



TOFFLER ASSOCIATES®

Guarding Our **Future**

Protecting Our Nation's Infrastructure





Table of Contents

Overview.....	3
Part One. The Rapidly Changing Infrastructure Environment.....	4
Part Two. Nine Conditions that are Shaping Future Critical Infrastructure...11	
Part Three. Convergences and Implications.....	29
Part Four. Eight Recommendations.....	33
Part Five. Conclusion.....	47
Appendix 1. Interviews and Workshop Participants.....	48
Appendix 2. Endnotes.....	50

PREFACE

Guarding Our **Future** *Protecting Our Nation's Infrastructure*

Toffler Associates, the Department of Homeland Security and the Office of Infrastructure Protection are pleased to present this report on protecting the future of the nation's infrastructure.

This report is a product of Toffler Associates. It reflects our interpretation of research and analysis, discussions, and workshops with a diverse set of thought leaders from business, government, and academia. We greatly benefited from the insights and support of our sponsor, Assistant Secretary for Infrastructure Protection, the Honorable Robert Stephan. This report reflects neither the views of all with whom we spoke nor those of the United States Government. It does not represent consensus findings or recommendations from the participants as a whole.

We commend our sponsors for steadfastly demanding a disciplined look into the future in order to assess the implications and inform the decisions that must be made to protect our critical infrastructure.

OVERVIEW

The attack on the Twin Towers on 9/11 was possible for several reasons but two especially stand out.

1) It was unthinkable, and therefore little or nothing was done to guard against such an attack, and 2) terrorists used an element of our infrastructure, airplanes, to attack our infrastructure, the Twin Towers. Over the next 20 years, adversaries are going to have access to much more sophisticated elements of our infrastructure than conventional airplanes. For just one example, nanotechnology and biotechnology represent emerging infrastructure sectors that in the coming years will produce myriad capabilities which, when put in the wrong hands, could kill untold numbers of people, destroy vast expanses of property and cripple our ability to retaliate. The purpose of this report is to explain how those who protect our infrastructure will need to address such complex new challenges while still addressing existing challenges. It explains that those responsible officials and executives must think the unthinkable in order to prevent future attacks.

The infrastructure of the United States underpins our economy and the American way of life, yet it is a weak and vulnerable link in protecting our country from natural disasters and malicious attacks. The problem is two-fold: 1) much of the existing infrastructure—which includes everything from roads and bridges to cyberspace—is in desperate need of repair and risk-based protective measures, and 2) this problem will worsen in the next 20 years as our infrastructure expands and new elements are added.

While it is difficult to predict how the infrastructure will change in the future and thus how to protect it, nine conditions that exist today provide a logical basis for forecasting how our infrastructure will

evolve in the coming years. The conditions are: climate change, migration and urbanization, condition of infrastructure, “disruptive” technologies, reliance on cyber, ubiquitous situational awareness, blurred national boundaries, hyper-empowered individuals and groups, and the legal and regulatory environment.

Changes in any one of these conditions will cause other conditions to change and thus alter the shape of our future infrastructure and the defenses needed to protect it. The conditions will change rapidly and unpredictably, so those organizations in charge of protecting the future infrastructure must be agile enough to adjust *their* plans just as rapidly.

Much can be done today to prepare our citizens for the changes that will take place in the future and help the organizations protecting our infrastructure to develop innovative defenses. While the cost to protect our infrastructure is high, the cost of not acting now will be even higher in the future, and measured in lives, property, and a decline in the American way of life. To address these issues, we recommend eight proactive steps to protect our country over the next 20 years.

1. Make infrastructure protection a more urgent and clear national priority: We must change the nation’s perception that infrastructure protection is not a vital priority by, among other steps, implementing a robust strategic critical infrastructure and key resources (CIKR) protection communications campaign and creating a commission on par with the 9/11 Commission to address our future infrastructure challenges before the next crisis occurs.

2. Prioritize and address what constitutes “critical” infrastructure in the future, understanding that it will continually evolve: As infrastructure changes in the future, we can redefine the most critical portions by defining and addressing the next generation of sectors that will require protection and bring the debate for infrastructure prioritization to those who know it best: local public forums.

3. Establish a knowledge integration center to analyze, coordinate, and integrate the nation’s knowledge about protecting our infrastructure: Such an entity can provide the analysis and advisory capability across all infrastructure sectors to help us better understand the impacts of the converging conditions and interdependencies of our future infrastructure.

4. Define and address where “desynchronization”—the government’s inability to keep pace with changes in society and the private sector—affects our ability to keep pace with infrastructure threats and needs: By defining where desynchronization takes place, we can identify vulnerabilities in infrastructure protection and create aggressive action plans to address them.

5. Understand the impacts of future interdependencies across all existing and emerging infrastructure sectors: The infrastructure of the future will be highly interdependent in ways that we can’t imagine today. Therefore we need to think

beyond a sector view of infrastructure in order to discern its critical interdependencies and the implications of those interdependencies. We can do this, for example, by gaining a better understanding of second- and third-order effects of future crises, and by establishing standards that foreign purchasers of U.S. infrastructure must meet.

6. Establish more innovative incentives for infrastructure protection: We can encourage governments and private owners of the infrastructure to voluntarily protect their sections of the infrastructure by offering incentives such as tax credits, rebates, limiting liability, and low-cost loans.

7. Conduct cross-sector infrastructure-protection games and simulations to understand emerging challenges, interdependencies and future risks that would affect the National Infrastructure Protection Plan (NIPP) and other key plans. By simulating how conditions will converge to affect our future infrastructure we can identify innovative solutions to protect it.

8. Get inside our adversaries’ decision space to proactively stop future attacks on infrastructure: Because adversaries can plan and carry out attacks faster than government bureaucracies can react to them, we must find innovative ways to out think them and prevent their attacks.

Report Objectives

To help organizations understand and better manage change, this report outlines the major forces of change and their relationships to infrastructure over the next 20 years. It raises questions and recommends actions that infrastructure owners, operators, partners and stakeholders must consider in order to protect what we value most as a nation. From a strategic perspective, the costs of taking these actions pale in comparison with the costs of non-action and complacency.

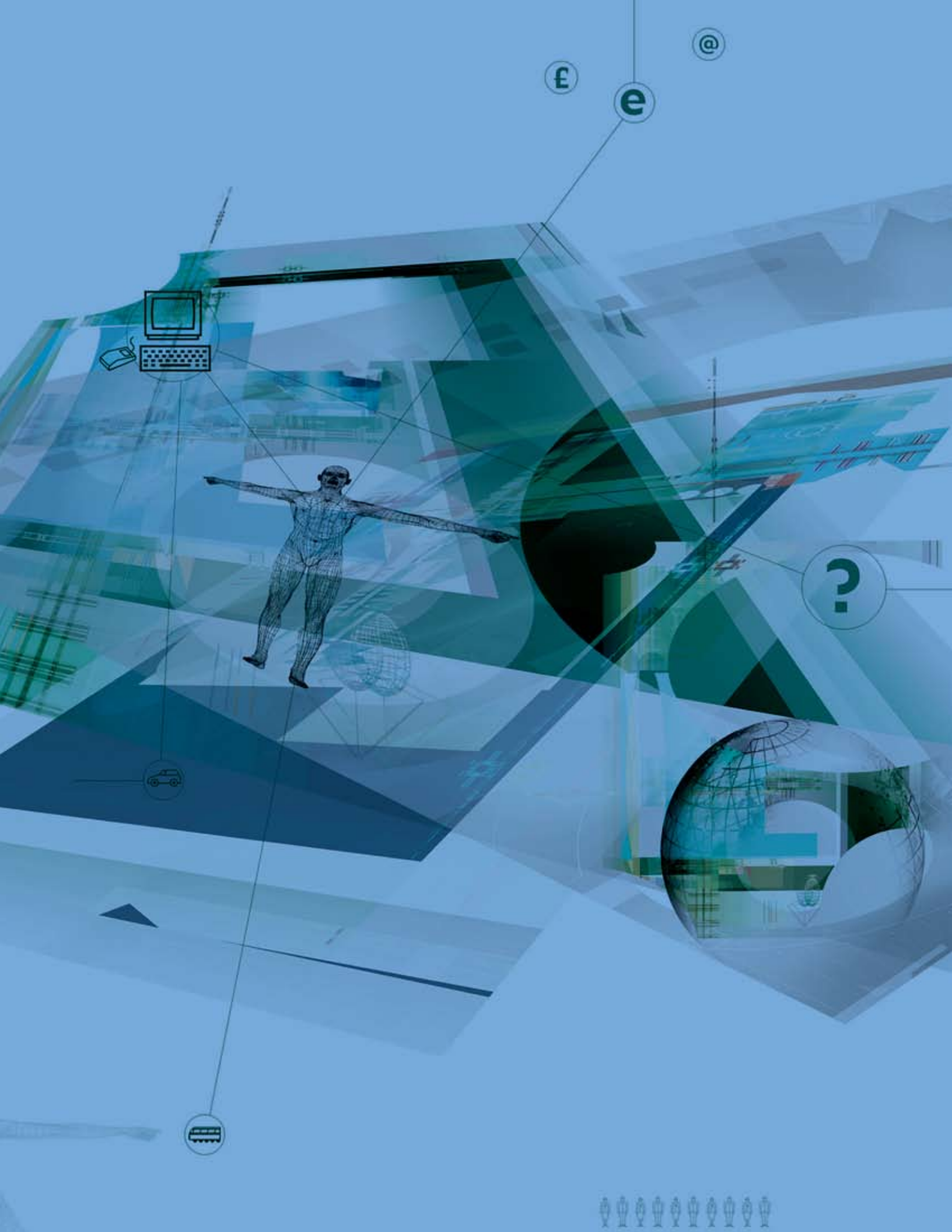
A key goal of this report is to challenge today's thinking and begin looking at critical infrastructure and key resources (CIKR) beyond the next budget cycle or within particular sectors. Significant parts of our existing infrastructure are deteriorating at a rapid rate. At the same time society is challenged by dramatic technological, market and social changes. Our CIKR must keep up with technological, societal, political, security, economic, and environmental changes. We must understand and appreciate how and why critical infrastructure will change, and what will drive these changes. By understanding these changes we can identify the challenges, opportunities, and threats that we must address to prevent the loss of life and to ensure our nation's future security and economic vitality.

Methodological Note

This report is based on extensive secondary-source research, interviews with over 50 thought leaders, and a series of workshops organized to address how infrastructure may change in the future. The synthesis and analysis of these data led to our identification of nine primary conditions that will shape the future of our nation and the world's infrastructure. We developed the implications and recommendations in this report by assessing the convergences of the nine conditions and how they will shape the future of infrastructure and infrastructure protection.

For purposes of this report, critical infrastructure (CI) is defined as the assets, systems, and networks, whether physical or virtual, which would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof if destroyed, degraded or attacked. Key resources (KR) are publicly or privately controlled resources essential to the minimal operations of the economy and government.

This report does not purport to predict the future. Rather it provides multiple insights into what will shape the infrastructure in terms of threats, opportunities and challenges that leaders need to address now and in the future.



The Rapidly Changing Infrastructure Environment

The environment in which we build and operate the nation's critical infrastructure will change significantly over the next 20 years—and in many ways, so will the infrastructure itself. As these changes evolve, the nation's approaches to infrastructure protection must proactively and rapidly adapt to new threats, risks and opportunities.

Over the next 20 years, those charged with protecting our infrastructure will face unprecedented challenges brought on by accelerating change. Technological, social, economic, and political changes will happen more quickly, and in many cases faster than legacy organizations can adjust their planning and risk management practices. Exacerbating the effects of accelerating change is the increasing interconnectedness of infrastructure systems, where an attack or event at one point affects multiple systems. These dense connections make it more difficult to determine the cause of an attack, to implement protective measures, or to respond to an event.

Figure 1 gives examples of what some elements of the infrastructure look like today and how they will change in the future.

Figure 1: Changes in the Future Infrastructure Environment

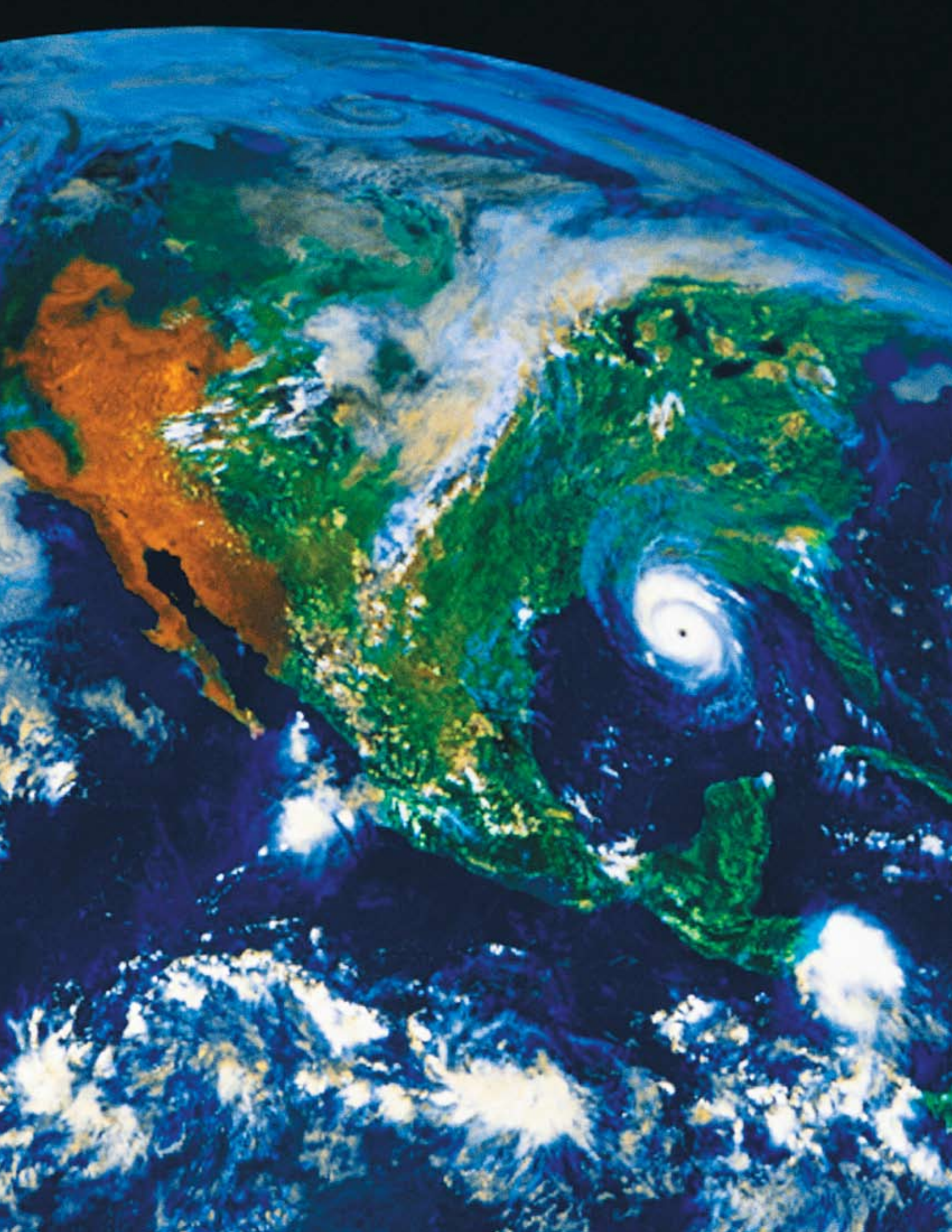
TODAY	THE NEXT 20 YEARS
Vehicles with GPS	Smart cars on smart highways that leave significant portions of driving to a computer
Traditional buildings with little sensing capability	“Smart” buildings that sense maintenance and risk issues, and may even be able to mitigate some risks (e.g. smart nano surfaces on some structures)
Classical computing (storage via standard 3-bit register)	Quantum computing (storage as quantum bits). Has new infrastructure and protection implications due to new ways of storing and protecting data
Partially interdependent supply chains	Highly interdependent supply chains
Healthcare, biotech, cyber and other infrastructures are primarily independent	Healthcare, biotech, cyber and other infrastructures are interdependent and linked to humans
Static and intermittent monitoring of CIKR (e.g., safety cameras, CCTV)	Continuous, real-time and autonomous sensing, tracking, and warning systems integrated for full range of CIKR
Pyramidal bureaucracies with obstacles to sharing information and collaboration	Diversity of organizational arrangements that are neither classically bureaucratic nor pure networks
Relatively clear authorities and governance	Cloudy authorities and governance due to increased interdependences and blurred borders
The government's inability to keep up with changes among the private sector and NGOs causes friction and disruption	The government's inability to keep up with changes among the private sector and NGOs causes breakdown of government institutions
The U.S. is the primary leader of technology innovation associated with infrastructure development and protection	Innovation development more dispersed world wide

