1

ORIGINS OF CRITICAL INFRASTRUCTURE PROTECTION

What is the motivation for studying *critical infrastructure protection* (CIP)? What are the central issues that need to be addressed in order to create a meaningful strategy for dealing with threats against infrastructure? We begin by tracing the development of *CIP* over several decades and noting that it has evolved through at least eight phases: from initial awareness to combating terrorism, emphasis on natural disaster response, an early definitional phase, a public–private cooperation phase, a federalism versus states phase, a resilience awareness phase, a risk-based decision-making phase, and after massive computer security breaches and the failure of government to "wake up to" the realities of computer and network exploits at both misdemeanor and warlike levels, the cybersecurity phase.

CIP is a multifaceted topic because it cuts across many disciplines and jurisdictions. It cuts vertically across federal, state, local, and tribal political boundaries, and it cuts horizontally across public and private organizations. It has a variety of policy issues at one extreme and a diverse set of scientific and engineering issues at the other extreme. The most glaring example of this is the electric power grid, which is pulled in many different directions by political, social, engineering, and public–private forces. The rapid emergence of online e-commerce, social networks, and misinformation campaigns also raise political, social, and engineering issues broadly classified as cybersecurity threats and exploits. The topics in this book touch on all of these, at architectural and policy levels, by applying complexity theory and network science to the practical problem of securing critical infrastructure and key resources (CIKR).

One of the most difficult tasks of protecting critical infrastructure (CI) is the problem of deciding who is responsible for what across these political and organizational lines. While policy at the Department of Homeland Security (DHS) offices in Washington, DC, may advocate an all-hazard risk-informed decision-making process and encourage community action, actual operational and organizational processes at the state and local level may be entirely different due to a number of factors. Federalism and top-down policy-making may look good on paper, but actual implementation at the local level often lacks jurisdictional clarity, required expertise, willpower, or all three. For example, what is the role of public safety responders such as firefighters and law enforcement officers when something goes wrong with a gas pipeline, electrical power fails during a storm, or hackers exploit the Internet in a city without cybersecurity expertise?

There remain gaps in knowledge, jurisdictional clarity, and organizational fitness—challenges this book attempts to address—in the emerging field of CIP. As this chapter illustrates, the field is still evolving. Some issues are being resolved, while others are still in the early stages of their evolution. The field has matured, circa 2019, after decades of slow but steady maturation, such as follows:

- *Recognition*: No such field of study existed prior to the mid-1900s. Although awareness of the importance of infrastructure began in 1962 with the Cuban Missile Crisis, nearly 30 years passed before the term *critical infrastructure protection* was defined. Throughout

Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation, Third Edition. Ted G. Lewis.

Companion website: www.wiley.com/go/Lewis/CriticalInfrastructure_3e

these 30 years, the roles and responsibilities of governmental agencies as well as the definition of CIP changed as the field evolved. Nonetheless, much remained to be resolved in this initial phase.

- *Natural disaster recovery*: In the beginning, CIP was nearly identical to *consequence management*—recovery from disasters such as floods, hurricanes, and earthquakes. The Stafford Act[1] established the Federal Emergency Management Agency (FEMA)—a federal agency dedicated to recovery after a flood, hurricane, earthquake, tornado, and so on. Terrorism was not a factor in CIP in the beginning. It would take a decade of attacks before CIP was linked with terrorism in the United States. But a focus on terrorists—human-caused incidents—soon faded as natural disasters occurred more often than terrorist attacks, and headlines focused the public's attention on billion-dollar natural disasters.
- *Definitional phase*: The term "critical infrastructure" did not exist before the 1990s. There was no definition of CIP, and infrastructure was taken for granted. The public was confident that freshwater always flowed from faucets and electric light switches always produced light. The terrorist attacks of 9/11 changed all that, of course, even though the earliest definition of CIP was made in 1997. Then, from 1997 through 2003, the identification of CI sectors expanded from eight to 13 sectors plus 5 *key assets*, expanded again to 18 sectors and key resources (KR), and then consolidated into 16 CIKR sectors in 2013. Today it is difficult to identify sectors of the national economy that are *not* critical; however, this book attempts to define criticality in a rigorous and operational way.
- *Public–private cooperation*: The role of the private sector in CIP was slow to take root until the late 1990s. But so many CIKR assets are in the hands of corporations—not local, state, or federal government—that it is difficult to separate public versus private assets. Public safety and health, law enforcement, and emergency response are largely a function of local government, but energy, power, communications, and commercial air travel are largely a function of the private sector. Water and key assets such as dams fall somewhere in between. Who should respond when something happens to these systems? Even today, the federal government and private sector owners of infrastructure are not clear on their respective roles and responsibilities with respect to CIP, although the role of government in protecting systems of all types has narrowed over the decades. Nonetheless, when a small business in mid-America is hacked by a teenager running scripts downloaded from the dark web, it is not clear who is responsible for the protecting the small business from the availability of the script, dark web, teenager, or Internet service provider.
- *Federalism*: Because terrorists attack at the local level, the solution to the problem must also come from the local level—states, cities, and tribes. The future of homeland security rests in the hands of local governments, and yet the local level lacks sufficient technology, skills, and funding to cope with global terrorism, computer criminals, or major catastrophes. Superstorm Sandy, Fukushima Daiichi power plant disaster, the Horizon Gulf Oil spill, Russian hackers from the Internet Research Agency, and major droughts throughout the Midwest routinely outstrip local government's capacity to deal with catastrophic events—both physical and virtual. Federal–state–local–tribal federalism does not seem to be able to cope with CIKR events spanning political boundaries or that are so consequential that local authorities are overwhelmed.
- *Resilience*: By the mid-2000s it became obvious that asset hardening and 100% security of the vast CIKR sectors was an impossible and impractical goal of CIP. CIKR systems are too big, too complex, and too expensive to protect in their entirety. Thus, the field entered a period of reevaluation and government agencies began to focus on *resiliency* rather than absolute security.[2] Although the definition of risk and resilience went through many iterations, the concept of a resilient society began to take root as an objective of CIP. However, like the term *risk*, the term *resiliency* still lacks a standard definition, making the application of resilience-informed decision-making difficult and often ineffective. A plethora of frameworks such as the DHS risk management, the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), and Hodges Community Fragility model appeared at about this time as early attempts to formalize resilience.
- *Risk-informed decision-making*: Ten years after the horrific terrorist attacks of September 11, 2001 (9/11), the notion of resilience remained a laudable goal but difficult to measure. Therefore, the field of CIP entered a more quantifiable phase loosely called *risk-informed decision-making*.[3] During this phase, a variety of methods and practices emerged to quantify risk and

[1]The Stafford Act is a 1988 amended version of the Disaster Relief Act of 1974.

[2] From PPD-21, resiliency is defined as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents."

[3]From the DHS Risk Lexicon, risk-informed decision-making is "determination of a course of action predicated on the assessment of risk, the expected impact of that course of action on that risk, as well as other relevant factors."

resilience and to measure the return on investment (ROI) for a variety of techniques ranging from target hardening, public–private partnerships (PPP), regulation of chemicals, and others to rigorous methods of assessing risk and resilience. Risk-informed decision-making seeks to prioritize investments in infrastructure on the basis of quantitative risk assessment. The DHS and FEMA released a semiquantitative measure of risk to assist local agencies quantify risk of CIKR within their agencies.

- *Cybersecurity and infrastructure*: Mounting losses due to computer security breaches both commercially and within government began to be counted as viable threats to national security. Perhaps the initial awareness occurred with the weaponized Stuxnet exploit, but it is more likely that Russian meddling and misinformation campaigns by Russia during the 2016 US presidential election was the lightning rod that prompted action by President Trump in 2018 to re-organize the DHS's CIP bureaucracy via the *Cybersecurity and Infrastructure Security Agency Act of 2018* (CISA). CISA elevated computer security as a major threat to CIKR in particular and government-owned and government-operated computer and network systems in general. In 2019 we entered the cybersecurity phase of CIKR evolution.

There is little reason to believe the cybersecurity and infrastructure phase is a final stage of evolution because of unforeseen threats ahead. Modern society is in a headlong dash toward even greater global connectivity and adoption of Promethean technologies such as 5G, artificial intelligence, cryptocurrencies, quantum computing, quantum communications, and elevated consequences of global climate change. Greek god Prometheus gave fire to humans—perhaps the first technology with both good and evil applications. The Promethean challenge of our age is to enjoy the benefits of technology while also controlling it. This challenge has yet to be met in the field of CIP.

1.1 RECOGNITION

Prior to the dramatic and horrific attacks of September 11, 2001 (9/11), the US public had little awareness of terrorism or how it could impact them personally. Attacks on the homeland were something that happened in other countries—not the United States. But a growing number of "national security emergencies" culminating in 9/11 exposed terrorism for what it is—a challenge to the security of the people of the United States. Even before 9/11 however, a few policy-makers were busy formulating various strategies and policies that culminated in a national strategy for homeland security. A major part of this national strategy involved CIP—the protection of basic infrastructure sectors such as water, power, telecommunications, health and medical services, the Internet, and transportation systems. The early work of this small group peaked in the late 1990s, which marks the origins of what we now call *homeland security*. During this same time, CI and CIP emerged as a key element of homeland security.

