

# Chapter 70

## ICT Resilience as Dynamic Process and Cumulative Aptitude

Paul Theron  
Resilience Studies Team, France

### ABSTRACT

*Many definitions of resilience coexist today, whether within the domain of telecommunications or in the vaster world. Is it a process? Is it a production? Is it a learnt aptitude? This debate has been going on in social sciences for decades and ICT revives it in its own ways today. This chapter proposes a definition of resilience founded on three findings: (1) resilience is the aptitude of a sociotechnical system to surmount a crisis; (2) whether in the telecommunication sector or elsewhere, a crisis is an experience of collapse that stems from critical incidents; (3) critical incidents are a complex dynamic phenomenon, and resilience is its counterpart, a dynamic, adaptive attempt to master circumstances, a form of dynamic struggle against adversity. To support this thesis, first the chapter reviews some of the main elements of literature on hand, browsing through different currents of research, including computing science and social sciences. Next, the chapter presents a short analysis of some significant incidents to show their dynamic nature and how systems they affect collapse and react, possibly resiliently. Third, it suggests an articulated definition of resilience, very applicable to ICT and largely discussed with scientists and professionals in the past three years. The chapter concludes that this definition acts as a paradigm that opens new questions for research, standardisation, and change management projects.*

### INTRODUCTION

Resilience is a composite notion that has been studied from various angles in different domains of science, from Psychology to Computing Science. In the field of Psychology, the focus is

placed on successful coping with highly adverse (traumatic) circumstances at hand. In sociological studies, resilience is an aptitude necessary to deal with crises affecting communities and their environment and that may stem from decisions made in the high spheres of politics. From an organisational perspective, there is an hesitation between considering that reliable organisations

DOI: 10.4018/978-1-4666-4707-7.ch070

are resilient and the view that there resilience is an organisation's elasticity in response to adversity materialised by procedures as well as non-technical skills. In the domain of Critical Infrastructure Protection (CIP) and more specifically of Critical Information Infrastructure Protection (CIIP), resilience is a term that still covers a wide spectrum of abilities and dispositions. Resilience has also been equated to critical software that is resistant to cyber attacks. But there is today a vast recognition of the fact resilience is needed because extra-ordinary events may occur and, in parallel, that ordinary risk management measures would fall short of efficiency in that case. And resilience has even been deemed an opportunity to develop new strengths in business and Critical Infrastructures and to grow organisations to a higher level of performance.

In ICT systems, resilience is a dynamic, engineered aptitude that allows to survive critical incidents that occur despite defence barriers crafted into those systems.

As the variety of views expressed on this concept in our literature review suggests a general instability of its understanding, this chapter tries to capture its essence out of the analysis of case studies and by breaking the barriers of scientific disciplines.

Four case studies are briefly evoked here: hurricane Katrina, which had devastating impacts on telecommunication systems not mentioning the human tragedy it sparked; 9/11 attacks against the World Trade Center in Manhattan, which also triggered a similar tragedy and knock-on effects on telecommunications; the likely cyber attack against Palestine on November 1<sup>st</sup>, 2011; and the Mann Gulch Disaster, a tragedy in the social sphere of American Smokejumpers that helps to grab in a few words only the very nature of the resilient reaction to major adversity.

Resilience is an interactive struggle between hostile circumstances on one hand, which have the power to destroy men, systems, organisations and

societies, and, on another hand, decision-makers who seek both to keep acting on their missions and to resist destruction.

This chapter tries to articulate a definition of resilience respectful of its dynamic nature and of the understanding of those, engineers and managers, who on a day-to-day basis build systems to deliver their functionality, to avoid and to surmount challenges.

The reflections presented here stem from previous studies and have been influenced by research in the fields of Trauma Psychology, Social Ecological Systems Resilience and Internet Survivability. They synthesise seven years of research efforts.

From the literature review and the cases presented earlier, we show that resilience can be understood only as a response to incidents that occur despite prevention and protection measures taken to avoid them. We present a way to categorise incidents affecting telecommunication systems that was elaborated in a prior study. This Incident Severity Scale defines six levels of resilience and helps those who already have notions of resilience to situate their past choices in relation to new resilience requirements. It organises the engineering of resilience into three complementary disciplines.

Besides, we propose a synthetic model of the dynamics of systems degradation under adversity. The Collapse Ladder model helps to shed some new light on the difficult circumstances of sociotechnical systems' survival. The notion of crisis is situated in relation to that of incidents. In particular it is made clear that crises are the experience of collapse systems undergo when they are confronted to critical situations that take them aback and destabilise them. This helps to understand that between the two realms a change occurs in the way people pilot the response to adverse events. Instead of founding the response to a challenge upon prescribed procedures, one has to rely upon its tactical intelligence and decision-making capability to respond to the challenges that occur. Our finding has constantly been that

35 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

[www.igi-global.com/chapter/ict-resilience-as-dynamic-process-and-cumulative-aptitude/90783](http://www.igi-global.com/chapter/ict-resilience-as-dynamic-process-and-cumulative-aptitude/90783)

## Related Content

---

### Looking Glass

Anni R. Coden, John R. Harrauld, Michael Tanenblatt, Theresa Jefferson and Pamela Murray-Tuite (2012). *International Journal of Information Systems for Crisis Response and Management* (pp. 17-28).

[www.irma-international.org/article/looking-glass/66345](http://www.irma-international.org/article/looking-glass/66345)

### Expectations vs. Practice in Critical Infrastructure Operator Crisis Communication: Lessons Learned From Portugal, France, Norway, and Sweden

Laura Petersen, Laure Fallou, Paul Reilly and Elisa Serafinelli (2021). *Information Technology Applications for Crisis Response and Management* (pp. 24-50).

[www.irma-international.org/chapter/expectations-vs-practice-in-critical-infrastructure-operator-crisis-communication/278599](http://www.irma-international.org/chapter/expectations-vs-practice-in-critical-infrastructure-operator-crisis-communication/278599)

### A Novel Concept of Biomorphic Hyper-Redundant Snake Robot: An Approach for Rescue Operation During Earthquake and Landslide

Yash Dinesh Shethwala, Ravi Pravinbhai Patel, Darshankumar Rajendrakumar Shah and Saurin M. Sheth (2019). *International Journal of Disaster Response and Emergency Management* (pp. 33-49).

[www.irma-international.org/article/a-novel-concept-of-biomorphic-hyper-redundant-snake-robot/233880](http://www.irma-international.org/article/a-novel-concept-of-biomorphic-hyper-redundant-snake-robot/233880)

### Curriculum Design and Development at the Nexus of International Crisis Management and Information Systems

Keith Clement (2012). *Managing Crises and Disasters with Emerging Technologies: Advancements* (pp. 187-196).

[www.irma-international.org/chapter/curriculum-design-development-nexus-international/63312](http://www.irma-international.org/chapter/curriculum-design-development-nexus-international/63312)

### A Social Media Content Based Location and Situation Analysis Model for Disaster Management

Renya N. Nath, N. Priya and C.R. Rene Robin (2019). *Emergency and Disaster Management: Concepts, Methodologies, Tools, and Applications* (pp. 312-323).

[www.irma-international.org/chapter/a-social-media-content-based-location-and-situation-analysis-model-for-disaster-management/207578](http://www.irma-international.org/chapter/a-social-media-content-based-location-and-situation-analysis-model-for-disaster-management/207578)