TOPICS INCLUDE:

- Five significant future threats to maintaining a sound infrastructure, and what can be done to address them.
- Potential consequences of inaction.
- Data and analysis of the multiple variables impacting infrastructure.
- How the Chemical sector worked with the government to ensure the safety of vital infrastructure while protecting the growth of their industry.

Five Critical Threats to the Infrastructure of the Future

Leading infrastructure protection experts discuss strategies for protecting your enterprise.

EXECUTIVE SUMMARY:

The threats are real. From terrorism and natural disasters to aging bricks and metal, the infrastructure of this country is more vulnerable than ever. In March 2008, Toffler Associates®, the consulting firm founded by Alvin and Heidi Toffler, authors of Future Shock and Revolutionary Wealth, assembled leaders of industry and government experts to answer a critical question regarding the nation's transportation, utility and communication networks: "What are the most critical infrastructure challenges for industry over the next 15 years?" These are the highlights of that thought-provoking forum.

Infrastructure Challenges for the 21st Century: Defining the Road Ahead

The threats are out there. Leading government officials, heads of industry and industry associations are all trying to raise awareness of just how vulnerable the U.S. infrastructure is. Many fear the long-term consequences of a collapse in infrastructure, whether due to an attack or unexpected failure in systems or technology.

Toffler Associates answered this issue by assembling a group of senior thought leaders from government, industry and associations to discuss what they believe needs to occur in order to better secure the nation's infrastructure and assure its viability far into the foreseeable future. Part of an ongoing program sponsored by Toffler Associates, this informal March 2008 dinner was designed to bring the strongest knowledge resources together in a way that stimulates new ideas to be exchanged freely.

Their first step was to define the threat facing us in the 21st century.

Malevolent Forces vs. Malignant Forces

So what are the threats we're facing? One view of the forces impacting infrastructure divides them into two distinct categories—Malevolent Forces and Malignant Forces[1].

Malevolent Forces are the external forces that threaten to physically attack and disrupt the normal operation of infrastructure. These threats include:

- Terrorist organizations, both foreign and domestic
- Elements working on behalf of a competitive foreign power
- Individuals with malicious intent towards the government, or towards a particular business or organization, who are "super-empowered" by modern information, communications, and other technologies

The problem is that many of these entities have an extremely rapid planning cycle. They are constantly adapting new strategies to attack U.S. interests and can dynamically evolve their tactics to adjust to new security measures. This brings us

to a very important question: How do we evolve our strategy to stay ahead of the enemy?

Malignant Forces are mostly natural forces that deteriorate infrastructure. These are the relentless forces of time, weather and neglect, and include:

- Critical support failure of aging steel, concrete or other material
- Structures weakened by hurricanes, earthquakes or other natural events
- Structures weakened by overuse, or usage that exceeds the original design specifications
- General failures in technology, systems or processes

The American Society of Civil Engineers report card gives America's infrastructure a "D" rating in regards to dealing with these malignant forces. And the situation is only getting worse over time:

- **Bridges**: It will cost $9.4b a year for 20 years to eliminate all bridge deficiencies.
- **Dams**: $10.1b is needed over the next 12 years to address all critical non-federal dams.
- **Drinking water**: There is an $11b annual funding shortfall to replace aging facilities and comply with safe drinking water regulations.
- **Energy**: Existing transmission facilities were not designed for the current level of demand, increasing cost to consumers and the risk of blackouts.

Impact of Nature: What's the Effect on Infrastructure?

Many are conducting ongoing analyses of climate change but few are thinking about its future impact on infrastructure. The connections may be major:

- The impact of climate change will manifest in various, inter-related ways, including global warming, more intense natural disasters, or greater consequences of these disasters.
- Changes in climate are expected to increase acidification of the oceans, changing pH levels. That will have significant impact on marine infrastructures.
- Increased droughts will stress global and domestic water resources and impact farming methods.
- Earthquakes near megacities with populations of 2-28 million are expected to rise to 61% by 2030[2].