Although CIP was defined and recognized as a major component of national security rather late in the game (1996), it really began with the creation of the National Communications System (NCS) in 1963 after communications problems between the United States and the Soviet Union threatened to interfere with negotiations during the Cuban Missile Crisis[4]:

> In October [1962], President John F. Kennedy, on national television, revealed that the Soviets had placed nuclear missiles in Cuba. As a result of this aggressive action, he ordered quarantine on all offensive military equipment under shipment to Cuba until the Soviets removed their weapons. … For nearly a week, the Nation was transfixed by the actions of Soviet Premier Nikita Khrushchev and President Kennedy. During this time, ineffective communications were hampering the efforts of the leaders to reach a compromise. Without the ability to share critical information with each other using fax, e-mail, or secure telephones such as we have today, Premier Khrushchev and President Kennedy negotiated through written letters. Generally, Washington and Moscow cabled these letters via their embassies. As the crisis continued, hours passed between the time one world leader wrote a letter and the other received it. Tensions heightened. On October 27 and 28, when urgency in communications became paramount, Premier Khrushchev bypassed the standard communication channels and broadcast his letters over Radio Moscow.
>
> Following the crisis, President Kennedy, acting on a National Security Council recommendation, signed a Presidential memorandum establishing the NCS. The new system's objective was "to provide necessary communications for the Federal Government under all conditions ranging from a normal situation to national emergencies and international crises, including nuclear attack."
>
> At its inception on August 21, 1963, the NCS was a planning forum composed of six Federal agencies. Thirty-five years later, it is a vital institution comprising 23 member organizations that ensure NS/EP (National Security/Emergency Preparedness) telecommunications across a wide spectrum of crises and emergencies. … During the 1980s and 1990s, the NCS expanded its focus to develop Government wide NS/EP procedures and enhancements to the Nation's public networks and information infrastructures.

The role of the communications infrastructure grew more important as the United States entered the information age. In 1978, two communications regulatory agencies (Department

[4] http://www.ncs.gov/about.html

of Commerce's Office of Telecommunications and the White House Office of Telecommunications) were combined into the National Telecommunications and Information Administration (NTIA) by Executive Order 12046. NTIA handled the process of selling spectrum to telephone, radio, and TV networks. It also has the distinction of being the federal agency that oversaw the commercialization of the Internet in 1998–1999. The NCS was formally assigned responsibility for the telecommunications infrastructure in 1984 by Executive Order 12472.

In 1982 President Reagan established the National Security Telecommunications Advisory Committee (NSTAC) by Executive Order 12382. This important presidential advisory body is made up of the CEOs of the major telecommunications companies.

NSTAC is perhaps the first organization to advise a president on CIP.

The NCS and the NSTAC were the first CI agencies within the US government. Twenty years would pass before the term *critical infrastructure* would be defined and the entire US population would become aware of its importance in their daily lives. The DHS absorbed NCS in February 2003, but the NSTAC still reports to the President of the United States.

1.2 NATURAL DISASTER RECOVERY

While the NCS and NSTAC were active throughout the 1970s and 1980s, responses to disasters—both human caused and natural—were still on the back burner as far as CIP was concerned. The FEMA was created in 1978–1979 to respond to hurricanes and earthquakes.[5] Soon after its creation, FEMA was assigned the (temporary) responsibility of responding to terrorist attacks by Executive Order 12148 in 1979[6]:

> All functions vested in the President that have been delegated or assigned to the Defense Civil Preparedness Agency, Department of Defense, are transferred or reassigned to the Director of the Federal Emergency Management Agency.
>
> All functions vested in the President that have been delegated or assigned to the Federal Disaster Assistance Administration, Department of Housing and Urban Development, are transferred or reassigned to the Director of the Federal Emergency Management Agency, including any of those functions re-delegated or reassigned to the Department of Commerce with respect to assistance to communities in the development of readiness plans for severe weather-related emergencies.
>
> All functions vested in the President that have been delegated or assigned to the Federal Preparedness Agency, General Services Administration, are transferred or reassigned to the Director of the Federal Emergency Management Agency.
>
> All functions vested in the President by the Earthquake Hazards Reduction Act of 1977 (42 U.S.C. 7701 *et seq*.), including those functions performed by the Office of Science and Technology Policy, are delegated, transferred, or reassigned to the Director of the Federal Emergency Management Agency…. *For purposes of this Order, "civil emergency" means any accidental, natural, man-caused, or wartime emergency or threat thereof, which causes or may cause substantial injury or harm to the population or substantial damage to or loss of property*.

FEMA was confronted by perhaps the first major terrorist attack on US soil in Oregon in 1984. Members of the politico-religious commune founded by Bhagwan Shree Rajneesh[7] attempted to influence a political election by poisoning voters with salmonella:[8]

> In a bizarre plot to take over local government, followers of Bhagwan Shree Rajneesh poisoned salad bars in 10 restaurants in The Dalles in 1984, sickening 751 people with salmonella bacteria. Forty-five of whom were hospitalized. It is still the largest germ warfare attack in U.S. history. The cult reproduced the salmonella strain and slipped it into salad dressings, fruits, vegetables and coffee creamers at the restaurants. They also were suspected of trying to kill a Wasco County executive by spiking his water with a mysterious substance. Later, Jefferson County District Attorney Michael Sullivan also became ill after leaving a cup of coffee unattended while Rajneeshees lurked around the courthouse.
>
> Eventually, Ma Anand Sheela, personal secretary of the Bhagwan, was accused of attempted murder, conspiracy, arson, and other crimes and disowned by the Bhagwan. Convicted of the charges against her, she spent 29 months in federal prison, then moved to Switzerland.[9]

The salmonella incident in Oregon was an attack on one of many infrastructure sectors identified as critical over the past decade: *agriculture*. But in 1984 there was no generally accepted definition of *infrastructure*, nor any recognition of what sectors belonged to the list of national *CI*.

The importance of infrastructure began to dawn on the federal government when in 1988 President Reagan issued Executive Order 12656. This order alludes to "essential

[5]Presidential Reorganization Plan No. 3 issued by President Carter in 1978 established the Federal Emergency Management Agency (FEMA), which went into effect on April 1, 1979.

[6]http://www.archives.gov/federal_register/codification/executive_order/12148.html

[7]http://www.religioustolerance.org/rajneesh.htm

[8]"The group settled on the 65,000 acre 'Big Muddy Ranch' near Antelope, Oregon, which his *sannyasins* had bought for six million dollars. The ranch was renamed *Rajneeshpuram* ('Essence of Rajneesh'). This 'small, desolate valley twelve miles from Antelope, Oregon was transformed into a thriving town of 3,000 residents, with a 4,500 foot paved airstrip, a 44 acre reservoir, an 88,000 square foot meeting hall…'" http://www.clui.org/clui_4_1/lotl/lotlv10/rajneesh.html

[9]http://home.att.net/~meditation/bioterrorist.html

resources" and places responsibility for their protection in the hands of federal departments:

> The head of each Federal department and agency, within assigned areas of responsibility shall:
>
> **Sec. 204.** *Protection of Essential Resources and Facilities*.
>
> (1) Identify facilities and resources, both government and private, essential to the national defense and national welfare, and assess their vulnerabilities and develop strategies, plans, and programs to provide for the security of such facilities and resources, and to avoid or minimize disruptions of essential services during any national security emergency;
> (2) Participate in interagency activities to assess the relative importance of various facilities and resources to essential military and civilian needs and to integrate preparedness and response strategies and procedures;
> (3) Maintain a capability to assess promptly the effect of attack and other disruptions during national security emergencies.

This executive order contains a number of objectives that remain problematic even today. It calls for identification of public and private facilities that are essential to national welfare—a task that remains unfulfilled today, as political and socioeconomic forces complicate the definition of "essential" and "national welfare." A bridge in one county may be considered essential by voters in that county, but not essential in an objective sense, because of alternative routes. Moreover, when limited resources are considered and there is funding for only one bridge, objective selection of which bridge is saved or repaired quickly enters the political realm instead of the rational realm.

Part two of President Reagan's executive order calls for interagency cooperation to address military and civilian needs. When a severe emergency such as a devastating superstorm or terrorist attack happens, however, interagency cooperation often vanishes and the military takes over. Civil–military relations theoretically means that the military takes orders from civilians, but in practice, only the military has the capacity to deal with major catastrophes. This inequality between the authority of local law enforcement agencies and the readiness of federal troops is revealed over and over again whenever major incidents such as Hurricane Katrina and New Orleans spin out of control.

Finally, the third part of the executive order remains problematic because state and local agencies often do not or cannot afford to maintain capabilities to meet the need. For example, a smallpox outbreak in Manhattan—a population of 8 million—would quickly overwhelm public health and safety agencies in New York. The state and local authorities would have to maintain 40,000 trained emergency responders to head off the spread of smallpox. Forest fires in California quickly overwhelmed firefighters in 2018 and illustrated the importance of interagency and interregional (reciprocal) response agreements in the Department of Interior.

1.3 DEFINITIONAL PHASE

Even in the early 1990s the trend toward greater awareness of human-made and natural disasters was subtle—it had not yet reached a point where it was of national concern. But by 1993–1995 the rate and severity of acts of terror, for example, was increasing and becoming more alarming to the federal government. The 1993 attack on the World Trade Center by Ramzi Yousef, the acts and eventual capture of the Unabomber (1995), the devastating attack on the Federal Building in Oklahoma City, Oklahoma (1995), and the sarin gas attack in a Tokyo subway in 1995 suggested a trend. Acts of violence by nongovernmental organizations (NGOs) were increasing, and as a by-product, raising the level of public awareness. Soon these acts would be attributed to terrorists and move from the back to the front page of the media. Within a short 5–6 years, response to unlawful terrorism would become known as the *Global War on Terrorism* (GWOT) and reached a threshold that deserved national attention.