Today we recognize 18 infrastructures, specifically:

- Agriculture and food
- Banking and finance
- Chemical
- Commercial facilities
- Communications
- Dams
- Defense industrial base
- Emergency services
- Energy
- Government facilities
- Information technology
- Critical Manufacturing
- National monuments and icons
- Nuclear reactors, materials, and waste
- Postal and shipping
- Public health and healthcare
- Transportation systems
- Water

Not all infrastructure will change dramatically. Technological developments will affect many aspects of our infrastructure: economic, social, and natural events will cause other aspects to change.

Although these sectors will continue to be vital to national interests, we can expect some to merge and new sectors to emerge in the future. For example, will the information technology and communications sectors merge due to their strong interdependencies? Will convergences and interdependencies in healthcare, biotech, and information technology create a new infrastructure sector that focuses on protecting the cyber linkage between medically implanted devices and the wireless networks that monitor and control them? It is difficult to predict which sectors will merge and which sectors will newly form, but we can be sure that as society rapidly changes some infrastructure sectors will morph to meet societal needs.



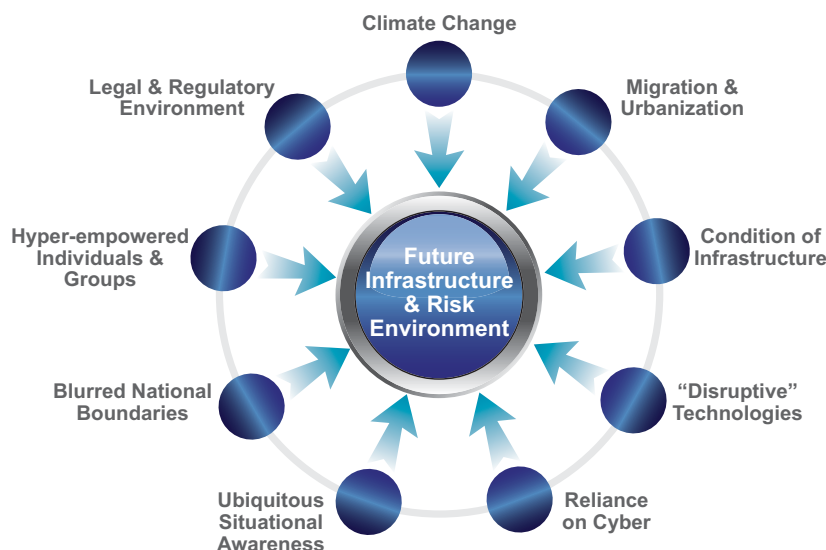
Nine Conditions that are Shaping Future Critical Infrastructure

The infrastructure of 2028 will challenge us in ways we can't imagine today. Today's risks will change dramatically over the next 20 years, and those changes will occur more rapidly each day. The accelerating rate of change makes it vital for those charged with infrastructure protection to anticipate challenges and develop the agility to respond to an evolving environment.

Unlike changes of the past, the future will evolve more and more quickly, creating inextricable links among people, places, and things, so addressing sector or security threats individually becomes almost futile. Today's infrastructure has become so interconnected and interdependent that every action sends ripples throughout multiple domains. In the future, we must access critical infrastructure protection as a whole.

Nine conditions (Figure 2), already visible today, will shape the future infrastructure environment. By exploring these conditions and their influences on one another and on various infrastructure sectors, we can gain a better understanding of the potential risks associated with the future operating environment. However, it is important to consider each one in the context of the others, as convergence among the nine conditions will create the future infrastructure environment. The relevant features of each condition are described below.

Figure 2: Nine Conditions Affecting the Future Infrastructure Environment



1. Climate Change

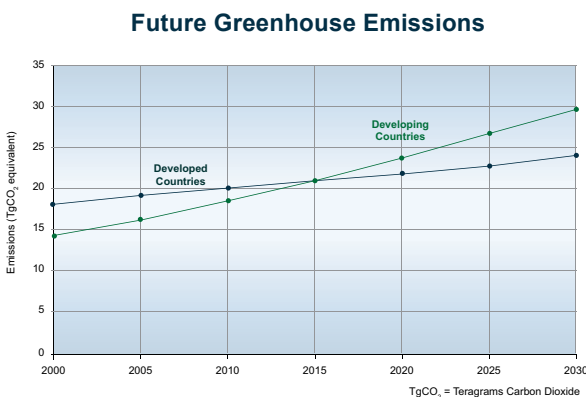
Climate change will affect critical infrastructure over the next 20 years just as it will affect numerous other dimensions of our lives and our security. While no one can predict future weather patterns with absolute accuracy, realistic projections argue for near-term proactive measures to contend with their impacts. Fortunately, advances in modeling technology and increased data on observed climate change have improved our ability to project the effects of global climate change, which will help planners understand what they must do to secure our infrastructure against these effects.

Carbon emissions are among the most well known—yet frightening—causes of climate change. Global emissions of carbon dioxide are predicted to reach 43-44 billion metric tons in 2030, a 74 percent increase from 2007 levels¹. As a result, the average surface temperature of the Earth could increase—relative to 1980-90 temperatures—by 2 to 7.2°F or more by the end of the century². This warming will be unevenly distributed around the globe, requiring different approaches for infrastructure owners, operators and stakeholders. Land areas will warm more than ocean areas, and high latitudes will warm more than low. Warming will differ by season, with winter warming more than summer.

Climate change will influence all industries and sectors of society, in part by affecting the infrastructures on which they rely. For example, droughts may necessitate changes to the infrastructure that controls water for agriculture and drinking. Storm damage will batter the already deteriorating infrastructure in highly populated areas, and these structures may not be capable of supporting the migration patterns that changing weather conditions likely will stimulate. Transportation systems' ability to operate in severe weather may necessitate structural or other changes to the systems, or the development of new, more robust transportation systems.

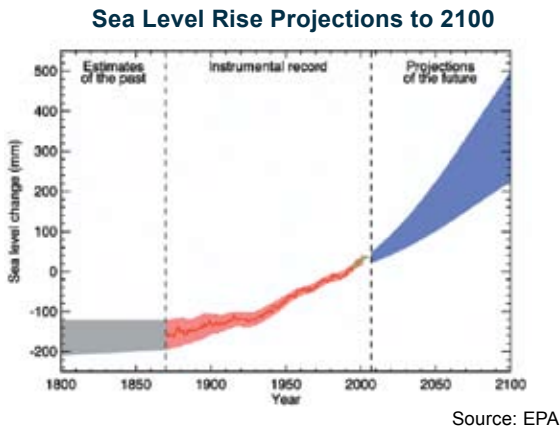
As global temperature rises, we can anticipate a host of other impacts on our infrastructure, particularly through changes in worldwide sea levels and precipitation patterns. Rising sea levels—accelerated by rapid glacial melting and other factors related to changing atmospheric conditions—will threaten many coastal cities over the next two decades. These cities will have to address the integrity of their coastal infrastructures, including homes, businesses, public works and maritime assets.

Some experts estimate that tropical storms and hurricanes will become more intense, produce stronger peak winds and generate increased rainfall over some areas. The implications of this on local and regional infrastructure have already been felt in Louisiana, Florida, and other areas hit by major hurricanes in the past several years, and will likely multiply. If stronger storms can be expected, infrastructures will require additional protection to



Source: EPA

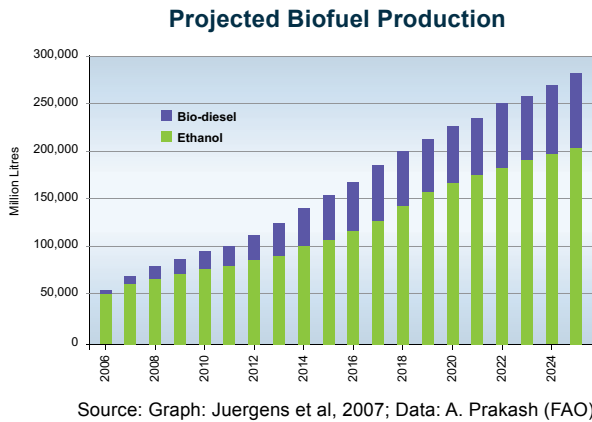
survive them or must be able to recover quickly after a significant natural event. For example, buildings in certain areas will need changes in design and materials to withstand more violent winds.



In addition, as infrastructure becomes more interconnected globally, natural disasters abroad will also affect the U.S. by disrupting international supply chains and possibly U.S. corporate and government assets abroad.

As our understanding of the effects of climate change grows, additional risks will emerge. For example, scientists are beginning to expect that changes in climate will increase the acidification of the oceans. Even very small increases in the pH levels may eat away at, weaken and have other significant impacts on bridges, dams, and other marine structures and ecosystems³, with far-reaching cascading effects on transportation, energy, global trade, food and agriculture, and other systems.

The debates on the causes and impact of climate change will continue. What is more certain is that global energy demand will grow. Climate change concerns have already prompted drastic changes in human behavior to mitigate these impacts—and these behavioral changes have their own implications for the future of infrastructure. For example, more

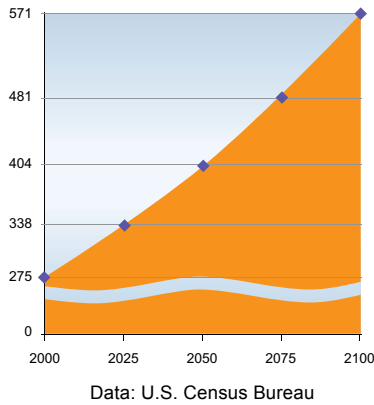


countries and companies are increasing their use of alternative energies. By 2020 the European Union plans to replace 10 percent of its transportation fuels with biofuels made from crops such as sugar cane and rapeseed oil.⁴ As wind power becomes more popular and cost effective, global wind energy markets, valued at \$5 billion in 2000, are expected to grow to \$50 billion by 2012. Solar energy is expected to expand from \$3.5 billion to \$28 billion in the same time period.⁵ As major world economies invest time, money, and attention to alternative energy, other countries may follow suit, changing global agricultural economics—and changing the kinds of infrastructure we need to support and enable these new energy systems.

At the same time, we can anticipate unintended consequences from these changes, which will have their own infrastructure implications. For example, while biofuels are generally viewed as positive alternatives to carbon-based fuels, recent debates point out they can have a potentially adverse environmental and economic impact on land use and food prices. As more information and new solutions appear, it is likely that industries will change their basic operations, such as the type of energy they rely on, and their dependence on other sectors, causing a ripple effect across many infrastructures.

2. Migration and Urbanization

Projected U.S. Population Growth

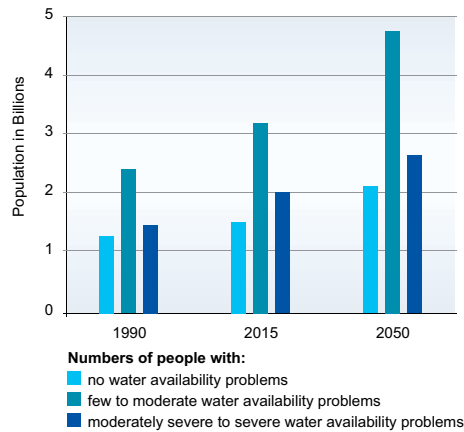


Future migrations, urbanization, and population growth will change the way citizens rely on local infrastructure. The population growth in cities will elevate congestion levels, slow the delivery of public services, and result in other changes to urban centers. By 2025, 75 percent of U.S. residents are expected to live on the country’s coasts, affecting preservation of wetlands, healthcare systems, housing, transportation systems, and insurance costs associated with the larger number of people who will be affected by the tropical storms and hurricanes that are frequent in these areas. Many will migrate to cities seeking improved living, working, and recreation benefits, creating “24/7 cities” across the U.S.⁶

The U.S. will see its population grow in the next few decades, which will increase demands on our domestic infrastructure. Between now and 2025, the Census Bureau projects the U.S. population will grow by 24 percent to 350 million Americans. The greatest growth will take place in the Western states, while the Northeast and Midwest can expect declines. The top four states by population will be: California (49 million representing 15 percent of the U.S. population), Texas (27 million), Florida (21 million), and New York (20 million). By 2025, the foreign-born population

in the U.S. will reach 15 percent, a historic high. All of these changes will put significant stress on the infrastructure in the regions where population growth is high, and compel new kinds of decisions about the infrastructure in the regions experiencing population decline.

