Critical Infrastructure Systems:
Security Analysis and Modelling Approach

Graeme Pye, Deakin University, Australia

ABSTRACT

A system security analysis and system modelling framework tool is proposed adopting an associated conceptual methodology as the basis for assessing security and conceptually modelling a critical infrastructure system incident. The intent is to identify potential system security issues and gain operational insights that will contribute to improving system resilience, contingency planning, disaster recovery and ameliorating incident management responses for critical infrastructure system incidents. The aforementioned system security analysis and modelling framework is applied to an adverse critical infrastructure system incident case study. This paper reports on the practical application of the framework to a case study of an actual critical infrastructure system failure and the resultant incident implications for the system and the wider regional communities.

Keywords: *Analysis, Critical Infrastructure, Modelling, Security, System*

1. INTRODUCTION

Historically, Australia's infrastructure was originally owned and operated by the public sector at the federal, state and local government levels (Smith, 2004), however the majority of Australia's critical infrastructure has been privatised with as much as 90% of the critical infrastructure under private sector ownership in some areas (Allard, 2008; TISN, 2004a). Some common examples of critical infrastructure systems and services that people rely upon include such essential services as electricity, water, health services, telecommunications and banking to name a few (AGD, 2008), although this may differ depending on the national circumstance of a particular country.

The Australian contextual definition of critical infrastructure as defined by the Trusted Information Sharing Network (TISN) is as follows. "Critical infrastructure is defined as those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic well-being of the nation, or affect Australia's ability to conduct national defence and ensure national security" (AGD, 2008; NCTC, 2004; TISN, 2004b, p. 3).

Importantly, in the context of this definition, "significant is defined as an event or incident that puts at risk the public safety and confidence, threatens our economic security, harms Australia's international competitiveness, or impedes the continuity of government and its services" (TISN, 2004b, p. 3).

DOI: 10.4018/ijcwt.2011070103

This briefly defines and outlines an interpretation of critical infrastructure as a prelude to further discussing critical infrastructure in the context of a systems environment. A generic methodological approach is proposed as the foundation of the ensuing framework for the practical system security analysis and modelling of a critical infrastructure incident. It also seeks to determine a response to the research question of: how to critique and model critical infrastructure systems?

This is followed by a case study overview of the critical infrastructure incident and its subsequent system security analysis and modelling as applied utilising the TARDIS framework. Finally, a reflective look at the TARDIS framework briefly discusses its applied analysis and modelling approaches and concludes with identifying future research alternatives for improving the TARDIS framework structure and application.

2. CRITICAL INFRASTRUCTURES: A SYSTEMS ENVIRONMENT

The dominate architecture of distributed infrastructure network systems is typically spanning long distances in the provision of infrastructure services from increasingly centralised production modes (Zimmerman, 2004) and be it direct connectivity, policies and procedures or geographic proximity, most critical infrastructure systems interact. The ability to do this is a result of the complex dependency relationships and interdependency relationships that cut across infrastructure boundaries (Pederson *et al.*, 2006).

Furthermore, the concept of critical infrastructure connection is important to a wide range of social, economic and political issues depending on the potential implications and state of these reciprocal connections. In this context, the beneficial influences of two or more interconnected entities is the exchange of ideas, information, currency and other valuable goods and services that are for mutual benefit (Murray & Grubesic, 2007).

However, typically these infrastructures operate in a physical environment that is reflective not only of the individual inputs, outputs and states, but also influenced by other infrastructure behaviours and characteristics. Add to this the context in which owners and operators are pushing their own goals and objectives, constructing value systems for defining and viewing their businesses, analysing and developing models of their operation, and making decisions that impinge upon infrastructure architectures and operations. Even the operational state and physical condition of infrastructures influence the environment that in turn influences stress and demand on individual infrastructures; in these terms the environment and the infrastructure systems are interdependently linked (Brown *et al.*, 2004; Peters *et al.*, 2008; Rinaldi *et al.*, 2001).

Another aspect of the systems environment is the heterogeneous aspects of infrastructures and the fragmentation between infrastructure systems where the connections via large technical systems enable the different systems to technologically coexist and function cooperatively. With such an array of differing systems and purposes a realisation is that the collapse of services from these systems would be potentially disastrous for entire economies and societies (de Bruijne & van Eeten, 2007).

In terms of critical infrastructure systems particularly, there has been some disagreement between scholars and experts in the field, but the body of work shares some common points of view that (Egan, 2007):

- Creating reliability over multiple management generations in complex, tightly coupled systems is difficult and extraordinarily demanding;
- The hope of doing so grows increasingly distant as technological systems grow larger and more complex.

In addition to these two points, as infrastructure systems increase in criticality, through societal reliance, they produce potentially greater security vulnerabilities. The proliferation of