

PREFACE

The chapters of this volume of *Homeland Security* focus on the protection of our nation's critical infrastructure. Each author was asked to simplify as much as possible the complexities of policy and practice, while highlighting both pre- and post-9/11 security challenges. After a brief introductory chapter, the volume is organized into four sections. In the first, authors examine the meaning of, and threat to, critical infrastructure and describe various local, national, and multinational strategies for improving security. The second section examines the threat to specific energy, food, and water supply targets. The third section offers a set of analyses on the threat to the nation's transportation systems, and the final section explores the financial and technological aspects of critical infrastructure. As a collection, the chapters advance our understanding of key national security challenges, as well as raise important questions and issues for further research.

PART I: UNDERSTANDING CRITICAL INFRASTRUCTURE

The first section of the volume begins with a chapter by three colleagues at the Monterey Institute of International Studies: Dr. Gary Ackerman, Dr. Jeffrey Bale, and Kevin Moran. Their discussion of the threat to critical infrastructure (CI) includes an extensive description of how the concept of CI evolved, with special attention to how various government commissions, presidential directives, and national strategies have defined it. Based on their analysis, they offer a formulation of the concept of critical infrastructure that is somewhat more concise than existing official definitions. From this definition, the authors frame a discussion about what sorts of targets might be of most interest to certain kinds of terrorist groups and why. In addition to constituting a target, they note, CI could also be turned into a weapon or otherwise exploited as a means of causing harm—for example, using a mass transit vehicle (like an airplane) to attack a stationary target (like a skyscraper). They conclude that terrorists are blessed with an almost infinite number of CI target possibilities, which warrants greater attention to, and sophistication of, CI vulnerabilities throughout the United States.

The next chapter is by Alane Kochems, a national security policy analyst at The Heritage Foundation, who argues that the primary objective of a national CI security effort must be to share information among federal, state, and local governments and the private sector, so that they can better address terrorist threats to critical infrastructure. After examining the principles of risk management, Kochem notes that, because over 85 percent of the critical infrastructure in the United States is controlled by the private sector, Congress and the Administration should encourage the creation of a risk-based system for CI protection that engages the private sector. She also endorses Secretary of Homeland Security Michael Chertoff's plans for reorganizing the Department of Homeland Security (DHS) and calls for DHS to create effective means for sharing information among federal and state governments, the private sector, and other entities. She concludes that neither the federal government nor private CI owners and operators can fully protect critical infrastructure against terrorist attacks—they must work together to be successful. Among her specific recommendations, she suggests that the federal government needs to define clearly what it believes are reasonable actions for the private sector and address liability issues.

This is followed by a discussion of specific science and technology initiatives developed by the Department of Homeland Security, authored by Dr. William Rees, Jr., and Kevin Gates of the Homeland Security Advanced Research Projects Agency. Their chapter provides a brief overview of the historical development of critical infrastructure protection, with the aim of explaining how the Department of Homeland Security is organized to protect those infrastructures. While their analysis leads to many questions without easy answers, they suggest that meeting the challenges of CI protection demands a dialogue with infrastructure providers, and the first step in that dialogue is to define the scope of the issues so that both sides have a common understanding of perspectives. Their chapter then describes several initiatives of the DHS Infrastructure Protection (IP) Division, which provides direct operational support and interface with the infrastructure sectors through two subsidiary divisions: The Physical Security Division of IP conducts assessments of individual infrastructure facilities through direct, on-site visits, while the Infrastructure Coordination Division of IP supports a private-public partnership for homeland security. They also describe the efforts of the research and development arm of DHS, the Science and Technology Directorate, in supporting the work of the IP and other divisions of DHS. They conclude their discussion by addressing several challenges and opportunities for DHS in the area of critical infrastructure protection, including prioritization of funding, improving coordination at the federal, state, and local levels, and sharing (while protecting) important information.

Next, Patrick Belton, president of the Foreign Policy Society and a doctoral student at Oxford University, provides an international dimension to our understanding of critical infrastructure security, with an examination of the British experience in dealing with terrorism in their homeland. While the terror campaign of militant Irish republicans has drawn to a close, the threat from radical Islamists, as demonstrated in the summer of 2005, shows every sign of continuing. The United Kingdom's experience in protecting its public transport infrastructure is unusual among countries in both intensity and duration, and as such merits unusual scrutiny for lessons to be learned by other countries coming now to confront similar counterterrorist challenges. His chapter draws attention to the history of attempts against the British transportation infrastructure, the differing strategic and doctrinal imperatives of attackers, ways in which these attacks were countered, lessons to be drawn from these experiences to benefit present efforts in counterterrorism and infrastructure protection, and salient characteristics of the current operating environment pitting counterterrorist against terrorist amid the battleground of the underground and other transportation infrastructure.

And the final chapter of this section, by Kevin Freese (a researcher who works for an agency of the U.S. government), carries forward this international theme by addressing a number of cross-border issues in protecting critical infrastructure from terrorism. He notes that the northern and southwestern borders of the United States pose a unique problem for homeland defense and homeland security. Communities near these borders, and indeed much of the country, are physically dependent upon infrastructure that either is shared by both countries or else falls outside the legal jurisdiction of the United States. By targeting infrastructure in either of these categories, a terrorist or other enemy seeking to harm the United States directly would not even have to set foot on U.S. soil in order to carry out a devastating attack. Protecting this cross-border critical infrastructure is essential in order to defend and guarantee the security of the homeland, but the United States is completely dependent upon the cooperation and assistance of Canada and México—meaning that this link in the security fence must fall under the purview of international diplomacy. He concludes that for the sake of all the citizens of North America, our governments must foster the political will, resources, organizational structure, and legal framework for improving multilateral cooperation in CI protection.

PART II: ENERGY, FOOD, AND WATER

The second section of the volume explores challenges specific to certain segments of the nation's critical infrastructure. The first chapter of this section is provided by Canadian counterterrorism expert Tom Quiggin,