Population subject to water scarcity (billions)



Source: RIVM/UNEP; Klepper *et al*

The population over age 60 is expected to nearly double by 2050. As a result, the U.S. will need to upgrade or replace much of its basic infrastructure, such as housing, health care, and transportation, to support the rapidly growing group of retirees. Also, as the population ages, the nation will have to choose among: higher taxes, lower non-entitlement spending, a reduction in outlays for entitlement programs, a sharply higher budget deficit, or some combination of these options—and local infrastructures will also have to adjust to changing needs and resources.

These effects on infrastructure extend worldwide, and will have cascading effects on domestic infrastructures in an increasingly interconnected world. By 2025, the global population is expected to be 7.9 billion, with the majority of people living in developing countries. Just as in the U.S., by 2025 a substantial segment (60 percent) of the world’s population will live in cities (increasing to 66 percent

by 2030), many of which will be located on coastlines just as in the U.S.⁷ A major concern is that many cities, including many in the U.S., are in harm's way from natural disasters. Miami, Houston, New Orleans, and New York, among others, are in hurricane-prone areas. Cities such as Los Angeles, San Francisco, and Seattle are on the highest-risk earthquake fault lines in the continental U.S., and the second largest fault line, the New Madrid, sits in the heart of our country threatening the populations of St. Louis, Nashville, and other locations. There are other risks associated with flood plains, on or near which many U.S. cities are built. In short, in the future a significant part of the U.S. population and infrastructure will be located in "geographic risk zones."

Global population growth will increase the demand for scarce natural resources and strain the infrastructure that controls and distributes those resources (water, food, energy, etc). International pressures to meet water and energy needs will likely create global tensions. For example, by 2025 an estimated 54 countries, home to 4 billion people (nearly half of the world's population), will face serious food production and water shortfalls and problems with the associated infrastructure.

Global water shortages and allocation problems will affect two-thirds of the world population by 2025, which in turn will inevitably affect local economies and create conflicts.^{8,9} The demand for infrastructure will continue to expand significantly in the decades ahead, driven by changes in global economic growth, technological progress, climate change, urbanization, and growing congestion. All of these changes have the potential to catalyze conflict.

Some of the forces influencing massive global migration and urbanization include the availability of jobs and technology, access to energy and water, aging populations in developing countries, and the growing populations in less developed countries. Some cities will not be able to manage these changes and will experience civil unrest. Impacts may be felt regionally or globally, and may affect U.S. national security. Densely populated areas around the world face greater risk of infrastructure breakdown, disease outbreaks, weather disasters, or attack—all situations that could stimulate U.S. involvement and divert attention and resources from our own infrastructure issues.

3. Condition of Infrastructure

Significant portions of our national infrastructure, from rail to road to water systems, are rapidly deteriorating. At the same time, trends in population, urbanization, and economic integration will increase demands and interdependencies on this already weakening infrastructure. The growing demands in turn exacerbate the deterioration, as well as the challenge of

"The basic fundamental infrastructure in the country is in decline... It is a house with a weak foundation. Adding technology, processes, and protection systems to a weak foundation can still result in the house collapsing."

~ Toffler Associates Interview

maintaining and repairing the infrastructure to stave off this decline, in an increasingly "spiral" pattern. Over the next 20 years, the maintenance, repair, and replacement of aging bridges, roads, railways, and other infrastructure will require substantial investments to ensure the functioning of our society and economy. In the U.S., the American Society of Civil Engineers (ASCE) estimates that addressing the immediate shortcomings in maintenance and repair will require \$1.6 trillion over the next five

years.¹⁰ Routine investment in maintenance will be necessary to avoid failures or disruption of services, and will require a concerted effort among business, government, and citizens. Not only will a significant infrastructure failure from deterioration prevent the delivery of critical goods and services, such as water, food or energy, it will also allow adversaries to exploit new vulnerabilities in our society—such as cities unable to evacuate effectively as congested highways, tunnels or bridges fail, with potentially catastrophic impacts on human life.

Railway and highway capacity shortfalls illustrate two areas where the physical condition of infrastructure is declining while reliance on that same infrastructure is increasing—causing already strained systems to become even more brittle. Freight rail tonnage is expected to increase at least 50 percent by 2020, requiring an investment of \$12-\$13 billion per year over 20 years to address capacity issues. Although there are currently no plans for a major increase in the nation’s rail capacity, passenger rail is expected to double in the next 20 years and triple within the next 50 years.¹¹ Similarly, of the 257 locks on the more than 12,000 miles of inland waterways operated by the U.S. Army Corps of Engineers, nearly 50 percent are functionally obsolete now and by 2020, 80 percent will be. The cost to replace the locks is more than \$125 billion.¹²

Like rail, the demand on our network of highways already exceeds supply. Between 1980 and 2000, vehicle miles traveled (VMT) on U.S. roads increased

80 percent while lane miles of public roads increased only 2 percent. By 2020, at least 40 percent of urban highways will be congested or approaching congestion during peak periods. In addition, experts expect heavy truck VMT increases of 3 percent annually. Air travel is expected to grow 4.3 percent annually through 2015, but America’s aging airports and related infrastructure are not expected to keep pace with the rise in demand. Another real concern that highlights the same problem of deterioration with rising demand is the fact that existing transmission facilities on the national energy grid are not designed for the current level of demand, not to mention future demand. We are already seeing an increased risk of

blackouts and increased costs to upgrade facilities.

The effects of this deteriorating infrastructure in the U.S. are far reaching. If domestic infrastructure

is unable to meet the needs of the economy it will influence the U.S.’s relative competitiveness worldwide. Many other countries globally face similar challenges due to deteriorating infrastructure. As the world becomes increasingly interdependent, deteriorating infrastructure systems in other countries will have spillover effects on the U.S.

4. Disruptive Technologies

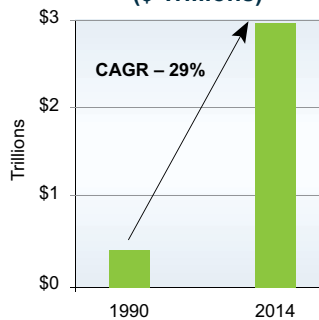
Another condition that will affect future infrastructure is the emergence of disruptive technologies. Disruptive technologies “disrupt” or alter the economy either positively or negatively (and in some cases

“In the national transportation area, we have gone from an agile transportation system to one that it is almost at a bottle neck right now - and in 15 years we could be driving to a halt there.”

~ Toffler Associates Interview

both). Radio, television, and the Internet are familiar examples of disruptive technologies—they have changed the way we work and live, and part of their effect is how they have added new definitions of what is “critical infrastructure.” Not all disruptive technologies are new technologies. Some may be old technologies applied in new or asymmetrical ways. For example, improvised explosive devices (IEDs) can be assembled anywhere with materials acquired from almost any hardware store. When applied with remote detonators and information shared over the Internet, IEDs represent “old” technology combined with new into a devastating weapon with strategic disruptive effects.

Revenue from Products Incorporating Nanotechnology (\$ Trillions)



Source: Lux Research Nanomaterials Forecast January 2007

Future advances in computer chip processing, bandwidth, and data storage will continue to produce revolutionary technologies and products that will disrupt entire societies, and those societies’ infrastructures. By 2018, we will see nearly 10 billion transistors per chip—permitting the creation of sensors too small to see—with PC processing capabilities approaching that of today’s super computers.¹³ Bandwidth will continue to double every 18-24 months, and data storage will become essentially free. Such advances will enable previously unimaginable abilities to monitor infrastructure

conditions and security—a “good disruption”—but they can provide enemies unprecedented new abilities to threaten our infrastructure as well.

Other technological developments will contribute to the emergence of disruptive technologies that will transform infrastructure. For instance, nanotechnology—a technology area that makes products miniscule, lighter, stronger, less expensive and more precise—show promise to develop “smart” and stronger structural components for bridges that make them stronger and last longer. These dramatic increases in miniaturization and functionality will expand the range of devices and applications in sectors ranging from computing and telecommunications to defense and healthcare.

But in addition to such beneficial disruptive uses, adversaries may apply nanotechnologies to weapon development which could seriously disrupt a country’s military, society, and economy, and cause human suffering on a large scale. Additional aspects of nanotechnology include:

- Benefits for criminal terrorist activity from smaller, more capable weapons.
- Unprecedented privacy invasions from small, widely available, cheap surveillance devices.
- Widespread microscopic litter of cheap microscopic products, with possible environmental or health consequences.

Similarly, advances in biotechnology—technology based on biology and used in agriculture, food science, and medicine—will present significant benefits and pose significant risks in the future. The life sciences will inevitably use biotechnology to create new opportunities for curing disease, but there is also the increased risk of bioterrorism because the technologies are widely dispersed, easily accessible, and increasingly global.

Biotechnology-enabled threats to infrastructure include:

- Accidental or intentional release of genetically modified organisms that have serious adverse consequences for the biosphere.
- Use of biotechnology to build new kinds of biological weapons of mass destruction.
- Easy access to biotechnology information through the Internet makes bio-weapons widely available.

We need to monitor “wild card” disruptions too. For example, some scientists believe quantum computing will be available on a large scale within 20 years. The potential impacts are significant, and can range from changing computing as we know it to changing how IT security is conducted worldwide. Other potential disruptive technologies include regular use of and “living” in virtual worlds; emergence of neural networks (networks that mimic the architecture of the human brain); the potential of regular space travel; and other things we may consider science fiction today.

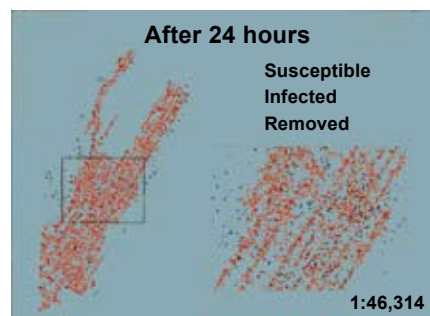
As the IED example suggests, not only will new technologies disrupt our way of life, it is also likely that familiar technologies used in new ways will fundamentally change the way we interact with our environment. For example, wireless technologies combined in new ways with explosives or biological agents and sensors, could pose new threats to the infrastructure. At the same time there will also be technologies—old or new—that cause positive disruptions that may help us strengthen, and protect infrastructure, or manage risk.

Typically, private industry and academia view disruptive technologies as potentially positive, while government must often identify potential dangers. A challenge for the U.S. will be to make the best use of its knowledge about existing and new technologies to ensure they make positive contributions to our society—and introduce as little vulnerability as possible.

5. Reliance on Cyberspace

While disruptive information technology advances will pose challenges and create opportunities for infrastructure protection, our growing reliance on information and communication technologies will present different issues to consider. Although cyberspace is already a part of our daily lives, its influence on the American way of life—including infrastructure—grows exponentially every day. Over the next 20 years we will become more reliant on our cyber systems for communication, commerce, government, transportation, and almost every aspect of every day life. Cyber is a critical dimension of every infrastructure sector.

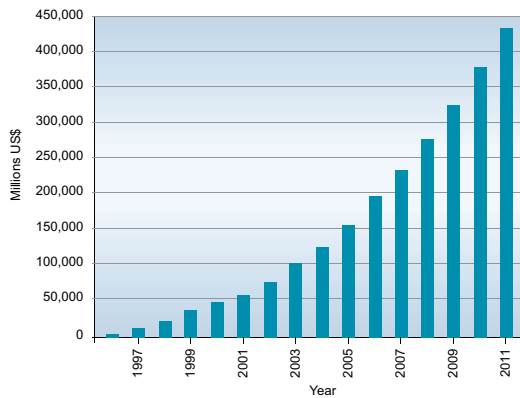
Malware Takes Manhattan



A map of a simulated Wi-Fi worm attack on Manhattan shows that 42 percent of the city's 36,807 known routers would be infected within the first 24 hours

Source: Hao Hu/Indiana University School of Informatics

Expected Intelligent Transportation Systems Worldwide Sales



Source: Transport Canada

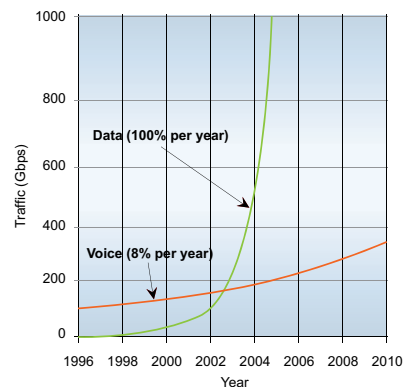
Information and technology will enable a “smart” or more computer-controlled infrastructure and smarter protection of it. Networked computer systems will permit more intelligent coordination among sectors of the economy, but exacerbate the challenge of managing interdependencies among these sectors. On one hand, open, dense electronic interconnections between people and organizations promise immense value. On the other hand, many open interconnections expose organizations to risks that could reduce their future value and effectiveness. For example, computer malware will spread in new ways. While it is still hypothetical, researchers are examining the possibility of localized Wi-Fi outbreaks, where viruses jump from Wi-Fi connected computers, as opposed to traditional viruses spreading through the Internet.¹⁴

Data storage demand combined with nano-engineering and molecular science advances suggest that computing devices will continue to shrink—some to the size of a dust speck—which will lead to even more innovative cyber devices to make daily tasks more efficient. Wireless devices implanted in humans will continuously monitor their health, enabling the medical profession to diagnose and treat many diseases in their infancy.¹⁵ As our dependence on

such devices becomes so engrained that they are taken for granted, they become part of the critical infrastructure we must protect. Similarly, technologies that virtually take control of vehicles on highways—such as Automated Highway Systems (AHS) and Intelligent Transportation Systems (ITS)—will continue to advance. However, concerns over the safety and ethics of external control systems suggest that AHS will develop first in niche markets such as the bus and trucking industries within the next 20 years.

With these developments, we must also understand how adversaries may use such technologies to create disruption, panic or death. Supervisory Control and Data Acquisition Systems (SCADA) will become more sophisticated and will control increasingly more complex systems of systems. We will rely on SCADA systems to monitor and control critical infrastructure functions which, if shut down or are comprised, could result in chaos.

