SEEDS OF DISASTER, ROOTS OF RESPONSE

HOW PRIVATE ACTION CAN REDUCE PUBLIC VULNERABILITY

In the wake of 9/11 and Hurricane Katrina, executives and policymakers are more motivated than ever to reduce the vulnerability of social and economic systems to disasters. Most prior work on "critical infrastructure protection" has focused on the responsibilities and actions of government rather than on those of the private-sector firms that provide most vital services. *Seeds of Disaster, Roots of Response* is the first systematic attempt to understand how private decisions and operations affect public vulnerability. It describes effective and sustainable approaches – both business strategies and public policies – to ensure provision of critical services in the event of disaster. The authors are business leaders from multiple industries and experts in fields as diverse as risk analysis, economics, engineering, organization theory, and public policy. The book shows the necessity of deeply rooted collaboration between private and public institutions, and the accountability and leadership required to go from words to action.

Philip E. Auerswald, PhD, is director of the Center for Science and Technology Policy and an assistant professor at the School of Public Policy, George Mason University. Professor Auerswald's work focuses on linked processes of technological and organizational change in the contexts of policy, economics, and strategy. He is the co-editor of *Innovations: Technology | Governance | Globalization*, a quarterly journal from MIT Press about people using technology to address global challenges.

Lewis M. Branscomb, PhD, is professor of Public Policy and Corporate Management, Emeritus, at Harvard University's Kennedy School of Government. He also holds faculty appointments at the University of California, San Diego. Branscomb was the co-chairman of the project of the National Academies of Science and of Engineering and the Institute of Medicine, which authored the 2002 report *Making the Nation Safer: Science and Technology for Countering Terrorism.*

Todd M. La Porte, PhD, is an associate professor at George Mason University. He was a member of the Faculty of Technology, Policy and Management at the Delft University of Technology in The Netherlands. He also served for six years as an analyst in the information technology and the international security programs at the Office of Technology Assessment (OTA), a research office of the U.S. Congress.

Erwann O. Michel-Kerjan, PhD, is managing director of the Center for Risk Management and Decision Processes at the University of Pennsylvania's Wharton School. His work focuses on financing extreme events, with a prime interest in the creation and implementation of private–public collaboration among top decision makers of organizations or countries in America and Europe. He is a member of the Global Risk Network of the World Economic Forum.

Seeds of Disaster, Roots of Response

How Private Action Can Reduce Public Vulnerability

Edited by

PHILIP E. AUERSWALD
School of Public Policy, George Mason University

LEWIS M. BRANSCOMB
Kennedy School of Government, Harvard University

TODD M. LA PORTE
School of Public Policy, George Mason University

ERWANN O. MICHEL-KERJAN
The Wharton School, University of Pennsylvania

CAMBRIDGE UNIVERSITY PRESS

Shaftesbury Road, Cambridge CB2 8EA, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

314–321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre, New Delhi – 110025, India

103 Penang Road, #05–06/07, Visioncrest Commercial, Singapore 238467

Cambridge University Press is part of Cambridge University Press & Assessment, a department of the University of Cambridge.

We share the University's mission to contribute to society through the pursuit of education, learning and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9780521857963

First published 2006

A catalogue record for this publication is available from the British Library

Library of Congress Cataloging-in-Publication data
Seeds of disaster, roots of response : how private action can reduce public vulnerability / edited by Philip E. Auerswald . . . [et al.].
p. cm.
Includes bibliographical references and index.
ISBN-13: 978-0-521-85796-3 (hardback)
ISBN-10: 0-521-85796-1 (hardback)
ISBN-13: 978-0-521-68572-6 (pbk.)
ISBN-10: 0-521-68572-9 (pbk.)
1. Emergency management. 2. Infrastructure (Economics) – Security measures.
3. Public-private sector cooperation. 4. Crisis management. 5. Risk management.
6. Preparedness. I. Auerswald, Philip E. II. Title.
HV551.2.S44 2006
363.34´60973 – dc22 2006015888

