1

The Challenge

CHAPTER MENU

Before the terrorist attacks of 9/11 infrastructure both critical and otherwise was of interest only to civil engineers, planners, and a handful of regulators. Afterward, infrastructure became critical and the media began to show interest. It became even more interesting when global warming and climate change became an acceptable topic at cocktail parties. Even the politicians fought over it, leading up to the Inflation Reduction Act of 2022, which was essentially a global warming act. Infrastructure became mainstream.

This chapter provides definitions of CIKR (Critical Infrastructure and Key Resources), threat, vulnerability, consequence, risk, resilience, and sustainability. In addition, it identifies the challenges due to vastness, political willpower, NIMBY

Critical Infrastructure Resilience and Sustainability Reader, First Edition. Ted G. Lewis.

(not in my back yard), and the exceptional long-term effort needed to protect and maintain resilience and sustainable infrastructures. The emphasis is on *resilience* and *sustainability* under increasing stress due to climate change, and the exponentially increasing threat of cyberattacks, although other threats are considered.

CIKR manifests as *systems* – collections of interacting or connected assets that act according to a set of rules to form a unified whole. They form a community or industrial commons much like the military-industrial complex of yore. While the plumbing is real or virtual, CIKR is embedded in a complex collection of public and private organizations with rules and regulations spelled out in detail.

CIKR systems respond to stresses placed on them by nature and humans. These are qualitatively or quantitatively spelled out in terms of risk, resilience, and sustainability:

- Risk: expected loss due to a CIKR fault or system failure.
- Resilience: the ability of a CIKR system to resist, absorb, adapt, and recover from a fault or system failure under stress.
- Sustainability: the ability to maintain or support a process continuously over time.

We start with a history lesson: how did critical infrastructure begin and evolve into a major responsibility of government? Then we identify the major threats and consequences confronting infrastructures in America. The focus is on climate change, the prominent challenge of the twenty-first century, followed by cybersecurity.

At the top of the list of threats is extreme weather due to climate change, because it threatens civilization as well as CIKR across the globe. Secondary threats are cyberattacks, accidents/neglect/aging, and terrorists. These are the four horsemen of CIKR sustainability and resilience.

1.1 The Evolution of Critical Infrastructure Protection

CIKR (Critical Infrastructure and Key Resources) systems are considered critical because of their importance to modern life. They could just as well be defined as essential because without them, civilization as we know it is not possible. Modern society is dependent on roads, bridges, communication systems, food production and delivery, drinking water and wastewater management, energy and power, transportation, medical and emergency services, etc. Without them, society would devolve back to a more primitive state.

CIKR systems have evolved over a long period of time, accelerating in sophistication with technology. But the definition of CIKR, along with the realization of its importance and fragility, reaches back to World War II and the Korean conflict, when the United States realized that fuels used to power transportation was a critical asset. Without gasoline and oil, the United States would have been unable to fight.

The criticality of CIKR systems after WWII was soon forgotten until the terrorist attacks leading up to 9/11. The trauma of 9/11 led to the development of plans and procedures for protecting CIKR from accidents, terrorists, cybercriminals, and climate change. As the threat evolves, so does the doctrine of protection in homeland security. The following is a brief introduction and description of this evolution.

1.1.1 In the Beginning

In 1942, the United States was in deep trouble. With the Japanese attack on Pearl Harbor came the prospect of an energy supply shortage. In particular, petroleum products such as gasoline were about to run low or even run out. This prompted the Petroleum Administration for War to create the Petroleum Administration for Defense Districts, aka PADDs – Executive Order 9276 – "to assure for the prosecution of the war the conservation and most effective development and utilization of petroleum in the United States and its territories and possessions."[1] This was better known as "gas rationing," because, to some people, it meant going without gasoline.

The reaction was interesting: some people turned to walking, bicycling, and simply staying at home. A few turned to inventing electric bicycles. One worker borrowed a 12-V battery from a car and an electric motor from a washing machine, put them in his bicycle, and rode to work in what was perhaps the first electric bike.

1 https://www.presidency.ucsb.edu/documents/executive-order-9276-establishing-the-petroleum-administration-for-war.

Creation of PADDs was the first attempt at critical infrastructure protection in homeland security by the United States. Conservation of gasoline and oil in the face of Nazi attacks on oil tankers in the Atlantic meant producing more in PADD 3 and consuming less in the other PADDs. PADDs have been with Americans ever since.

EO-9276 divided the country into five districts:

PADD 1:
A. New England states
B. Central Atlantic states
C. Lower Atlantic states
PADD 2: Midwest states
PADD 3: Gulf Coast states
PADD 4: Rocky Mountain states
PADD 5: West Coast, Alaska, and Hawaiian Island states

Most of the domestic oil came from PADD 3, and refined products like gasoline came from PADD 2. PADD 1 was then, and still is, the largest consumer of oil products. PADDs were no longer needed at the end of WWII, but they were revived again in 1950 because of the Korean War. Eventually, two more PADDs – 6 and 7 – were added, but by 1954, the Petroleum Administration for War was abolished, and along with it, the need for PADDs! So, why are they still used?

Paragraph (e) states an additional purpose that is still with us today:

> Compile data and make continuing surveys with respect to the effect of the prices charged for petroleum upon the efficient wartime operations of the petroleum industry and the maintenance of adequate supplies of petroleum for war and essential industrial and civilian uses. On the basis of such surveys, the Petroleum Administrator shall consult with and recommend to the Administrator, Office of Price Administration, such upward or downward adjustments in the schedule of prices charged for petroleum as will, in the judgment of the Petroleum Administrator, assure the efficient wartime operation of the petroleum industry and the maintenance of adequate supplies of petroleum for war, and essential industrial and civilian uses. In order to enable the Petroleum Administrator to make appropriate recommendations, the Price Administrator shall advise with the Petroleum Administrator prior to the establishment or alteration by the Price Administrator of any schedule of prices to be charged for petroleum.

Recognition of the energy sector of the US economy as critical faded as gasoline shortages abated. Americans went about their business as usual until the second major event in the history of critical infrastructure occurred[2]:

> 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.

2 http://www.ncs.gov/about.html.