Growth in Data Traffic



Source: Advanced Network Architecture Lab

Our dependence on the Internet juxtaposed with the potential use of it by adversaries makes its pervasiveness a double-edged sword. An association of chief executive officers, The Business Roundtable, suggests there is a 10 to 20 percent chance of a “breakdown of the critical information infrastructure”

in the next ten years, brought on by “malicious code, coding error, natural disasters, [or] attacks by terrorists and other adversaries.”¹⁶ In addition to cyber attacks, routine uses of the Internet by terrorists, for example, as a tool for communication, education, propaganda, fundraising, and cyber attacks will continue to be a pervasive threat. As it becomes harder to detect malicious software and to combat sophisticated cyber capabilities, future attacks will be increasingly aimed at the integrity of information such as financial transactions, health records, military movements or public works.

6. Ubiquitous Situational Awareness

The convergence of sensor technologies and wireless networking will give many people, both good and bad, unprecedented situational awareness about our critical infrastructure—that is, knowledge of the environment surrounding an infrastructure that is critical to decision makers. The continuing development of wireless technologies and networks will soon result in 24/7 data access around the world. A nearly ubiquitous broadband wireless architecture for electronic telecommunications devices may be available globally by 2015. By 2020, multiple network architectures will offer users nearly ubiquitous access—through high-bandwidth digital voice, text, graphic data, and media communications

“Once the plumbing is available, you can deploy sensors everywhere. It’s easy.”

~ Toffler Associates Interview

“We need to think about—as systems become more dependent on technology and become more centralized they will become more vulnerable. Do we worry about a driverless vehicle system the way we think of the current one? There is the potential for mischief or mayhem.”

~ Toffler Associates Interview

services—to information about our infrastructure and its security that once was very closely held and which remains highly sensitive.¹⁷

Advances in radio frequency identification (RFID) technology—which uniquely identifies and tags physical objects such as products, animals, or people using radio waves—already are used in many areas, from military to industrial. A much more pervasive use of RFID tagging systems is expected by 2015. In that same timeframe, entire systems, such as satellites and automated laboratory processing equipment, will be built with integrated micro-scale components at a fraction of the cost of current macro-scale systems, revolutionizing our ability to monitor a variety of

infrastructure systems.

Wireless networks that communicate with sensors will be prevalent across the country, allowing almost anyone to deploy largely

undetectable “spy” sensors that enable them to know whatever they wish to know about our infrastructure. While these and other advancements in surveillance technology (for example, face recognition technology, and the ability of commercial systems, such as GM’s On-Star, to track upwards of 1.5 million cars globally)

have the potential to enhance security capabilities, they also have the potential to aid adversaries.¹⁸

The nature and degree of situational awareness that will come from these and other technology advances will enable us

to do more in the infrastructure arena than just better monitoring. For example, nanotechnology-based sensors that can be embedded in “smart” concrete, bricks and other building blocks of our infrastructure will enable us to use temperature readings to improve occupant comfort in buildings, track the movement of people within buildings, monitor structural integrity, reduce energy use, and reduce the downtime of manufacturing machinery. New authentication approaches will allow users to move from one online site to another with a single sign on, improving protection of privacy and identification.¹⁹

Sensor proliferation and technological development will enable governments and citizens to monitor a wide range of activity around our critical infrastructure in real time—an inherent benefit. What is less appreciated, but could be just as important, is how the knowledge that actions are being tracked might influence the behavior of those who have influence over our future infrastructure—by either promoting desired behavior on the part of those responsible for ensuring security, or by deterring the undesired behavior of potential attackers. At the same time, we must be mindful of the flip side of the impact that ubiquitous situational awareness can have on those in position to influence our infrastructure.

For example, issues of privacy and security will emerge to affect how we collect and use the information that our revolutionary new sensor capabilities provide. This in turn will enable us to do certain things with respect to infrastructure protection

that we cannot do today, and inhibit us from doing other things that we may wish to do. And technology advances can, and almost certainly will, be used to counter the information sharing and consequent situational awareness that future sensor advances can provide. For example, the potential of quantum technology to encrypt data and improve computing may enable “unbreakable” coded transmissions among adversaries, impossible for government or individuals to intercept.²⁰

In addition, more communication channels will increase the volume of information to be managed. This will drive further developments in storage technologies. It will also drive advanced IT systems that can turn a significant increase in data into useful information from which better decisions can be made.

“There are systems to let us know where the trains are and we want to keep this secure. There are automated systems and we will continue getting into this ... someone can control them if they want to. We have to make sure they are secure.”

~ Toffler Associates Interview

All the information that comes from our immense future situational awareness can be used to avert potential infrastructure disruptions—such as the use of sensors to continually monitor drinking water quality,

detect structural damage in buildings and vehicles, etc. It can also be used to heighten national security, given the security protocols that are likely to emerge. However, this information can also support malicious actors, opening up an entire world of data that until recently did not exist. Unless infrastructure owners and operators and policy makers are able to anticipate the vulnerabilities introduced by ubiquitous situational awareness, this condition will allow adversaries access to sensitive infrastructure

information. Some examples of potential future threats include:

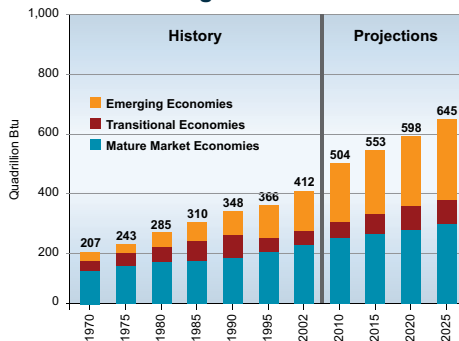
- As part of a multi-tiered attack, a terrorist group gains control of sensor networks on a dam in Arizona, a bridge in San Francisco and a skyscraper in New York, then shuts down the sensors, “blinding” law enforcement.
- A foreign intelligence organization or NGO accesses a sensor network in a stealth-like manner to learn more about U.S. capabilities and vulnerabilities.
- A terrorist organization accesses or monitors infrastructure sensor information to determine which bridges or tunnels are most susceptible to a devastating attack.
- An adversary monitors an open sensor system or gains access to a secure sensor system so they can precisely track individuals or groups they plan to attack.

7. Blurred National Borders

As the U.S. becomes more connected to the global economy the distinction between domestic and foreign infrastructure is increasingly unclear. The blurring of economic and physical borders will force us to consider how our critical infrastructure will be affected by forces outside of the U.S. and to rethink our approach to securing it. As we depend more on the global supply chain, our security increasingly will depend on infrastructures in other countries that are owned and controlled by foreign entities. Our lack of direct control could limit our ability to protect such infrastructures, for example, a foreign-owned-and-located factory that provides a particular part or software code, or cyber storage facilities. The reverse is true as well, that is, we will have U.S.-owned infrastructure assets that are critical to our society and economy that reside in foreign countries, and whose security we might not be able to directly

control. There are foreign-owned institutions in the U.S. today and the U.S. owns assets abroad, but it will be more widespread and commonplace in the future. In addition, distinctions about what needs protection and how to protect it will become more blurred.

World Marketed Energy Consumption by Region 1970-2025

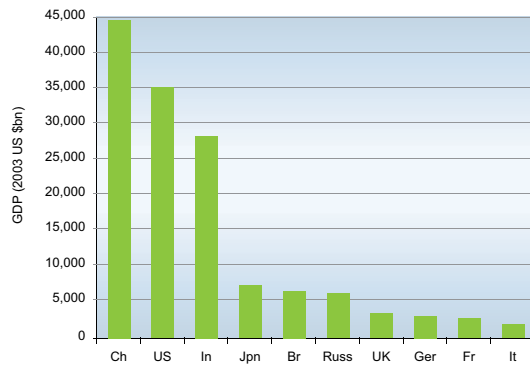


Source: Energy Information Administration

The U.S. highly values foreign investment in many areas including infrastructure. However, as more infrastructure is owned by foreign entities, we must ensure that these entities implement protections for the infrastructures they own, particularly those infrastructures that if disrupted could cause grave harm to our citizens and our economy. In the worst case scenario, foreign ownership could mean unvetted foreign employees have access to U.S. networks or other types of infrastructures that can be degraded or manipulated by individuals or groups that wish our nation harm.

Domestic U.S. infrastructures will become more connected to international infrastructures as a result of outsourcing, the growth of multi-national corporations, and the growth of other economies. This rise of globalization and international collaboration will create yet more closely interconnected infrastructures systems, each containing sensitive information about the other.

The Largest Economies in 2050



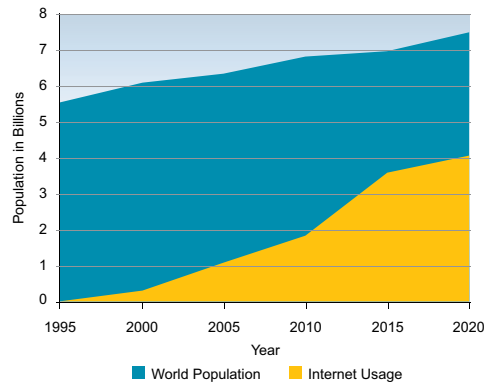
Source: Goldman Sachs. Dreaming with BRICs: The Path to 2050

With increasingly blurred borders, the U.S. will depend more on international trade, which will put more stress and strain on the infrastructure that supports and enables that commerce, and exposing it to new threats. For example, maritime trade is expected to double by 2020, resulting in greater pressure and congestion on the nation's ports, and waterways, and distribution systems. Rising international trade will increase the amount of goods entering the U.S. through our ports and strain domestic transportation systems, and it is projected that trade with Asian-Pacific and Latin American countries will increase more than with other world regions. As a result, efficient maritime transportation will become more critical to America's economy and competitiveness, and more difficult to secure because our inland and coastal commerce routes will experience increased barge and tow traffic. Just-in-time delivery of raw materials and finished goods will become the norm, magnifying the consequences of disruptions and placing greater importance on the reliability of our marine transportation system.

As physical borders between countries blur, goods, people and information will flow easily among them, making protection of the international information and communications technology infrastructure

immensely important. Unfortunately, because that infrastructure crosses borders and is owned and operated by many different actors, responsibilities for protecting it will become an increasingly difficult question to answer clearly. Multi-national corporations and non-national civil organizations will gain influence as Internet communications and globalization will fuel these exchanges, making physical distance less relevant. At the same time, global financial, energy, environmental and other systems will be increasingly interconnected. Such closely integrated systems may be vulnerable to attacks, which could cause a domino effect as changes to the integrity or robustness of any one of these systems will have an impact on others.²¹ Similarly, crime will be more globalized as individuals and groups operate in the cracks between laws and gain access to knowledge and technology that makes them more powerful than today.

Growth of World Population and Internet Usage



Source: AMD Smarter Choice

8. Hyper-Empowered Individuals and Groups

In the future, individuals and groups will continue to attain greater access to worldwide sources of knowledge, technology, and finances formerly achievable only by nation-states, and will use it to influence economies and societies, and the

infrastructure on which they rely. These “hyper-empowered” individuals and small groups will have a greater ability to affect the global infrastructure in positive and negative ways. We have already seen numerous manifestations of this effect. For example, French bank Société Générale trader Jerome Kerviel ran up \$7 billion in trading losses. An individual like Bill Gates, through his Bill and Melinda Gates Foundation, has affected positive change throughout the world, including making significant investments in critical infrastructure for domestic and international healthcare and cyber infrastructures in places from North America to Africa and beyond.

Increased access to resources, people, information and control systems will give individual and small groups of adversaries more power as they pursue their goals.

Individuals and small groups likely will increase their efforts to acquire chemical, biological, and nuclear weapons; manipulate information systems; disrupt response systems; halt public services; disable security systems; gain intelligence; and compromise the public trust. These efforts will increasingly succeed thanks to the rapid and largely unregulated flow of information throughout the world via the Internet and other means. User-friendly protocols and interconnected systems will allow individuals the opportunity to manipulate critical information and resources. Overall, these and other resources will allow individuals and small groups of adversaries to be more sophisticated in their attacks on global infrastructure. And the criminal or terrorist of tomorrow may also be different: instead of a global organization like Al Qaeda staging an event, a

four-person clique of school-age hackers might take down a critical portion of infrastructure “just for fun”; and a new, small virtual coalition of people might attack because of social, environmental, political and economical grievances they may have. In addition, insider/individual threats may grow to be more common.

Terrorists currently focused on producing single, dramatic events will be able to launch more strategic, disruptive attacks on interconnected systems. As

attacks are strategically aimed at disrupting systems and supply chains, there will be more significant second- and third-order effects of incidents perpetrated by groups that are ever-smaller and thus ever more difficult to track and thwart. Where a terrorist today might attack a train station or school aimed at instantly

“The war against terror has triggered another conflict with important implications: a war of pyramids vs. pancakes. The United States and Al Qaeda are seen as unevenly matched, which is why think-tank experts and TV pundits call the conflict “asymmetric.” In fact, Al Qaeda’s strength derives precisely from the fact that it is small, fast, flexible and pancake-flat, while the American government is huge, slow, sclerotic and pyramidal.”

~ Alvin Toffler

killing many, attacks may become more strategic in the future—destroying an asset that supplies critical food, water, or energy to thousands of people. The economic and psychological implications—not to mention the loss of life—could far exceed those of today’s attacks.

Those charged with protecting domestic infrastructure are largely accustomed to a given set of threats—threats that are easily discernible by their size, patterns of behavior, and dependence on the resources and trappings of nation-states or other organized entities. As hyper-empowered individuals and groups gain power, however, the “identity” of those threats will change. Infrastructure owners, operators and stakeholders will have to account for changes in their environment that are being caused

by benevolent, disruptive, or even malicious groups we don't yet know—who may not even have formed as a group—and whose effects will demand that we quickly learn who they are and pay attention to what they can do.

creative ways to take down or disrupt infrastructures. Many adversaries will learn how to attack infrastructures through simple means such as data gathered from the Internet, including information on how to build biological, explosive, and other weapons.

