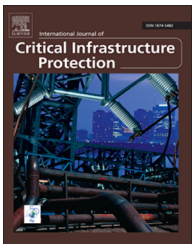
Available online at www.sciencedirect.com

ScienceDirect

www.elsevier.com/locate/ijcip



Identifying critical infrastructure sectors and their dependencies: An Indian scenario

Abhishek Narain Singh[a,*], *M.P. Gupta*[a], *Amitabh Ojha*[b]

[a]*Department of Management Studies, Indian Institute of Technology Delhi, New Delhi 110016, India*
[b]*Research Design and Standards Organization, Lucknow 226011, India*

ARTICLE INFO

Article history:
Received 9 July 2012
Received in revised form
16 October 2013
Accepted 4 April 2014
Available online 13 April 2014

Keywords:
Critical infrastructure sectors
Identification
India
Interpretive structural modeling
MICMAC
Critical infrastructure dependencies

ABSTRACT

Across the globe, critical infrastructures constantly face the risk of cyber and/or other attacks from hostile and malicious entities as well as damage inflicted by natural disasters. This paper seeks to identify the critical infrastructure sectors of a country, namely India, and to explore the dependencies existing among them. The research draws on the extant literature as well as expert opinion and judgments to identify the critical infrastructure sectors. Following this, the interpretive structural modeling (ISM) technique is employed to discover the relationships and dependencies existing among the identified critical infrastructure sectors. Next, cross-impact matrix multiplication applied to classification (MICMAC) analysis is used to categorize the critical infrastructure sectors into four subgroups based on their driving power and dependence on other sectors. Policy implications for government entities and businesses in India are also discussed.

1. Introduction

The protection of the critical infrastructure, which includes power, transportation, telecommunications, banking, information and communications technology, from cyber and/other attacks by hostile or malicious entities as well as natural disasters continues to be a serious concern across the globe. Definitions of the term "critical infrastructure" as appearing in the literature (Table 1) hold good for this paper as well. Since infrastructure assets are owned and/or managed by the public and private sectors, the protection of these infrastructure resources is no longer an issue that concerns governments alone. Further, the various critical infrastructure sectors in modern economies are so interconnected and interdependent that a disruption of one critical infrastructure can impair or adversely affect the functioning of several other critical infrastructures. Imagine a scenario where the power grid as well as backup power supply in a region goes down because of a natural calamity or sabotage. In such a situation, telecommunications, banking, manufacturing, etc. would all be crippled, potentially producing serious economic and social consequences for the affected region.

A classic example is the Hyogoken-Nanbu earthquake that struck Kobe, Japan and surrounding areas on January 17, 1995. The earthquake resulted in more than 6000 deaths and 30,000 injuries, and accounted for an estimated economic loss of 200 billion USD [1]. Trains were derailed and a power failure left approximately one million people without electricity [2]. Another example is the 2005 Hurricane Katrina in the United States, which caused severe floods and critical infrastructure collapse that completely paralyzed New Orleans, Louisiana and severely affected several Gulf Coast states. More recently, in July 2012, a number of power grids failed in India, resulting in power blackouts in most of the northern and north-eastern states.

*Corresponding author.
E-mail address: singhabhi444@gmail.com (A.N. Singh).

http://dx.doi.org/10.1016/j.ijcip.2014.04.003
1874-5482/

Table 1 – Definitions of critical infrastructure.

Definition	Reference
"…Critical infrastructures are organizational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences."	FOIS (BSI), Germany [5]
"…Critical infrastructure means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social wellbeing of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions."	Council Directive-European Union [6]
"…Those physical facilities, supply chains, information technologies and communication networks that, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security."	CIRS-Australia [7]
"…Critical infrastructure includes systems and assets so vital to the United States that their incapacity or destruction would have a debilitating impact on national security. Key resources are resources essential to the minimal operations of the economy and government."	GAO-USA [8]

The blackouts and their crippling effects on the other critical infrastructures affected the lives of approximately six hundred million people [3].

Motivated by these examples, this paper seeks to identify the critical infrastructure sectors in India and discover the dependencies existing among them. Drawing on expert opinion and judgment, a list of thirteen critical infrastructure sectors are identified and the interpretive structural modeling (ISM) technique is used to demonstrate the dependencies existing among the thirteen critical infrastructure sectors. The primary justification for this India-focused study is that the understanding of the critical infrastructure and the development of critical infrastructure protection strategies in India are still in an evolving stage.

While the threat of physical attacks has always existed in varying degrees, critical infrastructures now increasingly face the threat of cyber attacks. The emerging scenario has been elegantly stated by Richard George, former Technical Director of Information Assurance at the U.S. National Security Agency: "*…there will never be another war in which the critical infrastructure is not both, a cyber and physical target*" [4]. Although this paper has been motivated by the increasing risk of cyber attacks, the research results are certainly relevant to other types of attacks on the critical infrastructure.

The next section reviews the major initiatives undertaken worldwide in the area of critical infrastructure protection as well as the measures adopted by India. Section 3 presents the research methodology and data analysis using ISM and MICMAC (matrice d'impacts croisés multiplication appliqués à un classement, i.e., cross-impact matrix multiplication applied to classification). Section 4 discusses the ISM and MICMAC analysis results vis-à-vis previous research findings, the implications for government and business, and the research contribution. Expert viewpoints are summarized in Section 5. Section 6 discusses the limitations of the research and identifies avenues for future work. The final section presents the conclusions.

2. Literature review

In keeping with focus of the paper on critical infrastructure dependencies and cyber security concerns, the literature on the mutual dependency of critical infrastructures as well as cyber attack motives and countermeasures are briefly reviewed. Following this, the extant literature is explored to clarify the measures undertaken by India with regard to cyberspace security.

2.1. *Types of dependencies and shared vulnerabilities and threats*

Dependencies among critical infrastructures have their unique characteristics and effects. Rinaldi et al. [9] have grouped infrastructure dependencies into four categories: (i) physical dependencies; (ii) cyber dependencies; (iii) geographical dependencies; and (iv) logical dependencies. However, more recent research has suggested that vulnerabilities or threats shared by two infrastructures should not be treated as a dependency [10]; according to this point of view, the geographical factor should not be considered to be a dependency. The present research is motivated by critical infrastructure vulnerability concerns that arise from cyber dependencies.

2.2. *Critical infrastructure dependencies, cyber attack motives and countermeasures*

The task of securing the critical infrastructure of a country is extremely difficult due to the multifaceted functions and dependencies of the various critical infrastructure sectors. Indeed, the dependencies among critical infrastructures renders them more complex as well as more vulnerable. According to Setola et al. [11], the dependencies are often hidden and not well recognized even by infrastructure operators. In other research, Little [12] has captured the dependencies of electric power, water, oil, transportation, natural gas and telecommunications sectors using directional graphs, along with their causes. Several researchers [13,14] have designed interactive visualization tools to analyze the dependencies existing among critical infrastructures. Numerous sector-specific studies have been carried out by scholars across the globe to understand the complexities of various infrastructure sectors (see Table 2). The dependencies among critical infrastructures and their cascading effects have been investigated by Rahman [34]. Theoharidou et al. [35] have developed a common body of knowledge for information security