- **Wastewater**: The EPA estimates that it needs $390b over the next 20 years to meet increasing demand[3].

Five Key Future Infrastructure Challenges

Once the threats were defined, the dinner participants shifted their focus to a simple, yet vitally important question:

What are the most critical infrastructure challenges for industry over the next 15 years?

Discussion of this question resulted in the identification of five primary problem areas. These areas are where vulnerabilities exist in our infrastructure protection architecture. They include how we identify and deal with threats, and how we are maintaining our essential infrastructure systems for the future. The challenges are:

#1. Challenge: Improve Coordination Between the Government and Private Sector

Many attendees believe that major strides have been made in the information sharing from the federal government to the private sector. Increasingly since the terrorist attacks of September 11, 2001, Federal agencies are relaying classified information to private sector infrastructure operators who have the necessary security clearance at an unprecedented level. However, much more needs to be accomplished.

Currently, there is no unified system for the various government agencies to provide industry with a concise understanding of the threats to the Nation's infrastructure. Sources of information vary from agency to agency. The result is that different businesses and utilities have disparate understandings of the security vulnerabilities, the protections that are effective, and the investments that may be required to secure their infrastructure.

Solution: Trust Building and Communication Between Government and Private Entities

To help with these issues, many state governments are experimenting with things like integrating private enterprise into state fusion centers. The group believes that this is a positive approach. Not only does it provide a novel way to build distributable intelligence and make it deliverable in a consistent and timely fashion to the key leaders of industry who need it most, it also helps ensure this information is translated into the language of the owner-operators.

What is a State Fusion Center?

The Commonwealth of Massachusetts answers the question this way: "The Commonwealth Fusion Center collects and analyzes information from all available sources to produce and disseminate actionable intelligence to stakeholders for strategic and tactical decision-making in order to disrupt domestic and international terrorism."[4]

Another positive step are the efforts DHS is making to communicate the logic and facts behind its risk-based approach to commercial companies and others who may be targets in the future. The risk profile facing companies will continue to change. There is a need to educate business on how this will impact their critical infrastructure. Some participants at the dinner feel that this risk profile also needs to be raised in the context of what companies care about most—their customers.

Some attendees also feel new kinds of confidence-building measures are needed to motivate companies to share what is normally trade-sensitive information. For example, the government needs to demonstrate adequate safeguards relating to the protection of proprietary data, and incentives are needed to eliminate the barriers to effective information sharing.

A primary roadblock to effective communication centers on complacency. Many companies tend to take infrastructure as a given. Businesses must be educated on the fact that their infrastructure might not always be there if they don't take steps to ensure its survival.

#2. Challenge: Infrastructure is Too Centralized

The current trend is to centralize the nation's infrastructure, with both technology platforms and supply chain assets functioning around a central hub, in order to

reduce costs and maximize every supply chain investment. In fact, many industries, such as electric, gas and telecommunications are part of a national or regional grid structure. The dinner participants feel there are several flaws with this thinking:

- The threats of the future will be asymmetrical, and attacks can come from many different directions, but all converge on these potential single points of failure.
- With such a high level of interdependency among sub-systems, penetration at one hub of an infrastructure network has a cascading effect that can be catastrophic to the whole.
- Today's efforts to protect infrastructure naturally tend to focus on defensive measures around these large, primary assets, without considering the fact that distributing these assets might become its own form of security.

Another issue with the centralization mindset is that decision-makers tend to manage infrastructure upgrades as a continuous set of marginal improvements over time. What's missing is an extensive vision for the future state of the nation's infrastructure. The consensus of the group was that a vision, strategy and roadmap are necessary to treat the infrastructure as a comprehensive, interconnecting unit and to make plans for its defense in the long term.

