Chapter 2
Resilience Principles for the ICT Sector

Scott Jackson
University of Southern California, USA

ABSTRACT
This chapter summarizes a set of abstract principles extracted from the literature pertaining to the resilience of systems in the ICT sector from which concrete solutions can be developed. Case studies are discussed that illustrate the validity and criticality of these principles. Also discussed is the interdependency among these principles that show that, in general, concrete solutions cannot be developed from principles individually but must be implemented in combination with other specific principles. A model of the phases of a disruption is shown and the applicability of these principles to these phases is discussed. Both single and multiple threat scenarios are discussed that reflect historical cases.

INTRODUCTION
A recurring pattern among major catastrophes is the loss of communications, command and control, and other capabilities that are intended to enable rescue and recovery efforts. These catastrophes may be caused by natural phenomena such as earthquakes or hurricanes. Or they may be terrorist attacks, or they may be caused by operator error or design error. These disruptions sometimes occur in a plurality of events when one disruption gives rise to another disruption. It is the purpose of this chapter to present a set of principles which may be used as guidelines for experts in the ICT sector to create concrete solutions that would either prevent these losses or enable the ICT system to recover to an acceptable level of functionality.

So what is the scientific value of this chapter? First, the science of resilience engineering is an emerging discipline. Many engineers may not appreciate the strategies for enabling a system, in particular an ICT system to avoid, survive, and recover from a major threat such as a natural or human-made threat. This chapter is an introduc-
tion to the science of accomplishing that goal. Second, many engineers will not appreciate all the options for accomplishing that goal. One goal of this chapter is to illustrate that by viewing the principles from an abstract point of view, these options will become clearer.

Furthermore, by viewing the principles from an abstract point of view the principles can be applied to different designs in different scenarios against different threats. Finally, by showing the interdependencies among the principles, the engineer will be able to see how the principles must be implemented in combination and not singly. Since the only concrete solutions to these principles are the ones extracted from the case studies, there will be many others the readers will discover in their own scientific pursuits. It is hoped that this chapter will assist the reader in achieving that goal.

While the focus of this book is the ICT sector, this chapter will remind the reader that the ICT sector does not operate in isolation. For an infrastructure system to be resilient one has to ask the questions: Within what kind of organizational environment do the ICT elements operate? Do the human operators understand the information being transmitted? If not, what are their alternatives? These questions and others will be explored through the expertise of researchers in the field and through case studies to be summarized in this chapter.

**An ICT Engineered System**

In the current context an ICT system is considered to be an engineered system in the broadest sense of the word. The International Council on Systems Engineering (INCOSE, 2006, p. 5) defines a system as:

An integrated set of elements, subsystems, or assemblies that accomplish a defined objective. These elements include products (hardware, software, and firmware), processes, people, information, techniques, facilities, services, and other support elements.

This definition includes the physical assets of the system, the humans, and the techniques for assuring the functionality of the system. These techniques may consist of protocols used to operate the system.

**A Disruption**

A disruption is an interruption in functionality caused by a threat, such as a terrorist attack or natural event. The schematic in Figure 1 shows the progression in the state of a system as it may detect the threat, encounter it or perhaps one or more additional threats, and then reaches a final state of recovery hopefully to a satisfactory level of functionality.

In the initial state the ICT system may be at rest or in an operational state. In Phase 1 the threat may be detected and action taken to avoid or minimize the impact of the threat. Following the first event, the encounter with the threat the system may lose functionality and enter an interim state in which one or more additional threats are encountered. Historically, multiple sequential threats are common. The 1906 San Francisco earthquake followed by fires that destroyed much of the city is an example. Following this cycle the system will enter its final state in which it may be repaired or restored for future use. In the discussion to follow it will be shown how each principle will apply to one or more of these phases.

*Figure 1. Disruption and recovery diagram; adapted from (Jackson & Ferris, 2013)*