are part of this approach, and such attacks leave evidence trails, they are not likely to be carried out by parties who wish to remain anonymous.

Policy Issues and Options

At the risk of oversimplifying a complex subject, we will group all possible response options into three broad categories: prevention and protection; resilience; and deterrence.

Prevention and Protection. This category includes all actions taken to either prevent an incident from occurring or minimize the impact that an incident will have on a given CI/KR. If the incidents in question are natural disasters or normal accidents, the response options generally focus on prediction and safety measures. If the incidents are manmade, the response options may include things like border security, counterterrorism, intelligence-gathering, and military operations.

Since 9/11, the United States has focused the bulk of its energy and resources on trying to prevent terrorist-sponsored infrastructure attacks. Such efforts are absolutely necessary, but they are not sufficient; it is practically impossible to prevent some kind of terrorist attack in the United States. In addition, by focusing on the threat from manmade attacks, the government has diverted attention from the risks posed by both natural disasters and industrial accidents, neither of which can be prevented by antiterrorism measures. For both of these reasons, the Nation should weigh the costs and benefits of initiatives that go beyond purely preventive measures and explore ways to increase the resilience of critical infrastructures.

Resilience. History has clearly demonstrated that infrastructure failures are inevitable. The goal of decisionmakers should be to minimize the impact that such failures will have on the Nation as a whole. Recent disasters such as Katrina have shown that one critical factor in restoration of infrastructure performance and maintenance of public order is the ability to mount a rapid, coordinated, and well-planned response. This can be accomplished through a variety of resilience programs. Such programs could involve a number of ideas: better insurance, continuity of operations capabilities, investments in redundant capabilities for vulnerable single points of failure, and the creation of coordinated and trained rapid-response teams similar to Germany's *Technisches Hilfswerk*. While such resilience programs can be extremely effective, funding them can be difficult because they impose short-term costs and benefits are unpredictable. However, a resilience-based approach is helpful for all types of infrastructure incidents and is almost certainly cheaper than a strategy of simply waiting for events to occur and then paying for the resulting damage. It can also save lives.

U.S. leaders focused on national security policy will need to confront the possibility that sustained attacks on national infrastructures could potentially limit American ability to project power

Deterrence. Although deterrence could be viewed as a prevention measure, we believe that it is sufficiently different from the usual range of prevention and protection options to deserve a separate analysis. Deterrence refers to the development of retaliatory capabilities to dissuade adversaries from launching an attack against U.S. assets. It is a psychological approach built upon the premise that if the costs of an attack outweigh its potential benefits, the attack will not be carried out. One can affect this calculus by increasing the likely costs of an attack (usually through the threat of retaliation) and/or by reducing the potential benefits of an attack (usually through defensive measures that fall under both protection/prevention and resilience).

The United States is already acting to prevent attacks on its CI/KR by a range of adversaries. Hopefully, it will also take additional steps to improve the resilience of its infrastructures. The deterrence issue raises another policy question: should the United States develop plans, processes, and capabilities to threaten potential adversaries with retaliatory, infrastructure-focused operations to deter them from attacking in the first place? This is not a simple question to answer. Deterrence will not work unless the following conditions exist: we must be able to identify the adversary; the adversary must know that we have the capability to cause them great harm as well as the willingness to use that capability; and the adversary must wish to avoid the harm we can cause.

When it comes to infrastructure attacks, it is not easy to satisfy all four of these preconditions. This is especially true if an adversary uses cyber attacks. Such methods can make identification of the attacker uncertain. Will the United States be willing to retaliate in kind if it is not sure about who has attacked it? Also, what kind of response would the United States be willing and able to use in response to a cyber attack? Would that response be sufficiently robust to prevent adversaries from attacking in the first place?

To complicate matters further, some of the adversaries that the United States may wish to deter include powerful national states such as China and Russia. Is the United States prepared to convince these countries that it has the means and will to cause great harm to their infrastructures if the United States is attacked? With what capabilities will the United States threaten them credibly? How can the United States signal to these and other countries that it has specific capabilities without giving away its attack plans or escalating tensions? (This is a major problem with cyber attacks.)