Solution: Strike the Right Balance Between Security and Innovation

The participants are convinced that the paradigm needs to shift from centralizing infrastructure with a strictly low cost and efficiency perspective to one that considers distributing assets and the strategic impact of security. The key is government developing a joint plan in unison with industry, rather than dictating to it.

In order for this to be effective, a system of collaboration needs to be in place that aggregates information such as consumption and distribution of commodities within a particular industry. And we need a system that integrates the databases of different industries to provide a picture of the complete infrastructure system without necessarily

One of the attendees cited a conversation with a former representative of Congress. This individual suggested that the agencies constructing and/or protecting the 21st century's critical infrastructure should be given the task of developing five-year planning documents similar to those of the Department of Defense.

integrating the infrastructure assets themselves. (The group realized that much of the data required to develop detailed models would be viewed by industry as competitive or trade sensitive, hence the need for more incentives and better collaboration as listed in the previous section.)

This is new territory, which is why a primary element of this strategy may be the concept of modeling and simulation, also known as "war gaming." Through the use of various threat scenarios to consider the attendant failure conditions, we can quantify the effects of any disruption in infrastructure. The group believes that when we've succeeded as a nation it is because we've rehearsed, and we've found extra solutions from modeling and simulation.

The resulting plan from this approach should enable companies to leverage their investments and grow their business for the long term, while planning for the protection and defense of their infrastructures.

#3. Challenge: The Nation's Crumbling Infrastructure

Participants agreed that a major threat to infrastructure comes not from outside, but from within. The fact is that our infrastructure is aging, and too many are doing too little to forestall and reverse this "natural" decline. Moreover, this deterioration is accelerating as society grows and changes. As evidence of this, review the forecast for the future estimated demands on infrastructure:

- By 2025, 75% of U.S. residents are expected live on the country's coasts, impacting the infrastructure around wetlands, healthcare, housing and transportation, and insurance costs associated with tropical storms and hurricanes.
- Many will return to central cities for living, working and recreation, creating "24/7 cities" across the U.S.—whose infrastructure can never "rest."
- By 2025, the global population is expected to be 7.9 billion, mostly in developing countries. A growth rate that well exceeds the ability of many countries to upgrade and expand capacity of existing infrastructure.
- Climate change will impact cities in coastal locations, resource-dependent regions and economies that are closely linked with climate-sensitive infrastructure [5].

Now contrast this with the American Society of Civil Engineers opinion of our infrastructure's resilience. According to the ASCE, "The condition of our nation's roads, bridges, drinking water systems and other public works have shown little to no improvement since they were graded an overall D+ in 2001, with some areas sliding toward failing grades." The opinion of William Henry, former President of the ASCE is that "We need to establish a comprehensive, long-term infrastructure plan as opposed to our current 'patch and pray' method to ensure a better quality of life for everyone." [6]

The Future Role of Technology in Protecting Infrastructure

There are many new technological developments on the horizon that can aid in monitoring and protecting infrastructure assets. These include:

- Nano- and micro-technology that enables sensor proliferation in all infrastructure systems, forming "smart" concrete, bricks, bridges, etc. able to detect tampering.
- Nationwide wireless networks that enable almost anyone to deploy largely undetectable sensors, allowing the monitoring of a variety of infrastructure systems.
- Motor vehicle sensor information that can report information about their own condition and the local environment, such as the condition of the infrastructure that they are currently passing over[7].

Solution: Focus Needs to be on Restoration as well as Prevention

It's irrelevant whether critical infrastructure is lost due to terrorism or to deterioration. That's why the dinner participants believe it's essential to develop a long-term infrastructure plan, in accordance with ASCE's ideas, in order to address infrastructure upgrades with foresight. Restoration of assets is sometimes forgotten, with the focus more on prevention.

The group feels this issue needs to rise to the level of a national agenda. And new innovations in technology (such as those at left) are needed to help monitor infrastructure and ensure that repairs are performed when needed.

