

IV.6

Critical Infrastructure Protection in the Information Age

Peter S. Anderson

INTRODUCTION

A new theme emerging in the information age is critical infrastructure and, in particular, information infrastructure. Infrastructures are indispensable for human welfare, not only because of the important economic, social and other benefits they provide, but also because of the consequences for society-at-large when they fail to meet expected service requirements. Critical infrastructures consist of physical and information-based facilities, networks and assets, which, if disrupted or destroyed would have a serious impact on the health, safety, security or well-being of citizens or on the effective functioning of governments and industries. They include, but are by no means limited to, telecom, energy, banking and financial, transportation, water and sewage, healthcare, government and emergency systems.

Historically, many of these infrastructures were physically segregated. However, with rapid changes since the 1970s in technology, national regulatory practices, market conditions and industrial realignments, critical infrastructures have progressively converged. Technological advances have also enabled significant automation in the operation and control of critical infrastructures.

In our information age, information infrastructure has emerged as one of the most important critical infrastructures because it now lays the foundation for managing and integrating all other critical infrastructures as well new forms of communication, information exchange and commerce.

CONVERGENCE AND THE CRITICALITY OF INFORMATION

Convergence within the computer and telecom technology sectors is also challenging underlying concepts of traditional infrastructures. For example, within the telecom industry, the Public Switched Telephone Network (PSTN) traditionally consisted primarily of a narrowband, mature, switched telephone network designed and scaled primarily to support voice communication with data overlaid on separate networks. Increasingly, public telecom infrastructures are consisting of networks of circuit-switched networks interoperating and converging with broadband, packet-based Internet Protocol (IP) networks and associated applications.

Electric power utilities, for example, are expanding their use of information systems and interconnecting previously isolated networks because of competition, reductions in staff and operating margins, ageing proprietary systems and the need to integrate national and even continental power grids. Further, as with the telecom sector, as new players enter the power generation and distribution markets, existing utilities are being required to offer open access to their transmission systems and integrate new subsystems into an ever growing complex power management system where different players have to communicate in real time in order to carefully balance power demand and supply arrangements. Simultaneously, many utility companies are moving away from using their own private network infrastructures and towards widespread dependency upon public telecom facilities to integrate transmission and distribution control centres and corporate networks.

Of course, dependency upon public network infrastructure is not unique to the electricity sector. In the transportation sector virtually all traffic control systems rely upon public telecom infrastructure. Similarly, in the financial sector, much of the electronic fund transfers and trading transactions are carried over public networks, as are links used by producers and suppliers to lower costs through just-in-time manufacturing. Businesses of all kinds regard the ability to exchange information internationally across single, multi-site virtual enterprise networks overlaid on public networks as a strategic necessity.

The same pattern holds for the provision of government services. In the United States, over 95% of government communication is carried over public information networks. In Canada, the federal government directly controls only 10% of its infrastructure, with the remainder supplied by the private sector. These arrangements not only support basic administrative services, but military as well as important public safety services. In particular, public commercial mobile cellular technology is now perceived by most emergency management organisations as a strategically important solution to traditional problems of incompatibility and interoperability among agencies' private radio networks and as a crucial bridge between wireless systems and the PSTN. Moreover, commercial mobile wireless services offer this interoperability without the added costs of establishing and maintaining agency-specific networking arrangements.

The resulting convergence of voice and data applications is leading to the evolution of hybrid networks that combine infrastructures of different jurisdictions and disciplines with those of public wireline and wireless carriers. Such infrastructure arrangements increasingly support mission critical functions ranging from seismic

monitoring, to weather and tsunami public warning, to disaster situation reporting and facilitating appeals for assistance. Such examples illustrate how essential societal functions progressively are becoming entangled in an interdependent network of critical infrastructures, where each infrastructure is required for the effective operation of the other, and whose management and overall quality control is simultaneously becoming increasingly decentralised, less coordinated and exceedingly complex.

