Chapter 54
Critical Infrastructure Protection in Developing Countries

Amr Farouk
Arab Academy for Science, Technology, and Maritime Transport, Egypt

ABSTRACT

Not all infrastructures are critical. In most countries' definitions, a critical infrastructure (CI) is a collection of indispensable assets that provide an essential support for economic and social well-being, for public safety and for the functioning of key government responsibilities. CI assets can be classified into three broad categories: Physical, Cybernetic and Human. In the present era, Information and Communication Technology sector (e.g., Cloud Computing, Big Data, Internet of Things) can be regarded as the backbone of the economies of developed and the developing countries worldwide since they provide basic services to all segments of a society. Critical infrastructure protection (CIP) is a concept du jour in many developed countries. The present chapter discusses the method of protecting critical infrastructures in developing countries. It observes many developing countries experiencing massive growth in Internet capacity and the use of Internet-based technologies. Attacks on the information infrastructure can severely affect the ability of a country to function effectively.

CRITICAL INFRASTRUCTURE

Critical infrastructure (CI) refers to those essential physical and information technology facilities, networks, services and assets, which, if disrupted or destroyed, would have a serious impact on the health, safety, security, economic or social well-being or the effective functioning of government as proposed in Graham (2011).

According to Bennett (2007), not all infrastructures are critical. A product or service is critical when either it provides an essential contribution in maintaining a defined minimum level of national or international law and order, public safety, economic life, public health, and environmental protection, or if the disruption of its ability to provide product or services hurts citizens or government administration and may endanger security. Some are critical only when others are damaged (e.g., emergency services).

As proposed in Schrogl and Hays (2015) a critical infrastructure is a collection of indispensable assets. An asset, a subset of a critical infrastructure, is something of high importance or high value and

DOI: 10.4018/978-1-5225-8897-9.ch054

can include people, property, or information systems. Critical infrastructures are best selected by each individual jurisdiction, as they know their specific circumstances best, e.g., Global Positioning System (GPS) timing signals currently provide the "heartbeat" that synchronizes all global telecommunications networks, yet there is a lack of appreciation for this dependency and underdeveloped policies to ensure protection of this critical space infrastructure.

The definitions of "infrastructure" used in official descriptions of critical infrastructure tend to be broad. Most also include intangible assets and/or to production or communications networks.

The danger when discussing CI is making it either too broad or too narrow. Any country has fully defined what is critical and what is not. Critical infrastructure, key resources, and key assets are located everywhere and anywhere. They are present in all aspects of our daily routine. It is easy to define them as a collection of assets present within a jurisdiction. A jurisdiction is a responsible party that has authority and control over the activities within a specific geographical area.

The following qualifications impact the criticality of infrastructure:

- The more dependencies, the more critical.
- The more vulnerable, the more critical.
- Lack of alternatives increases its criticality.

Graham (2011) broke down CI assets into three broad categories that span all sectors of country's economy:

1. **Physical:** These are all the tangible assets e.g., roads, oil and gas pipelines, electrical power transmission and distribution networks, telecommunication (data, voice) networks, dams, and vital institutions such as hospitals that are deemed essential to maintaining our society. Physically stored information is a part of this category.
2. **Cybernetic:** This rapidly expanding category includes all the technology that depends upon information, hardware, software, data, and networks used within the CI context. This also includes all electronic information stored within these systems and controlling and monitoring systems that permit remote management of CI asset components.
3. **Human:** Often forgotten in this discussion are the people who operate CI systems. They have knowledge, know-how, and experience that, if lost, represents a major threat to the ability to sustain or restore CI systems. Also included are other elements of human threats such as the potential for insider access to physical plant and systems as well as the robustness of management and culture to be alert to threats and build in resilience.

According to Bennett (2007) critical infrastructure and key assets can be static or mobile. Static assets are those that are fixed in place, e.g., a hospital. Mobile assets are those that move around from place to place, e.g., a subway car. When comparing critical infrastructure and key resources from several different jurisdictions, it may be necessary to categorize or rank assets. This categorization may be necessary to ensure that proper resources, especially funding, are directed at the proper asset so that it can be protected. For this purpose, critical infrastructure and key resources are categorized based on national level of importance, state or regional level of importance, and local community level of importance.

Soft targets are those infrastructures or key resources that usually lack proper security or are difficult to protect and defend because they are open to the general public by their very design. They are