
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)