Chapter 1
Cyber Attacks on Critical Infrastructure:
Review and Challenges

Ana Kovacevic
University of Belgrade, Serbia

Dragana Nikolic
University of Belgrade, Serbia

ABSTRACT

We are facing the expansion of cyber incidents, and they are becoming more severe. This results in the necessity to improve security, especially in the vulnerable field of critical infrastructure. One of the problems in the security of critical infrastructures is the level of awareness related to the effect of cyberattacks. The threat to critical infrastructure is real, so it is necessary to be aware of it and anticipate, predict, and prepare against a cyber attack. The main reason for the escalation of cyberattacks in the field of Critical Infrastructure (CI) may be that most control systems used for CI do not utilise propriety protocols and software anymore; they instead utilise standard solutions. As a result, critical infrastructure systems are more than ever before becoming vulnerable and exposed to cyber threats. It is important to get an insight into what attack types occur, as this may help direct cyber security efforts. In this chapter, the authors present vulnerabilities of SCADA systems against cyber attack, analyse and classify existing cyber attacks, and give future directions to achieve better security of SCADA systems.

INTRODUCTION

In recent years cyberspace has been expanded significantly and evolved into a large, dynamic, and tangled web of computing devices. This situation has also influenced critical infrastructure systems. Besides positive effects of technological expansion, there are also drawbacks. Critical infrastructure is the backbone of everyday lives in modern society, and thus a proper functioning of it is essential. For a long time most critical infrastructure systems have been considered immune to cyberattacks because of their reliance on proprietary networks and hardware. However, recent experiences and cyber attacks indicate that this is unsustainable – the move to open standards and web technologies is making critical infrastructure systems more vulnerable.

DOI: 10.4018/978-1-4666-6324-4.ch001

Unintentional or malevolent actions taken in cyberspace have consequences on critical infrastructures in the physical world. After a few sporadic attacks it became clear that attacks in cyberspace are not limited to government activities for intelligence purposes, but any part of critical infrastructure may be subject to attacks, from the banking system and utilities to the transport or supply of essential goods and commodities. The modes of these attacks on critical infrastructure are diverse and include direct or anonymous access to protected networks via the Internet and Supervisory Control and Data Acquisition (SCADA), or breach of the employees who do not follow security procedures leading to malware propagation inside the firewall. The problem with analyzing cyber attacks in the field of critical infrastructure is that some cyber attacks remain unnoticed; and also some organizations are extremely unwilling to report incidents, because they are viewed as potential embarrassments. Furthermore, the appearance of new complex malware, such as Stuxnet, with unpredictable features, is creating new dimensions in cyber security. One of the most pernicious problems with cyberspace is that the fight is so unbalanced that it takes huge resources to protect critical infrastructure, but just one infected computer drive to launch an attack. Therefore, cyber defence has become one of the most important issues in national defence strategies. This paper presents an overview of the cyber attacks on critical infrastructure.

The remainder of this paper is organized as follows: Section 2 presents Critical Infrastructure. Section 3 presents SCADA systems that are used for Critical Infrastructure and vulnerabilities of SCADA systems against cyber attacks. Section 4 analyzes and classifies cyber attacks on SCADA systems for critical infrastructure. Section 5 discusses future directions to achieve better security of Critical infrastructure sectors using SCADA systems. Section 6 provides the concluding remarks.

CRITICAL INFRASTRUCTURE

There is a slight difference between countries concerning their definition of critical infrastructure (CI) sectors. CIs are defined as those systems, assets, or part thereof which are essential for the maintenance of vital societal functions, security and economic security, and the disruption or destruction of which would have a significant impact on the state/nation as a result of the failure to maintain those functions (European Commission, 2008). The US approach is more comprehensive and inclusive, and it has been particularly evolving since the attacks of September 11, 2001.The U.S. Patriot Act defined CIs as "systems and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" (USA- PA, 2001). *Homeland Security Act* of 2002 (P.L. 107-296, Sec. 2(4)) established the Department of Homeland Security (DHS) and also formally introduced the concept of "key resources**"** (Congress U.S., 2002). "Key resources" are defined as "publicly or privately controlled resources essential to the minimal operations of the economy and government" (Sec. 2(9)). Without articulating exactly what they are, the act views key resources as distinct from critical infrastructure, albeit worthy of the same protection.

The most conventional list of critical infrastructure sectors includes: agriculture and food, water, public health and safety, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, industry/manufacturing, postal and shipping.

Each of these sectors has its own infrastructures such as highways, electric power generation and distribution, etc. In any of these, a critical