During this definitional phase, the importance of infrastructure to the safety and security of the US population began to take shape. But the threat was still confined to human-initiated acts of terror. One of the earliest concerns was the fragility and vulnerability of the systems we depend on daily, such as roads, bridges, stadiums, schools, and office buildings. These facilities accommodate many people and yet they are completely open and unprotected. The communications systems and the energy and power systems that run cities and enable modern society to function were also open and unprotected. The emergency response systems and public health services taken for granted for decades were suddenly exposed as poorly prepared. Modern life depended on them, and yet, these essential systems were vulnerable to attacks by both humans and Mother Nature.

The modern origin of homeland security and one of its pillars, CIP, can be placed somewhere between 1993 and late 1995. In fact, 1995 is a reasonable start date because of the flurry of activity aimed at protecting national infrastructure and key assets after 1995. Presidential Decision Directive 39 (PDD-39) issued by President Clinton in 1995 set the stage for what was to come—a new federal Department of Homeland Security. PDD-39 essentially declared war on terrorists[10]:

> It is the policy of the United States to deter, defeat and respond vigorously to all terrorist attacks on our territory and against our citizens, or facilities, whether they occur domestically, in international waters or airspace or on

[10]http://www.fas.org/irp/offdocs/pdd39.htm

> foreign territory. The United States regards all such terrorism as a potential threat to national security as well as a criminal act and will apply all appropriate means to combat it. In doing so, the U.S. shall pursue vigorously efforts to deter and preempt, apprehend and prosecute, or assist other governments to prosecute, individuals who perpetrate or plan to perpetrate such attacks.
>
> We shall work closely with friendly governments in carrying out our counterterrorism policy and will support Allied and friendly governments in combating terrorist threats against them. Furthermore, the United States shall seek to identify groups or states that sponsor or support such terrorists, isolate them and extract a heavy price for their actions. It is the policy of the United States not to make concessions to terrorists.

The criticality of national infrastructure and associated key assets became an important issue when President Clinton issued Executive Order 13010 (EO-13010) in 1996. This executive order established a Presidential Commission on Critical Infrastructure Protection (PCCIP). The commission was chaired by Robert Marsh and subsequently became known as the *Marsh Report* [1]. It defined *critical infrastructure* in terms of "energy, banking and finance, transportation, vital human services, and telecommunications." The Marsh Report was the first publication to use the term critical infrastructure and has become one of the foundational documents of CIP.

The Marsh Report and EO-13010 provided the first formal definition of *infrastructure* as "a network of independent, mostly privately-owned, man-made systems that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services." And *critical infrastructure* is "an infrastructure so vital that its incapacity or destruction would have a debilitating impact on our defense and national security."

According to EO-13010,[11]

> Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government. Threats to these critical infrastructures fall into two categories: physical threats to tangible property ("physical threats"), and threats of electronic, radio frequency, or computer-based attacks on the information or communications components that control critical infrastructures ("cyber threats"). Because many of these critical infrastructures are owned and operated by the private sector, it is essential that the government and private sector work together to develop a strategy for protecting them and assuring their continued operation.

[11]http://www.fas.org/irp/offdocs/eo13010.htm

The work of the PCCIP resulted in PDD-63 (Presidential Decision Directive of 1998), which defined CI more specifically and identified eight basic sectors, listed in Table 1.1. According to PDD-63,

> Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private.[12]

Table 1.1 identifies the sectors initially defined by PDD-63 in 1998 and also identifies the sector-specific agency (SSA) responsible at the federal level. SSAs can be any government agency responsible for carrying out the various CIP missions (Page 50 in Ref. [2]):

- Leads, integrates, and coordinates the execution of the National Infrastructure Protection Plan (NIPP), in part by acting as a central clearinghouse for the information sharing, reporting, and coordination activities of the individual sector governance structures.
- Facilitates the development and ongoing support of governance and coordination structures or models.
- Facilitates NIPP revisions and updates using a comprehensive national review process.
- Ensures that effective policies, approaches, guidelines, and methodologies regarding partner coordination are developed and disseminated to enable the SSAs and other partners to carry out NIPP responsibilities.
- Facilitates the development of risk, risk-informed, and criticality-based assessments and prioritized lists of CIKR.
- Facilitates the sharing of CIKR prioritization and protection-related best practices and lessons learned.
- Facilitates participation in preparedness activities, planning, readiness exercises, and public awareness efforts.
- Ensures cross-sectoral coordination with the SSAs to avoid conflicting guidance, duplicative requirements, and reporting.

The definition of CI in PDD-63 went through rapid evolution and expansion after the attacks of 9/11. The Office of the President of the United States released the National Strategy for Homeland Security in July 2002 and then rapidly followed up with an expansion of the definition of CI sectors in February 2003 with the release of the National

[12]http://www.fas.org/irp/offdocs/pdd/pdd-63.htm

TABLE 1.1 The basic critical infrastructure sectors (8) defined by PDD-63 (1998)

Sector	Description	Sector-specific agency
1. Banking and finance	Banking and stock markets	Treasury
2. Emergency law enforcement services	Justice/FBI	Justice
3. Emergency services	Emergency fire and continuity of government	FEMA
4. Energy	Electric power, gas and oil production and storage	Energy
5. Information and communications	Telecommunications and the Internet	Commerce
6. Public health services	Public health, surveillance, laboratory services, and personal health services	HHS
7. Transportation	Aviation, highways, mass transit, rail, pipelines, shipping	Transportation
8. Water supply	Water and its distribution	Environmental Protection Agency

Strategy for the Physical Protection of Critical Infrastructures and Key Assets.[13]

According to the 2003 strategy document, the objectives of CIP include:

- Identifying and assuring the protection of those infrastructures and assets that we deem most critical in terms of national-level public health and safety, governance, economic and national security, and public confidence consequences.
- Providing timely warning and assuring the protection of those infrastructures and assets that face a specific, imminent threat.
- Assuring the protection of other infrastructures and assets that may become terrorist targets over time by pursuing specific initiatives and enabling a collaborative environment in which federal, state, and local governments and the private sector can better protect the infrastructures and assets they control.

In addition to the list of sectors shown in Table 1.2, the 2003 National Strategy lists five KR:

- National monuments and icons
- Nuclear power plants
- Dams
- Government facilities
- Commercial key assets

TABLE 1.2 CIKR (14) as of 2003

Sector	Sector-specific agency
Agriculture	Dept. of Agriculture
Food	
• Meat and poultry	Dept. of Agriculture
• All other food products	Dept. of Health and Human Services
• Water	Environmental Protection Agency (EPA)
• Public health	Dept. of HHS
• Emergency services	Dept. of Homeland Security
Government	
• Continuity of government	Dept. of Homeland Security
• Continuity of operations	All departments and agencies
• Defense industrial base	DOD
• Information and telecommunications	Dept. of Homeland Security
• Energy	Dept. of Energy
• Transportation	Dept. of Homeland Security (TSA)
• Banking and finance	Dept. of the Treasury
• Chemical industry and hazardous materials	EPA
Postal and shipping	Dept. of Homeland Security
Nat'l monuments and icons	Dept. of the Interior

1998 was a year of ramping up counterterrorism programs. Major initiatives besides PDD-62 (Countering Terrorism), PDD-63 (Critical Infrastructure Protection), and PDD-67 (Continuity of Government) were the creation of a variety of programs:

- National Infrastructure Protection Center established in the Department of Justice.
- Chemical Safety Board formed.
- National Domestic Preparedness Office created in the Department of Justice.
- Critical Infrastructure Analysis Office (CIAO) established.
- Counter-Terror Coordination Unit in National Security Council formed.

[13]The National Strategy for the Protection of Critical Infrastructures and Key Assets, February 2003. Department of Homeland Security. http://www.dhs.gov

- Congress earmarks $17 M for Special Equipment and Training Grants.
- Attorney General announces creation of National Domestic Prep. Office (NDPO).

1.4 PUBLIC–PRIVATE COOPERATION

By 1999 some experts believed that most infrastructure in the United States was owned by the private sector—not government. The Internet had just been commercialized in 1998 and the communications and electrical power sectors were in the process of being deregulated. Control of most public utilities was in the hands of corporations, and according to Table 1.1, it appeared that the private sector owned or operated most infrastructure considered "critical."[14] Thus, in 1999 President Clinton established the National Infrastructure Assurance Council (NIAC) to bring industry and government closer together. According to Executive Order 13130, NIAC was established to facilitate the partnership through the Public Sector Information Sharing and Analysis Centers (PS-ISAC)[15]:

> By the authority vested in me as President by the Constitution and the laws of the United States of America, including the Federal Advisory Committee Act, as amended (5 U.S.C. App.), and in order to support a coordinated effort by both government and private sector entities to address threats to our Nation's critical infrastructure, it is hereby ordered as follows:
>
> **Section 1.** *Establishment*.
>
> (a) There is established the National Infrastructure Assurance Council (NIAC). The NIAC shall be composed of not more than 30 members appointed by the President. The members of the NIAC shall be selected from the private sector, including private sector entities representing the critical infrastructures identified in Executive Order 13010, and from State and local government. The members of the NIAC shall have expertise relevant to the functions of the NIAC and shall not be full-time officials or employees of the executive branch of the Federal Government.
>
> (b) The President shall designate a Chairperson and Vice-Chairperson from among the members of the NIAC.
>
> (c) The National Coordinator for Security, Infrastructure Protection and Counter-Terrorism at the National Security Council (National Coordinator) will serve as the Executive Director of the NIAC.
>
> (d) The Senior Director for Critical Infrastructure Protection at the National Security Council will serve as the NIAC's liaison to other agencies.
>
> (e) Individuals appointed by the President will serve for a period of 2 years. Service shall be limited to no more than 3 consecutive terms.
>
> **Section 2.** *Functions*.
>
> (a) The NIAC will meet periodically to:
>
> (1) enhance the partnership of the public and private sectors in protecting our critical infrastructure and provide reports on this issue to the President as appropriate;
>
> (2) propose and develop ways to encourage private industry to perform periodic risk assessments of critical processes, including information and telecommunications systems; and
>
> (3) monitor the development of Private Sector Information Sharing and Analysis Centers (PS-ISACs) and provide recommendations to the National Coordinator and the National Economic Council on how these organizations can best foster improved cooperation among the PS-ISACs, the National Infrastructure Protection Center (NIPC), and other Federal Government entities.
>
> (b) The NIAC will report to the President through the Assistant to the President for National Security Affairs, who shall assure appropriate coordination with the Assistant to the President for Economic Policy.
>
> (c) The NIAC will advise the lead agencies with critical infrastructure responsibilities, sector coordinators, the NIPC, the PS-ISACs and the National Coordinator on the subjects of the NIAC's function in whatever manner the Chair of the NIAC, the National Coordinator, and the head of the affected entity deem appropriate.