ISBN 978-0-521-85796-3 Hardback
ISBN 978-0-521-68572-6 Paperback

CONTENTS

LIST OF CONTRIBUTORS

Philip E. Auerswald, School of Public Policy, George Mason University

Lewis M. Branscomb, John F. Kennedy School of Government, Harvard University

Todd M. La Porte, School of Public Policy, George Mason University

Erwann O. Michel-Kerjan, The Wharton School, University of Pennsylvania

Jay Apt, Carnegie Mellon University

Thomas Bowe, PJM Interconnect

Lloyd Dixon, RAND Corporation

John D. Donahue, Kennedy School of Government, Harvard University

Jacob Feinstein, Consolidated Edison (ret.)

Stephen E. Flynn, Council on Foreign Relations

Robert Allan Frosch, Kennedy School of Government, Harvard University

Sean P. Gorman, FortiusOne

Geoffrey Heal, Columbia Business School

Michael Kearns, The Wharton School, University of Pennsylvania

Paul Kleindorfer, The Wharton School, University of Pennsylvania

Michael Kormos, PJM Interconnect

Howard Kunreuther, The Wharton School, University of Pennsylvania

Patrick Lagadec, École Polytechnique in Paris

Todd R. LaPorte, University of California, Berkeley

Lester B. Lave, Carnegie Mellon University

Brian D. Lopez, Lawrence Livermore National Laboratories

James W. MacDonald, ACE USA

M. Granger Morgan, Carnegie Mellon University

Franklin W. Nutter, Reinsurance Association of American

Daniel B. Prieto, Reform Institute

Robert Reville, RAND Corporation

Emery Roe, California State University, East Bay

Paul R. Schulman, Mills College

Richard J. Zeckhauser, Kennedy School of Government, Harvard University

See author biographies on page 531.

FOREWORD

The nation's critical infrastructures are the great underlying strength of our country. In a word, things work. We take it for granted that when we throw the switch, the lights come on; when we turn the faucet, water flows; when we pick up the phone, we get a dial tone; when we dial 911, help arrives; and when necessary, we can confidently dispatch goods for overnight delivery to any location in the nation. These infrastructures underpin our economic strength, our national security, and our society's welfare – in simple terms, they are our nation's life support systems. It is the ready availability of reliable telecommunications, transportation, electrical power, fuel, financial, and emergency services that constitutes the solid foundation of our economy. Without ever-reliable telecommunications, power, and transportation infrastructures, our ability to mobilize and deploy the armed forces would be crippled. And finally, our modern society has become vitally dependent on these infrastructures for our most basic activities of subsistence, work, entertainment, transportation, and communications. Denial of any one of these services would cause widespread discomfort and discontent.

However, these infrastructures are not as robust as we might believe. Under continuing pressure to improve services, these systems' owners and operators eagerly pursued and incorporated the latest and best of information-age technology – computers to replace manual control, software to autonomously analyze and manipulate operations, higher communications speed and bandwidth to quickly move vast amounts of data, use of the Internet for commercial transactions and critical system control, and satellites to provide precision timing and location information for all the foregoing, to name a few. And in the rush to incorporate the latest technology, scant attention has been paid to resilience, survivability, and security. The modern information and communication technology incorporated in the late decades of the last century

contained early indications of increasing reliability problems and vulnerabilities. Widespread electric power outages appeared. Computer networks were invaded by unauthorized intruders. Thousands of computers were rendered inoperative by viruses. And cyber crime emerged as a serious law-enforcement challenge.

