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 though 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,

who notes that, since his country's oil supply to the United States plays such a critical role to the health of our economy, terrorists can be expected to view it as a strategic target for attack. Indeed, oil and natural gas infrastructure in general can be considered a natural target for "economic jihad" attacks, and this requires special attention by both corporate and public leaders. The main threat to the U.S. oil supply, he suggests, is to the critical transportation links that can be attacked by terrorists—physical assets like ships and pipelines that are immensely vulnerable. He then describes some specific vulnerabilities related to these physical assets and what can be done to help counter the threat to these vital energy supply lines.

The topic of energy is also addressed in the next chapter, on protecting nuclear power plants. Here, Dr. Edwin Lyman and Dr. David Lochbaum (both of the Union of Concerned Scientists) argue that ensuring the protection of nuclear power plants against terrorist attack is one of the most critical homeland security objectives of the United States. Nuclear power plants are uniquely attractive terrorist targets for sabotage, not only because of the massive damage that such an attack can cause but also because of the widespread fear that can be evoked by the specter of invisible yet deadly radiological contamination. If a number of well-trained and well-equipped terrorists were to succeed in gaining forced entry to the protected area of a nuclear power plant, within a matter of minutes they could do enough damage to vital safety systems and structures to initiate a meltdown of the radioactive fuel in the core, as well as a massive radiological release to the environment. Alternatively, an attack on the spent fuel storage pools at reactor sites, which are even less well protected and isolated from the environment than the reactor core, could lead to an outcome of similar severity. And the threat is not hypothetical: After 9/11, a Nuclear Regulatory Commission official reported that there were increased intelligence reports identifying nuclear power plants as potential targets, leading to the conclusion that there was a "general credible threat" of a nuclear plant attack. They conclude that, although some progress has been made in strengthening security at U.S. nuclear plants after the 9/11 attacks, it is still far from assured that the American public is adequately protected from the sabotage threat to nuclear plants. Thus, they argue, an independent technical assessment of the accomplishments of the NRC and the nuclear industry in this area, free of institutional biases, is badly needed.

Next, Dr. Lee Myers, the state veterinarian and assistant commissioner with the Georgia Department of Agriculture, examines the threat to the nation's agriculture and food supply and describes a number of federal and state strategies for countering this threat. The agriculture and food sector provides approximately 15 percent of all American jobs and accounts for 13 percent of the nation's current gross domestic product.

On the global scene, the United States is the world's largest exporter of agricultural products, accounting for $50 billion in exports annually. Thus, the agriculture and food sector can be seen as one of the most important elements of our nation's critical infrastructure. Her chapter examines the threat of agroterrorism, in which an attack would have serious consequences for the economy, social structure, and human health. Specific attention is
given to the biological threat—the deliberate introduction of diseased pathogens that are damaging to plants or animals. She concludes that agrosecurity requires a well-informed public as well as conscious planning, organizing, equipping, training, and exercising a multidisciplinary team that can respond to agricultural and food emergencies. Overall, agriculture and food defense relies upon an effective partnership between government, the private sector, academic institutions, and nongovernmental agencies.

In the next chapter of this section, Dr. Arthur Holst (government affairs manager for the Philadelphia Water Department) explores the terrorist threat to local drinking water supplies. He notes that in the post September 11 world, drinking water is not only under threat from traditional problem sources, such as untreated sewage dumping, storm runoff, and aging infrastructure, but also from terrorist activities. A biological attack on the drinking water system and the nation's water infrastructure, as well as water pollution resulting from attacks on chemical facilities, could certainly prove disastrous, potentially harming millions of people. After reviewing the history of drinking water quality, relevant legislation, and the pre-9/11 water security scare, Holst examines the efforts being made to counter the terrorist threat against the nation's water supply. These efforts include legislation, vulnerability assessments, emergency and incident planning, security enhancements, and research and technology. He concludes that regardless of how prepared water systems operators, government officials, and physicians are for potential attacks, truly successful drinking water security may only come from the complete commitment of everyone, not just those involved in the production, distribution, planning, and oversight of water systems.

Jonathan G. Herrmann and Charlotte S. Bercegeay, two senior representatives of the U.S. Environmental Protection Agency (EPA), conclude this section by expanding on the discussion of protecting America's drinking water supplies. Their chapter provides a brief historical perspective about homeland security priorities and policies, and describes the EPA's requirement to collaborate with and provide guidance to state and local governments and the private sector to ensure water infrastructure protection. These partnerships are critical to ensuring the safety of the nation's water infrastructure. Their chapter concludes with a review of EPA's Action Plan, a comprehensive approach that addresses water

infrastructure security issues and needs. Research continues on current and future projects, and the Action Plan will be updated to reflect EPA's current understanding of threats to, and vulnerabilities of, drinking water systems. Using research results, appropriate methods and technologies can be developed and applied to drinking water systems to protect this vital national infrastructure.