The role of the communications infrastructure grew more important as the United States entered the information age. In 1978, two communication regulatory agencies (Department of Commerce Office of Telecommunications and the Whitehouse 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 National Communications System (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 major telecommunications companies. NSTAC is perhaps the first organization to advise a President on critical infrastructure protection.

The Petroleum Administration, NCS, and NSTAC were the first critical infrastructure agencies within the US government. Twenty years would pass before the term *critical infrastructure* was defined and the entire US population became aware of its importance in their daily lives. The Department of Homeland Security (DHS) absorbed NCS in February 2003, but the NSTAC still reports to the President of the United States.

1.1.2 Natural Disaster Recovery

While the NCS and NSTAC were active throughout the 1970s and 1980s, disaster response – both human-caused and natural – was still on the back burner as far as critical infrastructure protection was concerned. The Federal Emergency Management Agency (FEMA) was created in 1978–1979 to respond to hurricanes and earthquakes.[3] Soon after its creation, FEMA was assigned the (temporary) responsibility of responding to terrorist attacks by Executive Order 12148 in 1979[4]:

> 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[5] attempted to influence a political election by poisoning voters with salmonella.[6]

> 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.

---

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

4 http://www.archives.gov/federal_register/codification/executive_order/12148.html.

5 http://www.religioustolerance.org/rajneesh.htm.

6 "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.

> 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.[7]

The salmonella incident in Oregon was an attack on one of the 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 *critical infrastructures*.

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 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 mean 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 – population eight 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.

1.1.3 What Is Critical?

Even in the early 1990s, the trend toward greater awareness of human-made and natural disasters was subtle – it had not reached a point where it was of national concern. But by 1993–1995, the rate and severity of acts of terror, for example, were

7 https://www.grunge.com/355888/the-story-behind-the-largest-bioterrorist-attack-in-u-s-history.

increasing and becoming more alarming to the federal government. The 1993 attack on the World Trade Center led 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 byproduct, 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 period of 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.

The importance of infrastructure for 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, shopping malls, and office buildings. These facilities accommodate many people and yet they are completely open and unprotected. The communication systems, health care, 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, critical infrastructure protection, 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 (CIKR) 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[8]:

> 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 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 tov 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 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 critical infrastructure protection.

The Marsh Report and executive order 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 Executive Order 13010[9]:

> 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

8 http://www.fas.org/irp/offdocs/pdd39.htm.

9 http://www.fas.org/irp/offdocs/eo13010.htm.

> 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.

The work of the PCCIP resulted in PDD-63 (Presidential Decision Directive of 1998), which defined critical infrastructure more specifically and identified basic sectors of CIKR. 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.[10]

The definition of critical infrastructure 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 critical infrastructure sectors in February 2003 with the release of The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets [2].

According to the 2003 strategy document, the objectives of CIKR protection 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; and
- 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, the 2003 National Strategy lists five key resources (KR):

- National Monuments and Icons
- Nuclear Power Plants
- Dams
- Government Facilities
- Commercial Key Assets

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 Department of Justice
- Critical Infrastructure Analysis Office (CIAO) established
- Counterterror Coordination Unit in National Security Council formed
- Congress earmarks $17 M for Special Equipment and Training Grants
- Attorney General announces creation of National Domestic Prep. Office (NDPO)

1.1.4 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 was 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. It appeared that the private

10 http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.

sector owned or operated most infrastructure considered "critical."[11] Thus, in 1999 President Clinton established NIAC (National Infrastructure Assurance Council) to bring industry and government closer together. According to Executive Order 13130, NIAC was established to facilitate the partnership through PS-ISAC (Public Sector Information Sharing and Analysis Centers)[12]:

> 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.

1.1.5 Federalism: Whole of Government

The National Strategy document of 2003 declares that homeland security, and CIKR 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."[13]

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 responsible agencies are federal government agencies instead of state, local, or tribal agencies. The federal government assumed this responsibility even before the creation of the DHS in 2003. The President's Critical Infrastructure

---

11 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 in the United States.

12 http://www.archives.gov/federal_register/executive_orders/1999.html#13130.

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 additional government bureaucracies created to counter terrorism and natural disasters – incidents that appeared to be rising exponentially.

By Executive Order 13231 (October 2001), President Bush created the President's Critical Infrastructure Protection Board (PCIPB), with primary responsibility to develop policies to protect the information infrastructure of the federal government. EO-13231 recognized the growing importance of 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 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 critical infrastructure 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."[13] In December 2003 President Bush replaced PDD-63 with HSPD-7 (Homeland Security Presidential Directive #7). It rewrote the list of sectors and sector-specific agencies responsible.

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 in-fighting 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.

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.[14] In less than a decade, the number of CIKR expanded from 8 to 18. At this pace, CIKR would embrace just about every aspect of society, from communications, power, and health care, to the food we eat, water we drink, and work we do. If CIKR embraces nearly everything, perhaps it means nothing. What then is the main goal of CIP?

HSPD-5/HSPD-8 were expanded by President Obama on 30 March 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, cyberattacks, pandemics, and catastrophic natural disasters."[15] President Obama pared down the number of CIKR in HSPD-7 to 16 sectors and key resources in PPD-21 (2013), see Table 1.1. Postal and shipping was folded into Transportation and National Monuments and Icons was removed. In addition, the sector-specific agencies

13 HSPD-5 (2003).
14 National Infrastructure Protection Plan (NIPP): Partnering to enhance protection and resiliency, 2009.
15 PPD-8 (2011).

Table 1.1 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	U.S. Department of Agriculture and Department of Health and Human Services
Government facilities	Department of Homeland Security and General Services Administration
Health care 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

responsible for each CIKR were sharpened with more authority given to the DHS. Thus, the long-term definition of critical infrastructure was established, but it emphasized physical assets more than cyber assets. This changed in 2018.

A series of events precipitated a major re-alignment within DHS in late 2018. Major information security breaches of NSA (National Security Agency) documents by Edward Snowden in 2013, followed by Wiki leaks 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.

On 16 November 2018, President Trump signed into law the *Cybersecurity and Infrastructure Security Agency Act* of 2018 (CISA). 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 critical infrastructure 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.