Sample Assessment of Threat from Known Terrorist Groups

Terrorist Group	Ideology	Sophistication			Weapons			Resources	
		Network	ISR	CS2	WMD	Bomb	Arms	Personnel	Funds
Al-Qaeda	High	High	High	High	High	High	High	High	High
Hezbollah	High	High	High	High	Low	High	High	High	High
Yemen Islamic Jihad	Moderate	High	High	High	Low	High	Moderate	High	High
Mujahedin -e Khalq Organization	Moderate	High	Moderate	High	Low	High	High	High	High
Aryan Nations	Moderate	High	High	High	Low	High	Moderate	Moderate	Moderate
Aryan Resistance Army	Moderate	High	High	High	Low	High	Moderate	Moderate	Moderate
Al-Fuqra	High	High	High	High	Low	High	Moderate	Low	Moderate
Cambodian Freedom Fighters	Low	Moderate	Low	Low	Low	High	High	Low	Moderate
Ku Klux Klan	Moderate	High	Low	Low	Low	High	Low	Moderate	Moderate
American Front	High	Moderate	Low	Low	Low	Low	Low	Low	Low
Army of God	Low	Moderate	Low	Low	Low	Moderate	Low	Moderate	Low
Hammerskin Nation	Low	Moderate	Low	Low	Low	Low	Low	Low	Moderate
Animal Liberation Front	Low	Moderate	Moderate	Low	Low	Low	Low	Low	Low
Jewish Defense League	Low	Low	Low	Low	Low	Moderate	Low	Low	Low
Earth Liberation Front	Low	Moderate	Low	Low	Low	Low	Low	Low	Low
Coalition to Save the Preserves	Low	Low	Low	Low	Low	Low	Low	Low	Low

Toffler Associates Analysis

■ High Threat ■ Moderate Threat ■ Low Threat

The chart above depicts a rough assessment, based on Toffler Associates analysis, of the current threats posed by *known* terrorist entities, according to what we know about them *today*. The picture is concerning enough as it stands, but we must realize that some of these groups may still exist in the future, some will disappear to be replaced with new international or home-grown adversaries, and some new ones will emerge that we cannot yet foresee.

We can expect adversaries such as those listed above, as well as the potential new groups of adversaries, to target for attack the most populated areas with the most stressed infrastructures. Experts also indicate that we can expect more asymmetrical threats as future terrorists use inexpensive and

And perhaps one of the most menacing adversaries in the future may be the insider threat: the person who has special access to a facility and the ability to, for example, modify software to take down a cyber infrastructure or detonate a large explosive inside a chemical plant.

9. Legal and Regulatory Environment

Evolutionary and revolutionary changes to our technological, economic and social fabric will force changes in the laws and regulations for infrastructure protection. Because technology will develop rapidly, the process of regulating it will become more challenging as governments struggle to keep up with a changing IT environment.

Tight controls governing what we can do in the name of infrastructure protection are vital, but our adversaries will not be bound by our rule of law or the time constraints inherent in large bureaucracies. Adversaries will have new sources of information and new technologies with which to exploit it. Meanwhile, governments will have to first develop policies and devote resources to balancing access to this data with the protection of individual privacy. In developing policies and resources, governments will be compelled to leverage the skills and resources of intermediary bodies—such as banks, ISPs and software vendors—to protect the public from malware, hacking and social engineering.

Further, as the U.S. becomes more connected to the global supply chain, it increasingly will be affected by international laws and a variety of regulations associated with international relations, standards and trade. Also, as other nations benefit from the economic, technological, military and political aspects of globalization, they will seek more power in, and exert greater influence on, international bodies such as the United Nations. International standards and regulations will take on a less Western quality because most of the increase in world population and consumer demand will be in China, India and other more rapidly developing nations. Already we can see interest-rate decisions made by Asian central bankers having greater impact on global financial markets, while the returns from Asian stock markets are likely

“We will be constrained by privacy issues, and the bad guys will not. There needs to be research about how to handle the privacy environment for data so we can understand how to use data and technology for good purposes.”

~ Toffler Associates Interview

to become a global benchmark. Analogous effects in other infrastructure sectors are easy to foresee, but their impacts will be difficult to discern for some time.

Laws and regulations that are not directly related to infrastructure or infrastructure protection at all will nonetheless have a significant impact on our future ability to secure the assets most vital to our nation. For example, mandatory spending in the federal budget—on Social Security, Medicare, Medicaid and debt interest—is rising faster than the gross domestic product (GDP), and there are an increasing number of complex laws and regulations that will

determine what we can and can't do with our national treasury. Without fundamental restructuring, federal discretionary spending will remain in a downward spiral, thus putting at further risk our ability to make

the investments we need in critical infrastructure protection. By 2018, mandatory federal spending will consume 1.5 percent more of the GDP than it does today (assuming a 4.5 percent GDP growth). In addition, the number of Social Security recipients will grow by 30 percent between 2007 and 2018, and Medicare recipients will grow by 42 percent. An expected decline in mandatory spending in 2012 assumes Congress allows the tax credits authorized since 2001 to expire. However, tax credits could increase spending projections, forcing Congress and the President to increase taxes or the national debt.²²

Private corporations are likely to play an increased role in traditionally public domains, including infrastructure protection, but the public does not necessarily trust corporations to be socially responsible. Companies are rethinking the role they should play in society and working to improve their corporate social responsibility (CSR). Climate change and other shocks to our environment and society will drive CSR in substantial and unpredictable ways in the future. CSR will improve, but it will improve inconsistently across sectors, depending on a company's economic performance, economic downturns, the competitiveness of its market, and other factors.

The need to be “green,” transparent, and socially responsible in other ways, will change the operation and regulation of our future infrastructure by civil

society, corporations and government. To meet the rising expectations of the public, companies will be challenged to find innovative ways to resolve social, environmental, infrastructure, and other problems. Corporations will be compelled to focus simultaneously on “the People, the Planet, and Profits”²³ in order to balance social, environmental, and economic factors to achieve short- and long-term performance goals for their companies. Mega corporations will work at decreasing the impact of their operations on our infrastructure—such as using less electricity or fuel—influencing others to do the same.

“Some less developed countries that have benefited [from globalization] are now in position to weigh in and will seek more power in international bodies and greater influence on the ‘rules of the game.’”

~ Toffler Associates Interview

In a world of accelerating change, finding ways to maintain useful checks and balances while ensuring a secure future for people promises to be a significant challenge for governments. The government will continue to find it difficult to keep up with the pace of change. Most government institutions and structures were built to support our industrial era society. In our current knowledge era, characterized by rapid change, networked structures and information and knowledge generation, we need government structures that support how society operates. The inability of government structures to keep pace with how rapidly and unpredictably business and society

are changing causes a “desynchronization” between the government and the private sector, and affects our ability to protect critical infrastructure.

Global coalitions of nation-states, technology companies, and academia all have knowledge that can help advance protection of the infrastructure and ultimately of society. By building relationships with other players in the global system, and strengthening state and local relationships, governments can address challenges by sharing knowledge with a wide range of partners.



Convergences and Implications

The nine conditions described in the preceding pages are not “what if’s.” They are the reality of the future. We *will* see new technologies emerge that will disrupt how we’ve traditionally lived our lives and done business. We *will* see a growing number of business, communication and other connections among nations that will “blur” the borders that separate us. We will see weather patterns change, and new laws replace old ones, and a continuing movement of individuals from one part of the country and the world to another. What we don’t know is how each change in these conditions will manifest itself. We can’t predict exactly what the most revolutionary new technologies will be, or exactly what the new laws will allow, or how they will proscribe undesirable behaviors. But we can be confident that change in all nine of these areas will be significant, and in some cases rapid and dramatic. And we can be confident that changes in these nine areas will have a significant impact on our infrastructure upon which our nation relies, that is, on the assets we need, on how we protect those assets, and on whom we rely to ensure the integrity and continuous operation of those assets.

Even more importantly, changes in all nine of these areas will be simultaneous and convergent, meaning that changes in one will stimulate changes in others. It will be difficult to discern these changes and to prepare to manage them effectively. Anticipating and preparing for convergences will be the primary challenges for those protecting our critical infrastructure in the 21st century. We can, and must, do the rigorous and creative thinking that will provide insight into the unknown, for example:

- How urbanization and cyber developments might accelerate the development of “hyper-empowered” groups of adversaries and provide them “settings” in which to practice their tactics and strategies for attacking our infrastructure.
- How blind spots in our current laws and regulations might enable a powerful new “disruptive” weapon technology developed in one country to flow easily into our own.
- How changing weather and climate patterns might drive people to move to places that offer better protection from the elements—but where the local infrastructure is already at the breaking point and unable to withstand a surge in usage.

“We have not done enough to understand the interdependencies and how to deal with the problems that result. We learn from events – but we don’t appreciate the interdependencies.”

~ Toffler Associates Interview

- How wireless cyber technologies may enable future terrorists to kill significant numbers of Americans in an urban area by remotely shocking their medically implanted devices such as pacemakers or defibrillators.

Convergences like these are the “what-if’s” that those responsible for critical infrastructure protection must consider. Many of them are already suggested in the pages above. What can we do to secure ourselves in a future where new infrastructure innovations like Intelligent Highway Systems emerge alongside terrorists increasingly adept at hacking into such

IT systems to cause injuries, chaos, and diminished public trust? What can we do to improve the state of today’s infrastructure in large Western cities before millions more Americans migrate to

them, including older, retiring Americans who rely more on infrastructure such as public transit and health care systems? What can we do to anticipate which laws, regulations, and bureaucratic processes will be most out of sync with the kinds of future actions we must take to protect our increasingly essential cyber-infrastructure?

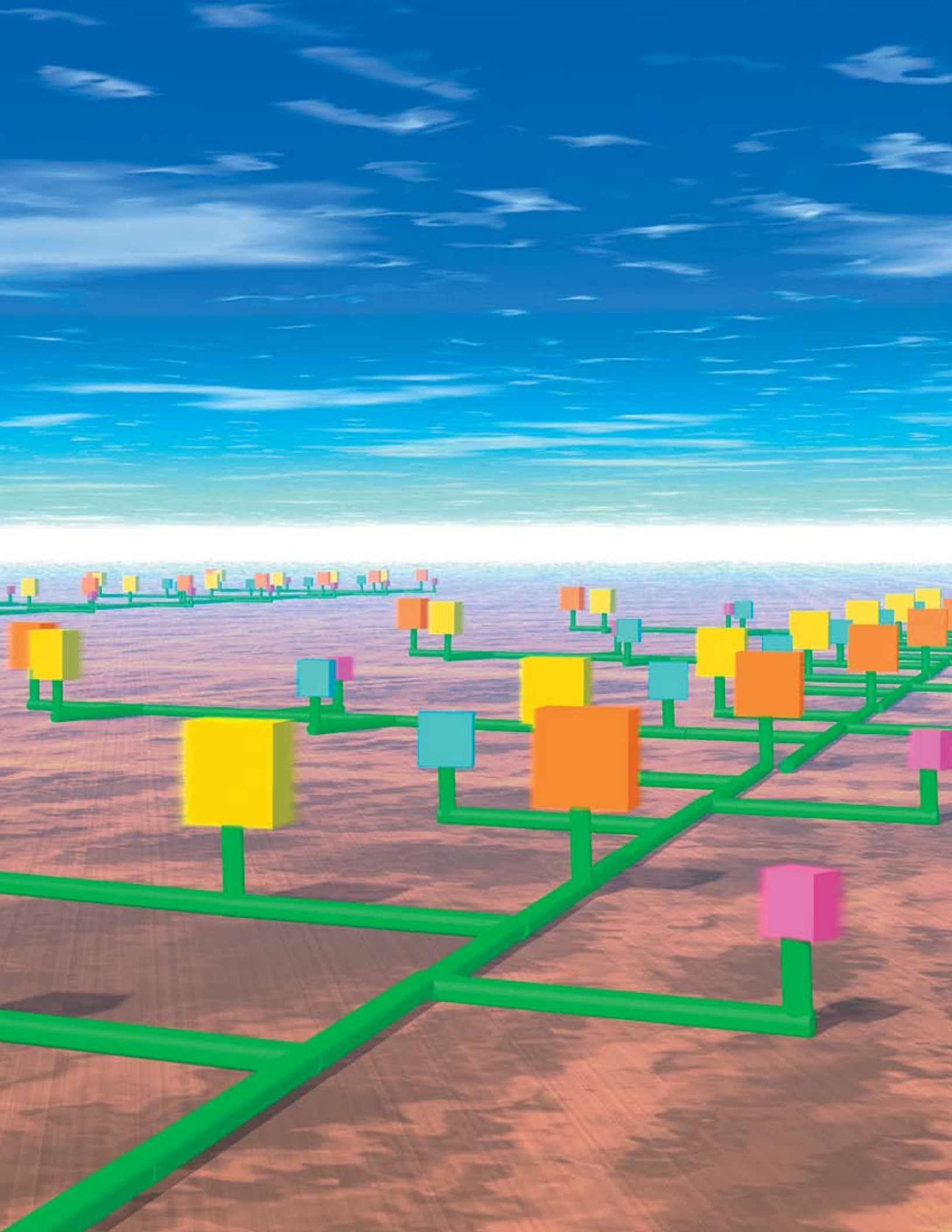
Analyzing and tracking the changes in any one of the nine conditions in isolation will not prepare us for the challenges we'll face in the future with respect to infrastructure protection. And no single convergence of changes in multiple conditions, however accurately projected, will capture the full scope of future developments. Only by taking a holistic approach can individuals and agencies anticipate the character of the nation's future infrastructure and the associated risks that may emerge.

The pace of societal change will accelerate and the threats we face will be decentralized. However, our government bureaucracies are not designed to adapt quickly to these and other convergences. Our government institutions' reflexes are slowed by decades-old policies and procedures that were effective in the Industrial Age, but represent roadblocks in a rapidly changing Information Age. In the future, in order to ensure the viability of our nation's infrastructure we need organizations, systems and strategies that are agile enough to out maneuver future threats, both manmade and natural.

There will be more and more global networking of critical infrastructure. Our state critical infrastructure will be tied in various ways to other states and other countries. You will need to be concerned about how they network with each other, the transportation systems, networking the critical infrastructure, the cyber links between the pieces of critical infrastructure. I believe interdependencies will become more sophisticated.