In recognition of these happenings and following a growing concern with domestic and foreign terrorism, a governmental interagency working group was formed to assess the magnitude of the emerging problems and to recommend a course of action to address them. After a year of deliberation, the working group concluded that the problems were of such importance, magnitude, and complexity that they warranted a concerted, high-level deliberative effort by a Presidential commission. Because of the preponderant ownership of the infrastructures by the private sector, the working group recommended that the commission comprise representatives from both the private and public sectors. Such a commission was directed by President Clinton by Executive Order 13010 on July 15, 1996. The resulting President's Commission on Critical Infrastructure Protection was charged with identifying the threats to the United States' critical infrastructures, assessing their vulnerabilities, and devising a strategy and plan for their protection. I had the pleasure of chairing that effort.

The commission was uniquely tailored for its task. As envisioned by the working group, the commission comprised representatives from federal departments and agencies and from the private sector; a steering committee of senior government officials helped us weave our way through the tangled web of government equities, and an advisory committee of key industry leaders (appointed by President Clinton) provided advice from the perspective of infrastructure owners, operators, and consumers. The commission deliberated full time over a period of 15 months and rendered its report in October 1997.

Much of the Commission's 15-month effort was devoted to researching and characterizing the infrastructures. They were then subjected to detailed analyses to identify their principal vulnerabilities. These analyses were conducted on a sector-by-sector basis. We found that networks of computers, databases, and communications (which can be called the cyber infrastructure) underpin each of the critical infrastructures. In other words, we found that every infrastructure relies on a cyber infrastructure to provide the communications and data handling necessary for its functioning. And we found that the critical infrastructures are interdependent – they are linked in a mutually supportive web that is not well understood. In addition, increasing the network linkage is creating unknown intersections and dependencies among infrastructures. This linkage increases the likelihood that a major disruption in one infrastructure will cascade into another. The bottom line is that the complexity of our

systems, the almost frenetic manner in which they have evolved with little or no attention to security, has created a seemingly endless range of vulnerabilities.

As to the threat, we did not find a "smoking keyboard" – we found no evidence that our nation's infrastructures were in immediate danger of a devastating cyber attack. Essentially, we found no credible information that a nation-state or international terrorist organization was prepared and poised to launch a debilitating cyber assault. However, we did learn that the capability to do serious damage to these systems was widely available. All it would take were the right skills and the right tools – skills that most teenagers have already mastered and dangerous tools that are readily available on the Internet. In short, we found that the capability to do harm was widespread and growing. Our conclusion, reached early in our deliberations, was that waiting for a serious threat to develop was a dangerous strategy. We needed to act immediately to protect our future.

I do not intend to recount all of the findings and recommendations of the commission. The reader can review them in the published commission report "Critical Foundations – Protecting America's Infrastructures." However, several key conclusions and recommendations warrant discussion here because of their special relevance to the writings in this book.

Having concluded that our infrastructures were highly vulnerable and that a serious threat was sure to emerge, the central question before the commission was how to apportion responsibility for fixing the problem. As one would expect, there was lively debate regarding the many possible options. They ranged from government-centric solutions involving legislation and regulation prescribing mandatory remedial actions by industry and government, to the opposite extreme of voluntary actions prompted by political leaders' urgings through stressing patriotic duty and the national interest. After much deliberation, we concluded that the private sector has a clear responsibility to protect itself from the lesser threats, such as individual hackers and criminals, and the government has the larger responsibility to protect citizens from national security threats. In short, we found that infrastructure protection is a shared responsibility. A complicating factor, however, is that the tools or weapons that hackers and criminals use are in many cases the same weapons used by terrorists and information warriors, albeit for more dangerous purposes. Therefore the sharing of responsibility for protection is somewhat blurred. Further exploration and discussion of this concept of shared responsibility is woven throughout the chapters of this book.

A second basic question faced by the commission involved what specific measures were required to "harden" the infrastructures in order to withstand a debilitating attack. Again, the solutions discussed ranged from issuing government-mandated standards on protection – involving such things as

firewalls, access control, system administration, redundancy, and back-up – to leaving the matter entirely in the hands of the owners and operators who have unique understanding of the operations and vulnerabilities of their systems. In this case, we opted for putting the matter primarily in the hands of the owners and operators, but strengthened by strong information-sharing mechanisms among owners and operators and between them and the government. The chapters in Parts III, IV, and VI of this book explore this matter in considerable detail.