1.2 Defining CIKR Risk and Resilience

A number of competing and sometimes overlapping frameworks exist for organizing efforts to protect critical infrastructure systems. These frameworks can be roughly categorized as **political**, **qualitative**, **quantitative**, and **regulatory/legal**. It is important to note that other frameworks exist in both theory and practice. Frameworks are used as a lens through which the practitioner views his or her job.

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 critical infrastructure assets are high valued or high impact, regardless of population or risk.

Qualitative frameworks such as the National Institute of Standards and Technology (NIST) *cybersecurity framework* began to appear as checklists and recommendations to owners and operators of industrial control systems, power grids, and water system Supervisory Control and Data Acquisition **(**SCADA). Executive order 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 critical infrastructure 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:

1) 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.
2) 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.
3) Detect: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
4) Respond: Support the ability to contain the impact of a potential cybersecurity incident.
5) 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
Failsafe, 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.

Quantitative frameworks – the use of formulas and equations to quantify risk and resilience – have become known as *risk-informed decision-making* within DHS. This is a rigorous and disciplined approach that assigns numbers to assets representing probabilities and consequences. For example, the USCG MSRAM quantifies risk in terms of threat probability, vulnerability probability, and consequence or cost due to damage. This rigorous approach assigns numbers to each attack scenario on a port, and then ranks them for the purpose of funding improvements.

Regulatory/legal frameworks follow a similar process. 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 more to safety and environmental protections 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 cyberattacks.

1.2.1 Risk Strategy

The purpose of a risk strategy is to allocate resources optimally, according to some criterion. Specifically, infrastructure is too vast, complex, and expensive to protect everything, and expertise among sector-specific agencies is generally nonexistent. This called for a narrower definition of objectives and operational definitions of goals, e.g. government had to define what is critical in a critical infrastructure, and both public and private parties had to agree upon metrics for prioritizing projects. Before a CIKR 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, and earthquakes. Protection included both hardening and response when something bad happens. Funding is inadequate to protect everything, so implementation depended on prioritization of critical infrastructure 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 critical infrastructure 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.

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 DHS for definitions and guidance:

Threat/hazard: A human attack poses a threat while a weather event poses a hazard. Both terms are used to describe something that can harm CIKR, e.g. a terrorist with a bomb or a hurricane-force wind to power lines.
Vulnerability: A weakness in a CIKR that may be exploited or lead to failure due to a threat or hazard.
Qualitative risk: *The potential for an unwanted outcome resulting from threat/hazard – an incident, event, or occurrence, as determined by its likelihood and the associated consequences*.
Quantitative risk: *Expected loss,* i.e. *the probability of a damaging threat/hazard multiplied by its 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 five-step process described above. Instead of dividing funding according to pressures from politicians, risk-informed decision-making allocates funding according to the likelihood and consequence of an event. Risk is defined in different ways by different sector-specific agencies, but given a rigorous definition of risk, agencies can allocate funds according to their impact on risk reduction.

1.2.2 Resilience Strategy

The vastness of single sectors makes it impossible to protect everything. When multiplied by the large number of sectors and key assets, the challenge becomes 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, terrorist attack, cyberattack, etc.

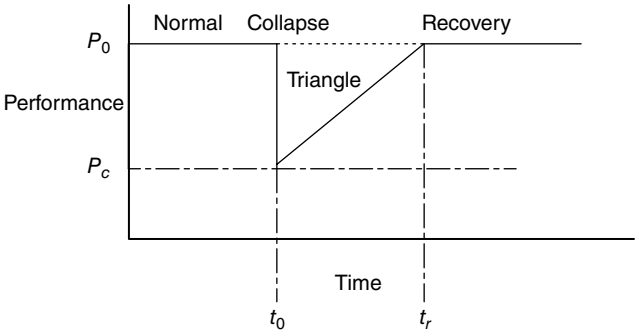

Figure 1.1 A resilience triangle is formed by a collapse followed by gradual recovery.

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 uses the word 44 times.[16] By 2013, the focus of CIKR had shifted from counterterrorism and all-hazards preparedness to building resilience in both infrastructure and the population. With the rising awareness of global warming as a major hazard, resilience and sustainability became a dominant theme. The era of resilient and sustainable infrastructure began, and terrorism, all-hazards response, and weapons of mass destruction faded into the background.

Even 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 and sustainability are properties of a *system* – not a single asset. For example,

> 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. [4]

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 1.1. Damage to a system in the form of magnitude and duration is represented by a triangular area notched out of the performance-versus-time diagram shown in Figure 1.1. 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: (i) recovery time, (ii) precipitous drop in performance, or (iii) 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: $(P_0 - P_c)$ and.
3) Decrease the probability of failure, V.

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* (pp. 111).
>
> More generally, **resilience** is the ability of a CIKR system to resist, absorb, adapt, and recover from a fault or system failure under stress.

16 Presidential Policy Directive-21 – Critical Infrastructure Security and Resilience.

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 Chapter 2.

In this book, risk and resilience will be defined in stochastic terms. The probability of a collapse of random size and duration becomes a problem of statistical analysis. Just as the probability or frequency of hurricanes of an uncertain size are stochastic events, so is the ability to resist, adapt, and recover. The full story depends on at least a rudimentary understanding of probability and statistics – a topic beyond the scope of this book.

Instead of a rigorous definition of resilience, we opt for defining measures that enhance resilience or processes that reduce resilience. In general, resilience is a property of CIKR systems rather than single components, buildings, roads, or computer systems. CIKR systems are stressed by a variety of threats and are plagued by a variety of weaknesses called vulnerabilities. These are described in the next chapter.

1.2.3 Sustainability Strategy

Along with increased interest and concern for global warming and its impact on CIKR, the US DHS began emphasizing sustainability as a goal. Once again, a clear and concise definition is lacking. Qualitatively, sustainability is defined somewhat loosely as:

Sustainability: the ability to maintain or support a process continuously over time.

This simple definition belies the difficulty of building systems that are sustainable for extremely long periods of time. Automobiles require replacement parts and eventually wear out over 20–30 years. And where can a 30-year replacement part be found? Sustainability implies a robust support system that defies wear-and-tear, obsolescence, and constantly supplying "infinite" resources.

The 10,000-year clock project initiated by Danny Hillis is an extreme example of the challenge of sustainability.[17] According to its website, "[Hillis] wanted to build a clock that ticks once every year and decade, the century hand advances once every 100 years, and the cuckoo comes out on the millennium. The vision was, and still is, to build a clock that will keep time for the next 10,000 years."