1.5 FEDERALISM: WHOLE OF GOVERNMENT

The National Strategy document of 2003 declares that homeland security and CIP in particular are "whole of government" responsibilities. "Homeland security, particularly in the context of critical infrastructure and key asset protection, is a shared responsibility that cannot be accomplished by the federal government alone. It requires coordinated action on the part of federal, state, local, and tribal governments; the private sector; and concerned citizens across the country."[16]

But in practice, the strategy places most of the power—and all of the funding—in the hands of the federal government. For example, all SSAs are federal government agencies. The federal government assumed this responsibility even before the creation of the DHS in 2003. The President's Critical Infrastructure Protection Board (PCIPB) was one of the earliest federal government agencies created as a consequence of 9/11. It was followed by a flurry of

[14]The source of this claim has never been found, but a popular meme of the time was that the private sector owned or operated 85% of the critical infrastructure listed in Table 1.1.

[15]http://www.archives.gov/federal_register/executive_orders/1999.html#13130

[16]http://www.fas.org/irp/offdocs/pdd/pdd-63.htm

additional government bureaucracies created to counterterrorism and natural disasters—incidents that appeared to be rising exponentially.

By Executive Order (EO) 13231 (October 2001), President Bush created the President's PCIPB, with primary responsibility to develop policies to protect the information infrastructure of the federal government. EO 13231 recognized the growing importance of the telecommunications and Internet infrastructure as well as its interdependency with other sectors. Without information systems, the US federal government could not continue to operate in the event of an attack:

> Consistent with the responsibilities noted in section 4 of this order, the Board shall recommend policies and coordinate programs for protecting information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems.

In 2002 President Bush signed the Homeland Security Bill, establishing the new DHS. It began operation in February 2003 and incorporated 22 agencies that were scattered throughout the federal bureaucracy. This included the NCS, CIAO, and the Department of Justice Office of Domestic Preparedness, along with a number of other large agencies such as the TSA, INS, Border Patrol, and Coast Guard. Protection of CI continued to expand and become one of the major responsibilities of the DHS.

Presidential Directive HSPD-5 (February 2003) and its companion, *HSPD-8* (December 2003), authorized the Secretary of DHS "to prevent, prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies"[17] In December 2003 President Bush replaced PDD-63 with HSPD-7 (Homeland Security Presidential Directive No. 7). It rewrote the list of sectors and SSAs responsible (see Table 1.3).

Unfortunately, HSPD-7 sectors and KR departed from the list given by the National Strategy and clouded the issue of which department or agency was responsible for energy, power, and the information and telecommunications sector. The list of CIKR in Table 1.3 was short-lived.

Indeed, HSPD-7 does *not* specify who is responsible for several of the sectors previously identified as "critical." It appears that HSPD-7 was written to address infighting among departments and agencies that may have felt left out of the National Strategy. Alternatively, the purpose of HSPD-7 may have been to include departments and agencies that have expertise in fields such as cyber, chemical, and nuclear security. For whatever reason, HSPD-7 leaves some responsibilities unspecified and spreads others across multiple departments.

[17]HSPD-5 (2003).

TABLE 1.3 CIKR (16) and responsibilities as defined by HSPD-7

Sector	Sector-specific agency
Agriculture/food (meat, poultry, eggs)	Department of Agriculture
Public health/food (other than meat, poultry, eggs)	Department of Health and Human Services
Drinking water and treatment systems	Environmental Protection Agency
Energy (production, storage, distribution of gas, oil, and electric power, except for commercial nuclear power facilities)	Department of Energy
Nuclear power plants	Department of Homeland Security and Nuclear Regulatory Commission and Department of Energy
Banking and finance	Department of the Treasury
Defense industrial base	Department of Defense
Cybersecurity	Department of Commerce and Department of Homeland Security
Chemical	Not specified
Transportation systems, including mass transit, aviation, maritime, ground/surface, and rail and pipeline systems	Department of Transportation and Department of Homeland Security
Emergency services	Not specified
Postal and shipping	Not specified
National monuments	Department of the Interior
Key assets: dams, government facilities, and commercial facilities	Not specified

For the first time, HSPD-7 declared that it is impractical to protect everything and focused effort on major incidents—ones that cause mass casualties comparable to the effects of using weapons of mass destruction:

> While it is not possible to protect or eliminate the vulnerability of all critical infrastructure and key resources throughout the country, strategic improvements in security can make it more difficult for attacks to succeed and can lessen the impact of attacks that may occur. In addition to strategic security enhancements, tactical security improvements can be rapidly implemented to deter, mitigate, or neutralize potential attacks… Consistent with this directive, the [DHS] Secretary will identify, prioritize, and coordinate the

> protection of critical infrastructure and key resources with an emphasis on critical infrastructure and key resources that could be exploited to *cause catastrophic health effects or mass casualties* comparable to those from the use of a *weapon of mass destruction*. [3]

By 2009, the number of sectors and KR had expanded even more, culminating in 18 CIKR: *critical manufacturing* was added and information technology and communications were separated into two sectors [2]. In less than a decade, the number of CIKR expanded from 8 to 18. At this pace, CIP would embrace just about every aspect of society, from communications, power, and healthcare to the food we eat, water we drink, and work we do. If CIP embraces nearly everything, perhaps it means nothing. What then is the main goal of CIP?

HSPD-5 and HSPD-8 were expanded by President Obama on March 30, 2011, to strengthen "… the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the Nation, including acts of terrorism, cyber attacks, pandemics, and catastrophic natural disasters."[18] President Obama pared down the number of CIKR in HSPD-7 to 16 sectors and KR in PPD-21 (2013) (see Table 1.4). Postal and shipping was folded into transportation and national monuments and icons were removed. In addition, the SSAs responsible for each CIKR were sharpened with more authority given to the DHS. Thus, the long-term definition of CI was established, but it emphasized physical assets more than cyber assets. This changed in 2018.

TABLE 1.4 CIKR as defined by PPD-21 (2013)

Sector	Sector-specific agency
Chemical	Department of Homeland Security
Commercial facilities	Department of Homeland Security
Communications	Department of Homeland Security
Critical manufacturing	Department of Homeland Security
Dams	Department of Homeland Security
Defense industrial base	Department of Defense
Emergency services	Department of Homeland Security
Energy	Department of Energy
Financial services	Department of the Treasury
Food and agriculture	US Department of Agriculture and Department of Health and Human Services
Government facilities	Department of Homeland Security and General Services Administration
Healthcare and public health	Department of Health and Human Services
Information technology	Department of Homeland Security
Nuclear reactors, materials, and waste	Department of Homeland Security
Transportation systems	Department of Homeland Security and Department of Transportation
Water and wastewater systems	Environmental Protection Agency

[18]PPD-8 (2011).

A series of events precipitated a major realignment within the DHS in late 2018. Major information security breaches of National Security Agency (NSA) documents by Edward Snowden (1983) in 2013, followed by WikiLeaks releasing emails and documents exfiltrated from the Democratic National Committee during the 2016 US presidential election campaign, and misinformation campaigns waged by the Russian Internet Research Agency attempting to influence the 2016 US presidential election precipitated a renewed focus on cyber as well as physical security within the DHS. The 2018 CISA legislation created the CISA organization as shown in Figure 1.1.

On November 16, 2018, President Trump signed into law the *Cybersecurity and Infrastructure Security Agency Act* of 2018. This legislation emphasized cybersecurity for the first time and replaced the National Protection and Programs Directorate (NPPD) with the Cybersecurity and Infrastructure Security Agency also referred to as CISA:

> **CISA's Cybersecurity Division** works with government and private sector customers to ensure the security and resilience of the Nation's cyber infrastructure. The division includes the National Cybersecurity Communications Integration Center (NCCIC).
>
> The **Emergency Communications Division** enhances public safety interoperable communications at all levels of government, providing training, coordination, tools and guidance to help partners across the country develop their emergency communications capabilities.
>
> The **Infrastructure Security Division** coordinates security and resilience efforts using trusted partnerships across the private and public sectors, and delivers training, technical assistance, and assessments to federal stakeholders as well as to infrastructure owners and operators nationwide.
>
> The **National Risk Management Center** (NRMC) works to identify and address the most significant risks to our nation's critical infrastructure.