Finally, a key challenge faced by the commission was determining what, if any, restructuring of the government bureaucracy was needed to implement the resulting strategy and plans for securing the nation's critical infrastructures. Underlying all of our deliberations in this area was the conviction that top-level political leadership was essential to fostering the unprecedented public–private partnership so essential to carrying out the plan. We made a series of recommendations of how the government should be organized to address this challenge. Many of the distinguished contributors to this book place special emphasis on the role of leadership in addressing this problem.

The efforts of the President's Commission on Critical Infrastructure Protection were only a beginning. But they were the beginning of a broader government-wide effort to deal with the nation's homeland security, a central feature of which was the protection of its critical infrastructures. A decade later, we have tragic evidence of the criticality of our infrastructures, our dependencies on them, and their vulnerabilities. Their physical vulnerability is clear, and we have ample evidence of their vulnerability to cyber attack, demonstrated by the many virus and denial-of-service attacks capturing the headlines over recent years. As analyzed in detail in Part V of this book, there is also clear evidence of the potential for major economic losses. That questions the financial vulnerability of our infrastructures as well, and it calls for the development of effective risk-transfer mechanisms to ensure prompt recovery of our nation after a disaster.

With the structuring of the new Department of Homeland Security, we now see organizational emphasis on the mission of protecting our critical infrastructures. We see physical and cyber security being stressed throughout government and even more generally in commerce, education, and industry. And finally, we see a surge of financial resources for both development and investment being devoted to this vital area.

Perhaps most important in the critical infrastructure area, we recognize the need for complementary, focused public and private action. Various councils, agencies, committees, and task forces have been spawned and are actively addressing a wide range of critical infrastructure security topics. Still, this is a relatively new mission area for our government, and we are defining new

relationships between levels of government and public and private infrastructure institutions. No doubt, we should expect a few missteps as we plot a course toward safety in a world of new threats, vulnerabilities, interdependencies, and an unprecedented pace of change. But we now need to get it right – 10 years have elapsed with too little progress in this vital area.

A specific challenge that still eludes us is defining an effective relationship between the public and private sectors. Effective sharing of threat, vulnerability, and incident information – essential to the protection of our infrastructures – has advanced little in spite of the rhetoric, commissions, councils, and strategies that dot the critical infrastructure landscape. Effective frameworks for working together, schemas for information sharing, and incentive mechanisms, here and abroad, still have not emerged.

The faltering steps of the new Department of Homeland Security – especially those elements charged with critical infrastructure protection – to assume the leadership role envisioned by the commission has delayed progress. State and local governments, which have been collectively patient for the last four years, have little tolerance left for promises of leadership in protecting our infrastructures. Private-sector companies – infrastructure and security providers alike – are concluding they can no longer afford to wait for leadership and are stepping out on their own. These companies are simply hoping that they are picking the right solutions and making the right investments in the absence of leadership.

I regret ending on a negative note. But I remain convinced, as my colleagues and I wrote 10 years ago, that waiting for a serious threat to develop is a dangerous and ineffective strategy for protecting the nation's critical infrastructures. It is in this light that I urge you to read the words of the distinguished authors in this book. They make an important contribution to the future security of our nation by carrying the exploration of this vitally important matter forward.

General Robert T. Marsh, USAF (Retired)

PREFACE

Shortly after the September 11, 2001, attacks, the presidents of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine in the United States initiated a study of science and technology for countering terrorism. Lewis Branscomb, a co-editor of this book, and Richard Klausner were appointed co-chairs of the committee. The study team included more than 100 scientific and technical authors and 46 reviewers. Within seven months, the committee produced *Making the Nation Safer: Science and Technology for Countering Terrorism*, a report that focused on research and development strategies, describing actions to reduce immediate risks using existing knowledge and technologies and research to reduce future risks through the development of new capabilities. Many of the report's recommendations for research and development priorities were later incorporated into the science and technology strategy for the Department of Homeland Security.