Building a durable clock is the least of Hillis' problems. Where does one obtain replacement parts, say, 1000 years from now? To be sustainable, the clock must be made of sustainable materials. Hillis favored rust-proof metal and wood. Metal does not rust or wear out, but it can break. So, Hillis had to accommodate repairing the sustainable clock. Wood is grown in a nearby forest so that when wooden parts need to be replaced, workmen can chop down a tree. Hillis assumed that humans will still be around 10,000 years from now!

The clock is located inside a mountain in West Texas to protect it against the weather. An orrery is included – a small physical model of Earth's solar system. At the time of this writing, the clock has not been started on its 10,000-year journey.

> Carved into the mountain are five room-sized anniversary chambers: 1-year, 10-year, 100-year, 1,000-year, and 10,000-year anniversaries. The one-year anniversary chamber is a special orrery. In addition to the planets and the Earth's moon, it includes the interplanetary probes launched during the 20th century. The Clock will activate and run the orrery once a year on a pre-determined date at solar noon.

The 10,000-year clock is a good example of sustainability. However, CIKR is not designed to last 10,000 years, but perhaps it should last hundreds of years.

The 10,000-year clock is an extreme illustration of sustainability, and yet it does not get to the heart of the matter. To more fully understand sustainability, we need to consider thermodynamics – the study of energy and energy transformation in a working system. An *adiabatic process* occurs without transferring heat or mass between the system and its surroundings. That is, it is closed. All systems are either adiabatic or *diabatic*, meaning there is a loss of mass or energy during operation. Diabatic systems typically discard energy in the form of heat or light.

In general, CIKR are open diabatic systems with loss, while only a few Earth processes approximate the adiabatic ideal. How might diabatic systems be constructed to approximate the adiabatic ideal? This is the challenge of sustainability because an adiabatic system can theoretically run forever without wearing out or running down.

---

17 https://www.10000yearclock.net/learnmore.html

A *circular economy* is one that attempts to achieve adiabatic perfection. It is called circular because products of a circular economy are recycled. Recycling consumes more energy, of course, so circular economies are approximations of adiabatic systems that preserve energy and mass – an unrealistic goal. Instead, a circular economy attempts sustainability by recycling and/or *reusing* mass and energy.

Contemporary examples of circular economies, i.e. sustainability – are cogeneration (the production of electricity using waste heat from an industrial process or the use of steam from electric power generation as a source of heat), regenerative braking in an electric car, and recycling of household garbage. Recycling solar panels makes electricity production circular, as does the production of electricity from windmills when the windmills are recycled after they wear out. Sustainability includes circular reuse of greenhouse gas (GHG) CO_2 scooped out of the air, chemically combined with water to produce kerosine that produces CO_2 when burned to power, say, an airplane. Hence the cycle is completed.

Thus, sustainability is a goal defined as follows:

Sustainability goal: the goal of sustainability is to produce goods and services using processes as close to adiabatic as possible and employing circular economy principles where diabatic processes are used. In the context of CIKR, the goal is to improve CIKR sustainability using circular economy principles.

Societal investments in six key green technologies could yield massive and lasting benefits for the US economy:

- Advanced nuclear power generation
- Clean steel production
- Direct air CO_2 capture
- Mass adoption of electric vehicles
- Green hydrogen as a natural gas replacement and for use in fuel cells
- Long-duration or grid-scale energy storage

Together, a future green economy can have a market value of $2 trillion a year by 2050, equal to roughly 10% of current US gross domestic product. This is the challenge for the twenty-first century.

1.2.4 The Four Horsemen

The DHS recognizes the following threats/hazards[18]:

- Climatological events (extreme temperatures, drought, wildfires)
- Hydrological events (floods)
- Meteorological events (tropical cyclones, severe convective storms, severe winter storms)
- Geophysical events (earthquakes, tsunamis, volcanic eruptions)
- Pandemics (global disease outbreaks)
- Space eeather events (geomagnetic storms)
- Technological and industrial accidents (structural failures, industrial fires, hazardous substance releases, chemical spills)
- Unscheduled disruptions (aging infrastructure, equipment malfunction, large-scale power outages)
- Criminal incidents and terrorist attacks (vandalism, theft, property damage, active shooter incidents, kinetic attacks)
- Cyber incidents (denial-of-service attacks, malware, phishing)
- Supply chain attacks (exploiting vulnerabilities to cause system or network failure)
- Foreign influence operations (to spread misinformation or undermine democratic processes)
- Untrusted investment (to potentially give foreign powers undue influence over American critical infrastructure)

This extensive list would fill a dozen books! Instead, we will examine four major groups, beginning with weather/climate change/global Warming:

- Weather/climate change/global warming
- Accidents/aging/neglect
- Terrorism/extremists
- Cyber exploits/criminals

18 https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf

1.3 Weather/Climate Change/Global Warming

Global warming has become a controversial topic. Often weaponized for political purposes, the argument is moot – the Earth is getting warmer, which leads to greater risk, especially to CIKR systems. Climate change is responsible for storms, winds, fires, and perhaps even earthquakes of greater magnitude and duration than ever before – at least as far back as we can tell. The impact on CIKR is obvious – we experience larger events more often and with greater consequences.

Hence, a thorough understanding of climate change is a prerequisite to understanding the threat/hazard surface. The following is a survey of climate change and its impact on risk and resilience of infrastructures [5]. Hopefully, the skeptical reader will find answers to the following questions:

1) How do we know the Earth is warming up?
2) Hasn't it happened before, so why worry?
3) Is it caused by humans, if so, can we do anything about it?
4) Is global warming just a passing bump in the weather road?

Life on Earth has been threatened so many times before that reports of existential near misses have become rather routine. For example, the *Carboniferous Rainforest Collapse* (CRC) 305 million years ago sent Earth into a short ice age that eliminated dense vegetation in Europe and America. CRC created vast coal seams that we now burn as power plant fuel. Some scientists claim it was the result of very large volcanic plumes that blotted out the sun. Others say it was caused by a swarm of asteroids attacking all at once.