#4. Challenge: Foreign Ownership of Infrastructure

Participants discussed the high dependency on technology manufactured and maintained outside of the United States. This trend goes beyond the simple use of foreign equipment and systems, and includes a number of critical nodes that are either operated by, or that are completely owned by, foreign business.

The concern is that while this strategy makes perfect sense in this age of globalization and international growth, it also presents a new threat—not from a direct physical or cyber attack, but from a potential malicious consortium of actors who could choose to simply turn off the lights. This international dependency puts a new concern on the nation's ability to provide continuous, uninterrupted operations in the event of diplomatic or military conflict.

Growth of Maritime Trade
The US will depend more on international trade, including maritime trade, in the future. Maritime trade is expected to double by 2020. Working with foreign interests is good for our country. We just need to be aware of the risks[8].

Another issue is the quality problems that arise as parts of our supply chain are produced overseas. The recent cases of lead found in toys produced abroad illustrate the dangers we are already facing today. Dangers may escalate in the future as more of the supply chain that sustains our infrastructure moves offshore.

Solution: More Visibility into Infrastructure

The group feels that the answer to this challenge is to pay more attention to who is exerting control over our infrastructure and supply chain. Three primary areas of focus should be:

- We need to identify what entities are purchasing parts of our infrastructure. And we need new and rigorous methods to answer the question: "Are these entities operating in our best interests?"
- We need to enlist the help of our international allies in identifying any groups that are attempting to acquire sections of infrastructure for non-constructive purposes or reasons contrary to our interests and the interests of the international community.

- When parts of our supply chain are produced overseas, we must ensure that the same quality control standards apply that are in place domestically.

The Growing Cyber Threat
120 countries or groups are currently developing information warfare systems and there are approximately 30,000 hacker-oriented websites[9].

#5. Challenge: Cyber-Interdependency

In addition to physical infrastructure, the group cited the commonality of computer operating systems, and the high degree of interoperability across these systems, as an area of vulnerability. Cyber-interdependency was born out of an effort to improve effectiveness of operations through the new capabilities that information technology provides, as well as to streamline operations, reduce costs through economies of scale and maximize technology investments. But this also creates security problems including:

- Increased vulnerability to asymmetric attacks by surrogates of rogue states or by non-state actors that are empowered in previously unimaginable ways by the Internet and the easy, inexpensive, ubiquitous connectivity it provides.
- Loss of control over technology as “cyberspace” and its related technologies become globalized — when you’re dealing with cyber assets in an international environment, exactly who has sovereignty over these assets becomes unclear.

The reality is that enemies always attack the weak seams. The group believes that cyber-interdependency will continue to be a weak seam in infrastructure protection in the foreseeable future.

Solution: Risk Mitigation, Not Just ROI, Needs to Drive Technology Decisions

With so much of our nation dependent on networked controls, it is essential that we examine how open our infrastructure systems are to cyber attack.

At the dinner, representatives from the telecommunication industry discussed efforts to protect the critical elements of their systems through the imposition of

standards that limit vulnerability to external attack. But they realized that these efforts could stifle innovation and place the industry out of phase with the pace of technology—thereby limiting their ability to deliver the enhanced low-cost services that customers are demanding.

The group recognizes that a balance must be struck between risk mitigation and ROI. But the fact remains that focusing on the lowest cost solution only could cost us far more in the future. When planning future systems, we must include the idea of protecting customers, not just attracting them.

Final Thoughts

The dinner participants agreed there are many serious challenges to securing the nation's infrastructure to a point where it would be considered acceptable by most security experts and yet still be efficient and profitable to the business leaders that make this country work. But those challenges can—and must—be met.

The group pointed to the recent successes in securing the infrastructure of the chemical industry as a potential model for the future. A roadmap to success for other industries may be to receive expert advice, as the chemical industry and some others have done, on where the holes exist in their current infrastructure security, and to create a concrete action plan to correct those vulnerabilities. When this is combined with a willingness to work with government agencies and all other stakeholders to develop a comprehensive, holistic approach to infrastructure protection, the issues of security and reliability become very correctable problems.

