ASHGATE

Policymaking for Critical Infrastructure

A Case Study on Strategic Interventions in Public Safety Telecommunications

Gordon A. Gow

Policymaking for Critical Infrastructure

A Case Study on Strategic Interventions in Public Safety Telecommunications

GORDON A. GOW
London School of Economics and Political Science

ASHGATE

Published by
Ashgate Publishing Limited
Gower House
Croft Road
Aldershot
Hampshire GU11 3HR
England

Ashgate Publishing Company
Suite 420
101 Cherry Street
Burlington, VT 05401-4405
USA

Ashgate website: http://www.ashgate.com

British Library Cataloguing in Publication Data
Gow, Gordon A.
Policymaking for critical infrastructure : a case study on strategic interventions in public safety telecommunications
1.Emergency communication systems - Security measures
2.Public key infrastructure (Computer security) 3.Wireless communication systems - Security measures
I.Title
384'.043

Library of Congress Cataloging-in-Publication Data
Gow, Gordon A.
Policymaking for critical infrastructure : a case study on strategic interventions in public safety telecommunications / by Gordon A. Gow.
p. cm.
Includes bibliographical references and index.
ISBN 0-7546-4345-X
1. Telecommunication--Security measures. 2. Public key infrastructure (Computer security) 3. Wireless communication systems--Security measures. I. Title.
TK5102.85.G69 2005
384'.043--dc22

2004025399

ISBN 0 7546 4345 X

Printed and bound by Athenaeum Press, Ltd.,
Gateshead, Tyne & Wear.

Acknowledgments

I wish to thank Professor Robin Mansell for the kind words of encouragement that led me to pursue this book project. I am especially grateful to Peter Anderson, David Mitchell, Richard Smith and Roman Onufrijchuk for their enduring support over the years.

Preparation of the final manuscript would not have been possible without assistance from the Department of Media and Communications at the London School of Economics. Johanne Provençal's copyediting has no doubt improved upon the flow and clarity of my ideas.

The case study research presented in the book was funded through programs sponsored by Public Safety and Emergency Preparedness Canada (formerly Office of Critical Infrastructure Protection and Emergency Preparedness) and the Social Sciences and Humanities Research Council of Canada.

For taking that courageous decision to join me in London, this book is dedicated to Sulya Anne.

I am, of course, responsible for reporting on and interpreting the evidence included in this study. Any errors or omissions are entirely my responsibility.

List of Abbreviations

AEAA	Alberta E9-1-1 Advisory Association
ALI	Automatic Location Identification
ANI	Automatic Number Identification
ANT	Actor Network Theory
BCSPA	British Columbia 9-1-1 Service Providers Association
CAS	Call-path Associated Signalling
CISC	CRTC Interconnection Steering Committee
CLEC	Competitive Local Exchange Carrier
CRTC	Canadian Radio-television and Telecommunications Commission
CTA	Constructive Technology Assessment
CWTA	Canadian Wireless Telecommunications Association
EPC	Emergency Preparedness Canada
ESRD	Emergency Services Routing Digits
ESWG	CISC Emergency Services Working Group
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
ICLR	Institute for Catastrophic Loss Reduction
ILEC	Incumbent Local Exchange Carrier
LTS	Large Technical Systems
MIN	Mobile Identification Number
MSAG	Master Street Address Guide
NCAS	Non Call-path Associated Signalling
NENA	National Emergency Numbering Association
OAB	Ontario 9-1-1 Advisory Board
OCIPEP	Office of Critical Infrastructure Protection and Emergency Preparedness
PSAP	Public Safety Answering Point
PSEPC	Public Safety and Emergency Preparedness Canada
PSTN	Public Switched Telephone Network
SCOT	Social Construction of Technology
TIF	Task Information Form
VAS	Value-added Services
WEWG	CWTA Wireless E9-1-1 Working Group
WSP	Wireless Service Provider

Introduction

This book represents an effort to weave together developments in the field of disaster management with an approach known as 'Constructive Technology Assessment' to provide a new perspective on policymaking for critical infrastructure. The essential argument that I put forward is that well-founded public policy must be based on an understanding of the social roots of risk and vulnerability in large technical systems and that this understanding must come from studying how these systems grow and change as *socio-technical* entities. It is precisely this knowledge that is prerequisite for the design and adoption of appropriate public policy interventions to achieve sustainable societies nationally and internationally.