PART III: TRANSPORTATION SYSTEMS

The third section of the volume explores challenges specific to certain elements of the nation's transportation systems. First, University of South Florida professor Randy Borum and retired Police Chief Arthur J. Kelly III explore vulnerabilities and strategies for protecting public transit systems from terrorist attacks, and discuss contingency planning and the use of incident command systems to mitigate, contain, and respond to attacks that may occur. Recent attacks on mass transit systems in London, Tokyo, Chechnya, and Madrid provide examples of why homeland security officials in the United States are justifiably concerned. Further, the evolving nature of transnational terrorism makes the targeting of public transportation even more worrisome. Clearly, they argue, safeguarding systems that are designed and required to be open, accessible, and efficient carries a multitude of challenges, but the right combination of personnel, technology, and access to information can help to keep these systems safe. Exceptional technologies exist and are emerging to support the surveillance, impedance, detection, and assessment of unauthorized persons and materials within a designated perimeter. From their analysis, Borum and Kelly conclude that the current best practice approach to transit security is to use a layered system of defense, particularly with regard to physical security measures.

British counterterrorism experts Paul Cardew and Chris Boucek then add an international dimension to this discussion, by examining lessons that the United States can learn from other countries who have grappled with threats to their mass transit systems—specifically France, Spain, and the United Kingdom. They argue that subways are inherently vulnerable to terrorist attack because of their emphasis on convenience and efficiency. It would be infeasible and greatly impractical to transfer security measures such as those now in place in airports to mass transit systems. However, lessons learned from Europe can help inform American security planners in their decision making, prioritization, and resource application. Recommended security measures include increasing the police presence (with canine teams); installing more surveillance cameras, explosive detectors, and chemical sniffers; removing all trash and recycling cans; and replacing benches in stations capable of concealing suspect

packages with wire mesh seating that will allow security personnel unobstructed views of the stations. Such visible security measures, they argue, do contribute to deterring terrorists. Terrorists instinctively seek out vulnerable targets, particularly as our societies become more resilient. Further, random baggage inspections should also become commonplace, as they have been proven to deter potential bombers—raising the likely failure rate for suicide terrorists intent upon inflicting mass casualties drives them to revise their plans. And finally, they call for federally mandated security standards and a nationwide effort to educate passengers and administrators about the terrorist threat to mass transit systems and how to counter this threat.

Since the attacks of 9/11, aviation security has obviously been an enormously hot topic in the United States and is addressed in the next chapter by Albright College professor Guillaume de Syon. Within the last four years, he argues, new aviation security measures, managed through a variety of domestic and international efforts, are largely responsible for the absence of any air-related terrorist attacks in the United States since 9/11. However, in pursuing greater security of our nation's airlines, there are lessons to be learned from other parts of the world. Further, since many airlines owned by foreign companies (and often foreign states) transit to and from the United States, airline security in our country takes on a uniquely international dimension. His discussion is focused primarily on European airlines and how they have dealt with terrorism since the late 1960s, when the first serious wave of aviation-related terrorist incidents began. He notes that ironically some foreign carriers display stricter security than their American counterparts in order to ensure that they comply with U.S. regulations. (Passengers on Air France and Lufthansa, for example, face as many as seven scheduled and random checks from airline and airport personnel prior to boarding an aircraft.) What is missing, however, remains a clear coordination among airlines and governments worldwide.

The next chapter examines the threat posed by transporting hazardous materials through America's cities. Homeland security consultant Dr. Fred Millar argues that rail security is off track for a number of reasons. No national planning has been conducted to determine how to make rail operations, particularly in major urban centers, more secure. Railroad and chemical industry security adjustments have been voluntary and limited. Only the corporations' high-stakes economic and legal-political interests can explain the astonishing recklessness of continued hazmat shipments, and what looks like another giant "failure of imagination" (similar to the earlier one the 9/11 Commission cited) that leaves the nation still vulnerable to horrendous risks in all our major cities. Both the federal government and the rail industry have employed bullying legal and political tactics and excessive secrecy that preclude necessary

involvement by local authorities. Thus, he concludes, in the struggle to reduce risks from hazmat transportation, right now each city must fend for itself.

