Critical Infrastructure

Long-term Trends and Drivers and Their Implications for Emergency Management

June 2011

Overview

The state and nature of infrastructure is likely to change over the next several decades. These changes could have significant implications for emergency managers. There are several trends in the field of infrastructure that will affect these implications, including:

- The aggressiveness with which infrastructure construction and improvement is pursued and the associated expenses;
- Whether the public or private sector is expected to fund infrastructure construction and improvement;
- Whether the Nation continues to rely on large, centralized infrastructure projects or moves toward developing a larger number of smaller-scale projects;
- The increased incorporation of computers and other technology into physical infrastructure; and
- The government's role in providing and securing information and communications infrastructure.

This document contains preliminary research conducted on behalf of the Strategic Foresight Initiative on the Critical Infrastructure driver. This research is intended to serve as a discussion point for further discussions, and does not represent a forecast by the Federal Emergency Management Agency (FEMA). This paper is a starting point for conversations around a highly complex topic, and SFI encourages feedback about this paper from the emergency management community.

SFI is a collaborative effort of the emergency management community that is being facilitated by FEMA. SFI was launched so the emergency management community can seek to understand how the world is changing, and how those changes may affect the future of emergency management. It will do so by encouraging members of the community to think about how the world may look over the next 15 years, and what steps the community should begin taking to thrive in that world. Participants in SFI include emergency managers at the Federal, state, and local level, subject matter experts on relevant topics, and other stakeholders.

Anybody who would like more information about SFI should contact the team at FEMA-OPPA-SFI@fema.gov.

Key Trends and Drivers

Infrastructure in the United States is becoming more prone to failure as the average age of structures increases. Infrastructure is owned and managed by both the public and private sector, and includes a number of structures that improve living conditions and commerce, including schools, hospitals, roads, bridges, dams, sewers, and energy systems. For some types of infrastructure, such as dams, the age of a structure is a leading indicator of the potential for the failure of the structure,[1] and the average age of infrastructure in the United States is rising. Between 2000 and 2009, the average age of government and privately-owned structures (excluding housing) increased by about one year.[2] For government structures, the trend was even more pronounced over the long term—United States structures' average age rose from 18 years in 1970 to 25 in 2009, indicating that structures are being replaced at a slower rate.[3]

There are several examples of infrastructure becoming more prone to failure as it ages. The number of dams rated as deficient—or those with structure or hydraulic deficiencies leaving them susceptible to failure—tripled between 1999 and 2008.[4] Over a third of the Nation's dams are fifty years old, a number that will increase to nearly 70 percent in ten years.[5] In addition, bridges are generally designed to last 50 years, and the average bridge in the United States is 43 years old.[6] Although the U.S. Department of Transportation rated fewer rural bridges as deficient in 2008 as they had three years ago, the Department rated nearly 3,000 more urban bridges as deficient over the same time period, which is significant because they are more heavily trafficked.[7]

The cost of improving infrastructure in the United States is significant and rising. Independent assessments have warned that infrastructure in the United States is deficient. The American Society for Civil Engineers (ASCE) estimated that the United States needs to invest $2.2 trillion to meet future infrastructure needs, of which $1.1 trillion is unfunded.[8] The ASCE's 2009 estimate of necessary funding represented an increase of roughly $500 billion since their last estimate in 2005.[9] This includes funding necessary to improve structures that have been classified as deficient or hazardous in some way. For example, 2,047 "high hazard" dams were deemed in need of remediation by the FEMA,[10] 12 percent of the National 600,000 bridges were classified as structurally deficient by standards set by the Federal Highway Administration, and 14 percent of bridges were classified as functionally obsolete by the same standards.[11]

The private sector may begin to finance historically government-funded infrastructure. The private sector owns the vast majority of the Nation's critical infrastructure and key resources—roughly 85 percent.[12] However, the government historically has funded the construction and maintenance of certain infrastructure sectors (e.g. transportation and water infrastructure).[13] Some think tanks suggest that public/private partnerships may be used to fund investments in infrastructure for transportation, water, schools, and manufacturing.[14] [15] For examples, states and localities have explored, and in some cases implemented, plans to lease toll roads to private companies.[16] However, there have also been proposals to increase government spending on infrastructure. In October 2010 the Obama Administration proposed establishing a National Infrastructure Bank and spending $50 billion to build infrastructure.[17]