Finally, transnational groups such as al Qaeda may be difficult to deter for two reasons: they may not provide easy targets for retaliatory actions, and they may not be afraid of the U.S. response. In fact, they may want the United States to attack their assets in Muslim countries to further their goal of convincing Muslims that the United States is a great enemy.

Deterrence options do pose challenges. However, a deterrence strategy could also prove useful in some situations. Decisionmakers need to analyze the advantages, disadvantages, and obstacles associated with developing a deterrence strategy for critical infrastructures and/or cyberspace. A full discussion of the implications of such a strategy is beyond the scope of this paper but seems likely to become an increasingly important part of national security thinking in the future.

The Private Sector

Finally, the fragility question poses new issues for public-private coordination. In many societies, including the United States, most of the critical infrastructures are owned and/or operated by private firms. This arrangement has its advantages; the private sector is usually far more flexible and adaptive, quicker to innovate, and more efficient than the public sector. However, it also carries several challenges, especially in terms of homeland security. For example, because no single private entity is responsible for an entire national or global infrastructure, and there are at least 17 critical infrastructures in the United States alone, the task of developing and mounting a coordinated private-sector

response to threats or incidents requires dozens if not hundreds of companies to work together (not to mention that cooperation with local, state, and Federal government agencies is also required). These firms often show an admirable sense of civic obligation and patriotism, especially in times of emergency.

Nonetheless, for a variety of legal, financial, and competitive reasons, full cooperation among companies is unlikely. In addition, firms will naturally put their own business interests ahead of broader, vaguer public interests; after all, they have a fiduciary responsibility to their shareholders. Thus, while individual companies may take steps to improve their own security (which may make good business sense), it can be difficult for competing enterprises to cooperate effectively to reduce national vulnerabilities in homeland security.

If private firms lack market incentives to deal with cross-cutting infrastructure risks, society faces a dilemma—either tolerate the situation or create new incentives for cooperative efforts. These incentives could include rewards to encourage desired behaviors, such as accelerated tax write-offs or grants, and/or penalties for undesirable behaviors, such as levies that would help fund reinsurance risk pools. Determining what incentives the government should offer, how such incentives would be implemented, and how their efficacy would be measured is a vexing problem with no easy solution.

If incentives fail to produce the desired outcomes, policymakers must then decide if at least a few critical infrastructures should be regarded as public goods that the government has a responsibility to protect from "market failures." A number of policy options flow from this perspective, ranging from government ownership of selected CI/KRs (such as the Nation's air traffic control system) to terrorism risk insurance to legal and regulatory actions. The fundamental policy dilemma facing the United States is whether to leave things as they are and accept a higher degree of vulnerability or try to reduce vulnerability by tackling constitutional, political, and economic issues that have their own huge costs. This is an issue that deserves further debate.

If one accepts that the forces pushing advanced societies toward strategic fragility are likely to persist and accelerate, then one comes face to face with a range of difficult policy issues. For example, U.S. leaders focused on national security policy will need to confront the possibility that sustained attacks on national infrastructures could potentially limit American ability to project power. In a broader sense, policymakers will need to think about the best ways to manage the Faustian bargains that shape our societies by mitigating risks and creating more resilience to guard against the inevitable slings and arrows of outrageous fortune. None of this will be easy, fast, or cheap. But inaction will inevitably impose its own costs, and they are likely to be higher than those exacted by prudent foresight.

Defense Horizons *is published by the Center for Technology and National Security Policy. CTNSP publications are available online at http://www.ndu.edu/ctnsp/publications.html.*

The opinions, conclusions, and recommendations expressed or implied within are those of the contributors and do not necessarily reflect the views of the Department of Defense or any other department or agency of the Federal Government.

