Infrastructure Interdependencies and Homeland Security

Yacov Y. Haimes

L. R. Quarles Professor of Systems and Information Engineering, and Civil Engineering, and Director, Center for Risk Management of Engineering Systems, Univ. of Virginia, 112A Olsson Hall, Charlottesville, VA 22903. E-mail: haimes@virginia.edu

Introduction

As we can see from the following quotes, infrastructure interdependencies have a strong impact on homeland security.

"The speed, virulence, and maliciousness of cyber attacks have increased dramatically in recent years. More and more people are capable of launching significant assaults against the nation's infrastructure and cyberspace because of the increasing sophistication of computer attack tools. The consequences of a cyber attack on our critical information networks and infrastructures, which are composed of private and public institutions in many different sectors under the guidance of federal-led departments and agencies, can have significant negative effects on the United States" (Dept. of Homeland Security, 2004).

"Our national defense, economic prosperity, and quality of life have long depended on the essential services that underpin our society. These critical infrastructures—energy, banking and finance, transportation, vital human services, and telecommunications—must be viewed in a new context in the information age. The rapid proliferation and integration of telecommunications and computer systems have connected infrastructures to one another in a complex network of interdependence. This interlinkage has created a new dimension of vulnerability, which, when combined with an emerging constellation of threats, poses unprecedented national risk" (President's Commission on Critical Infrastructure Protection 1997).

The quantification of infrastructure interdependencies is central to an effective assessment and management of risks of terrorism to critical infrastructures.

A Need for Research

The advancement in information technology has markedly increased the interconnectedness and interdependencies of our critical infrastructures, including telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services, and continuity of government. There is an emerging need to better understand and advance the art and science of modeling the interconnected large-scale complex economic systems. As quoted above, this need stems from the vulnerability of critical infrastructures to the threats of terrorism.

Historically, many critical infrastructures around the world were physically and logically separate systems with little interdependence. For example, water resource, electric power, and transportation systems, to cite a few, were designed, built, and operated without a threat to their integrity. Today, these and other similar infrastructures have close relationships that can take many forms. These interdependencies and interconnections among infrastructures pose a threat to our society.

To illustrate this complexity further, let us consider the U.S. electric power utility, which is a large-scale, hierarchical, and interconnected system. At the national level, it consists of three main power grids: (1) the Eastern Interconnected System, covering the eastern two-thirds of the United States; (2) the Western Interconnected System, covering the southwest and areas west of the Rocky Mountains; and (3) the Texas Interconnected System, consisting mainly of Texas.

At the network level, each network, as its name implies, is an interconnected system in itself, comprising numerous generators, distribution and control centers, transmission lines, converters, and other elements. Proper functioning of these interacting components is crucial to the continuous operation of the entire power system. In addition to its essential internal dependency, the U.S. power system is externally dependent upon other infrastructure systems, notably telecommunications, fuel supply, and transportation, to name a few.

One significant by-product development attributed to the advancement in information technology has been the reliance of the private and public sectors on supervisory control and data acquisition (SCADA) systems. These systems work remotely to improve the efficiency and effectiveness of the control, operations, and management of critical physical infrastructures. The fact that sectors of the economy and other critical infrastructures are highly coupled renders them at-risk to cyber terrorist attacks. This risk is further exacerbated because they are often remotely controlled and managed through SCADA systems, which are vulnerable to such cyber intrusion. Myriad data collection, control, communication, and management activities, which are essential for the effective operation of large-scale infrastructures, are being performed by SCADA systems.

Since the fundamental purpose of a SCADA system is to control and monitor specific operations (local and/or remote), the need to store business information has added a new function to SCADA: the *management information system* (MIS). MIS enables managers and customers in remote locations to monitor the overall operations and to receive data that allows higher-level business decisions to be made or reviewed. Increasingly, SCADA systems and related technology are replacing and displacing human operators and data collectors in many critical infrastructures. Examples of the functions that railroad SCADA systems are performing include computer-aided train dispatching, underground track heaters for sensors, and control devices. Other systems that are SCADA-controlled include transportation, oil and gas, water, and energy management systems.

To further appreciate the nature of these interdependencies, consider the operation of the electric power system, which is heavily dependent upon voice and data communications. Data

communications provide real-time updates (i.e., every few seconds) of electrical system status to SCADA systems in distribution and bulk electric control centers. Data communications are also used for the remote control of devices in the field, such as circuit breakers, switches, transformer taps, and capacitors. Moreover, data communications allow generating units to follow the real-time signals from the control center that are necessary to balance electricity generation with consumer demand instantaneously. Although the power industry owns and operates the majority of its communications equipment, a substantial portion is dependent on local telephone carriers, long-distance carriers, satellites, cellular systems, paging systems, networking service providers, Internet service providers, and others—all of which are vulnerable to cyberterrorism.

Thus, there is little doubt that in order to ensure the stability, sustainability, and operability of critical infrastructures, it is imperative to fully understand their complexity and interconnectedness, as well as the risk associated with these characteristics. Nonetheless, despite all the research efforts to date, our knowledge about these factors remains limited. In large part, this is because of the daunting complexity involved. Yet it is also because we are still lacking a high-level, overarching framework for modeling interdependencies among large-scale, hierarchical, interconnected complex systems.

Call for Papers

Several groups of researchers in the United States and around the world are responding to the need to better our understanding of complex infrastructure interdependencies. In the United States, teams from the National Laboratories, universities, and the private sector are developing analytical and simulation models with varied levels of success. Although no silver-bullet solution has been developed for this intricate modeling problem, much progress has been made during the last several years to merit the exchange of the state-of-knowledge among these researchers. The *Journal of Infrastructure Systems* will publish a special issue on infrastructure interdependencies and homeland security in 2006. To this end, researchers are encouraged to submit original papers on this theme for this special issue. The complete manuscripts must be submitted to the *Journal* by September 30, 2005. Following the peer review process, authors will be notified on the status of their papers by January 31, 2006.

References

U.S. Dept. of Homeland Security. (2004). "Progress and challenges in security the nation's cyberspace." *OIG-04-29*, Office of the General Inspector, Washington, D.C.

President's Commission on Critical Infrastructure Protection. (1997). "Critical foundations: Protecting America's infrastructures." President's Commission on Critical Infrastructure, Washington, D.C.