The CISA leads the national effort to defend CI against the threats of today while working with partners across all levels of government and in the private sector to secure against the evolving risks of tomorrow.

1.6 RISE OF THE FRAMEWORK

A precursor to the risk-informed decision-making phase of DHS was the rise of the framework. A framework is a particular set of rules, ideas, or beliefs used to structure

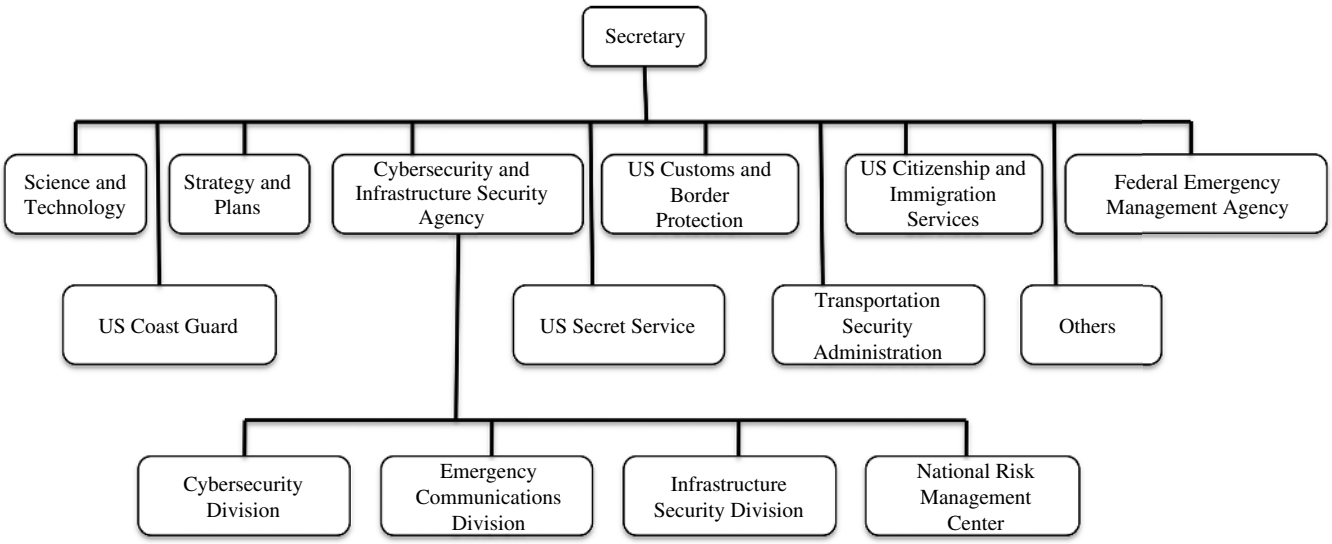

FIGURE 1.1 The structure of the cybersecurity and infrastructure protection offices within the Department of Homeland Security as of 2019 is focused on cybersecurity, emergency communications, infrastructure security, and risk management.

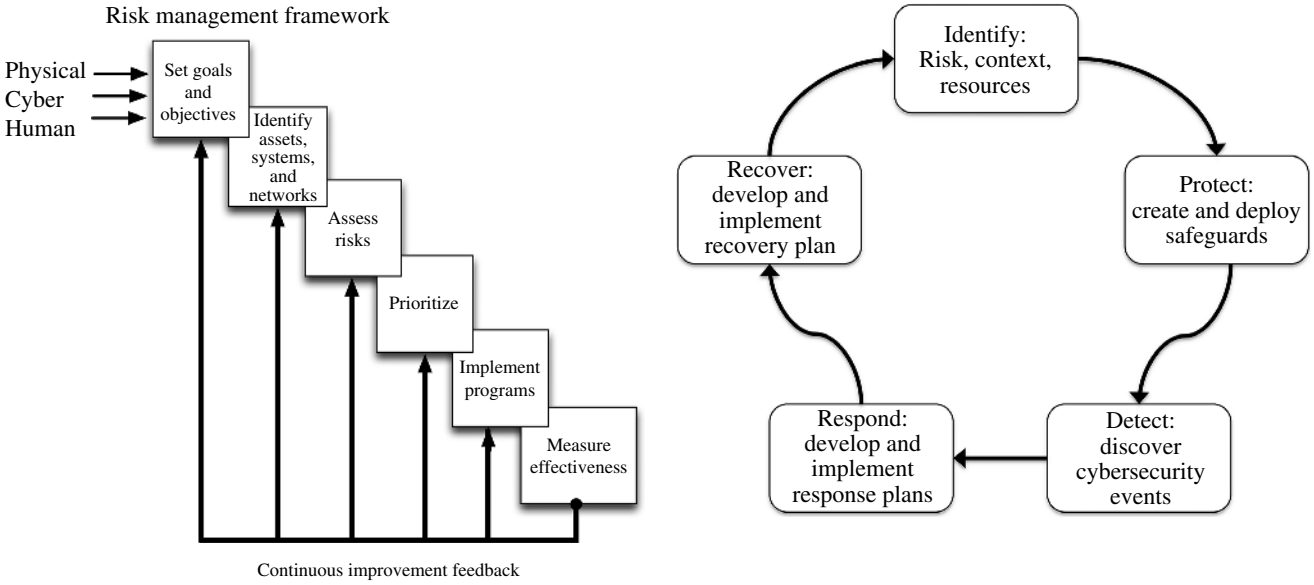

FIGURE 1.2 Two frameworks for qualitative risk management—one for physical assets and the other for computer and network exploits. (a) An early DHS risk management framework for critical infrastructure. (b) The NIST Cybersecurity Framework (CSF) for defending against computer and network exploits.

decision-making. Figure 1.2a is an early framework for risk-informed decision-making within DHS. Figure 1.2b is a specialized framework for evaluating risk and making qualitative risk-based decision-making within the cybersecurity realm.

A number of competing and sometimes overlapping frameworks exist for organizing efforts to protect CI systems. These frameworks can be roughly categorized as **political**, **qualitative**, **quantitative**, and **regulatory/legal**. This book leans toward the quantitative frameworks, but it is important to note that others exist in both theory and practice. A short description of each type is given here with longer descriptions of quantitative frameworks given throughout this book.

Political frameworks have existed since the beginning of government's recognition of CIKR as a federal, state, local, and tribal responsibility. For example, the first allocation of resources formula to combat terrorist attacks on CIKR was based on a mix of population and politics. Each region was

allocated funding regardless of the need. Emergency response facilities such as firefighting equipment were funded regardless of risk or the likelihood of threats. Politically, this made sense because large population centers are where the voters are. However, the embarrassing reality is that some of the most critical assets such as the largest nuclear power plant in the nation are located far from population centers. Threats are more likely to be high where CI assets are high impact, regardless of population or risk.

Qualitative frameworks such as the NIST CSF began to appear as checklists and recommendations to owners and operators of industrial control systems, power grids, and water system SCADA. Executive Order 13636 (EO-13636), *Improving Critical Infrastructure Cybersecurity* (February 2013), and the *Cybersecurity Enhancement Act* of 2014 (CEA) established the role of the NIST in identifying and developing cybersecurity risk frameworks (CSF) for use by CI owners and operators. NIST claims the CSF is "a prioritized, flexible, repeatable, performance- based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks."

Version 1.1 (April 2018) of the CSF prescribes a five-step process along with checklists of recommended practices (see Fig. 1.2b):

- **Identify**—Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.
- **Protect**—Develop and implement appropriate safeguards to ensure delivery of critical services. This step supports the ability to limit or contain the impact of a potential cybersecurity event.
- **Detect**—Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond**—Support the ability to contain the impact of a potential cybersecurity incident.
- **Recover**—Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

The framework is a hierarchical checklist for computer system owners and operators. For example, the **Protect** step might be further decomposed into sub-steps:

User credential verification, revocation, and device authorization.

Physical access permissions.

Remote access permissions.

Network configuration and integrity.

Personnel awareness and training.

Data security—at rest and in transit.

Data capacity assurance.

Separation of development systems from operational systems.

Configuration change controls.

Backup maintenance.

Response and recovery plans are tested.

Vulnerability management plan in place.

Audit records implemented and maintained

Removable media is protected.

Communications and control networks are protected.

Fail-safe, load-balancing mechanisms implemented for resilience.

While NIST claims CSF is a risk-based approach to managing cybersecurity risk, the framework does not define risk or resilience and offers no specific risk assessment methodology or model. Users are left to their own definition of risk and resilience, which is often qualitative rather than quantitative.

Regulatory/legal frameworks follow a similar process diagram of continual improvement. However, for most of its history, DHS has deferred to other agencies when it comes to tying CIKR security to regulations and legal requirements. Generally, regulation has been applied to safety and environmental protections more than security. However, this remains a largely untapped potential source of CIKR protection. For example, the vulnerability of the communications sector is heavily dependent on regulation and the 1996 Telecommunications Act, which created the highly critical carrier hotels and concentrated assets vulnerable to both physical and cyber attacks. This topic is covered in more detail in Chapters 5–8.

The final category of framework is the one emphasized in this book—quantitative—the use of formulas and equations to quantify risk and resilience in what has become known as risk-informed decision-making. A preview of this approach is given here, but the remainder of this book focuses on quantitative measures as much as possible.

1.7 IMPLEMENTING A RISK STRATEGY

The overall strategy of CIP was set by 2012 with PDD-21, but implementation remained a challenge. Policy dictated a vertically integrated effort from federal–state–local and tribal governments and a horizontally integrated effort across public and private organizations. Government was supposed to cooperate, and the private sector was supposed to help the

public sector. But what does this mean? What was each party supposed to do?