An even more serious event called the *Permian–Triassic Extinction* (*Great Dying*) occurred 252 million years ago, and nearly ended us before we had a chance to begin. The Great Dying wiped out 96% of marine animals and 70% of terrestrial life. It took 10 million years to recover! Again, the calamity was due to an abrupt climate change – a sudden release of methane, which is a *GHG*. These gases are thought to have emanated from fires and volcanoes.

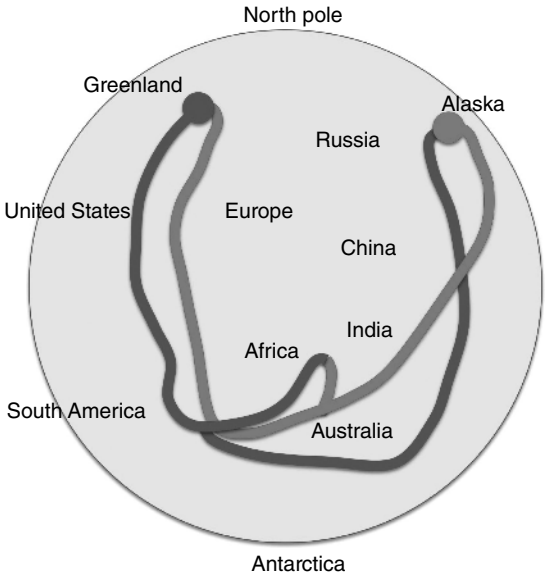

Figure 1.2 The Atlantic conveyor is part of the global circulation system of water currents called *Thermohaline Circulation* – the movement of oceans from the Southern Hemisphere to the North. Warmer water flows from the Indian Ocean, around South Africa, up the Gulf Stream bordering Eastern United States, and to Greenland. It distributes its heat to North America and Europe and then cools in the North Atlantic. The cooler water sinks below the surface, and returns back to the Antarctic and Indian Ocean, where the cycle repeats. *Source:* Adapted from NASA/JPL [6].

More recently, scientists using archeological traces found in rocks, soils, and trees have evidence of abrupt cooling. The *Younger Dryas Stadial* event 12,000 years ago is known as the *Big Freeze* because immediately after the event, Earth's temperature suddenly dropped. This cold spell lasted for 1300 years and established the Siberian land bridge that opened the door between Asia and North America so humans could migrate into the Western Hemisphere.

The Big Freeze might have been caused by a shift in the jet stream or an extreme solar flare, but a more likely explanation is that spillage from Lake Agassiz stalled the *meridional overturning circulation* (MOC) system of ocean currents that warms the Northern Hemisphere. MOC is also a kind of *thermohaline* circulation system that moves water and heat from the southern to the northern hemisphere. But MOC and thermohaline circulation are mouthfuls, so many people call the North American thermohaline circulation system the *Atlantic conveyor* because it works like a heat conveyor belt moving warm water northward and cold water southward, see Figure 1.2. The Atlantic conveyor controls the temperature of the entire planet much like a thermostat controls a room's temperature.

Earth's temperature has never traveled in a straight line. It seems to oscillate from one extreme to another extreme. *Dansgaard–Oeschger (D–O) Events* are periodic warming episodes lasting a few decades followed by longer cooling periods.

The last one was 11,500 years ago. Greenland warmed by 4 °C within a relatively short 40 years, and then cooled down only to warm up again.

Large sheets of ice, called glaciers, can also change the Earth's temperature by melting and freezing. *Bond Events* are warming-cooling oscillations that occur about every 1470, plus or minus 500, years. They mostly happen in the North Atlantic. Nine cycles have been observed so far. Fred Singer and Dennis Avery report, "The Earth has been in the Modern Warming portion of the current cycle since about 1850, following a Little Ice Age from about 1300 to 1850. It appears likely that warming will continue for some time into the future, perhaps 200 years or more, regardless of human activity."[19]

Recorded history of global warming and cooling suggests that the current warming period is just another natural event and there is nothing to worry about. *The difference now is that warming is happening at the speed and intensity never before experienced*. There is very little time to plan and adapt. Critical infrastructure must be protected now, and there is not much time. Climate change is different this time because it is made by humans and it is happening fast.

1.3.1 The Carrington Event

Early in the morning of 1 September 1859, amateur astronomer Richard Carrington cranked open the dome of his private observatory to scan the bright London sky. The sunspots attracted his attention, so he aimed his nineteenth century telescope toward the sun and began sketching what he saw, "two patches of intensely bright and white light" erupting from the sunspots.[20] The flares vanished almost as suddenly as they appeared, but within hours, their impact was felt across the entire globe. Later that day, telecommunications (telegraph) began to fail around the world. Some machines showered operators with sparks and set papers on fire. Bright and colorful aurora borealis "light shows" appeared all over the planet. Some birds and people thought it was the beginning of a new day and set about chirping and going to work. Other animals and people thought it was the Big One and began preparing to meet their creator.

Carrington observed the largest known solar flare – a massive solar explosion with the energy of 10 billion atomic bombs. Traveling at the speed of light across the 93 million miles between the sun and Earth, the flare eventually reached Earth. Its electrified gas and subatomic particles produced a *geomagnetic storm* – dubbed the *Carrington Event*. Geomagnetic storms contain highly charged EMP (electromotive potential) particles that play havoc with electronic systems. In 1883, this meant telegraphy. But in 2023, messing with electronics means messing with just about everything we depend on for modern life.

Ice core samples confirm that the Carrington Event was twice as big as any other solar storm in the last 500 years. A 2008 report from the National Academy of Sciences claims it could cause "extensive social and economic disruptions" due to its impact on power grids, satellite communications, and GPS systems [7].

Power grid engineers are concerned that a Carrington Event might melt the copper wires in power lines and scramble circuits in control computers. The impact could be enormous because modern life depends on electrical power to run the Internet, transportation systems, factories, offices, and food and water supply systems. For example, a geomagnetic storm in March 1989 left six million people in Quebec, Canada, without power for nine hours.

While scientists have been measuring Earth's evolving and complex nature for perhaps hundreds of years, the Carrington Event marks the beginning of *climatology* – the study of Earth's climate. It embraces elements from atmospheric sciences, physical geography, oceanography, and biogeochemistry. Moreover, Carrington's hand-drawn sketches of sunspots mark the beginning of a new idea – that Earth is part of an ecosystem that extends beyond land, sea, and air.

