Chapter 28
SCADA Systems Cyber Security for Critical Infrastructures: Case Studies in Multiple Sectors

Suhaila Ismail
School of Information Technology and Mathematical Sciences, University of South Australia, Adelaide, Australia

Elena Sitnikova
Australian Centre for Cyber Security (ACCS), University of New South Wales at ADFA, Canberra, Australia

Jill Slay
Australian Centre for Cyber Security (ACCS), University of New South Wales at ADFA, Canberra, Australia

ABSTRACT

Past cyber-attacks on Supervisory Control and Data Acquisition (SCADA) Systems for Critical infrastructures have left these systems compromised and caused financial and economic problems. Deliberate attacks have resulted in denial of services and physical injury to the public in certain cases. This study explores the past attacks on SCADA Systems by examining nine case studies across multiple utility sectors including transport, energy and water and sewage sector. These case studies will be further analysed according to the cyber-terrorist decision-making theories including strategic, organisational and psychological theories based on McCormick (2000). Next, this study will look into cyber-terrorist capabilities in conducting attacks according to Nelson's (1999) approach that includes simple-unstructured, advance-structured and complex-coordinated capabilities. The results of this study will form the basis of a guideline that organisations can use so that they are better prepared in identifying potential future cybersecurity attacks on their SCADA systems.

DOI: 10.4018/978-1-7998-2466-4.ch028

1. INTRODUCTION

We rely heavily on services provided by the operators of Critical infrastructures on a daily basis. These services include water, energy, gas, transportation, telecommunications, finance and banking, food and agriculture, etc. The services mentioned are categorised as critical infrastructures due to its crucial importance to society as a whole. On this note, attacks that are tailored for this system can leave the systems compromised and cause financial and economic damage to organisations and nations.

The nature of critical infrastructures is complex. The interconnectivities and interdependencies of these critical infrastructures are highlighted security risks that might lead to a collapse of services. The dependence on information systems and the increasing interdependencies between systems are directly related to the severity of the threat. Cyber security was propelled into the political security agenda in the mid-1990s when it was persuasively linked to both terrorism and critical infrastructures protection (Dunn, 2005). The worst possible consequences of risks created by information and communication technologies (ICT) manifest themselves in the possible failure of so-called critical infrastructures, which are systems and assets whose incapacity or destruction would have a debilitating impact on national security and a state's economic and social well-being (Kjaerland 2006). As noted by Schultz (2005), information security is primarily a people problem. Technology is designed and managed by people, leaving opportunities for human error.

It is necessary to evaluate past attacks so that organisations learn and prepare themselves better in terms of securing their environment. A report published in the *Journal of Homeland Security* by (Donahue & Tuohy, 2006) focused on the need for physical security- concerned planning, resource management, evacuation, situational awareness, communications, and coordination before Hurricane Katrina, 2005. Incidents such as 9/11 (2001), the Oklahoma City bombing (1995) and Hurricane Andrew (1992), did not mean that lessons were taken seriously even though these disasters could have been avoided if better precautions were taken including; improved communication systems, command and structure; faster deployment of resources, etc. These features are linked to previous attacks on SCADA systems and organisations must be prepared for possible future attacks on the system. There is also a need to address the issues of SCADA organisations preparedness in terms of cyber security, as we explore the multiple case studies below which includes attacks internally and externally that was perpetrated by attackers that had knowledge on the complex architecture of the SCADA systems. A Critical Infrastructure Protection (CIP) 2011 survey results reflected that there are lower awareness and engagement in CIP initiatives and global organisations feel less prepared (Symantec, 2011). Risk and vulnerability assessments in terms of evaluating the existing security policies and procedures, configurations, access controls, network hardware and software vulnerabilities, remote control access and operational controls within SCADA organisations must be vigorously implemented in order to prepare organisations in preventing potential catastrophic attacks.

This research seeks to explore previous attacks on SCADA systems for Critical infrastructures focusing on the transport, energy and water and sewage sector and the intelligence operations as well as the role of security in each case study. The following section will then focus the discussion on the attackers' decision-making based on the existing framework on how cyber-terrorist decisions are reached, and the cyber-terrorist capabilities in penetrating a system. Finally, the results of this research will articulate guidelines for organisations to better prepare themselves in identifying future cyber-security attacks on SCADA systems.