VULNERABILITY OF CRITICAL INFRASTRUCTURE

Not surprisingly, these rapid advances in interconnectedness have created major challenges for protecting critical infrastructures. In today's global environment, national security is measured in both economic and military terms, and a nation's social advancement and world competitiveness rely upon efficient, robust and secure information, electrical power, transportation and other critical infrastructures.

The increased interdependency fostered by Critical Information Infrastructure (CII), combined with greater operational complexity, have made critical infrastructures particularly vulnerable to a variety of potential threats, including natural hazards, cascading failures due to human error and technical problems as well as new forms of cyber mischief, crime, terrorism and warfare. Each of these threats can result in severe service degradation or outright infrastructure failure.

The pace of technological change and the drive to automate control systems are aggressively challenging society's ability to design and implement necessary safeguards, including appropriate hazard detection, prevention and mitigation standards and practices. The vulnerability created by these gaps affects not only utility services, but also databases and systems that maintain vital confidential and/or proprietary information in all sectors.

Many of our most critical systems are highly vulnerable to damage from earthquakes, extreme weather and other natural hazards. Even when they are not physically impacted, sudden demand surges during crises can foster blackouts, brownouts and/or service congestion, leading to loss or denial of service. Similar scenarios can take place through deliberate or accidental human action. The CII has become especially vulnerable to fun-seeking hackers, criminals and even deliberate cyber attacks from nation states and terrorists. Every day, computer viruses and worms move rapidly across the world-wide Internet destroying data and overloading systems with superfluous e-mails, shutting down government, industry, academic, community and even private residential systems. Cyber-crime

is becoming a growing transnational phenomenon, making prosecution extremely difficult. It is even perceived as a threat to national security, and in its most virulent form, cyber-war is now ranked in between nuclear and conventional war by the United States government as having one of the highest levels of threat impacts.

PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURE

While physical restoration of the CII can often be completed quickly, even the most temporary failures can result in longer-term harm. They can seriously undermine public and business confidence in electronic commerce and government initiatives. The human and economic costs associated with recovery or initiating new mitigation strategies is enormous. The value alone of lost business and productivity is now measured in billions of dollars from each world-wide virus attack, and even the largest software vendors are hard pressed to keep up with security enhancements.

As important as our infrastructures are, many legal, institutional, economic, social and even conceptual issues continue to challenge protection efforts. Securing information infrastructure requires significant ongoing capital investment and evolving expertise, as well as coordination with other infrastructure sectors. Fortunately, these requirements have been identified world-wide already as a result of international planning and coordination efforts in the attempts to alleviate potential Year 2000 (Y2K) computer date rollover problems. Many factors contributed to successful organising efforts, including a universally recognised potential threat; a fixed deadline for reducing the risk and preparing contingency plans; compelling political and economic reasons for government and non-government interaction, and a shared knowledge base of common technical problems and solutions. Most importantly, Y2K provided, for the first time, a comprehensive view of international interdependence brought about by networked systems.

However, it also revealed as much about the differing perceptions of risk associated with CII consequences, variations in the protective actions that countries are prepared to initiate, and in the scope of participation that is considered necessary.

Some consider CII to be primarily a national security issue that needs protection measures to be directed by law enforcement, military and intelligence services. Representatives of businesses and of industrial sectors often view criticality in terms of what they need to conduct business and strategically protect proprietary

interests. The public sector wants to reduce cost and improve efficiencies delivering services online, while protecting the privacy of citizen records.

Vendors and service providers may view risk in terms of new market opportunities to introduce a range of value-added security services and products, including technical support, software and hardware enhancements (encryption, firewalls, access control systems, etc.). The public wants assurances that financial and other electronic transactions are secure, and that appropriate control mechanisms are in place to prevent objectionable material reaching children.

Conclusion: Towards Practical CII Protection

One of the key features of our networked environment is that individuals, corporations and governments all share a responsibility in securing this environment. While not all of the potential residual benefits of Y2K efforts may have been widely garnered, countries are moving beyond this event to establish longer term CII protection strategies. Some of these initiatives were catalysed by the 11 September 2001 terrorist events.