The public information infrastructure plays a vital role and is at the heart of all critical systems in advanced industrial societies, and as such, it provides the central point of focus in the book. On the one hand, regulatory reform has resulted in a tremendous wave of technological innovation and ground-breaking opportunities for enhanced value-added services that could reduce risk and vulnerability by providing continuity services to a wide range of businesses and government institutions. On the other hand, such developments harbour hidden risks, particularly in light of rapid technological change and competitive pressures among service providers seeking to retain control over strategic network elements.

In many respects, this book is a product of my professional interest in an understanding of the process of growth and change in the public information infrastructure as a necessary step toward the identification and assessment of public policy intervention strategies. Originally, the project began with a general inquiry into the role of the telecommunications sector within Canada's National Disaster Mitigation Strategy, a public-private joint initiative launched in 2000/2001 and intended to reform that country's policy framework for emergency management. At the same time, I also discovered that Canada was not alone in adopting this mitigation-oriented policy framework but that such a framework was being introduced in countries around the world, corresponding in part to the aims and spirit of the United Nation's International Decade for Natural Disaster Reduction that had run from 1990 to 1999. Mitigation, it seemed to me, had emerged as the new *paradigm* for emergency and disaster management around the world.

As I continued my research, two important research questions surfaced. First, what would be the impact of a national mitigation strategy on the information infrastructure? Second, and conversely, how might the public information infrastructure be drawn upon to actively promote the objectives of such an initiative? Working on these questions, I began to realize that the term 'mitigation' itself was problematic and that many of the existing programs in emergency

telecommunications, business continuity planning, and critical infrastructure protection did not seem to conform to what I sensed to be the more fundamental concerns implied by Canada's National Disaster Mitigation Strategy or the promising objectives of other national and international initiatives.

This realization led me to conclude that the term 'mitigation,' despite the volumes that have been written on it, remains an ambitious but *ambiguous* idea that must be more clearly defined so it can stand apart from—and yet remain integrated with—other activities in disaster management. To achieve clarity on this matter, I looked beyond the typical descriptive model of disaster management based on a four-phase cycle and adopted an explanatory model of disasters that could more clearly account for the root causes of vulnerability and unsafe conditions in society. My adaptation and interpretation of the 'Pressure and Release' model for the management of critical infrastructure (found in the first chapter) suggests that mitigation-oriented policy research is appropriately directed toward the early processes and influences on network development—that is to say, the social roots of risk and vulnerability.

Having worked out a more satisfactory definition of mitigation, using what I felt to be a more suitable model for policy research, I then turned my attention to the theoretical and methodological issues of understanding and studying the fundamental forces of growth and change in large technical systems. This stage of my research led me to look for a body of theory that was consonant with an application of the mitigation paradigm, yet suitable to a study of critical infrastructure. The result is an assemblage of several related approaches from science and technology studies and Constructive Technology Assessment, operationalized through a selection of telecom policy research literature. Together these sources are integrated and form an analytical framework to study growth and change in networked systems, providing what I believe is a much-needed bridge between a growing body of scholarly research in science and technology studies, and the practical and pressing concerns of policymakers working in disaster mitigation and critical infrastructure protection.