Climatology is about systems and how they interact in complex ways. And as Earth's ecosystem evolves, it changes the very life it spawned. Humans are a product of this ecosystem. As it changes, so must we. The Carrington Event illustrates the stochastic nature of catastrophic events – they are unpredictable, and their impact can be relatively small or black swans.

---

19 *The Physical Evidence of Earth's Unstoppable 1,500-Year Climate Cycle*. S. Fred Singer President, Science and Environmental Policy Project, Adjunct Scholar National Center for Policy Analysis, and Dennis T. Avery, Senior Fellow, Hudson Institute. NCPA Policy Report No. 279 September 2005 ISBN #1-56-808-149-9.

20 http://www.thetruthdenied.com/news/2012/12/10/geomagnetic-storms-and-their-impacts-on-the-u-s-power-grid-pole-shift/.

1.3.2 Black Bodies

A few decades before Carrington discovered sunspots from observations made using his personal telescope, a Scottish engineer named William Thomson was knighted for his role in laying the first transatlantic cable connecting Europe with the new world. Sir William Thomson, Baron Kelvin of Largs, Lord Kelvin of Scotland (1824–1907) is better known for his breakthrough paper, *On an Absolute Thermometric Scale*, an even greater contribution to science. Lord Kelvin calculated the temperature of the coldest thing in the Universe, and established the yardstick used today to measure global temperature. *Absolute zero* is the temperature of matter when not a single molecule moves. Zero is −273 °C to you and me. It is 273 °C below the temperature of frozen ice. One-degree K is equal to 1 °C, but measurements begin at zero in the Kelvin scale, denoted by K.

All life on Earth depends on radiant energy from the sun, as shown in Figure 1.3. That energy is quickly turned into heat to keep the oceans circulating, the air cycling, and plants and animals growing. Accordingly, the Earth must maintain a balanced *energy budget* – an accounting system whereby heat arriving on Earth must also leave because if any heat is trapped here on Earth, it contributes to a gradual (or abrupt) rise in temperature. And since terrestrial life has adapted to temperatures in a relatively mild range centered on 288 K, any departure from this sweet spot is considered a threat to all life. Simply put, all living things on planet Earth depend on a fragile balance between heat coming in and heat leaving the planet.

The famous *Stefan–Boltzmann Law* relates heat to Kelvin temperature. It says the amount of heat radiated by a completely black ball of matter is proportional to its temperature raised to the fourth power. As a result of these pioneers work, today we measure temperature in °C or °K. The goal is to limit the rise in temperature to 1.5 °C. This may not seem like much, but 4.0 °C crosses a tipping point leading to disaster.

The Earth is considered as *gray body* instead of a perfect black body, because much of sun's energy bounces off the atmosphere, clouds, land, and sea. The process of reflecting heat is called *albedo*, and the fraction of energy reflected by a body is called *emissivity*. The average emissivity of Earth is about 39%. This means only 61% of sun's energy reaches Earth. Even after the Earth's continents and seas are heated by the remaining 61%, Earth temporarily stores accumulated heat and then radiates it back into space, according to the Stefan–Boltzmann Law.

When Earth's energy budget is in balance, heat in equals heat out, and life goes on.

If the sun were to stop shining, Earth would eventually return to absolute zero. If the sun's radiation increased, as it does during solar storms, Earth's temperature rises until another equilibrium temperature is reached and the Stefan–Boltzmann Law kicks in and radiates heat back into space to maintain equilibrium. If the sun's rays remain unchanged, Earth's heat

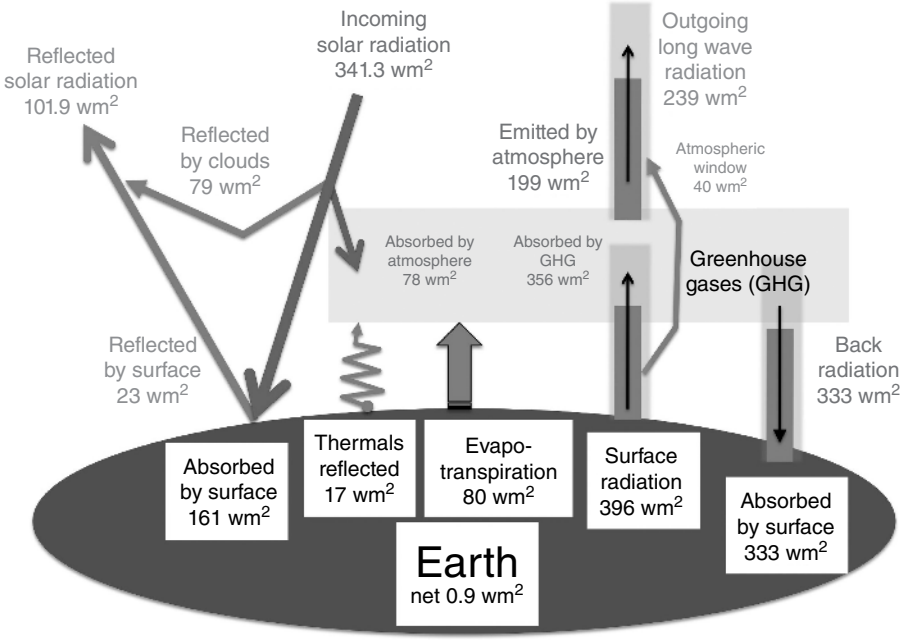

Figure 1.3 A simple model of the Earth's heating and cooling system is sometimes referred to as the Earth's energy budget.
Source: Adapted from NASA/JPL [6].