Government entities are increasing their efforts related to information and communications infrastructure. The private sector owns and operates most of the Nation's information and communications infrastructure.[18] However, in recent years the Federal government increased its role in providing and securing information and communications infrastructure. For example, the 2008 Farm Bill required the Federal Communications Commission to develop a comprehensive strategy for providing broadband internet access to rural areas.[19] The National Security Council also recommended that "Federal leadership and accountability for cybersecurity … be strengthened" and the Department of Homeland Security stated that "safeguarding and securing cyberspace has become one of the homeland security community's most important missions."[20] [21]

The Nation may begin constructing and employing more "light" infrastructure. Currently, much of the Nation's infrastructure consists of large, centralized facilities designed to serve regions. However, trends suggest that future infrastructure could be smaller in scale and more locally focused. For example, wind power has been the fastest growing source of new electric power for the last several years,[22] and utilities are building some turbines in a distributed rather than centralized (e.g. "wind farm") fashion.[23] However, single wind power facilities do not match traditional power sources in terms of power output. The average nuclear power plant in the United States can produce 1,000 megawatts of power and the average coal power plant can produce 235 megawatts of power,[24] while the average modern wind turbine produces between 1.5 and 4 megawatts of power.[25] There is also increasing research in the adoption of decentralized water treatment systems in the United States.[26]

Computers and other technologies are being integrated into the design and function of physical infrastructure. Computers already have been incorporated into numerous physical systems, such as vehicles, heating and cooling systems, and manufacturing devices. In the future, it is likely that computers will be integrated into—if not a crucial part of—physical infrastructure into what is called "cyber-physical systems."[27] One example of this is "smart grid" technology, where networked computers and communications technology would be used to work autonomously to resolve problems in the electric grid, manage consumer electronic usage during peak and off-peak times, and administer energy production.[28] Cyber-physical systems may be incorporated into transportation infrastructure (e.g. automated traffic control),[29] water infrastructure (e.g. "smart" water meters),[30] and to monitor the structural health of all physical infrastructure.[31]

Implications for Emergency Management

Emergency managers will be greatly affected by how the Nation approaches its aging infrastructure over the next few decades. Aging infrastructure may become less reliable and impede response and recovery operations. For example, degrading transportation infrastructure would hinder the movement of materiel and personnel to disasters, degrading water infrastructure would make firefighting more difficult, and degraded health care infrastructure would make it more difficult to treat disaster survivors. Failing infrastructure could also become a hazard in its own right. Like the I-35 bridge collapse in Minnesota in 2007, people could be hurt or killed when a deficient structure collapses. An even more troubling hazard would be the collapse of structurally deficient dams. The construction of a dam encourages development in

areas at risk of flooding if the dam were to break, which actually increases the number of people who are at risk over time. [32]

On the other hand, emergency managers may use significant investments in infrastructure as an opportunity to enhance community resiliency. Currently, emergency managers are not always active participants in the discussions that surround infrastructure construction, such as community planning meetings. If they participated in these discussions, emergency managers could offer insights into how to view a community's or region's infrastructure investments as a system, with consideration to making the area more resilient. Emergency managers could also offer advice in other areas, such as building code standards, risk assessments, consequence mitigation, and land use.

Government's growing role in protecting information and communications infrastructure will present interesting challenges to emergency managers. Restoring broadband and cellular service in a disaster-afflicted area could become almost as critical as restoring electricity and water as emergency managers and the public utilize technology to communicate with each other. In addition, the attention of law enforcement and other emergency management partners may become more focused on cyber crime and related issues, reducing the resources they are able to put toward disaster planning and response. Finally, increasing reliance on information and communications infrastructure by individuals, businesses, and government could cause vulnerabilities to which emergency managers need to devote attention.

Light infrastructure adoption has the potential to aid or impede a community's disaster recovery efforts. On one hand, communities capable of generating power and cleaning water locally would not be as vulnerable to service disruptions at large, centralized facilities. Service disruptions like blackouts and water treatment problems would affect fewer people. However, light infrastructure likely would be more susceptible to destruction in a disaster than large, hardened facilities and communities may not have redundant facilities that allow them to recover more quickly. A community may see its only wind turbine destroyed in a disaster, leaving it without reliable electrical service for an extended period of time.