Making the Nation Safer also highlighted a number of policy issues to be addressed for the nation's safety and security to benefit fully from any technical successes. Foremost among these policy issues was the role of private action in reducing public vulnerability. Then as now, most of the likely targets of terrorist attack are owned by private-sector firms. Furthermore, the severity of any attack (or, for that matter, of any major natural disaster) may be seriously aggravated by the disruption of critical services such as energy and water – services that are also mostly provided by private-sector firms. *Making the Nation Safer* addresses this concern in the following terms:

> Economic systems, like ecological systems, tend to become less resilient (more prone to failure when strongly perturbed) as they become more efficient, so our infrastructures are vulnerable to local disruptions, which could lead to widespread or catastrophic failures. In addition, the high level of

> inter-connectedness of these systems means that the abuse, destruction, or interruption of any one of them quickly affects the others. As a result, the whole society is vulnerable, with the welfare and even lives of significant portions of the population placed at risk.

While the U.S. government has, in the past five years, advanced an agenda to promote science and technology for counterterrorism, it has done little to provide the firms that ultimately assure the delivery of critical services with incentives to invest in reducing public vulnerability.

This book represents an attempt to seriously address the private role in public security. In particular, what factors affect the investment decisions of the firms that provide critical infrastructure services – those that assure the social and economic continuity of nations and groups of nations?

The work in this volume draws from the efforts by more than half a dozen research teams, each of which has long been active in research on risks and consequences of terrorism and other disasters – particularly as they affect the continuity of the critical infrastructure services. Among these teams are those represented by the editors: George Mason University's School of Public Policy, Harvard's John F. Kennedy School of Government, and the Wharton School at the University of Pennsylvania. Researchers at George Mason's Critical Infrastructure Protection Program have since 2003 advanced policy-relevant work concerning infrastructure vulnerabilities and strategies to ensure the provision of critical services. The Belfer Center for Science and International Affairs at Harvard's Kennedy School has also applied longstanding contributions to the study of terrorism and national security to the study of public–private partnerships in homeland security. For more than 20 years, the Risk Management and Decision Processes Center at the Wharton School has also been furthering knowledge about the nature of extreme events from terrorism, technological failure, or natural hazards and the contribution that markets and governments can make to address the new large-scale dimension associated with these emerging catastrophic risks.

The efforts of these research teams complemented those of other leading teams at a variety of institutions in the United States and abroad, notably Carnegie Mellon University, Columbia University, the Lawrence Livermore National Laboratory, Mills College, RAND Corporation, the University of California at Berkeley, and the École Polytechnique in Paris.

In the winter of 2004, George Mason University's Critical Infrastructure Protection Project funded a project titled "Private Efficiency, Public Vulnerability: Developing Sustainable Strategies for Protecting Critical Infrastructure." Philip Auerswald from George Mason and Lewis Branscomb from Harvard served as lead investigators of the project. Its centerpiece was a workshop held at

Harvard's Kennedy School, May 27–28, 2004. A premise of the project was that the threat to critical infrastructure from terrorist attacks is best addressed as part of an overall strategy for national safety and security. While each category of risk has specific characteristics, the mitigation of risk from terrorist attack is inherently linked to the mitigation of risk from natural and technological disasters, and from service failures due to human error.

Following the workshop, the lead investigators undertook to produce a research volume that would organize the multiple perspectives offered at the workshop. The goal was to provide senior executives, policymakers, and citizens with a systematic analysis of issues and potential actions. Erwann Michel-Kerjan from the Wharton School and Todd M. La Porte of George Mason joined Auerswald and Branscomb as author-editors of the volume. To provide additional balance and depth to the collection of papers, the author-editors soon broadened the list of invited contributors to include academics and private-sector leaders who had not originally participated in the May 2004 workshop.