~ Toffler Associates Interview





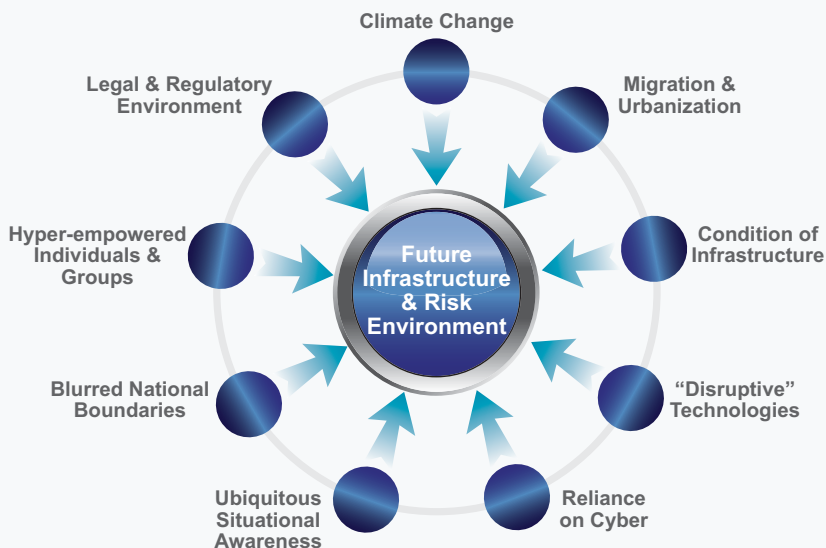
Eight Recommendations

DHS and its Office of Infrastructure Protection (DHS IP) have made significant progress in addressing and improving the nation's infrastructure protection in coordination with other government agencies and the private sector. But much more must be done to address the range of future challenges and complexities.








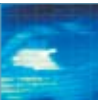
The conditions and convergences highlighted in this report will significantly affect the future infrastructure and thus the economic and physical security of our country. We must be proactive and act now to address how we sustain deteriorating legacy infrastructures while creating and implementing future infrastructures. We must create more urgency regarding national infrastructure protection. We must develop the risk assessments, flexible policies, budgets and structures to ensure we keep pace with rapid societal changes. We need additional incentives to encourage individuals and groups to identify innovative infrastructure solutions. And we need to proactively understand and stop the adversaries of the future from disrupting our emerging infrastructures. The cost to our country of not acting quickly will be enormous.

The following recommendations flow from the understanding that emerging infrastructure conditions will intersect in multiple ways, influenced by the nine conditions discussed earlier and the convergences among them, causing possibly devastating effects. By anticipating the kinds of issues and events that could occur, we will be better able to manage risk and protect the nation's critical infrastructure.

The recommendations address the impact of nine conditions on the future environment.



Eight Recommendations

ISSUE	RECOMMENDATION	
1) The nation doesn't see infrastructure protection as an urgent national priority	1) Make infrastructure protection a more urgent and clear national priority	
2) Emerging convergences will reshape how we define and prioritize infrastructures over the next 15 years	2) Prioritize and address what constitutes future "critical" infrastructure in the future	
3) We need strong cross-sector analysis and advisory capability to better understand impacts of emerging conditions and interdependencies	3) Establish a knowledge integration center to analyze, coordinate, and integrate the nation's knowledge about protecting our infrastructure	
4) Government institutions are unable to meet the needs of our rapidly changing society	4) Define and address where "desynchronization" affects the ability of the government to keep pace with infrastructure protection needs	
5) Infrastructure failures have widespread regional impact and involve many sectors	5) Understand impacts of the future interdependencies across all existing and emerging infrastructure sectors	
6) No single incentive will encourage all infrastructure stakeholders. Different incentives will apply to different types of infrastructures	6) Establish more innovative incentives for infrastructure protection	
7) There is a lack of understanding on how conditions, convergences and challenges will affect the emerging future infrastructure	7) Conduct cross-sector infrastructure-protection games and simulations to understand emerging challenges, interdependencies and future risks that would affect the NIPP and other key plans	
8) Adversaries make decisions and plan attacks much faster than our government	8) Get inside our adversaries' decision space to proactively stop future attacks on infrastructure	



Recommendation 1: Make infrastructure protection a more urgent and clear national priority.

The Issue: The nation doesn't see infrastructure protection as an urgent national priority. Those within the infrastructure environment do, but much more must be done to focus infrastructure protection as a priority in the nation's eyes. The viability of our country rests on our ability to fix our serious existing infrastructure problems and to rapidly adapt and develop new infrastructures to meet the future needs of our people, our businesses and our government institutions.

Although the Secretary of DHS has placed infrastructure protection as his number three priority, the program is not structured or resourced appropriately, and lacks sufficient authority to accomplish its mission. Better coordination among the many federal, state, local, and private sector entities charged with pieces of the mission, and a data-driven framework for assessing and funding risk mitigation measures across the entire infrastructure protection portfolio, are essential initial steps. For example, considerable resources have been expended on controlling ammonium nitrate, an important goal. What work has been done to ensure that the dollars spent reflect the value realized and

the relative priority of that threat against all of the other infrastructure threats the nation faces?

In June 2008 the mayors of the nation's largest cities told Congress that they are overwhelmed by the infrastructure needs in their regions, and that the \$1.6 trillion the American Society of Civil Engineers estimates is needed to fix current infrastructure problems is probably not enough even if it were to magically appear today. Too few of their constituents are aware of this assessment. And tomorrow's problems—increased population, expanded wireless and sensor systems, enhanced biotechnology, climate change, new types of terrorism, and other challenges—will require an even bigger investment.

Although we think the short-term costs for our infrastructure are immense, the cost of not acting now will be disastrous for our future, and that reality is not well understood. A strong bi-partisan private-public-NGO-foreign partnership is needed to make infrastructure protection one of the country's top priorities. Therefore, to help the nation make infrastructure protection a priority, we recommend the following:

a) **Create a panel on par with the 9/11 Commission to address our future infrastructure challenges.** Currently, many entities from across the government, including Congress, address infrastructure protection. However, there is little coordination or integration among them resulting in a patchwork of suboptimal rules and regulations that the private sector often finds bewildering, expensive to implement, and less effective than desired. A forward-looking, private/public panel that can assess the entire scope of infrastructure protection efforts is needed to make

vivid in the minds of all Americans the pressing future critical infrastructure challenges.

This panel should: 1) define the appropriate role of the government and the private sector in protecting our future infrastructure; 2) recommend how to integrate the efforts across the government to determine budgets and prioritize future infrastructure spending holistically across sectors; 3) recommend specific legislative changes that enable organizations such as DHS to have the flexibility in creating policies and procedures to respond to the rapidly changing needs of the public and private sectors. Potential legislative changes could include, for example, creating multi-year versus annual budget cycles for government infrastructure protection funding to allow longer term focus by organizations such as DHS IP. A more integrated approach would enable laws and regulations to focus more on outcomes than on processes and would foster more innovative approaches to protection.

A national panel commands attention and educates the public on the value of data-driven, risk based infrastructure protection. The panel can support and focus work DHS is already conducting in specific areas, addressing some of the critical convergences we expect in the next 15 years. It would help define for Americans the roles of the government, NGOs and the private sector and make clear to them the importance of integrating the efforts of all these entities. In addition, such a panel may assist by helping to rationalize the infrastructure funding process within DHS and in Congress and helping Americans understand the critical benefits that will come from doing so.

Although existing DHS and other government agencies would respond to many emerging conditions, a panel such as the one proposed would be uniquely positioned to assess complex or cross-cutting issues that government has not yet adequately addressed and the public has not yet adequately appreciated. Some examples include:

- What are the impacts of increased urbanization and migration in areas of increased risk, such as cities on earthquake faults and flood plains?
- What are the most significant impacts that climate change will have on the nation's infrastructure?
- What protection or risk assessments are required to support emerging infrastructure sectors such as cyber or biotech?
- What are the specific impacts of a ubiquitous sensor environment on privacy concerns?
- What new, emerging conditions demand attention before they compromise critical infrastructure or national security?

b) Update and enhance Presidential directive HSPD-7 to indicate the urgency and priority of addressing emerging future infrastructure challenges. A Presidential directive associated with infrastructure protection exists but it should be revised and updated to reflect the importance of planning for and addressing future infrastructure issues including managing the risk of converging conditions that will shape and challenge infrastructure protection over the next 15 years. HSPD-7 (2003) established a national policy for federal agencies to identify and address CIKR protection issues. The Presidential directive is important; though it is not clear it focuses enough on the wide range of emerging conditions that

will impact the infrastructure. HSPD-7 primarily focuses on terrorist attacks associated with CIKR; *"...identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks..."* The directive does not focus on the other key dimensions of protection such as non-terrorist conditions including climate change, migration, urbanization, and deteriorating infrastructure. It also doesn't indicate the importance of understanding and protecting against emerging future threats, natural or manmade. Thus, we recommend that the 2003 directive be updated, or a new directive be developed that is more future focused and comprehensive to cover the full range of infrastructure protection challenges.

c) Implement a robust strategic CIKR protection communications campaign to indicate to all infrastructure owners and operators, the general public and foreign partners that critical infrastructure protection is one of the nation's most important challenges over the next decade. Currently, information and issues are primarily communicated via Presidential directives, DHS, associations, and the news media, but these forms of communication need to convey more of the momentum and urgency needed to make infrastructure protection a national priority. We should establish a public/private partnership council that works with public relations firms and others to create a national public service campaign to communicate the importance of CIKR protection. In conjunction with the partnership, we should create working groups at the state, local and private levels to work with infrastructure owners, operators, and users to communicate their role and what they can do to improve protection, now and in the future.

d) **Create a regional structure to better raise awareness of and address specific infrastructure protection needs.** Through the Panel or another venue, consider creating a regional structure for infrastructure protection to better meet needs at local levels. Regions across the country have different infrastructure needs; some are more flood prone, others more earthquake prone, and so on. Disruptions to one part of the infrastructure inevitably cascade first to other portions in the region. Include participants from the state, local, civil and corporate sectors in the region. Assess the value of structuring a portion of DHS IP responsibilities on regional levels similar to those of other government agencies such as FEMA, for example. A key purpose is improving awareness and understanding of regional issues and providing more tailored support to state, local and private owners, operators and overseers of infrastructure.

Another goal is to communicate about and manage infrastructure protection issues in a coordinated manner at a more local level. In time of crisis it makes sense that actions are coordinated at the levels affected and not just national levels. Regional control and coordination of infrastructure protection however should not be based on rigid boundary lines. Natural and manmade threats to infrastructure can cross regional boundaries so flexibility must be part of any regionalization approach.



Recommendation 2: Prioritize and address what constitutes “critical” infrastructure in the future.

Issue: As infrastructure changes in the future, so must infrastructure priorities change. Which critical infrastructures will require the greatest protection

in the future? It is a difficult question because some sectors will merge, morph and become more interdependent. But we know for example that most sectors will ride on a cyber backbone. We know that wireless technologies will evolve with advanced materials and ubiquitous sensor technologies enabling smart infrastructures such as smart highway systems and smart building materials. We know that biotechnologies and neurosciences will grow and converge with agriculture and communication systems to rapidly create new threats, challenges and opportunities. These and other convergences mean we need to rethink how we define and prioritize infrastructures over the next 15 years. Not everything will change, but enough will change that it will challenge and redefine much of what we consider to be critical in the future. Therefore we recommend:

a) **Define and address the next generation of sectors that will require protection in the future.** For example, will the development of human implanted medical devices that are connected via wireless networks create a new infrastructure sector that requires protection? In a world where so much is cyber-enabled, and sensors so ubiquitous, what does it mean to protect SCADA systems? Do SCADA systems become a new sector? Forecasting the emergence of new sectors becomes more difficult as some emerging technologies and environmental forces will occur sooner or later than predicted. However, by continuing to monitor developments in the conditions identified in this report, government and industry can look for signposts of emerging sectors that will need protection in the future.

b) **Facilitate enhanced thinking across academic, government and commercial organizations to develop prioritized frameworks that take into account the conditions and interdependencies that will affect future**

infrastructure. For example, approaches over the next decade must take into account climate change impacts, demographic migration patterns, banking and finance system changes, SCADA attacks, emergence of bio- and nano-technologies and many other conditions.

c) Create new capabilities to assess and prioritize future risks that emerge from the convergence of the factors we have discussed above. Significant portions of the transportation, water and other government-owned or -operated infrastructures are in need of significant repair or replacement. The government—with assistance from non-government organizations such as Sandia National Laboratory and the private sector—is already developing programs to formally evaluate and prioritize the infrastructures at most significant future risk. After mapping the most significant future risks, the government, NGOs, academic and commercial organizations should then consider the interdependencies and critical nodes in order to visualize the impact on critical infrastructures. Analysts will gain additional perspective by overlaying how adversaries might exploit the high-risk structures. After taking these steps, enhanced risk mitigation and communication approaches can be implemented to address the issues identified.

d) Create a private–public sector partnership that can bring the debate for infrastructure prioritization to local public forums. Major corporations may be aware of infrastructure risks and issues in their sectors, but medium and small businesses and the general public likely are not as aware of the importance of the issues. We should enlist the help of infrastructure owners and operators on local levels to help prioritize current and future risks in their local municipalities as well

as to determine what actions are required locally and federally to enhance CIKR protection in their communities.



Recommendation 3: Establish a knowledge integration center to analyze, coordinate, and integrate the nation’s knowledge about protecting our infrastructure.

Issue: In order to better understand the impacts and priorities of emerging conditions and interdependencies of the nation’s emerging infrastructure, there needs to be a strong **analysis and advisory capability across the infrastructure sectors.** This type of capability can help the public and private sectors better understand the impacts of future issues affecting critical infrastructure protection. Building on this concept, we recommend:

a) Develop a center that integrates the nation’s knowledge about infrastructure protection.

Many organizations already support government agencies. For example, DHS has the Homeland Security Institute that provides independent and objective analyses across DHS mission areas. A primary goal of a distinct infrastructure protection knowledge integration center will be to provide more significant CIKR analysis capabilities across federal agencies. A knowledge integration center can help the federal government and the private sector better understand the interdependencies and future conditions affecting critical infrastructure protection, and to identify and validate existing and emerging CIKR protection practices. One of the roles of this center could be to leverage capabilities and knowledge from the DoD, universities, and other organizations inside and outside of the U.S.

For example, range of DoD organizations have significant expertise, capabilities, knowledge and budgets for addressing military infrastructure issues. They are experts in many areas related to the protection of infrastructure assets, from planning and R&D to implementation and monitoring.



Recommendation 4: Define and address where “desynchronization” affects the ability of the government to keep pace with infrastructure protection needs.