The integration of computers and other technologies into infrastructure will create both strengths and vulnerabilities for emergency managers to consider in planning, response, and recovery. These technologies may make the delivery of services such as electricity, water, and communications more reliable, efficient, and resilient. For example, one of the expected benefits of smart grid technology is that it will be able to reduce the consequences of service disruptions by anticipating, detecting, and responding to them quickly.[33] In addition, sensors embedded into structures would allow infrastructure owners to anticipate failures. However, embedding computers and other technologies into infrastructure could also become a potential vulnerability. New threats, like computer hackers and viruses, could disrupt previously unaffected infrastructure sectors. In addition, the consequences of exotic threats to computers and electronics, like electromagnetic pulses and solar storms, would be compounded.

Correlation to Other Drivers

- **Climate Change:** Climate change could affect infrastructure. Coastal regions could see infrastructure permanently flooded due to rising sea levels. [34] In addition, weather events that become more severe due to climate change could damage infrastructure and put stress on water treatment and energy infrastructures.[35] Other infrastructure may need to be hardened or adapted due to the effects of climate change (e.g. bridges may need to be raised to allow ships to still fit underneath them).[36] These challenges may result in significant efforts to prepare infrastructure for the effects of climate change. Emergency managers would likely be asked to and desire to participate in these efforts.

- **Evolving Terrorist Threat:** The National Infrastructure Protection Plan (NIPP) notes that it is important to assess terrorist threats to infrastructure.[37] The NIPP also notes that the nature of the terrorist threat is often unpredictable. Thus, how the terrorist threat evolves over the next few decades will influence emergency managers' priorities with regards to infrastructure. If, for example, terrorist tactics begin to favor smaller scale attacks that are more likely to succeed, emergency managers would need to focus less on preparing for the consequences of a catastrophic infrastructure failure and more on preparing to repair localized damage to infrastructure.

- **Government Budgets:** Since the Federal government still has a significant role in constructing and maintaining certain infrastructure sectors, like roads and water treatment systems, there is a significant link between government budgets' health and infrastructure reliability. The Federal government has devoted a steady portion of its spending over the past 30 years on infrastructure investments—approximately 3 percent—and spending on infrastructure by Federal, state, and local governments as a percentage of the economy has remained steady as well.[38] Thus, as overall government spending increases or decreases, infrastructure spending is likely to follow the same trend.

- **Technological Innovation and Dependency:** The integration of technology into infrastructure, particularly computers and related technologies, will provide opportunities to operate infrastructure more efficiently and to correct problems, such as structural deficiencies, more proactively. However, the incorporation of technology into infrastructure could also make infrastructure more vulnerable to new threats. In addition, growing reliance on technologies that require new types of infrastructure, such as the increasing adoption of "smart phones" that are increasingly congesting cellular networks,[39] will require emergency managers and infrastructure owners to consider some types of infrastructure differently.

Conclusions & Questions

Infrastructure on which emergency managers rely may degrade in capacity and quality. What challenges would emergency managers face if roads and bridges begin to degrade? What infrastructure (e.g. dams and bridges) present a hazard if they suffer from structural failures?

Emergency managers would be presented with challenges and opportunities if significant changes in infrastructure are made. How could emergency managers engage with infrastructure builders and owners to improve resilience? What types of infrastructure (e.g.

buried infrastructure like water pipes) may not be improved even if overall funding for infrastructure increases?

The private sector may begin constructing roads, water infrastructure, and other traditionally government-owned infrastructure sectors. How would emergency managers engage with these new infrastructure owners and builders? What differences would affect emergency managers if infrastructure investment in these sectors was driven by the private sector?

Infrastructure may be smaller and more distributed in the future. Would distributing infrastructure throughout communities make communities more or less resilient, as opposed to relying on centralized facilities like large power plants and water treatment plants? What functions, like water treatment, may households be able to accomplish without the need for large infrastructure facilities in the future?

New technologies will affect future infrastructure needs. What benefits will infrastructure gain from incorporating new technologies? What vulnerabilities will embedded technologies create? What types of infrastructure will need to be built or expanded to accommodate new technologies?