Empirically, this study is intended to make a comparatively modest contribution to the history of technology and to applied policy research. The study also presents an operationalization of the analytical framework used to conduct a detailed analysis of the development of one instance of growth and change in the public information infrastructure. Historically, the study provides a detailed account of the development of a public safety telecommunications service known as Wireless 'enhanced' 9-1-1 ('Wireless E9-1-1'), a location-based emergency service for mobile telephone customers currently being deployed in North America. For applied policy research, the final chapter sets out a number of suggestions and examples of alternative intervention strategies based on observations made in the case study. These suggestions may prove useful to policymakers and other analysts who are considering how national mitigation strategies impact public policy for critical infrastructure and perhaps more importantly, how careful management of these large technical systems may serve to support the wider social objectives of mitigation-oriented initiatives.

Chapter One, 'A Public Policy Challenge,' introduces the background, rationale, and focus for the book. In this chapter I argue that modern societies face an interdependency dilemma that remains largely unaddressed in public policy that purports to be mitigation-oriented. I then critique and rethink the concept of mitigation by introducing the Pressure and Release model. I discuss the implications this model has for the management of critical infrastructure in general and for the study of the public information infrastructure in particular.

Chapter Two, 'The Design Nexus,' presents the theoretical and methodological foundations that I adopt to study growth and change in critical infrastructure. Here I look to Constructive Technology Assessment as a primary approach to the study of growth and change because of its emphasis on the early design phase of technology development. I also draw on Actor Network Theory and Social Construction of Technology to provide a theoretical model of technology dynamics for the book. I then bring together elements from each to establish a basic methodology and analytical framework for studying technological change. This framework takes the form of an 'intervention matrix' that serves as the principle analytical tool used in the case study on public safety telecommunications and throughout the book.

Chapter Three, 'Turning to the Empirical,' draws on research undertaken on Large Technical Systems (LTS) to establish the operational parameters needed to conduct empirical research on technological change. Among these parameters, I address the problem of setting boundaries on networked infrastructure and I identify 'interconnection' as a core operational concept. Interconnection also provides a crucial third dimension to the intervention matrix. On the basis of a selected range of literature in telecom policy research, I identify and discuss various issues related to interconnection, including technical standardization and the political economy of network design. Later in the book (Chapter Six), I return to the literature on Large Technical Systems and Social Construction of Technology to look at other issues associated with stakeholder participation in the management of critical infrastructure.

Chapters Four, Five, and Six present the case study in public safety telecommunications. The case follows in considerable detail the development and deployment of 'Wireless E9-1-1' in Canada. Wireless E9-1-1 is a public safety innovation that provides location-enhancement for mobile phone customers who dial emergency services. It is now being deployed in North America, as well as in Europe and Australia where it is variously referred to as 'E1-1-2' or 'MoLI' (Mobile Location Information). The service has significant impact at multiple levels of public information infrastructure, including service reconfiguration, operational procedure, and investment in new technology, and it provides a glimpse of the complexity of technological change in modern critical infrastructure.

Each of the three case study chapters is dedicated to one 'facet' of the Wireless E9-1-1 story. Chapter Four, 'The Standardization Effort,' focuses on the adoption of technical standards for Wireless E9-1-1 and illustrates the wide range of considerations that influence technological change in modern infrastructure and the corresponding challenges of identifying appropriate regulatory intervention to

ensure public interest objectives. Chapter Five, 'Innovation and Experimentation,' looks at the importance of industry-driven efforts toward innovation and experimentation in new value-added services and considers the role of policymakers in identifying obstacles to such efforts among new entrants and third parties. Chapter Six, 'Communities of Experts,' takes up the third facet of the case study and examines the difficulties associated with an expanded range and diversity of stakeholder participation in the management of critical infrastructure.

Finally, Chapter Seven, 'The Structures of Intervention,' provides an overall analysis of the Wireless E9-1-1 case study. This is undertaken in three steps. First I present a 'socio-technical mapping' of key actors and issues in the case and I discuss several predominant intervention strategies that became evident during my investigation. Second, I examine the case as a single unit of analysis using the intervention matrix to portray an overall structure to the observed interventions. I then critique this apparent structure to provide suggestions for its improvement, supported by real-world examples that together provide an alternative structure of interventions that I believe more closely corresponds to the principles and objectives of the mitigation-oriented policy framework presented at the beginning of the book.