And in the final chapter of this section, two retired U.S. Coast Guard officers—Joe DiRenzo III and Chris Doane—provide an analysis of the threat to the Western Rivers system. An often overlooked element of the nation's critical infrastructure, the Western Rivers—a system of 41 rivers, lakes, and supporting terminals and facilities spread across 18 states, centered upon the Mississippi River—are used to transport hundreds of tons of coal, petroleum, farm products, chemicals, and crude materials, such as aggregates for construction and other minerals, annually. Unfortunately, there are a variety of reasons why terrorists would find this an attractive CI target, given the tremendous flow of commerce along the rivers, as well as the many population centers, locks, and dams located along the system. Barges carrying dangerous cargos that might be exploited by terrorists as weapons of mass destruction also populate the rivers. They note that, prior to 9/11, there was a paucity of security for the Western Rivers, some of which has been remedied by new security measures initiated in the past few years. However, they conclude, shortfalls remain in the current state of security on the Western Rivers, and there is much that can be done to improve the situation.

PART IV: FINANCE AND TECHNOLOGY

The final section of the volume examines the terrorist threat to financial- and technology-related critical infrastructure targets. First, Erica Chenoweth (a terrorism researcher at the University of Colorado, Boulder) examines the financial services sector, noting that it "has been amazingly resilient after the devastation of large-scale terrorist attacks." Her chapter examines the precautions installed before 9/11 that established this resilience, the short- and long-term impacts of 9/11 on the financial services sector, and post-9/11 legislation that has affected financial services. Her analysis suggests that local entities are fairly well equipped for overcoming security challenges to financial services. However, she concludes, in order to further reduce vulnerabilities in the financial services sector, concerted efforts must be made to coordinate the combined resources, knowledge, and authority of both the public and the private sectors in order to adequately devise plans that can respond swiftly and effectively to the remaining challenges.

The next chapter is by Dr. James Lewis, senior fellow and director for Technology and Public Policy at the Center for Strategic and International Studies, who examines the relationship between cybersecurity and critical infrastructure protection. He first describes cybersecurity as the safeguarding of computer networks and the information they contain from

penetration and from malicious damage or disruption. Since the use of computer networks has become a major element in governmental and business activities, he notes, tampering with these networks can have serious consequences for agencies, firms, and individuals. The question is to what degree these individual-level consequences translate into risk for critical infrastructure. While some have overstated the threat, he argues, cybersecurity cannot be entirely ignored in planning for critical infrastructure protection. However, from his analysis of the threat, he concludes that the best path to better cybersecurity may lay outside of critical infrastructure protection. It is hard to motivate people to defend when risks are obscure or appear exaggerated. However, the risks of espionage (including economic espionage) and cybercrime are very real for individuals, firms, and agencies. A security agenda that focused on measures to respond to cybercrime and espionage would produce tangible benefits, win greater support, and reduce many vulnerabilities in computer networks used by critical infrastructure.

The discussion of cybersecurity is continued in the next chapter by terrorism scholar Aaron Mannes, who examines the threat to the Internet from the perspective of motivations and capabilities of the primary malicious actors using the Internet. His analysis illustrates how malicious activity on the Internet occurs and what countermeasures are available. He also provides an assessment of the potential means of attacking critical infrastructure via the Internet and the consequences of an attack on the Internet itself. In addition to attacking the Internet, malicious actors online can penetrate networks to obtain and manipulate sensitive information. The chapter then explores how terrorists have actually used the Internet for communications. Finally, the chapter ends with a review of the efforts to secure this core component of modern society, with a focus on the Department of Homeland Security's National Cyber Security Division.

And in the final chapter of the volume, Dr. Peter Siska, the director of the School of Agriculture and Geosciences at Austin P. State University, explores the relationship between homeland security and the global satellite systems upon which we rely for mapping, navigation, and communication systems. He notes that terrorist groups are ready to use every available aspect of modern technology to carry out their plans. Modern digital geospatial and communication technology is one such example. His chapter discusses modern advances in geospatial mapping and satellite-based communication systems and their potential misuse by groups such as terrorists, and he argues that key security vulnerabilities exist in our communication technologies, including cell tower systems, signals, and satellite-based mapping. Thus, as part of any strategy for homeland security (or, more importantly, global security), we must

constantly seek to better understand the potential misuses of modern technologies.

CONCLUSION

Together, these chapters improve our understanding of the challenges of protecting our nation's critical infrastructure from terrorism. However, there are obviously other avenues to explore beyond what is covered in this volume. Thus, this collection will hopefully also stimulate the reader to pursue further research on their own, in order to expand our collective understanding of homeland security at the national and local levels. In a country as vast as the United States, the challenges of homeland security require a broad, collaborative effort between government agencies at all levels, private corporations, community groups, and the general public.

ACKNOWLEDGMENTS

The views expressed herein are those of the author and do not purport to reflect the position of the United States Military Academy, the Department of the Army, or the Department of Defense.