Case Study: Success in the Chemical Sector

The chemical industry worked with the Department of Homeland Security (DHS), as well as state and local governments, to identify and correct the vulnerabilities in their own infrastructure. The resulting solution:

- Enabled DHS to provide the chemical industry with more information on how different compounds could be used elsewhere.
- Developed 4 levels of certification based on the type of facility and level of risk so that businesses with lower risk factors are not over-regulated.
- Enabled each chemical plant to design its own protection plan. With each unique plan, it becomes increasingly difficult for an enemy to predict security measures when making their own plans.

In the past, the regulators and the regulated were sometimes at odds. Now they're working together, and the bottom line is that enemy organizations such as Al Qaeda end up becoming the regulated party[10].

This paper is part of an ongoing series sponsored by Toffler Associates. Each paper documents the collaboration of the best minds and strategists to tackle the most critical challenges facing today's world. Look for upcoming issues in the future as this series evolves.

Bibliography

1 The idea of Malevolent Forces vs. Malignant Forces was discussed at the 2008 dinner event, but the original concept was identified by former CIA Director Jim Woolsey. He has raised the idea in multiple public appearances, including a recent talk at John Hopkins University.

2 Toffler Associates analysis of various sources and interviews; http://www.cpc.ncep.noaa.gov/products/expert_assessment/threats.shtml

3 Toffler Associates Interviews; American Society of Civil Engineers Infrastructure Report Card 2005 and the Action Plan for the 110th Congress.

4 Executive Office of Public Safety and Security (EOPSS), Commonwealth of Massachusetts; http://www.mass.gov/?pageID=eopsterminal&L=3&L0=Home&L1=Homeland+Security+%26+Emergency+Response&L2=Commonwealth+Fusion+Center&sid=Eeops&b=terminalcontent&f=msp_homeland_security_terrorism_fusion_center_fusion_center_overview&csid=Eeops

5 Toffler Associates Interviews and Analysis; Cornish, Edward. “Planning in a Age of Hyperchange,” March 2006, http://7revs.csis.org/pdf/conflict.pdf; IPCC, 2007a.; “Climate Change 2007: The Physical Science Basis,” Summary for Policymakers, Contribution of Working Group I to Fourth Assessment Report of Intergovernmental Panel on Climate Change. Approved at 10th Session of Working Group I of the IPCC, Paris, 02/07.

6 “Crumbling nation? U.S. infrastructure gets a 'D': Engineers' report card covers 12 categories, sees decline vs. 2001,” MSNBC, (March 9, 2005; http://www.msnbc.com/

7 Toffler Associates Interviews and Analysis; http://www.thenewamerican.com/node/5993

8 Toffler Associates Interviews and Analysis; http://www.dni.gov/nic/NIC_globaltrend2020_s1.html; http://www.pnwis.org/2004%20Events/PortAQ/Daniel_Yuska.pdf; Report Card for America's Infrastructure--2005", American Society of Civil Engineers, http://www.asce.org/reportcard/2005/page.cfm?id=103; Futurist, July-August, 2001

9 Toffler Associates Interviews and Analysis; http://www.cnn.com/TECH/specials/hackers/cyberterror; Phil Asmundson, deputy managing director of the Technology, Media and Telecommunications Group, Deloitte & Touche LLP, Dec. 2002.

10 Background for this case study provided during the March 2008 Toffler Associates-hosted dinner by a confidential source.

Contact

Toffler Associates builds insight into what's next. We can help you decide the best course of action in protecting your own infrastructure assets and guide you in the implementation of our recommendations. Overcome uncertainty, manage risk and start defining your own future with the help of Toffler Associates today.

Toffler Associates

302 Harbor's Point, 40 Beach Street
Manchester, Massachusetts 01944

Phone: 978-526-2444
Facsimile: 978-526-2445

Email: tofflerassociates@toffler.com