The book covers a lot of ground and some readers may be surprised at the unusual perspective it brings to the study of critical infrastructure. My hope is that readers will nonetheless find the book fruitful to the extent that it presents some new ideas for this important subject of study and encourages further theoretical and empirical work along the lines I have introduced. For practitioners and policymakers, I hope the book lends a measure of clarity to the problematic notion of 'disaster mitigation' and provides some practical insight for the design of programs and policy interventions. Scholars in science and technology studies may simply be interested in the historical details of the Wireless E9-1-1 case or my adaptation of SCOT, ANT, and LTS to a field of applied policy research. Some readers will find the details of the case study rather profuse; however, I feel it has historical value, so I have tried to include as much detail as possible even where such detail may not be directly related to the book's primary aim.

Contents

List of Figures

List of Tables

Chapter 1

A Public Policy Challenge

> Creativity involves breaking out of established patterns in order to look at things in a different way.
>
> -Edward de Bono

The Interdependency Dilemma

The risk of local accidents escalating rapidly into nationwide critical incidents is perhaps nowhere more acute than in advanced industrial societies, where telecommunications continue to foster a complex integration of social institutions with large technological systems. In a series of revisions to its 'Guidelines for the Security of Information Systems' first published in 1992, the Organisation for Economic Co-operation and Development (OECD) recognized the growing state of infrastructure interdependency, observing that 'ever more powerful personal computers, converging technologies and the widespread use of the internet have replaced what were modest, stand-alone systems in predominantly closed networks' (Organisation for Economic Co-operation and Development, 2002).

The interdependency dilemma on the one hand refers to the tight coupling of modern institutions through telecommunications. The terrorist attacks on the World Trade Center towers in New York City not only caused a tragic loss of life and property but revealed the vulnerability of North America's communications infrastructure. In the aftermath of the incident, reports in the trade press indicated that a major U.S. telecommunications carrier, Verizon, had five central offices serving some 500,000 telephone lines in the vicinity of the World Trade Center and that more than six million private circuits and data lines passed through switching centres in or near the site of the collapsed twin towers. Additional reports claimed that the AT&T and Sprint switching centres in the World Trade Center were destroyed, as were numerous cellular base stations in the vicinity (Angus Telemanagement Group, 2001). Data networks for major corporations, including AOL Time Warner and other broadband services, were also disrupted by the collapse of the towers (Ray, 2001). A society increasingly bound together by electronic networks is at constant risk of telecommunications outages ascending to major incidents with consequences that extend far beyond the initial site of impact. The terrorist attacks of 9/11 were not about perpetrating a telecom outage *per se*, yet they underscore the vulnerability of the modern telecommunications infrastructure to unforeseen events.

On the other hand, the interdependency dilemma also refers to the fact that minor, seemingly innocuous, failures in the telecommunications network may have social effects that are far-reaching and often surprising in their immediacy. In the summer of 1999, for instance, a technician working at a telephone switching office in downtown Toronto accidentally dropped a tool into a power supply unit causing a minor electrical fire. The next morning, the story was splashed across the Canadian media. What started as a minor incident had erupted into a nationwide 'phone crisis,' for not only did the Toronto switch fire affect local voice telephone service, its impact rippled outward across the city and quickly spread to affect businesses from coast to coast. As it happened, the switching office turned out to be a key node in a nationwide data network that supports transaction services including credit card authorization and automated teller machines. Locally, the disruption spread beyond plain old telephone service to affect data services for numerous private and public institutions, including those with a vital social support function. Details of the incident were recorded in extensive press coverage of the event (Blackwell, Craig and Bell, 1999; Cheney, 1999):

- 113,000 telephone landlines were disrupted
- mobile phone service was disrupted
- Art Gallery of Ontario security system went offline
- travel agents went offline (one location lost some $30,000 worth of sales)
- some retailers were unable to process credit/debit card transactions
- Ontario Lottery terminals went offline
- some stock trading was affected
- law offices were unable to close real estate deals (clearing house for title searches was offline)
- hundreds of bank branches went offline
- almost 1/10 of cash machines across Canada were out of service for parts of the day
- sequencing for about 570 traffic lights was disrupted
- Toronto police telephone and computer systems were disrupted
- Hospital for Sick Children and several others were affected by disruption to pager and telephone services
- poison control centre and medical information hotlines were affected
- 9-1-1 system was maintained but capacity to handle calls was impaired.