In Europe, Germany, the United Kingdom, The Netherlands and other countries are putting in place CII programmes to better educate enterprises and the public. The United States has established a new Critical Infrastructure Assurance Office to carry out functions relating to protection of information systems for critical infrastructure, including those functions assigned to the new Office of Homeland Security. Canada has folded similar responsibilities into a new civilian agency, the Office of Critical Infrastructure Protection and Emergency Preparedness, that combines protection from and response to threats involving national critical infrastructure with the need to respond to other more traditional hazards. Such an all-hazards approach has both administrative and operational advantages. Among other things, it recognises that threats of natural and human-induced disasters also pose threats to critical infrastructures. It also provides a single focal point for coordinating national planning and response efforts.

Regardless of what approaches countries pursue, all will necessitate a continuing dialogue to promote mutual understanding of public and private sector interests and concerns, as all stakeholders strive to meet the objectives of protecting critical infrastructures increasingly through non-regulatory solutions. In the coming years, CII protection could very well become the fertile ground for spawning new public policy paradigms.

Box IV.6.1 Critical Information Infrastructure Protection

PRODUCT DESIGN AND IMPLEMENTATION

Vendor product development and testing cycles are decreasing, creating or leaving exploitable vulnerabilities; infrastructures may have fundamental security design problems that cannot be quickly addressed; vendors produce software with vulnerabilities, including those where prevention is well-known and computer source code often is not required to find vulnerabilities; the sophistication of attacks and intruder tools is increasing and many are designed to support large-scale attacks. Using these automated tools, intrusions from remote systems can be achieved in a matter of seconds; Internet attacks can be easy to launch, are often low risk and increasingly hard to trace. During a confrontation with Iraq in 1998, widespread intrusions into US Army, Navy, Airforce and other systems were discovered with no clear indication of how long they had been penetrated, where the intrusions were coming from or what information had been compromised.

INFRASTRUCTURE INVESTMENT AND MANAGEMENT

In a competitive environment, the need for rapid innovation and the lack of a clear return on investment for specialised critical infrastructure-protection features often preclude risk reduction considerations during design and implementation phases; information networks are becoming globally integrated and widely distributed among numerous stakeholders, whose control over network functions extends beyond national boundaries, making overall quality control complex, difficult to achieve, sustain and even monitor; many users are willing to accept higher risk of security deficiencies in exchange for greater technical and other efficiencies associated with advanced technologies.

AWARENESS AND TRAINING

The vast majority of CII intrusions result from exploitation of known vulnerabilities or configuration errors; intruders do not have to be well-trained since tools, knowledge and access to expertise are widely available over the Internet. However, the overall effectiveness of intrusion is increasing as knowledge is passed on to less knowledgeable intruders. The capabilities needed for initiating a global information infrastructure attack are no more than a networked personal computer and an e-mail programme; organisations trying to prevent intrusions are usually constrained by a shortage of qualified system and network administrators and information security staff. End-users are often left to train themselves; new entrants may not possess the same level of knowledge as incumbents about system capabilities, potential vulnerabilities or risk reduction measures.

POLICY

Despite many lessons learned, these have not automatically led to a consolidation of knowledge; in many countries, there is no single authority or integrated programme for fostering innovation and new strategic approaches and there is little coordination across infrastructures. Public and private responsibilities for CII protection are evolving; many countries have yet to consider the Internet as a critical infrastructure; and in liberalised markets, governments are moving away from regulating new service markets. The international scope makes risk reduction strategies complex, and difficult to implement and enforce.

TRUST AND INFORMATION SHARING

While experience demonstrates the benefits of information sharing, widespread information sharing remains a significant problem. Liability and confidentiality concerns about disclosure of proprietary infrastructure data continue to deter firms from sharing information with governments, especially where there is the prospect of governments being forced to disclose such information under domestic access to information legislation.