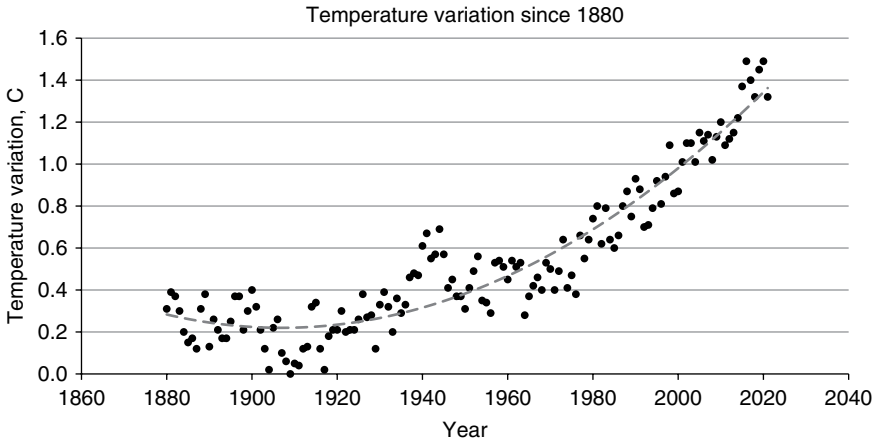

Figure 1.4 Rise in SST from 1880 to 2020. Global temperature is increasing at an exponential rate.

budget remains in equilibrium between heat in and heat out. The Earth's temperature remains steady under equilibrium conditions.

The key to understanding global warming is in Figure 1.3, but the underlying mechanisms driving the processes in Figure 1.3 are not well understood. This is why climatology is still a young science. A number of climatology models have been developed and back-tested to validate them against historical data. Admittedly, the evidence is more empirical than theoretical, so a certain amount of skepticism is warranted. But it is a start.

The first question most people ask is, "How do we know the Earth is warming up?" That is, how do we know there is an imbalance in Earth's energy budget? To answer this question, we can study temperature anomalies recorded over the past 100 years or more. *Anomalies* are departures from recent historical measurements of temperatures taken throughout the year and across the globe. Then we can compare recent measurements against previous years' measurements to determine the size of anomalies and determine any trends.

Figure 1.4 plots Sea Surface Temperature (SST) anomalies obtained from the dataset maintained by the UK Met Office Hadley Center. It is one of the most trusted and respected science centers in climatology. SST readings are collected from nearly 2600 latitude and longitude squares beginning at the International Dateline and the North Pole and moving eastward. Obviously, these measurements exclude land temperatures. Also, they are anomalies, not absolute values. Therefore, an anomaly of 0.5° means the temperature at that square is one-half of a degree above an historical baseline value. Typically, the baseline is an average calculated in 1960, 1980, or perhaps 1880 (pre-industrialization). Figure 1.4 shows measurements made relative to 1980.

Is warming caused by an increase in the world's population? Is it caused by the GDP or public debt? All of these are increasing, and all correlate with SST! Correlation is not the same as causation, but if we are looking for a perfect fit, the concentration of GHG in the atmosphere has the strongest correlation and a scientific basis for increasing SST. Using Occam's razor, increasing concentrations of GHGs are the best explanation for global warming. It is based on science, not politics.

Table 1.2 lists the top sources of CO_2 emissions in 2019. Note that two-thirds of the problem is concentrated on two sectors – transportation and electric power generations. Both are due to burning fossil fuels. This is where we need to focus attention. This is where transformation will happen.

Table 1.2 Contribution to global warming in terms of CO_2 emissions (2019).

Economic sector	%CO_2
Transportation	34.6
Electric power	30.7
Industrial	15.6
Residential	6.7
Commercial	4.8
Other	7.6

Source: Adapted from [8].

1.3.3 The Lightening Rod

James Edward Hansen has been called a hero for advocating *anthropogenic* (human-caused) global warming and also criticized for overestimating its dangers. He is perhaps the staunchest spokesperson for global warming, having received numerous awards for his 40 years of climatology research and "courageous and steadfast advocacy in support of scientists' responsibilities to communicate their scientific opinions and findings openly and

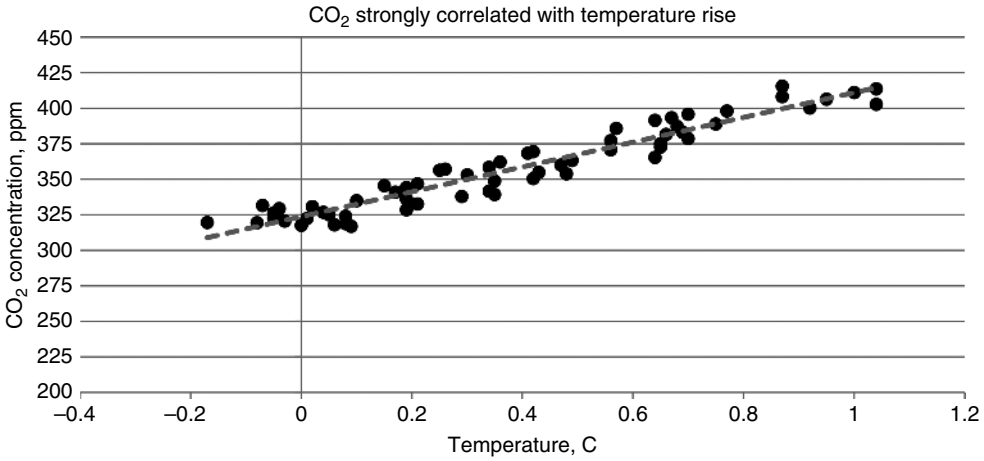

Figure 1.5 CO_2 is the most consequential GHG since 1960. SST is strongly correlated with CO_2 concentrations and suggests continued increases unless CO_2 emissions are reduced. *Source:* Adapted from [9].

honestly on matters of public importance."[21] In 2011, Hansen was arrested while protesting in front of the White House. He has become a lightning rod in the debate over whether climate change is caused by industrialization or is simply another Bond Event. If we believe Figure 1.5, CO_2 emissions are driving global warming just as they did on Venus.

Hansen began his journey to celebrity as a 1960s and 1970s student of the Venusian climate. Venus' climate may have been similar to Earth's several million years ago. But a *runaway greenhouse effect* evaporated its water and turned the second planet into an uninhabitable hothouse. Hansen worries that Earth's fate may be the same [10].

Furthermore, he believes that the future of Earth's climate is in humanity's hands. We can ruin the planet or save it, depending on our policy choices. We can prevent another runaway greenhouse disaster by shutting down coal-burning power plants, adopting energy efficiency policies, switching to renewable energy, converting our old dumb power grid to a smart grid, and producing electricity using fourth-generation nuclear reactors that burn nuclear waste rather than producing it [11].