Issue: The inability of the government bureaucracy to meet the needs of our rapidly changing society could likely create “institutional Katrinas” that could hamper operations and cascade from agency to agency. This, as indicated earlier in this report, is due to the government’s inability to keep pace with changes in society, a “desynchronization” between the government and the private sector, which compromises our ability to protect critical infrastructure. Although checks and balances were built into the government system deliberately, over time, society and business have changed at an accelerating rate, widening the gap between government and the governed. Federal agencies, for example, lock themselves into extremely complex planning and budgeting processes that may limit their ability to address rapidly emerging threats or to acquire newly emerging solutions. Decisions often require review and approval through multiple levels of bureaucracy—delays are compounded when decisions involve multiple agencies.

On the other hand, the private sector must respond quickly to competitive and market pressures or face irrelevance. Likewise, our adversaries have no such planning and budgeting limitation on their ability to

inflict harm, and push decision-making at the lowest possible level. DHS and other agencies charged with protecting national security are especially constrained by bureaucracy in today’s knowledge age where rapid response can mean life or death. Therefore, we recommend:

a) **Conduct two related desynchronization studies, one to assess vertical desynchronization and one to address horizontal desynchronization.** Vertical desynchronization refers to the differences in operating pace, or OPTEMPO, at different levels of hierarchy in an agency. Horizontal desynchronization refers to the differences in OPTEMPO, among agencies.

The vertical desynchronization study would answer questions like “How many hierarchy levels are in the agencies involved in infrastructure protection? How long does it take for the average message to reach the next higher level? How long does it take until you get a response to your message? What projects were delayed due to lack of response? What changes could accelerate the pace? What projects became unviable due to delays in response from the next higher level?”

The horizontal desynchronization study would answer the questions “What obstacles slow communication and collaboration between DHS and other agencies and state, local or private sector organizations? How does DHS compare to other organizations with which it must collaborate in terms of pace of operations? What must DHS and its partners do to remove obstacles to synchronize their OPTEMPO with the operating environment? What projects were hampered or abandoned due to delays caused by communication or collaboration difficulties?”

The objective of these studies is to share information about outcomes hampered or prevented by differences in OPTEMPO within DHS or among agencies and sectors with which DHS must collaborate. The studies would provide data on cost of delays and recommendations for correcting the problems. DHS and the federal, state, local and private sector organizations with which it must collaborate can use the information to align their processes and operating tempo at the optimal pace for protecting critical infrastructure. Organizations involved would identify desired outcomes, and the regulations, policies, and processes necessary to improve infrastructure protection.



Recommendation 5: Understand the impacts of future interdependencies across all existing and emerging infrastructure sectors.

Issue: In the future, infrastructures—especially our nation’s—will be highly interdependent in ways that are hard to imagine today. As a result, **we need to think beyond a single-sector view of the global infrastructure in order to understand the future critical interdependencies and their implications.** For example, cyber technologies will underpin every infrastructure sector. What are the implications and second- and third-order impacts of accidental or deliberate destruction of cyber infrastructures? Imagine the intelligent highway of the future after an adversary hacks into the cyber backbone of this infrastructure causing thousands of vehicle accidents. In order to protect our nation’s infrastructure, it is imperative that federal, state and local governments work in partnership with the private sector to address these issues. For this reason we recommend:

a) **Expand capabilities to better understand the second- and third-order effects of future attacks, crises, or natural disasters on the interdependent infrastructure system.** This would be an expansion of or addition to the work being conducted by the National Infrastructure Simulation and Analysis Center (NISAC). China’s recent earthquake is an example that brings this problem to the forefront. The country’s devastating 7.9 magnitude quake has had the secondary impact of weakening many dams, to the point where 69 dams were in serious danger of collapse, potentially causing devastating impacts such as flooding and the forced relocation of millions of people. We recommend current work in this area be expanded significantly to look at future infrastructure interdependencies. The resulting assessments should then be provided to owners, operators and designers so they can incorporate protection issues into the infrastructure technologies as they are being developed and implemented. DHS should also consider creating an initiative with academia or industry to develop advanced modeling capabilities to identify future second- and third-order impacts of disruptions to the system.

b) **Confirm which supply chains, domestic and international, will have the gravest impact on U.S. viability if disrupted or destroyed** by natural or manmade means, and then determine how to ensure their protection. As indicated in this report, the U.S. will rely on tighter and more efficient supply chains over the next 15 years. Many of these supply chains are, or will be, connected to the global economy and the distinction between domestic and foreign supply chains will continue to blur. The impact of disruption to a critical supply chain can have significant implications on the nation. For example, the inability of U.S.

manufacturers to obtain a needed chemical to manufacture computer chips because an earthquake or terrorist attack takes out the plant that produces 75% of the world's supply of that chemical could cripple a part of our high-tech industry. We must better understand which supply chains are most critical to our economic viability and way of life. This can include a public-private study initiative sponsored by DHS and conducted by a university, national laboratory or NGO with private sector support to identify and model which supply chains are most critical for U.S. viability. This would include defining and mapping the key future supply chains and modeling the second- and third-order affects if the supply chain is disrupted. These same organizations can then provide recommendations on how to protect these supply chains.

c) **Create a public-private partnership program similar in intent to the U.S. Customs-Trade Partnership Against Terrorism (C-TPAT), which is designed to strengthen global supply chains,** through voluntary agreements with private sector participants. Agreements can be reached with domestic- and foreign-owned entities to expand the C-TPAT concept to include supply chains deemed critical infrastructures, including products and information such as software and electronic commerce.

d) **Require foreign purchases of U.S. infrastructure to meet certain protection standards that are auditable by government or an independent organization.** The Committee of Foreign Investment in the United States (CFIUS) already evaluates which U.S. infrastructures can be purchased by foreign entities. CFIUS or another organization, such as a third-party NGO, should conduct a program that requires any foreign

purchase to meet certain infrastructure protection standards. The goal is to ensure that new owners make certain that important protections are put in place for the infrastructures they purchase. A possible model for this is the Chemical Facility Anti-Terrorism Standards (CFATS) process. CFATS focuses on securing the chemical infrastructure by identifying high-risk chemical facilities and requiring implementation of risk-based performance standards. Using the CFATS-type concept, the government could work with foreign infrastructure owners to ensure minimum infrastructure standards for ownership are met.

e) **Authorize an entity to play an integrating and coordinating function to address current and future infrastructure protection issues in more flexible ways, free from many of the decades-old policy, procedure, and budget requirements that impede a government organization's responsiveness.** Although not a perfect solution, the Director of National Intelligence has been effective in playing a similar role for the intelligence community. This might mean "fencing off" an organization within an organization to allow it to have more flexible planning, budgeting and coordination processes. In the case of infrastructure protection this may mean identifying a component in DHS and providing it with special status to allow it to better serve the nation's needs by freeing it from bureaucratic structures that inhibit agility. Some of the intelligence agencies have been given similar authorization. Congress, of course, would ensure that the component remains accountable for accomplishing its mission. The primary issue is that current government policies and procedures, even if improved moderately over the next decade, will continue to be too slow to meet the nation's rapidly changing future infrastructure protection needs.

Multi-year funding status can likewise enable certain components to better meet private sector needs and be effective to the nation by enabling longer term initiatives, such as may be required for repair and replacement of deteriorating infrastructure systems. For example, innovative precedents exist such as the MFP-11 program used by the DoD Special Operations Command (SOCOM) to give it significant flexibility in funding, setting policy, developing technology and making acquisitions. This program allowed SOCOM new means for continuity and adaptability outside standard policies and procedures, which has immeasurably increased their success. It also used existing organizational structures to improve their ability access their own resources.



Recommendation 6: Establish more innovative incentives for infrastructure protection.

Issue: No single incentive will encourage all infrastructure stakeholders to repair the current infrastructure and take action to reduce future infrastructure risks. Different incentives will apply to different types of infrastructures. This will become a greater challenge as interdependencies among sectors increase in the future. Economic forces will continue to drive infrastructure protection in certain sectors such as commercial facilities, banking and communication. Sectors not driven as directly by market forces, including water and transportation, will require different types of funding and incentives. Therefore we recommend:

- a) Federal, state and local governments need to better **understand which critical infrastructures**

will be protected by market forces and which will not. After defining infrastructure protection priorities, the federal government in coordination with state and local governments, NGOs and the private sectors should **define which actions are needed to enable infrastructure protection**, for example, enhanced government and private-sector collaboration, enhanced design standards, redundant or backup systems, improved maintenance, etc. Define which target groups need incentives to enhance protection and define where industry protects infrastructure adequately and continue to **encourage that behavior through voluntary adoption of preparedness and protection standards, tax credits or rebates, limiting liability, and/or providing low-cost loans to enhance protection.**

Implementation of voluntary standards may be the least controversial incentive to encourage infrastructure protection, and it is already a precedent. Title 9 of the 9/11 Commission Act requires that DHS establish and implement a voluntary private sector preparedness accreditation and certification program, which includes development, implementation and updating of voluntary preparedness standards. And programs such as the C-TPAT, which improves protection through voluntary agreements with private sector participants, is another example of a possible model.

The use of tax credits as incentives is probably the most commonly indicated form of incentive identified during the data gathering for this report. It provides tailored return on investment incentive for private sector entities. However, tax credit programs can get mired in bureaucratic processes

and take years to implement. This, at the same time Congress is already addressing tax credit requests from various constituencies on various topic areas. Tax credits must be considered as a means to incentivize protection, but should not be the only means.

Limited liability is particularly important at times of crisis in order to ensure that private sector organizations are willing to help Federal, state and local governments in quickly reconstituting infrastructures. These private entities need limited liability protection against potential lawsuits during and after the crisis. Consider a program at least at the Federal level where a private entity that meets certain infrastructure protection standards in advance would receive limited liability guarantees. For example, private entities that meet C-TPAT related standards for infrastructure protection would receive some type of assurance that they could reasonably expect limited liability protections.

b) **Incentivize innovation to develop enhanced future infrastructure protection.** DHS alone or in partnership with the private sector or academic institutions should consider creating a development and funding program to spark innovation for infrastructure protection. The mechanism could be a grant to incentivize organizations, especially academia and NGOs, to identify protection approaches and technologies that address hard questions not normally addressed by the private sector. In other words, **incentivize innovative ideas to protect infrastructure not readily protected by market forces** such as water supplies, government-owned roadways, etc. The goal is to incentivize new products, designs, and standards at the same time in order to, for example, ensure they are environmentally sound

ideas. This can be expanded to a broader range of “open innovation” in which the public can provide innovative ideas on how to protect current and emerging infrastructures. Open innovation approaches are widely in use in the private sector by R&D and consumer products companies and are likely to generate innovative solutions to difficult CIKR protection issues.

Another approach to incentivizing innovation may be through new or existing venture capital organizations to spur innovative solutions. Venture capital organizations such as In-Q-Tel and DoD’s DaVenCi assist the intelligence and defense communities in developing new and applying existing technologies to address hard problems. The Defense Threat Reduction Agency assesses venture capital deals to identify new technologies in non-military sectors to help combat weapons of mass destruction. The benefit of using venture capital processes is that they can provide incentives for the private sector to find solutions to government problems that the private sector might steer away from. In-Q-Tel and DaVenCi provide benchmarks on how to develop and run venture capital entities.

Infrastructure protection R&D also may be enhanced through a concept similar to that of Semetech in the 1990s. Semetech was created by semi-conductor manufacturing companies out of concern about foreign competition and a decline in their market base. DoD was also concerned and developed a partnership to raise research funds and sponsor semi-conductor technology development that served national security needs as well as the U.S. electronics industry. This partnership is one example of where the private sector and the federal government worked together

to share the cost of pre-competitive technology development. A similar program could be beneficial in addressing emerging infrastructure protection issues.

c) The government **should establish a national or sector “challenge” or “prize” to create low-cost and innovative approaches to protection.** For example, there could be a series of National Infrastructure Protection Prizes awarded to academic and/or private organizations that provide the most effective solutions to currently unsolvable questions associated with infrastructure protection. This program could be modeled after the DARPA Grand and Urban Vehicle Challenges, the Panasonic World Solar Car Challenge and other contests.

d) An incentive to involve the average person in infrastructure protection may be the **use of volunteers from an organization such as AmeriCorps.** AmeriCorps workers serve through a network of partnerships with local and national nonprofit groups to address national needs. This type of workforce might assist in helping state and local governments work with small infrastructure owners and operators to define their current and future CIKR priorities and provide guidance on how to better protect their businesses.

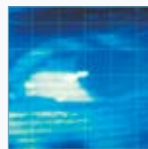


Recommendation 7: Conduct cross-sector infrastructure-protection games and simulations to understand emerging challenges, interdependencies and future risks that would affect the NIPP and other key plans.

Issue: Currently there are simulations, drills and games that focus on national security issues.

Cyber Storm II is perhaps one of the largest of the many simulations conducted by agencies such as DHS, and is an excellent way to examine cyber protection issues. DHS is also beginning to look at R&D scenarios for infrastructures. But much more attention is needed as little is currently being done in regards to gaming the conditions, convergences and challenges of the emerging future infrastructure. By simulating how conditions will converge to affect infrastructure in the future it is likely that innovative solutions can be identified to protect the emerging and existing infrastructures. Therefore we recommend:

a) Develop a wider range of **future-focused infrastructure protection scenarios and challenges**, for example, gaming or simulating 1) the future infrastructure interdependencies or the impact of climate change and urbanization on infrastructure, 2) the ability of hyper-empowered individual to attack SCADA systems linking emerging biotech and health care sectors, and other such scenarios. These public and private sector simulations need not necessarily be on the same scale as Cyber Storm II, but could be a series of smaller games that look at how conditions indicated in this report will affect different infrastructures and sectors in the future.