The contributors to this volume are among the most respected individuals in this field. Each draws on his own experience from business, government, and research institutions (responsibility for the content of this book, of course, lies with them, not with the institutions with which they are identified). While the contributed chapters represent the disparate views of the individual expert authors, all advance the collective objective of providing readers with a comprehensive and thoughtful analysis of the role of private firms in ensuring public security. Despite the complexity of the subject matter, a surprising degree of consensus emerged among the authors and editors concerning core policy-relevant issues. These are summarized in the book's conclusion.

In addition to being of immediate policy relevance, we believe this book will contribute to establishing a new field of interdisciplinary study on the topic of "security externalities," addressing, among other topics, the risks, physical and financial vulnerability, and organizational resilience of critical infrastructure services in times of disaster. Indeed, as events in this young century have regrettably illustrated, the experience of disaster in various forms may become more the rule that guides public policy and business strategy than the exception that is ignored. To the extent that this is the case, understanding of security externalities may emerge in this century as a major domain of study, just as environmental externalities did in the previous century.

The book is divided into six parts. The first and last parts comprise an introduction to the issues and a summary of its conclusions, both authored by the four editors. The parts in between address five linked challenges, each necessary but not sufficient in the overall effort to mobilize private action to reduce public vulnerability: (1) recognizing infrastructure vulnerability, (2)

managing high reliability organizations, (3) securing interdependent networks, (4) creating markets, and (5) building trust. Each of these sections is introduced by a chapter, written by the editors, that places the rest of the chapters in the section in the context of the overall analytic flow of the book.

This volume at once addresses a vitally important policy issue and contributes to developing a fundamentally new domain of academic inquiry. We hope readers will appreciate the various but complementary perspectives offered and will be prompted to further consider how routine private decisions can represent not only the seeds of disaster, but also the roots of response.

ACKNOWLEDGMENTS

This volume is a product of the "Private Efficiency, Public Vulnerability" project, supported primarily by grant #60NANB2D0108 from the National Institute of Standards and Technology (NIST) through the Critical Infrastructure Protection Program (CIPP) at George Mason University. Any opinions, findings, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of NIST or CIPP.

Beyond the project's sponsor, our first thanks goes to the authors of the chapters contributed to this volume and to the other participants in the May 2004 workshop that laid the groundwork for the book. We have greatly appreciated the dedication all have shown to the shared objective of advancing scholarship, improving policy, and increasing public awareness concerning the vital issues we have together sought to address.

We secondly would like to recognize the sustained support of CIPP director John McCarthy and the valuable assistance of staff members Kevin Thomas, Kathleen Emmons, and Christine Pommerening. We are also pleased to acknowledge the support of the Belfer Center for Science and International Affairs at Harvard's Kennedy School of Government, which hosted the May 2004 workshop that laid the groundwork for this book. Professor John Holdren, director of the Science, Technology and Public Policy Program in the Belfer Center, sponsored the event, and his assistants Patricia McLaughlin and Robert Stowe helped in many ways to make the workshop both productive and enjoyable. We are also pleased to acknowledge the support of the Risk Management and Decision Processes Center at the Wharton School of the University of Pennsylvania in helping to bring this project to fruition.

We want to express our special appreciation for the encouragement and guidance of John Berger, a Senior Editor at Cambridge University Press. He

saw the promise of this volume and contributed substantially to realizing the final product.

We save our most heartfelt thanks for last: to Bonnie Nevel, who edited every chapter in the book and prepared the volume for production. Much more than a copy editor, she helped create a book with a coherence of style and an organized flow of material that at the same time conveys the individual personality of each contributor. Her efforts were not only highly professional but reflected an exceptional commitment to a task whose complexity none of the editors fully foresaw at the outset.

– Philip E. Auerswald, Lewis M. Branscomb, Todd M. La Porte,
and Erwann O. Michel-Kerjan
July, 2006