A similar incident occurred in November 2000, when a contractor in a Chicago-area rail yard accidentally cut a cable providing access to the Canadian Venture Exchange (CDNX) trading system. The accident subsequently interfered with trading activities right across Canada when backup provisions for the system reportedly failed to work (Cattaneo, 2000). Modern telecommunications systems foster interdependencies whereby a distant event in a seemingly innocuous location can lead to serious disruptions for business and community organizations across vast distances. Some other examples of the interdependency dilemma (Robinson, Woodard and Varnado, 1998):

- The satellite malfunction of May 1998. A communications satellite lost track of Earth and cut off service to nearly 90 percent of the nation's approximately 45 million pagers, which not only affected ordinary business transactions but also physicians, law enforcement officials, and others who provide vital services. It took nearly a week to restore the system.
- The Northridge, California, earthquake of January 1994 affecting Los Angeles. First-response emergency personnel were unable to communicate effectively because private citizens were using cell phones so extensively that they paralyzed emergency communications.
- Two major failures of AT&T communications systems in New York in 1991. The first, in January, created numerous problems, including airline flight delays of several hours, and was caused by a severed high-capacity telephone cable. The second, in September, disrupted long distance calls, caused financial markets to close and planes to be grounded, and was caused by a faulty communications switch.

Increasing interdependency means that minor, local disruptions in telecommunications service due to a major earthquake, severe weather incident, workplace accident, or terrorist attack could quickly propagate nation-wide and even continent-wide second-order incidents of potentially disastrous magnitude in terms of unexpected social, economic, and even environmental repercussions. Such high stakes scenarios have not gone unnoticed by policymakers, particularly in the wake of the Y2K crisis and the terrorist attacks of 11 September 2001. These events have prompted a growing recognition of the interdependencies fostered by modern telecommunications, and serious efforts at reducing so-called 'common mode failures' (Hellström, 2003, p. 376) are now evident within the changing context of policy research for critical infrastructure (Gheorghe, 2004). The operational side of emergency preparedness and national security has also taken up the challenge. In February 2003, for example, the United States government issued its *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. In this strategy it calls for risk management based on the coordination of public and private interests:

> Because of growing interdependencies among the various critical infrastructures, a direct or indirect attack on any of them could result in cascading effects across the others. ... Critical infrastructures rely upon a secure and robust telecommunications infrastructure. Redundancy within the infrastructure is critical to ensure that single points of failure in one infrastructure will not adversely impact others. It is vital that government and industry work together to characterize the state of diversity in the telecommunications infrastructure. (United States, 2003, p. 49)

Similarly, in Canada the federal department of Public Safety and Emergency Preparedness Canada (PSEPC) has recognized the wide social interdependencies linked to the modern public telecommunications infrastructure:

> In this 'Information Age,' critical infrastructure is a key enabler to the modern economy. It is complex, interconnected and interdependent and relies heavily on information technology. Disruptions in one infrastructure could produce cascading disruptions across a number of other infrastructures, with significant economic and social consequences to Canada and Canadians. (Canada, 2001)

Concerns expressed in these official government statements are supported by research into critical infrastructure interdependencies. According to a study by Masera and Wilikens, this interdependency is a product of three major trends shared across the infrastructures that enable modern societies to function as they do. The authors summarize these as (1) the increasing complexity of technological systems; (2) a high degree of interconnectedness at both technical and organizational layers between these systems; and (3) a growing reliance on information and communication technologies to provide support for and control over various systems and subsystems. It is with this third trend that telecommunications enters into the picture as the vital link that integrates a variety of critical infrastructures into a complex network of co-dependent systems:

> The interconnections among infrastructures are facilitated by the internal use of ICT [Information and Communication Technologies], and by the availability of affordable means of establishing fast and reliable data communications. These communications means are beginning to be considered as a sort of public information infrastructure, and are increasingly employed for exchange of information and access to new value-added services such as trade tools for actors in a given market sector, and for getting connected with other infrastructures. ...
>
> ... the fact is that each and every infrastructure, and that means society at large, is attempting to benefit from the public information infrastructure. The end result is an overall, global dependence on a limited set of hardware and software technologies, with evolving and not yet mature interconnection and business models. (Masera and Wilikens, 2001)

An important facet of this observation is that the trajectory of the public information infrastructure remains contingent and relatively immature, reflecting the turmoil created by digital convergence and widespread regulatory reforms. On the one hand, such conditions breed greater vulnerability as a result of unforeseen risks and unexpected consequences of investment decisions. On the other hand, this contingency represents an opportunity for policymakers to embark on a coherent program of long-term risk reduction through the social shaping of critical infrastructure. It is in response to both the hidden risk and foreseeable opportunity that this book is principally addressed.

The astute reader may also have noticed a discrepancy between the 'public information infrastructure' mentioned above and the current telecommunications infrastructure that we tend to think about with respect to the regulation of circuit-based voice services. In their study, Masera and Wilikens are concerned with the information infrastructure made up of data networks that have in the past often been deployed separately from circuit-based voice networks. In other words, they

are concerned with the important distinction to be made between two types of information services that were originally established as separate infrastructures. Yet, the circuit-based voice network tends to remains synonymous in many countries with *regulated public access telecommunications*. While we should be careful not to conflate the two infrastructures because of their unique functional qualities and regulatory status, this situation is changing rapidly as voice and data services converge at trunk-side and as new voice-over-IP (VoIP) services and other digital standards are deployed at line-side. As voice service continues to evolve into just another data application, regulated public access telecommunications will become increasingly difficult to distinguish, either analytically or operationally, from other data networks. Therefore even *within* regulated public access telecommunications, we find a growing trend toward convergence of systems and new forms of infrastructure interdependency.

An integrated public information infrastructure may be nascent but even today we need not look far to glimpse the complexity of the emerging interdependencies. The electricity infrastructure is a case in point, caught in a double bind between supplying commercial power to operate communication networks and using communication networks to supply commercial power:

> An advanced management of the generation and distribution of electricity has been made possible by the establishment of monitoring and control systems relying on complex communications systems. In addition electric companies rely on information exchanges for their connections with the energy value chain and their customers. Thus *it is now possible to speak of the electricity infrastructure as composed of the power grid and an associated information network.* [emphasis added]

> ... energy producers and distributors, while trying to develop their markets and enhance their efficiency, are getting [*sic*] strongly dependent on the public open Information Infrastructure on both the demand and supply sides. They have to communicate with the other energy market actors, as well as complete the energy offer with information-related services. These could be energy information services related to the energy loads, generation and consumption, or pricing and billing; or derived services that take advantage of the link established with residential or industrial customers (for instance, alarm management, heating, etc.). (Masera and Wilikens, 2001)

From this example one can begin to further grasp how the public information infrastructure fosters wider interdependencies that are foundational for a range of services stretching across geographic, social, and economic strata. A major challenge for traditional approaches to the management of critical infrastructure, however, is that public policy and the resulting publicly funded programs for emergency management have encountered difficulties in coming to grips with these profound socio-economic interdependencies either as they exist in the present or as they are likely to intensify in the future. Not coincidentally, this difficulty reflects a much larger concern with the management of risk in modern societies, where there has been an increasing recognition of the need to reconcile technological development with wider social policy objectives such as privacy, economic and environmental sustainability (Misa, Brey and Feenberg, 2003).