Chapter 3.36
A National Information Infrastructure Model for Information Warfare Defence

Vernon Stagg
Deakin University, Australia

Matthew Warren
Deakin University, Australia

ABSTRACT

Information infrastructures are an eclectic mix of open and closed networks, private and public systems, the Internet, and government, military, and civilian organisations. Significant efforts are required to provide infrastructure protection, increase cooperation between sectors, and identify points of responsibility. The threats to infrastructures are many and various, and are increasing daily: information warfare, hackers, terrorists, criminals, activists, and even competing organisations all pose significant threats that cannot be sufficiently dealt with using the current infrastructure model. We present a National Information Infrastructure model that is based on defence against threats such as information warfare.

INTRODUCTION

Information technology has removed many of the traditional barriers that exist between organisations, both nationally and internationally. As links are formed within and between organisations, resources, services, and information are integrated into infrastructures of interrelated, interoperable, and interconnected elements. These infrastructures have rapidly grown to incorporate not only equipment and services, but elements deemed critical for survival or necessary for national capability.

Information infrastructures have become necessary and vital elements for nations worldwide, and are an eclectic mix of open and closed networks, private and public systems, the Internet, and government, military, and civilian organisations. They are important vehicles for

the generation of wealth, and can influence the power and capability not only of organisations, but also nations (Westwood, 1996). However a problem with many infrastructures is that they are excessive, continually growing, regularly reconfigured and reengineered, and lack suitable staff and resources to oversee them (Brock, Jr., 2000). With the growing trend for private ownership of critical infrastructure elements, responsibility shifts from government to private organisations and raises issues of who is involved, what their responsibilities and requirements are, and determining a focal point of authority for infrastructure control (Cordesman, 2000; PCCIP, 1997b; Waltz, 1998).

Numerous countries have developed national information infrastructures to reap the benefits they offer. However, with the growing demand on these infrastructures, along with the reliance and dependability on their operation, the threats and vulnerabilities they face have also increased (Stagg & Warren, 2001). This requires new methods of protection and security, especially when dealing with new and emerging threats such as information warfare.

NATIONAL INFORMATION INFRASTRUCTURE

A National Information Infrastructure (NII) has been defined as *a system of high-speed telecommunications networks, databases, and advanced computer systems that make electronic information widely available and accessible* (OMB, 1995). It has also been described as *an inchoate, multidimensional phenomenon, a turbulent and controversial mix of public policy, corporate strategies, hardware and software that shapes the way consumers and citizens use information and communications* (Wilson, 1997).

Defining and describing an NII is no easy process. Wladkowski (1996) describes an NII as a hierarchal structure with a base consisting of networks belonging to the power industry, a middle level of networks belonging to the telecommunications industry, and a high level of multiple networks involving government, business, finance, transportation, emergency functions, and the military. Garigue (1995) points out that with the introduction of such infrastructures, the strict organisational hierarchies, structures, and boundaries of time, space, and physical barriers are broken down or removed.

Another important consideration is that many elements within the NII, as well as those used to protect and defend it, come from the public and private sectors, particularly Commercial off the Shelf (COTS) software and hardware. With the growing trend of government and military organisations to procure commercial products, along with the need for system interoperability, there will be a greater amalgamation of government, military, and civilian infrastructures (Campen et al., 1996; Garigue, 1995).

The responsibility of the defence of an NII has primarily been the domain of government and military departments. However, with the increasing use of commercial hardware and software elements within an NII, the issue of who is responsible for defence has broadened considerably. The level of security and defensive measures has primarily focused on those elements deemed critical for the nation's survival, creating the concept of critical information infrastructure.

A critical information infrastructure considers the essential elements of a nation and implements special hardening, redundancy, recovery, and other protection mechanisms (Anderson et al., 1999; Nash & Piggott, 1999). The United States Presidential Critical Infrastructure Protection Commission (PCCIP, 1997a) identified five critical sectors:

- Information and communications
- Banking and finance
- Energy, including power, oil, and gas