Chapter 3
Critical Information Infrastructure and Cyber-Terrorism

Olivia Bosch
International Security and Communications Ltd., London, UK

1. INTRODUCTION

This chapter examines the relationship between Critical Information Infrastructure (CII), the protection of such informational assets from cyber incidents that compromise their security, and purposes for 'attacking' CII. CII is the computer and communications networks within and between critical national infrastructure (CNI) of the energy, water, transportation, manufacturing, finance and communications sectors, as well as law enforcement and security sectors, that underpin a country's national survival and well-being.

Increasingly over the last decade, such critical infrastructures span national borders and thus a cyber incident spreads more easily internationally while also posing new challenges to cross-border law enforcement and security investigations and defences. The general types of 'attacks' are often labeled as acts of nuisance, cyber crime and cyber terrorism, or cyber warfare, but until the intent of a particular cyber event is determined, the event remains neutral – hence use of the term 'incident' – until such time investigation can attribute origin and cause. Attribution is considered difficult to determine, and in taking a long time

DOI: 10.4018/978-1-61520-831-9.ch003

to do so can thus possibly lead to inappropriate protective measures or responses even if deemed to be defensive. This chapter does not address the specific technical ways and means by which malicious or unauthorized cyber attacks are conducted or general responses and protection strategies and policies, these being elaborated in other chapters; instead it presents a framework in which to better understand CII in relation to CNI and what distinguishes the types of incidents in relation to their often adverse impact on CII so as to require improved security and protection policies for CII.

2. CRITICAL INFORMATION INFRASTRUCTURE (CII)

CII is the computer and communications networks within a country's critical national infrastructure (CNI) which enables the various national sectors to function.(Chatham House, 2004) Since the late 1990s, CNI has gradually incorporated the newer communications and computer technologies, serving to improve productivity and safety. In some cases, this has provided access to the Internet to meet new commercial or business pressures to expand market share, improve efficiencies, and reduce costs of production such as by remote monitoring.

2.1 Industrial Control Systems within CII

The Year 2000 (Y2K) problem highlighted a particular feature of computing systems in CII: that of industrial control systems. Until that time, most public understanding and perceptions of information technology focused on the development of the Internet and the rise of dot.com businesses; what most people considered to be a computer was the personal computer (PC). The 'PC' was used in businesses and in the front offices of industry to process accounting, payroll and other administrative services. Other than information technology (IT) professionals, most people have tended not to give much thought to what happens in a data centre or about enterprise applications. Information and communications technologies are however, more pervasive than that. Industrial control system computers are not located in front offices and often not even in data centres but are of a different kind, usually found in larger scientific research establishments and industrial sectors including those in critical national infrastructure (CNI). Industrial controls vary and include process controls, batch controls, and the more commonly known SCADA (Supervisory Control and Data Acquisition) system, which, as its name, oversees and deals with the calculations and processing of many flows of data and component parts or services for geographically-dispersed production and delivery. Such computer processing necessarily involves communication of data within, and as relevant outside, the facility, in order to provide the electricity, energy, telephone, water, oil, gas, transportation and other critical services that underpin a country's survival.

As most CNI necessarily deals with or concerns a country's population, and thus large-scale delivery of reliable services, CNI engineers and operators focused their development and testing of computer systems with issues of public safety in mind, and thus with a robustness that is not normally associated with the development of personal computers. This testing process becomes more complicated when also taking into account vulnerabilities associated with the introduction of new information technologies of the Internet and dot.com age.

2.2 Features of Industrial Control Systems

Traditionally, industrial control systems were stand-alone computers using proprietary hardware and software, including for any related telecommunications. Oil, gas, chemical, water, and nuclear power plants as well as aluminum smelters, glass