---

[1] Patricia Dalton, *Physical Infrastructure: Challenges and Investment Options for the Nation's Infrastructure*, Government Accountability Office, May 8, 2008.
[2] Bureau of Economic Analysis, "Fixed Asset Tables, Current-Cost Average Age at Yearend of Fixed Assets and Consumer Durable Goods," August 17, 2010.
[3] Ibid.
[4] Association of State Dam Safety Officials, "State and Federal Oversight of Dam Safety Must Be Improved," December 2010.
[5] Ibid.
[6] American Association of State Highway and Transportation Officials, *Bridging the Gap*, July 2008.
[7] *2009 Report Card for America's Infrastructure*, American Society of Civil Engineers, March 25, 2009.
[8] Ibid.
[9] Ibid.
[10] Federal Emergency Management Agency, "Identifying High Hazard Dam Risk in the United States," July 28, 2010.
[11] *2009 Report Card for America's Infrastructure*, American Society of Civil Engineers, March 25, 2009.
[12] Government Accountability Office, *The Department of Homeland Security's (DHS) Critical Infrastructure Protection Cost-Benefit Report*, June 26, 2009.
[13] Congressional Budget Office, *Public Spending on Transportation and Water Infrastructure*, November 2010.
[14] Urban Land Institute and Ernst & Young, *Infrastructure Report 2010: Investment Imperative*, 2010.
[15] Robert Puentes, "State Transportation Reform: Cut to Invest in Transportation to Deliver the Next Economy," Brookings-Rockefeller Project on Stat e and Metropolitan Innovation, February 2011.
[16] Laura Coleman, "Toll Roads Tip to Privatization," *State News*, Council of State Governments, April 2006.
[17] *An Economic Analysis of Infrastructure Investment*, Department of the Treasury and the Council of Economic Advisors, October 11, 2010.
[18] U.S. National Security Council, *Cyberspace Policy Review: Assuring Trusted and Resilient Information and Communications Infrastructure*, May 2009.
[19] Michael J. Copps, *Bringing Broadband to Rural America: Report on a Rural Broadband Strategy*, Federal Communications Commission, May 22, 2009.
[20] NSC, *Cyberspace Policy Review*, May 2009.
[21] Department of Homeland Security, *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland*, February 2010.

[22] U.S. Energy Information Administration, *Electric Power Annual 2009*, U.S. Department of Energy, January 2011.
[23] Stacia Cudd, "Learning the Basics of Distributed Wind," U.S. Department of Energy Wind Powering America, March 29, 2011.
[24] U.S. Energy Information Administration, *Electric Power Annual*, 2011.
[25] GE Energy, "Wind Energy at GE," General Electric, 2010.
[26] Decentralized Water Resources Collaborative, *Integration: A New Framework and Strategy for Water Management in Cities and Towns: Meeting Summary Report*, Water Environment Research Foundation, July 2010.
[27] National Science Foundation, "Cyber-Physical Systems Program Solicitation," December 11, 2009.
[28] Department of Energy, *The Smart Grid: An Introduction*, 2008.
[29] NSF, "Cyber-Physical Systems," December 11, 2009.
[30] Urban Land Institute and Ernst & Young, *Infrastructure Report*, 2010.
[31] Jennifer A. Rice et al., "Flexible Smart Sensor Framework for Autonomous Structural Health Monitoring," *Smart Structures and Systems* 6 (July-August 2010).
[32] *2009 Report Card for America's Infrastructure*, ASCE, March 25, 2009.
[33] Department of Energy, *The Smart Grid*, 2008.
[34] U.S. Climate Change Science Program, *Impacts of Climate Change and Variability on Transportation Systems and Infrastructure: Gulf Coast Study, Phase I*, March 2008.
[35] U.S. Global Change Research Program, *Global Climate Change Impacts in the United States*, 2009.
[36] U.S. Climate Change Science Program, *Coastal Sensitivity to Sea Level Rise: A Focus on the Mid-Atlantic Region*, January 2009.
[37] U.S. Department of Homeland Security, *National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency*, 2009.
[38] *Trends in Public Spending on Transportation and Water Infrastructure, 1956-2004*, Congressional Budget Office, August 2007.
[39] Jim Giles, "Smartphone use makes cellular networks' collapse a real possibility," *The Washington Post*, November 30, 2010.