Roles and responsibilities could not be aligned vertically or horizontally without operational definitions of objectives. Broadly, the objectives of CIP were impractical as stated by policy. Specifically, infrastructure is too vast, complex, and expensive to protect everything, and expertise among governmental agencies is nonexistent. This called for a narrower definition of objectives and operational definitions of goals, for example, government had to define what is critical in a CI, and both public and private parties had to agree upon metrics for prioritizing projects. Before CIP policy can be implemented, goals and objectives must be defined rigorously enough to implement them.

Policy stated the obvious—protect infrastructure from hazards such as terrorists, storms, earthquakes, and so on. Protection included both hardening and response when something bad happens. Funding was inadequate to protect everything, so implementation depended on prioritization of CI assets, which in turn depended on the definition of *criticality*. Two approaches were initially attempted. The first prioritization strategy was called *risk-informed* and the second was called *resilience-informed*. Risk-informed decision-making means applying risk assessments to prioritize funding of projects to harden CI assets. Resilience-informed decision-making means applying various methods to enhance the resilience of infrastructure assets. Rather than hardening assets, resilience-informed decision-making attempts to make assets adaptable and anti-fragile. Both approaches have their strengths and weaknesses.

1.7.1 Risk-Informed Decision-Making

The fundamental question posed by a risk-informed strategy is this: given limited resources of the federal government, how should resources (funding) be allocated to reduce risk? How should priorities be set? Once again, we turn to the NIPP 2009 for guidance:

> ***Risk***. *The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences*.
>
> ***Risk-Informed Decision-making***. *The determination of a course of action predicated on the assessment of risk, the expected impact of that course of action on that risk, and other relevant factors*.
>
> ***Risk Management Framework***. *A planning methodology that outlines the process for setting goals and objectives; identifying assets, systems, and networks; assessing risks; prioritizing and implementing protection programs and resiliency strategies; measuring performance; and taking corrective action*.

The era of risk-informed decision-making evolved slowly from politically motivated allocation of resources to the quantifiable and measurable six-step process described in Figure 1.1. Instead of dividing funding according to pressures from politicians, risk-informed decision-making allocates funding according to the likelihood of a high-consequence event. Risk is defined in different ways by different SSAs, but given a rigorous definition of risk, agencies can allocate funds according to their impact on risk reduction. The risk-informed strategy follows a risk assessment process such as the following (see Fig. 1.1):

1. Set goals and objectives: Objectives may range from reduction of consequences to elimination of risk, increasing resiliency, and risk minimization. A risk-informed decision-making emphasizes risk reduction, but may also consider additional objectives such as sociopolitical benefits to a community.
2. Identify assets, systems, and networks: Single assets such as a building, bridge, computer, or ports are easy to identify, but most CIKR are part of a complex system. For example, there are numerous assets in a water system—pipes, pumps, treatment plants, and reservoirs. Thus, drinking water is a system containing many assets typically connected together in some fashion. Generally, these systems are modeled as a network of nodes and links: nodes representing pumps, treatment plants, and reservoirs and links representing pipes.

   Assess risks: Risks can be calculated in a variety of ways. A multi-criteria risk assessment is a spreadsheet containing risk factors and numerical ratings for each factor. A probabilistic risk assessment (PRA) approach is more exacting: the simplest form is $R = TVC$, where T is threat as defined by the probability of a human attacker, V is the vulnerability of the asset or system to a given threat, and C is consequence. V is a conditional probability that a given threat will succeed if attempted. C is consequence measured in a meaningful unit such as dollars, casualties, or economic damage. See Appendix B for mathematical details.

   For natural disasters and accidents, a different risk equation is used: $R = \mathrm{E}(c)C$, where $\mathrm{E}(c)$ is the probability of a hazardous event obtained from historical data and C is consequence as before. Hazard probabilities are known for floods, hurricanes, earthquakes, and tornadoes. For example, the famous Gutenberg–Richter scale for measuring the intensity of earthquakes is actually a probability distribution that relates the likelihood of an earthquake to its intensity c. An earthquake of 8 is 1 million times more intense than an earthquake of 4 on the Gutenberg–Richter scale. But the probability E(4) of a magnitude 4 earthquake is 10^{-4} and the probability E(8) of a magnitude 8 earthquake is 10^{-8}—10,000 times less likely.

Risk assessment becomes more complicated when analyzing a complex adaptive system such as a power grid, human population subject to an infectious disease, or large and complex transportation system. When such CIKR systems are assessed for risk, we must consider nonlinear effects, feedback loops, and a variety of factors. These are discussed in subsequent chapters.

Prioritize: CIKR are typically so large and expensive that it is necessary to identify the most critical assets of vital importance. This requires prioritization—a lengthy topic in itself. Simple prioritization in a risk-informed decision-making setting might be to rank assets according to risk. The highest-risk assets are allocated resources first. But this has limitations because the cost to reduce risk by 1% may differ greatly from one asset to another. If the goal is to reduce overall risk, then it may be better to reduce the most cost-effective risks first. In this case, reducing risk of the highest-risk assets may not be cost-effective.

A number of prioritization schemes should be considered. For example, consider highest-consequence, most-vulnerable, highest-risk, highest-return-on-investment, and highest-increase-in-resiliency schemes, depending on the goals and objectives of the risk management framework. A variety of optimization techniques may be applied to this step, because in the end, prioritization is a resource allocation problem that answers the question, "what is the best use of resources to minimize or maximize the objective?"

3. Implement programs: A typical assessment of CIKR produces a recommendation. For example, the assessment may advise the community to secure its drinking water system, repair bridges, or buy backup transformers for the local power grid. Each of these actions takes investment of resources—most often in the form of funding. The outputs from the previous step (Prioritize) are used to guide these investments.

   Measure effectiveness: Finally, the effectiveness of the implementation program needs to be measured and feed back into subsequent assessments. A simple measure is ROI. For example, if the objective is to reduce risk, ROI is obtained by calculating the difference in risk before and after program implementation and dividing by the amount of investment:

$$ROI = \frac{Risk(before) - Risk(after)}{\$Investment}$$

The risk-informed strategy is labor intensive, because all assets must be evaluated and numerical values of T, V, and C estimated. These measurements may number in the thousands, and because it involves probabilities, they may be inaccurate. Furthermore, the results of risk assessment may not satisfy sociopolitical objectives such as addressing assets critical to one segment of the population at the expense of assets in other segments of the population. How does one choose between protecting the drinking water system in one part of town versus the hospital in another part of town?

1.7.2 Resilience-Informed Decision-Making

Almost immediately upon the formation of the new DHS it became clear that CIKR assets numbered in the millions (see Table 1.5) (Page 50 in Ref. [2]). The vastness of single sectors makes it impossible to protect everything. When multiplied by the large number of sectors and key assets, the challenge became insurmountable without some kind of prioritization. Furthermore, the concept of "100% security" began to vanish and be replaced by an elusive concept—*resilience*. Instead of an unyielding goal of 100% security, resilience was an intangible property of CIKR somewhere between absolute security and absolute vulnerability. Instead of a secure infrastructure, a resilient infrastructure was able to bounce back after being attacked or damaged by a storm, earthquake, and so on.

The February 2003 National Strategy document contained the word *resilience* three times. The NIPP 2009 document mentions resilience 15 times. The 2013 PPD-21 directive from President Obama incorporates resilience in its title and

TABLE 1.5 Selection of CIKR assets

Assets in a select subset of CIKR
1,912,000 farms
87,000 food-processing plants
1,800 federal reservoirs
1,600 municipal wastewater facilities
5,800 registered hospitals
87,000 US localities
250,000 firms in 215 distinct industries
2 billion miles of cable
2,800 power plants
300,000 producing sites
5,000 public airports
120,000 miles of major railroads
590,000 highway bridges
2 million miles of pipelines
300 inland/costal ports
500 major urban public transit operators
26,600 FDIC insured financial institutions
66,000 chemical plants
137 million delivery sites
5,800 historic buildings
104 commercial nuclear power plants
80,000 dams
3,000 government-owned/government-operated facilities
460 skyscrapers

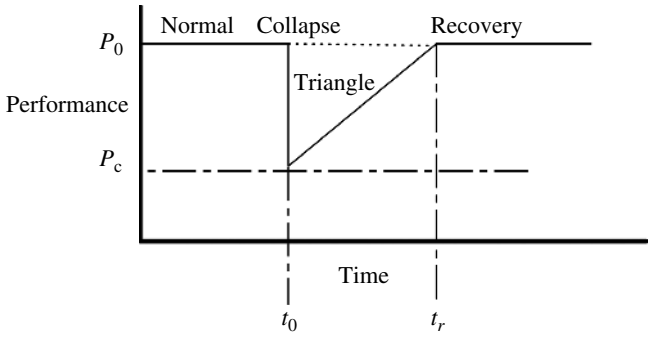

FIGURE 1.3 A resilience triangle is formed by a collapse followed by recovery.

uses the word 44 times.[19] By 2013 the focus of CIKR had shifted from counterterrorism and all-hazard preparedness to building resilience into both infrastructure and the population. The era of resilient infrastructure began, and terrorism, all-hazard response, and weapons of mass destruction faded into the background.