Center for Technology and National Security Policy

Hans Binnendijk
Director

Notes

[1] For a description of the evolution and impact of containerization, see Marc Levinson, *The Box: How the Shipping Container Made the World Smaller and the World Economy Bigger* (Princeton: Princeton University Press, 2006); and Brian Cudahy, *Box Boats: How Container Ships Changed the World* (New York: Fordham University Press, 2006).

[2] Most liquid and dry-bulk cargos continue to move in noncontainer ships. In 2003, container ships made up 30.5 percent of vessel calls to U.S. ports. See Congressional Research Service, *Port and Maritime Security: Potential for Terrorist Nuclear Attack Using Oil Tankers*, Report RS 21997 (Washington, DC: Congressional Research Service, December 2004), 1.

[3] The implications of the switch to container traffic were recognized as early as the 1970s.

[4] The five seaports are Los Angeles, Long Beach, New York, Charleston, and Savannah. Such long-established ports as Boston, San Francisco, Baltimore, and Philadelphia barely register on the list. See *Plunkett's Transportation, Supply Chain and Logistics Industry Almanac* (Houston: Plunkett Research Limited, 2004), 32. Similar trends are evident in other sectors.

[5] The security issues raised by concentrations of container traffic are discussed in Michael J. Babul, "No Silver Bullet: Managing the Ways and Means of Container Security," U.S. Army War College Strategic Research Project (2004), 1. See also Jon D. Haveman and Howard J. Shatz, ed., *Protecting the Nation's Seaports: Balancing Security and Cost* (San Francisco: Public Policy Institute of California, 2006), 2.

[6] U.S. Department of Transportation, *Intelligent Transportation Systems for Traffic Signal Control*, FHWA–JPO–07–004, January 2007, 2, available at <www.its.dot.gov/jpodocs/repts_te/14321.htm>.

[7] On this point, see Charles Perrow, *Normal Accidents: Living with High Risk Technologies*, 2d ed. (Princeton: Princeton University Press, 1999), and *The Next Catastrophe: Reducing Our Vulnerabilities to Natural, Industrial, and Terrorist Disasters* (Princeton: Princeton University Press, 2007), as well as Stephen Flynn, *The Edge of Disaster* (New York: Random House, 2007).

[8] U.S. Department of Homeland Security, *National Infrastructure Protection Plan* (Washington, DC: Department of Homeland Security, 2006), 103, available at <www.dhs.gov/xprevprot/programs/editorial_0827.shtm>.

[9] Ibid., 103.

[10] On this point, see Steven Rinaldi, James P. Peerenboom, and Terrence K. Kelly, "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," *IEEE Control Systems Magazine*, December 2001, 13, 24.

[11] For a good discussion of scale-free networks, see Albert-Laszlo Barabasi, *Linked* (New York: Plume, 2003).

[12] Sean Gorman, *Networks, Security and Complexity: The Role of Public Policy in Critical Infrastructure Protection* (New York: Elgar, 2005), 8.

[13] Congressional Research Service, *Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options,* Report RL 33206 (Washington, DC: Congressional Research Service, December 21, 2005), 4.

[14] The 2006 National Infrastructure Protection Plan (NIPP) defines the *cyber infrastructure* as including "electronic information and communications systems, and the information contained in those systems. Computer systems, control systems such as Supervisory Control and Data Acquisition systems, and networks such as the Internet are all part of cyber infrastructure," 13. Although other definitions differ slightly in terminology, there is general agreement on the basic parameters of this definition. Note that the cyber infrastructure in this definition includes both the mechanisms—the systems and networks—and the content of the information. It also includes 2 of the 17 critical infrastructures (information technology and telecommunications) identified in the NIPP.

[15] See Perrow.

[16] For an interesting discussion of the threats posed by non–nation-states, see John Robb, *Brave New War: The Next Stage of Terrorism and the End of Globalization* (New York: John Wiley and Sons, 2007).

[17] For a description of such a scenario, see James C. Mulvenon and Richard H. Yang, *The People's Liberation Army in the Information Age*, CF–145–CAPP/AF (Santa Monica, CA: RAND, 1999).