Recommendation 8: Get inside our adversaries’ decision space to proactively stop future attacks on infrastructure

Issue: The threat from adversaries attacking or using infrastructure in malicious ways will not go away. More importantly, adversaries make decisions and plan attacks much faster than our government bureaucracies can react to them. It can be said that

the terrorist's decision cycle is five days long, but the government decision cycle on the same issue is five years long. In other words adversaries are quick and agile in planning and conducting attacks, while governments usually take years to address how to thwart such attacks. By the time we figure out how to stop one type of attack, many terrorist groups quickly adopt a different approach. **We must determine how to “get in the decision space” of adversaries and influence their behaviors before they attack our infrastructure.** We must be more innovative and flexible to understand how and when adversaries might use our infrastructure against us. Therefore we recommend:

a) Develop a specific infrastructure protection intelligence program via DHS, FBI and the Office of the Director for National Intelligence to **better understand how adversaries now and in the future can attack our infrastructure and/or use infrastructure as a means to kill or threaten our citizens.** Such a program should focus on understanding how adversaries can use infrastructure to their advantage—such as in SCADA attacks, using cheap bio-weapons, disrupting critical supply chains, etc.—and use that data to define indications of possible attacks and threats, and then define appropriate proactive mitigation strategies.

b) There are many threat assessments available to government and industry that address the above concerns and other types of future threats. For example, DHS has its own threat forecast as do other organizations that are responsible for national security issues. DHS should **consider taking the lead in further consolidating future unclassified threats to infrastructures and communicating**

these threats to a wider audience, including the smaller infrastructure owners and operators at the local level. The goal is to communicate future threats so the private sector, academia and NGOs can help create innovative solutions for them more quickly than our adversaries can bring those threats to bear. For example, DHS might create a website or blog in coordination with an NGO that highlights *future* infrastructure threats and pose questions to the general public on how to address them. This uses an open innovation approach to get the public more involved in defining and implementing solutions before the threats manifest. The additional goal is to address current and possible future threats and determine how to deter an adversary from taking future action.

c) Large and small organizations across all infrastructure sectors worry about insider threat issues. The government can address this problem by creating a program to help these organizations to **identify and “pre-empt” threats from malicious insiders.** This could be as basic as a collaboration program for sharing tools and methods that identify, monitor and/or mitigate insider threats, such as advanced sensors, biometric tools, and IT-access assessments. The concept of open innovation also applies here. Hard problems associated with addressing specific types of possible insider threats can be communicated to universities, government agencies and even the general public. Specific vulnerabilities can be masked, but the basic problem can be communicated to thousands of people who may develop innovative solutions including those posed by the insider threat. Financial awards can be provided for ideas that result in solutions to CIKR protection issues.



Conclusion

The integrity of the nation's infrastructure, from water to rail to power, is fundamental to maintaining the American way of life. Over the next 20 years, this infrastructure will be affected by dynamic, rapidly occurring changes that will pose new challenges for those charged with its protection. Unlike at previous points in history, these changes occur more quickly than ever, in many cases before public or private sector entities can to adjust their risk management practices. Complicating matters further, these changes affect increasingly interconnected systems of infrastructure, where one change, attack or event, can have cascading effects on other infrastructure.

To manage future challenges for infrastructure protection successfully, infrastructure owners and operators must understand the forces that drive the future, how to manage change, and how to ensure they continually position themselves for a rapidly evolving risk environment. In other words, preparing for the future means anticipating events and taking action in to prevent catastrophic events. Better anticipation can help deter or avoid some threats, and results in more effective recovery, post event.

This report outlines changes with which infrastructure owners and operators should most concern themselves in preparation for the next 20 years. In this age where change happens exponentially faster than before, owners and operators must continually anticipate future effects on the risk environment, apply sound, data-based, risk analysis approaches, and act accordingly.

APPENDIX 1. INTERVIEWS AND WORKSHOP PARTICIPANTS

Conducted from October 2007 to March 2008

Armstrong, Sue. U.S. Department of Homeland Security, Office of Infrastructure Protection
Bates, Barry. National Defense Industrial Association (NDIA)
Beardsworth, Randy. Olive, Edwards & Cooper, LLC.
Belechak, Joseph. Westinghouse Nuclear
Bond, John. U.S. Department of Homeland Security, Office of Infrastructure Protection
Bracken, Richard. Hospital Corporation of America (HCA)
Broussard, Don. Lafayette (LA) Utilities System
Caverly, James. U.S. Department of Homeland Security, Office of Infrastructure Protection
Cheviron, Mark. Archer Daniels Midland
Clancy, Tim. George Mason University, Critical Infrastructure Protection Program
Conklin, Craig. U.S. Department of Homeland Security, Office of Infrastructure Protection
Cummings, George. Port of Los Angeles, California
Dale, James. Halliburton
Dalton, Marla. American Society of Civil Engineers
Deziel, Dennis. U.S. Department of Homeland Security, Office of Infrastructure Protection
Dozier, Steve. Wal-Mart Stores Inc.
Driggers, Richard. U.S. Department of Homeland Security, Office of Infrastructure Protection
Dunne, Thomas. U.S. Environmental Protection Agency
Dunphy, Robert. The Urban Land Institute
DuPont, Lammont J. DuPont Fabros Technology, Inc.
Dyer, Joseph W. i-Robot Corporation
Englot, Joseph M. HNTB Corporation
Erllich, Ev. Center for Strategic and International Studies (CSIS)
Fennewald, Paul. Missouri Office of Homeland Security
Fitzgerald, Lee. Sprint Nextel
Flynn, William. U.S. Department of Homeland Security, Office of Infrastructure Protection.
Gale, Stephen. Foreign Policy Research Institute, Center on Terrorism, Counterterrorism, and Homeland Security
Gioconda, Thomas. Bechtel Corporation
Hale, David. The University of Alabama, Aging Infrastructure Systems Center of Excellence
Harrison, Jerry. General Dynamics C4 Systems
Heller, Veronica. U.S. Department of Homeland Security, Office of Infrastructure Protection
Hickey, Michael. Verizon Communications, Inc.
Hightower, Paul. U.S. Department of Homeland Security, Office of Infrastructure Protection.
Holleyman, Robert. Business Software Alliance (BSA)
Holmes, John. Port of Los Angeles, California
Hooks, Robert. U.S. Department of Transportation, Science and Technology
Huddleston, Timothy. U.S. Department of Homeland Security, Office of Infrastructure Protection
Hyder, Anthony K. University of Notre Dame, Department of Physics
Jackson, Jason. Wal-Mart Stores Inc.
Johnson, Stanley. North American Electric Reliability Corporation (NERC)
Katona, Peter. University of California, Los Angeles, David Geffen School of Medicine
Kimberly, Laura. U.S. Department of Homeland Security, Office of Infrastructure Protection
King, Steven. U.S. Department of Homeland Security, Office of Infrastructure Protection
Kinton, Thomas. Boston Port Authority
Krause, Merrick. U.S. Department of Homeland Security, Office of Infrastructure Protection
Kunreuther, Howard. University of Pennsylvania, Wharton Risk Management and Decision Processes Center
Kurtz, Paul. Good Harbor Consulting
Larence, Eileen. U.S. Government Accountability Office
Lazisky, Richard, U.S. Department of Homeland Security, Office of Infrastructure Protection
LePage, Richard. U.S. Department of Homeland Security, Office of Infrastructure Protection

APPENDIX 1. INTERVIEWS AND WORKSHOP PARTICIPANTS

Link, Edward. University of Maryland, The James MacGregor Burns Academy of Leadership
MacLaren, Jon. U.S. Department of Homeland Security, Office of Infrastructure Protection
Madden, Turner. Madden & Patton, LLC
Marcello, Rocky. Duke Energy Corporation
Martínez-Fonts, Alfonso. U.S. Department of Homeland Security, Office of Private Sector
McAvey, Maureen. The Urban Land Institute. Fluor Corporation
McDonald, Melissa. U.S. Department of Homeland Security, Office of Infrastructure Protection
Michel-Kerjan, Erwann. University of Pennsylvania, Wharton Risk Management and Decision Processes Center
Moble, Michael. Duke Energy Corporation
Mongan, David. American Society of Civil Engineers
Norman, Michael. U.S. Department of Homeland Security, Office of Infrastructure Protection
Nye, Earle A. The National Infrastructure Advisory Council
Perlin, Jonathan. Hospital Corporation of America (HCA)
Pheto, Bev. U.S. Congress, House Committee on Appropriations, Homeland Security Subcommittee
Platt, Roger. The Real Estate Roundtable
Plehal, James. U.S. Department of Homeland Security, Office of Policy
Pommerening, Christine. George Mason University, Critical Infrastructure Protection Program
Prieto, Robert. Fluor Corporation
Raisch, William. New York University, International Center for Enterprise Preparedness (InterCEP)
Reardon, Kevin. U.S. Department of Homeland Security, Office of Infrastructure Protection
Roberson, Alan. American Water Works Association
Robertson, Joseph. Tyson Foods, Inc
Rudman, Warren. Stonebridge International, LLC
Ryan, Richard. Archer Daniels Midland
Sanfilippo, Matthew. Carnegie Mellon University, Center for Sensed Critical Infrastructure Research (CenSCIR)
Scott, Timothy. The Dow Chemical Company
Senser, Kenneth. Wal-Mart Stores, Inc.
Shortal, James. Home Depot, Inc.
Silver, Harris. The Goldman Sachs Group, Inc.
Simon, James. The Microsoft Institute for Advanced Technology in Governments
Smislova, Melissa. U.S. Department of Homeland Security, Homeland Infrastructure Threat Reporting and Analysis Center
Solheim, Linda. U.S. Department of Homeland Security, Office of Infrastructure Protection
Smith, Donald. U.S. Department of Homeland Security, Office of Infrastructure Protection
Smith, Glen. U.S. Department of Interior
Spinrad, Richard. U.S. Department of Commerce, National Oceanic and Atmospheric Administration
Stanton, Larry. U.S. Department of Homeland Security, Office of Infrastructure Protection
Stephan, Robert. U.S. Department of Homeland Security, Office of Infrastructure Protection
Strock, Carl. Bechtel Corporation
Stroeck, Kenneth. U.S. Department of Homeland Security, Office of Infrastructure Protection
Taylor, Greg. United Airlines
Thomas, Richard. AIG Insurance Company
Tritak, John S. Good Harbor Consulting
Toffler, Alvin. Toffler Associates
Vehmeier, Dawn. U.S. Department of Defense; Acquisitions Technology and Logistics; Industrial Policy
Wales, Brandon. U.S. Department of Homeland Security, Office of Infrastructure Protection
Wallace, Michael. Energy Constellation Group
Ward, Henry. The Dow Chemical Company
Watson, Kenneth. Cisco Systems, Inc., Critical Infrastructure Assurance Group
Watson, Thomas. U.S. Department of Homeland Security, Office of Infrastructure Protection
Wilt, Donald. General Dynamics C4 Systems
Wolff, Evan. Hunton & Williams LLP

APPENDIX 2. ENDNOTES

- ¹ U.S. Environmental Protection Agency. "Future Atmosphere Changes in Greenhouse Gas and Aerosol Concentrations." [Online] Available <http://www.epa.gov/climatechange/science/futureac.html>, IPCC 2007.
- ² U.S. Environmental Protection Agency. "Future Temperature Changes." [Online] Available <http://www.epa.gov/climatechange/science/futuretc.html>, IPCC 2007.
- ³ Henderson, Caspar. "Ocean Acidification: the other CO₂ problem." *New Scientist* magazine (NewScientist.com). August 2, 2006, pages 28-33.
- ⁴ "Biofuels may threaten environment, U.N. warns." CNN.COM/Technology. [Online] Available <http://www.cnn.com/2008/TECH/science/01/23/biofuels.fears.ap/index.html>, January 23, 2008.
- ⁵ Propper de Callejon, Diana; Donohue, Mark; and Day, Rob. "Clean Technology: A Compelling Investment Opportunity." [Online] Available <http://www.lohas.com/journal/technology.html>, January 2008.
- ⁶ Weiner, Edie, and Arnold Brown. *Future Think: How to Think Clearly in a Time of Change*, 2006
- ⁷ Center for Strategic and International Studies, *Seven Revolutions*, available at http://7revs.csis.org/sevenrevs_content.html
- ⁸ World Future Society. "Futurists Release Top Ten Forecasts for 2008 and Beyond", October 5, 2007, quoting James Canton, "The Extreme Future."
- ⁹ Toffler Associates, *Beyond the Crisis: Korea in the 21st Century*, 2001.
- ¹⁰ American Society of Civil Engineers. "2005 Report Card for America's Infrastructure," and "Action Plan for the 110th Congress." [Online] Available <http://asce.org/reportcard/2005/index.cfm>, January 2008.
- ¹¹ Federal Transportation Advisory Group. "Vision 2050—An Integrated National Transportation System." [Online] Available <http://web.mit.edu/aeroastro/www/people/rjhans/docs/vision2050.pdf>, February 2001.
- ¹² American Society of Civil Engineers. "2005 Report Card for America's Infrastructure," and "Action Plan for the 110th Congress." [Online] Available <http://asce.org/reportcard/2005/index.cfm>, January 2008.
- ¹³ World Information Technology and Services Alliance (WITSA). "WITSA Public Policy Report 2007." [Online] Available <http://www.witsa.org/cairo07/WITSA-PPReport07.pdf>, January 2008.
- ¹⁴ Anderson, Mark. "What a Wi-Fi Worm Outbreak Would Look Like." *IEEE Spectrum Online*. [Online] Available <http://www.spectrum.ieee.org/jan08/5877>. January 2008.
- ¹⁵ Asmundson, Phil, deputy managing director of the Technology, Media & Telecommunications Group, Deloitte & Touche LLP, December 2002
- ¹⁶ Anthes, Gary. "The Internet is Down—Now What?", *Computerworld*, January 21, 2008.
- ¹⁷ Silbergliitt, Richard, Philip S. Antón, David R. Howell, Anny Wong. *The Global Technology Revolution 2020, In-Depth Analyses: Bio/Nano/Materials/Information Trends, Drivers, Barriers, and Social Implications*, Rand National Security Research Division, 2006.
- ¹⁸ Alston, Wilton. "Living Under Surveillance", *The New American*, October 29, 2007.
- ¹⁹ Talbott, David. "Universal Authentication, 10 Emerging Technologies", *Technology Review*, March/April 2006.
- ²⁰ Jordans, Frank, *Swiss votes to use 'unbreakable' code*, Associated Press, October 11, 2007.
- ²¹ National Intelligence Council. "Report of the National Intelligence Council's 2020 Project - The Contradictions of Globalization." [Online] Available http://www.dni.gov/nic/NIC_globaltrend2020_s1.html, January 2008
- ²² The Congressional Budget Office. "The Budget and Economic Outlook: Fiscal Years 2008 to 2018", available at <http://www.cbo.gov/ftpdocs/89xx/doc8917/Chapter3.7.1.shtml#1070322>
- ²³ Elkington, J. (1994) "Towards the sustainable corporation: Win-win-win business strategies for sustainable development." *California Management Review* 36, no. 2: 90-100



Guarding Our **Future**
Protecting Our Nation's Infrastructure



TOFFLER ASSOCIATES®



TOFFLER ASSOCIATES®

302 Harbor's Point
40 Beach Street
Manchester, Massachusetts 01944
phone: 978.526.2444
facsimile: 978.526.2445
TofflerAssociates@toffler.com

www.toffler.com