Unfortunately, a variety of qualitative definitions of resilience make it difficult to measure and apply. Vurgin et al. surveyed the concept of resilience in infrastructure systems and offered a number of definitions [4]. Generally, resilience is a property of a system—not a single asset:

> Given the occurrence of a particular disruptive event (or set of events), the resilience of a *system* to that event (or events) is the ability to efficiently *reduce both the magnitude and duration* of the deviation from targeted system performance levels.[20]

Of course, this definition is difficult to put into practice, because it lacks quantifiable specifics. Bruneau et al. proposed a measurable and operational model of resilience as shown pictorially in Figure 1.3 and mathematically modeled in Appendix B. Damage to a system in the form of magnitude and duration is represented by a triangular area notched out of a performance-versus-time diagram shown in Figure 1.3. The resilience triangle represents loss due to a drop in performance followed by a recovery period that eventually restores the system to its previous level of performance.

The difference between full performance and diminished performance represented by the resilience triangle defines the system's resilience. Smaller triangular areas represent greater resilience. The size of the triangular area is reduced, by reducing (1) recovery time, (2) precipitous drop in performance, or (3) both. In addition, the likelihood of a precipitous drop in performance increases the frequency of collapses over time. Thus, reducing the size of the resilience triangle increases resilience:

1. Speedup recovery: $(t_r - t_0)$
2. Reduce performance drop: $(P_0 - P_c)$
3. Decrease the probability of failure, V

This definition suffices for single assets such as buildings, bridges, Internet servers, power plants, and pipelines, but it is inadequate to quantify the resilience of complex interdependent systems such as the power grid, communications network, or an entire municipal water system. However, this metric quantifies the qualitative definition of resilience proposed in the NIPP 2009:

> ***Resilience****: The ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions*. (Page 111 in Ref. [2])

But the resilience triangle model does not address resistance, absorption, adaptation, and recovery factors loosely defined by the NIPP. How does a CIKR resist, absorb, or recover from adversity? How is the ability to resist, absorb, or adapt to adversity measured? These complex properties are addressed by a *complex adaptive systems* model of CIKR described in more detail in Chapters 2–4.

1.7.3 Prevention or Response?

Both risk- and resilience-informed strategies beg the question "How much should be devoted to response versus prevention?" When it comes to CIKR protection, is prevention the best use of resources, or should money be spent mainly in response? In a prevention-only strategy, resources are applied to deter and prevent damage. A response-only strategy invests in response capability, such as emergency management services, law enforcement and firefighting capacity, and so on.

One way to answer to this question is to classify hazards according to their risk levels—low, high, or even complex. Figure 1.4 illustrates the difference between high- and low-risk hazards. The risk profile curve of Figure 1.4 shows how risk can increase without bound versus consequence or approach zero after a temporary increase. The profile of a

[19]Presidential Policy Directive 21—Critical Infrastructure Security and Resilience.

[20]The source of this claim has never been found, but a popular meme of the time was that the private sector owned or operated 85% of the critical infrastructure listed in Table 1.1.

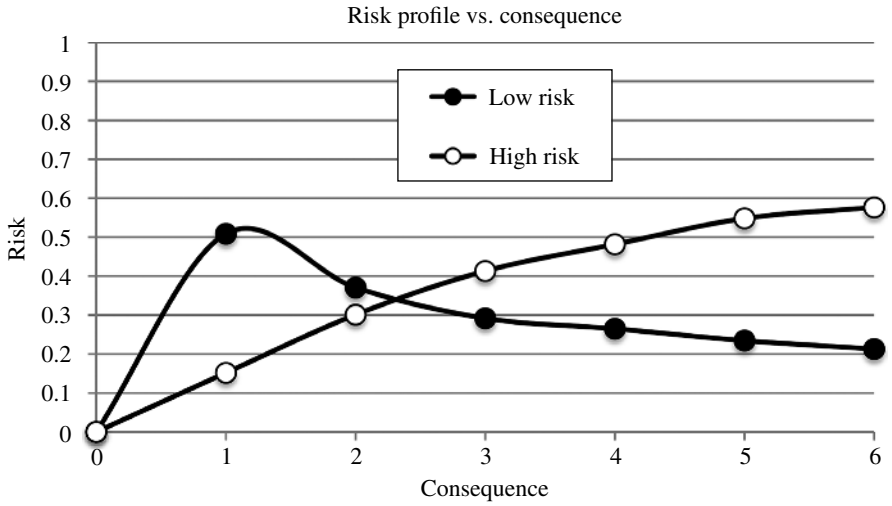

FIGURE 1.4 Some hazards are low risk and some are high risk. Risk increases for high consequences when a hazard is high risk, and the opposite is true for low-risk hazards.

low-risk hazard approaches zero as consequence approaches infinity. The profile of a high-risk hazard approaches infinity.

One of the persistently unresolved CIKR security issues is the question of how many resources should be applied to prevention versus response: is the strategy biased more toward response as the National Strategy seems to suggest, or does it provide just as much support for prevention? What should the balance between prevention and response be?

An argument for a greater emphasis on prevention is that prevention is cheaper than suffering mass casualties, economic damage, psychological damage, or damage to National pride. But 100% prevention is impossible. Some terrorist acts will always escape detection and natural disasters like hurricanes cannot be avoided. Still, roads, buildings, and power lines can be designed to withstand almost anything—for a price.

Table 1.6 lists some high- and low-risk hazards, based on their risk profiles. Note that some consequences are measured in deaths, some in financial loss, and others in impacted area. Consequence can be expressed in a number of different units. Furthermore, risk due to an earthquake is considered low, when measured in land area, but high when measured in deaths.

Figure 1.4 suggests a different risk-informed strategy for low- versus high-risk hazards. For example, the financial risk of small city fires is considered high risk. Therefore, strict building codes and inspections are called for to prevent them. The opposite strategy might apply to low-risk hazards such as terrorism and airline accidents. More resources should be applied to response. Thus, the best risk-informed strategy might depend on the profile of the hazard:

Prevention vs. Response: *Apply more resources to prevention of high-risk hazards and more resources to response to low-risk hazards.*

1.8 ANALYSIS

The evolution of CIP continues to expand and encompass a wider array of challenges. From a focus on terrorism, the homeland security enterprise has grown to encompass cybersecurity, response to natural disasters and climate change, concern for school safety, immigration, and other "whole of government" issues. Only three challenges are explored here: the public–private partnership conundrum, information sharing across jurisdictions, global climate change and its impact on natural disasters, and funding of decaying infrastructure.

TABLE 1.6 Some common high- and low-risk hazards are classified according to their consequences[a]

Low-risk hazard	Consequence
S&P500 (1974–1999)	Financial loss
Airline accidents	Deaths
Tornadoes	Deaths
Terrorism	Deaths
Floods	Deaths
Power outage	Megawatts
Earthquakes	Area
Asteroids	Impact area
Pacific hurricanes	Impact area
High-risk hazard	**Consequence**
Hurricanes	Financial loss
Hurricanes	Deaths
Forest fires	Impact area
Small city fires	Financial loss
Earthquakes	Financial loss
Earthquakes	Deaths
Measles	Deaths

[a] Reference [5].

1.8.1 The Public–Private Partnership (PPP) Conundrum

What is the role of the private sector in building resilient systems? What is the responsibility of government during response and recovery? In practice, the public–private partnership (PPP) comes down to regulation and regulatory processes that are determined by politics more than science. For example, the impact of the 1992 EPACT on energy and the electrical power grid, the 1996 Telecommunications Act on communications and the Internet, and the Safe Drinking Water Act (SDWA) of 1974 on environmental regulation profoundly shape the CI sectors, but none of these regulations reduce risk or improve resilience. In some cases, these sectors have become *less resilient* and *riskier* because of regulation.

The National Strategy calls for cooperation between government and private corporations that own and operate much of the most CI systems and KR, but this strategy is at odds with the way government and private companies operate. Government is motivated by politics, while the private sector is motivated by profit. Both parties want security, but they differ in how to achieve it.

Specifically, the 1992 EPACT dramatically weakened the electric power grid by making it unprofitable to improve the transmission assets underlying the grid, and the 1996 Telecommunications Act created the Carrier Hotel architecture that is now recognized as the communications sector's biggest vulnerability. The energy and telecommunications sectors can be improved only through modification or repeal of these regulations, but such radical modifications will require government and the private sector to understand the underlying complexity of these sectors. The necessary expertise does not exist in government and the motivation does not exist in the private sector.

Reversal of deterioration due to aging and wear is a second major factor hinging on PPP. Much infrastructure developed and paid for over the past 120 years is now near the end of its lifecycle. The Interstate Highway System, for example, continues to grow in length as it also crumbles due to inadequate maintenance. The nation's electric power grid is built on 1940s technology and power lines that can no longer support consumer demand. Most drinking water systems in major cities are decaying and slowly failing. Who should pay the mounting maintenance bill?

1.8.2 The Information Sharing Conundrum

Successful infrastructure protection requires information sharing across jurisdictions (*horizontal sharing*) up and down the various tribal, local, state, and federal levels (*vertical sharing*). For example, law enforcement information must freely ebb and flow among and between agencies—local law enforcement must report suspicious activity to regional intelligence centers that report aggregated information to federal agencies. Conversely, situational awareness information and alerts must flow seamlessly from federal agencies to intelligence collection and distribution agencies and finally back to the street level.

Information sharing—both horizontally and vertically—is key to prevention of terrorist attacks and saving lives during a natural disaster. This is why the National Strategy emphasizes, "… protection-related information sharing among private entities within sectors, as well as between government and private entities." These human networks must span tribal, local, state, and federal levels both horizontally and vertically. But information is often hoarded or filtered as if flows in both directions.

