Chapter 13
Lessons from Major Incidents Influencing and Influenced by Telecoms Failures

Chris W. Johnson
University of Glasgow, UK

ABSTRACT

Previous studies have proposed new methodologies for the protection of national critical infrastructures without grounding their proposals in a detailed analysis of previous contingencies. This chapter provides the background for subsequent parts of this book by summarising previous telecom-related incidents. In particular, it considers the causes and consequences of natural disasters, of blackouts across power distribution networks, of terrorist attacks, and of ICT infrastructure failures.

INTRODUCTION

This chapter identifies the numerous interdependencies that exist between conventional critical infrastructures and information infrastructures. The aims of this chapter are to:

- Present case studies of major incidents (natural disasters, blackouts and terrorist attacks) that have had an impact on critical infrastructures and in which telecommunications failures exacerbated attempts to get-by, to resist, to recover and eventually rebound from those incidents.
- Present case studies of telecommunications failures that themselves had major consequences for the continued operation of national critical infrastructures.
- Provide graphical overviews of the incidents and case studies using the V2 technique – this helps readers to map out many different events during complex contingencies.
- Introduce an analytical framework for previous major incidents.

DOI: 10.4018/978-1-4666-4707-7.ch013

A secondary aim of this chapter is to motivate the telecoms inclusion principle described in a separate chapter. The following sections analyse key features in the response to the following contingency events:

- **Blackouts:** North America (2003);
- **Natural disasters:** Hurricane Katrina (August, 2005);
- **Terrorist Attacks:** London Bombings (July 7th, 2005);
- **ICT Infrastructure Failures:** Mediterranean Cable Breaks (January, 2008); Pakistan IP-Hijack of YouTube Servers (February, 2008).

BACKGROUND

The following pages identify a number of common stages can be identified across previous telecoms incidents.

- *Getting-by* describes how infrastructure providers initially strive to maintains activity at the highest possible level of performance despite adverse circumstances. This phase is characterised by ad hoc innovations that find ways of working around systems failures. For instance, temporary cells on wheels have been used to maintain mobile telephone connectivity in the immediate aftermath of major floods.
- The second phase that characterises previous incidents is based on *Resisting*; withstanding the destructive pressure of circumstances in order to maintain an ability to perform. Telecoms companies were quickly able to route their services around the routing infrastructures that were damaged by the 9/11 attacks on the World Trade Centre.
- The third phase focuses on *Recovering*. This resumes a nominal course of activity and development. This can be seen in the ways in which power distribution companies were able to restore services in the aftermath of blackouts as simulation software was gradually configured to reflect the real state of underlying power networks.
- The final stage is termed *Rebounding*. This captures the manner in which organisations and individuals learn key lessons from previous adverse events. For instance, many infrastructures that were damaged by Hurricane Katrina are being deliberately rebuilt with a level of resilience that goes well beyond what existed before this disaster.

THE IMPACT OF BLACKOUTS ON TELECOM INFRASTRUCTURES

The increasing integration of complex safety-critical systems creates vulnerabilities across power distribution, water supply, transportation, and communications infrastructures. Failures quickly propagate across national borders. Further vulnerabilities arise because the exchange of monitoring information between countries has not kept pace with the physical transfers between national systems. In consequence, individual states are often poorly equipped to deal with knock-on failures that stem from neighbouring areas of a network.

The North American Blackout (14th August, 2003)

Large portions of Ohio, Michigan, Pennsylvania, New York, Vermont, Massachusetts, Connecticut, New Jersey and the Canadian province of Ontario experienced an electric power blackout on 14th August 2003. The outage affected approximately 50 million people and 61,800MW of electric load. Power was lost for 4 days with rolling blackouts continuing for more than a week (US-Canada Task Force, 2004). A number of failures affected