1.8.3 Climate Change Conundrum

A third consideration is the rising challenge of global climate change and its impact on CIKR. Clearly the intensity of storms is on the rise, as well as weather-related consequences. The number of billion-dollar natural disasters has outgrown the nation's ability to pay for them, which leads to the question of priorities: "Should we be spending money on target hardening, resilience, and lowering risk when the next super storm is likely to wipe out an entire sector?" Our response to weather and climate change in general may take all of our resources, leaving little to invest in security.

1.8.4 The Funding Conundrum

The national strategy says nothing about how to pay for CIP. And since the private sector exists to make a profit, they are not motivated to invest in target hardening without some financial justification. So what strategy leads to greater security and resiliency through costly enhancements? If we can learn to think asymmetrically about the architecture of infrastructure sectors, why not think asymmetrically about how to finance these needed improvements?

One idea is to "think dual purpose." Can an investment in security serve a dual purpose of also improving ROI? For example, can a private infrastructure sector company reduce operating costs by enhancing security? It might be economically feasible to reduce insurance premiums by decreasing theft at ports. A telecommunications company might increase profits by improving throughput and reliability of telephone calls per hour. Does redundancy in telecommunications also improve the security and reliability of the Internet? Can public schools be converted to hospital rooms during an emergency that requires surge capacity? Can local law enforcement improve service by using online social media and simultaneously reduce the cost of intelligence fusion centers and 911 emergency call centers?

Dual-purpose systems typically achieve greater security through redundancy, because redundancy provides a cushion

against both heavy loading and system failure. Extra standby telecommunications switches and alternate optical fiber lines may seem expensive if not used all the time, but they also provide a high degree of reliability because the system can switch to a backup when needed. Redundant components improve reliability and fill the gap during periods of surge in demand. For example, the New York Stock Exchange was closed for a week following the 9/11 terrorist attacks, because the exchange lacked redundancy. Had the exchange maintained a backup in a separate location, it could have bounced back more quickly.

The funding challenge may actually be an opportunity to rethink infrastructure. Rethinking the power grid in terms of distributed generation and storage reverses the century-old concept of centralized power plants connected to the consumer through an extensive and complex transmission and distribution network. Over the past 40 years, we have learned that the larger the grid is, the harder it falls. Distributed generation can reduce this vulnerability.

1.8.5 Spend 80% on 20% of the Country

The funding conundrum is partially alleviated by realizing that CI is spread unevenly across the country. CIKR assets are concentrated—typically around densely populated areas such as New York City, Silicon Valley, major ports, manufacturing centers, and key rivers and transportation hubs. Moreover, hubs from different sectors are often geographically clustered—typically around a small number of metropolitan areas. For example, Manhattan, New York, has a high concentration of assets in the banking and finance sector. In addition to the New York Stock Exchange, largest Federal Reserve Bank, and many of the world's largest banks, Manhattan is also home to major communication hubs and one-of-a-kind medical centers.

The largest concentration of energy refineries and major source of refined gas and oil products for distribution throughout the United States is located in Galveston Bay, Texas, and along the Louisiana coast. But Texas and Louisiana are also home to the Mississippi supply chain that supplies food and manufactured goods to the rest of the world.

Fairfax County, Virginia, is the home to a large concentration of Internet servers and defense industrial base companies. Chicago is a national hub for transportation and logistics—the sixth largest port in terms of the intermodal supply chain—and also a critical banking and finance center. Most of the 6 million cargo containers that form the backbone of US trade flow through three ports; most of the energy mined to supply fuel for coal-powered power plants is concentrated in Wyoming, and most of the industrial defense base is concentrated in two or three areas of the United States.

These examples suggest an 80–20% rule: 80% of the investment in CIP should be spent on 20% of the country. This, of course, is a political impossibility, but if we are to think asymmetrically about the challenges facing critical infrastructure, we must face reality: target hardening is too expensive to do everywhere. Instead, an optimal strategy invests in the most vulnerable and high-risk parts of the country. If funding is spread equally to all regions of the country, the most critical regions will be under-protected and the other regions will waste the funds.

1.9 EXERCISES

1. What report was the first to use the term "critical infrastructure"?
   a. EO-13010
   b. The "Marsh Report"
   c. The Patriot Act
   d. The National Strategy for Homeland Security
2. How many CIKR sectors and key resources were listed in the Marsh Report?
   a. 5
   b. 8
   c. 13
   d. 18
   e. 16
3. Which agency within DHS did CISA replace in 2018? (Select one)?
   a. NPPD
   b. NIAC
   c. ENIAC
   d. NIPC
   e. PCIPB
4. What sector is not on the list of Table 1.2: CIKR as of 2003 (Select one)?
   a. Agriculture
   b. Internet and the Web
   c. Water
   d. Transportation
   e. US postal and shipping
5. What organization was the first in the United States to advise a US President on critical infrastructure issues (Select one)?
   a. NCS
   b. NSTAC
   c. NIAC
   d. PCCIP
   e. FEMA
6. What federal government agency was the first to be assigned the responsibility of fighting terrorists in the United States?
   a. NCS
   b. NSTAC
   c. NIAC
   d. PCCIP
   e. FEMA

7. When and where was the first bioterror attack on US soil? Who perpetrated it?
   a. 2001: New York City; Al-Qaeda
   b. 1993: New York City; Ramzi Yousef
   c. 1984: Oregon; Ma Anand Sheela
   d. 1995: Oklahoma City; Unabomber
   e. 1995: Oklahoma City; Timothy McVeigh
8. When was critical infrastructure acknowledged as a major component of homeland security? By what document?
   a. 1995: PDD-39
   b. 1996: EO-13010
   c. 1998: PDD-63
   d. 2002: National Strategy for Homeland Security
   e. 2003: National Strategy for the Physical Protection of Critical Infrastructures and Key Assets
9. How many critical infrastructure sectors were defined in PDD-63 in 1998?
   a. 8
   b. 5
   c. 11
   d. 13
   e. 14
10. How many critical infrastructure sectors are defined in the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets in 2003?
    a. 8
    b. 5
    c. 11
    d. 13
    e. 14
11. NIAC was formed in 1999 by EO-13130. What does NIAC mean?
    a. National Industry Advisory Council
    b. National Infrastructure Assurance Council
    c. National Information Assurance Council
    d. National Information Advisory Committee
    e. National Infrastructure Advisory Committee
12. Geographically, critical infrastructure is concentrated around a few locations, which argues for:
    a. Investing to protect dense population centers
    b. Hardening the top 12 metropolitan areas
    c. Investing 80% of the money to protect 20% of the country
    d. Investing most of the money to protect Manhattan
    e. Distribute the generation of power to factories and shopping malls
13. Dual-purpose strategies for coaxing investment in infrastructure protection from the companies that own and operate most infrastructure are defined as:
    a. Enhancing productivity and availability while improving security
    b. Forcing companies to lower insurance policies to pay for improvements
    c. Taxing Internet companies to stop the spread of viruses
    d. Using redundancy to increase volume
    e. Spreading the components of an infrastructure across large geographical areas
14. Hazards can be classified according to their high or low risk according to:
    a. Consequences
    b. Likelihood of disaster
    c. Loss of power and energy
    d. Response versus prevention costs
    e. Emergency response capability
15. The PPP conundrum is:
    a. Companies do not appreciate homeland security.
    b. The private sector is profit driven and government is not.
    c. It is too expensive to protect everything.
    d. CIKR are owned by the private sector, not government.
    e. Companies ignore state and local jurisdictions.

1.10 DISCUSSIONS

The following questions can be answered in 500 words or less, in slide presentation, or online video formats.

A. The Department of Homeland Security has an evolving strategy that changes relatively quickly as compared with other governmental agencies such as the National Science Foundation, Department of Defense, and Department of Agriculture. Explain why this is the case and evaluate both pro and con arguments for a shifting strategy.
B. An enduring theme of critical infrastructure protection in the United States has centered on strong leadership from the federal government but with engagement at the state, local, and tribal levels. Alternatives to this vertical integration of governmental control have not emerged beyond early discussions of the National Guard as protector. Is vertical integration the best approach? What are alternatives and why might they provide better security?
C. Immediately following the 9/11 attacks the mantra of homeland security was to protect, defer, respond, and recover. This mantra has disappeared from the discussion over the years leaving most of the emphasis on recovery. Argue either in favor or opposition to this narrowing down of focus. Why isn't protection a bigger piece of the strategy?
D. Qualitative analysis methods are by far more prevalent in critical infrastructure analysis than quantitative methods. The reason is obvious—quantitative analysis is difficult. Argue either in favor of quantitative methods or qualitative methods pointing out pros and cons of each.
E. The Department of Homeland Security employed 225,000 people in 2019 and consumed nearly $50 billion. Is it worth it? What are the alternatives?

REFERENCES

[1] Marsh, R. T. *Critical Foundations: Protecting America's Infrastructures*. The Report of the President's Commission on Critical Infrastructure Protection, October 1997, pp. 3.

[2] U.S. Department of Homeland Security (DHS). National Infrastructure Protection Plan (NIPP): Partnering to Enhance Protection and Resiliency, 2009, pp. 111. Available at http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf. Accessed July 29, 2019.

[3] The Whitehouse. *Homeland Security Presidential Directive/Hspd-7*, pp. 1. Available at http://fas.org/irp/offdocs/nspd/hspd-7.html. Accessed December 17, 2003.

[4] Vugrin, E. D., Warren, D. E., Ehlen, M. A., and Camphouse, R. C. A Framework for Assessing the Resilience of Infrastructure and Economic Systems. *Sandia National Labs*, 2010.

[5] Lewis, T. G. *Bak's Sandpile*, 2nd ed, Monterey: Agile Press, 2011.