The bottom line is that we must turn to circular economy renewables to generate electricity and power everything with electric motors instead of burning fossil fuels. And we have less than a decade to transition.

1.4 Consequences

Regardless of whether Hansen's warnings come true or not, a prudent race of earthlings would be wise to prepare for the worst. Otherwise, the Big One may be a black swan we cannot recover from. What if nothing is done to repeal projected rises in temperatures around the globe? The Intergovernmental Panel on Climate Change (IPCC) report warns of disastrous consequences:

- Warming lakes will reduce water quality.
- Heat mortality will increase.
- Diseases will spread more widely.
- Droughts will induce water shortages.
- Crop failures will lead to starvation.
- Warming oceans will kill species and reduce food supplies. Rising sea levels will cause flooding.
- Higher coastal waves will cause tsunami damage.
- Intensified storms (superstorms) cause widespread damage.

It may be worse. The IPCC largely assumes linearity and ignores possible tipping points or black swans like a series of Krakatau-sized volcanoes, unexpected rises in aerosols, etc. Finally, nobody knows the effect of "deep-ocean mixing," whereby deeper layers of the ocean absorb heat and CO_2 to balance Earth's energy budget. What if absorption of heat into the ocean is delayed by 60 years?

21 http://en.wikipedia.org/wiki/James_Hansen.

We must hope for the best but be prepared for the worst. CIKR will be the first line of defense against crippling effects on civilization.

1.4.1 Accidents/Aging/Neglect

One of the greatest American tragedies of infrastructure failure due to neglect and aging is the Flint Michigan drinking water debacle. Flint is the birthplace of General Motors (GM) and had a population of 200,000 at one time. Then the city's economy failed, along with GM's decline due to foreign imports. But in the 1980s, the population declined to 100,000 citizens of which 45% were living below the poverty line. In 2011 the city failed, financially, and the state of Michigan took control.

In classic *normal accident* style (normal accidents will be studied in the next chapter), the state-appointed emergency manager ended the city's practice of piping treated water from Detroit in favor of a cheaper alternative of pumping water from the Flint River. Unfortunately, the Flint River served as a dumping ground for pollutants from adjacent industries and wastewater from the city.

> For more than a century, the Flint River, which flows through the heart of town, has served as an unofficial waste disposal site for treated and untreated refuse from the many local industries that have sprouted along its shores, from carriage and car factories to meatpacking plants and lumber and paper mills. The waterway has also received raw sewage from the city's waste treatment plant, agricultural and urban runoff, and toxics from leaching landfills. Not surprisingly, the Flint River is rumored to have caught fire – twice.[22]

It did not take long before the residents started complaining about the foul water in their water faucets. Things got worse when the city increased chlorine levels to treat the contaminated water. But this compounded the problem by making people sick from elevated levels of cancer-causing chemicals that are a byproduct of chlorination of water.

> In early 2016, a coalition of citizens and groups – including Flint resident Melissa Mays, the local group Concerned Pastors for Social Action, NRDC, and the ACLU of Michigan – sued the city and state officials in order to secure safe drinking water for Flint residents. Among the demands of the suit: the proper testing and treatment of water for lead and the replacement of all the city's lead pipes. In March 2016, the coalition took additional action to address an urgent need, filing a motion to ensure that all residents – including children, the elderly, and others unable to reach the city's free water distribution centers – would have access to safe drinking water through a bottled water delivery service or a robust filter installation and maintenance program.
>
> Those efforts paid off. In November 2016, a federal judge sided with Flint residents and ordered the implementation of door-to-door delivery of bottled water to every home without a properly installed and maintained faucet filter. A more momentous win came the following March with a major settlement requiring the city to replace the city's thousands of lead pipes with funding from the state, and guaranteeing further funding for comprehensive tap water testing, a faucet filter installation and education program, free bottled water through the following summer, and continued health programs to help residents deal with the residual effects of Flint's tainted water.[23]

This terrible incident in Flint illustrates how critical and fragile an infrastructure like water and water treatment is to daily life. Even simple things such as drinking water may be subject to collapse due to neglect, accident, or aging.

1.4.2 The Report Card

The American Society of Civil Engineers (ASCE) Report Card for America's Infrastructure gave infrastructure a C-grade in 2021, up from a D in 2020, see Table 1.3. When climate change is considered, the grade drops to an F. "We decided that, if we add climate change to those grades, everything would be an F."[24]

---

22 https://www.nrdc.org/stories/flint-water-crisis-everything-you-need-know#sec-summary.

23 https://www.nrdc.org/stories/flint-water-crisis-everything-you-need-know#sec-summary.

24 https://www.enr.com/articles/52849-asce-guide-examines-climate-change-threats-to-infrastructure-how-to-prioritize-projects.

Table 1.3 ASCE report card for 2021. Overall grade of C– but trending up.

Infrastructure	Grade
Aviation	D+
Bridges	C
Dams	D
Drinking water	C–
Hazardous waste	D+
Inland waterways	D+
Levees	D
Ports	B–
Public parks	D+
Rail	B
Roads	D
Schools	D+
Solid waste	C+
Stormwater	D
Transit	D–
Wastewater	D+

Source: Adapted from [12].

Of course, physical infrastructure is built by civil engineers, architects, and construction crews, so they are in a good place to evaluate physical infrastructure. In 2022, the ASCE estimated the cost to upgrade US physical infrastructure systems at $2.6 trillion over 10 years. How will the money be spent? Priorities are difficult to be set when CIKR is interdependent – a failure in one often cascades to another. The domino effect of one sector such as the power grid spreading a fault to another sector such as communications and transportation (stop lights) complicates setting of priorities. Interdependencies introduce complexity and complex systems behave in unexpected and nonlinear ways.

1.4.2.1 The Domino Effect

Interdependent complex systems that domino require special considerations. *Cascading* is the term used to describe the spread of a fault in one place causing faults in other places. For example, the state of Texas experienced a black swan power grid failure in 2021 due to an unusually cold winter storm. The Electric Reliability Council of Texas (ERCOT) relies on natural gas production to generate electricity, and natural gas production relies on electricity to produce natural gas. Any fault in the loop breaks the entire system. At one point during the 2021 storm, more than half of the state's natural gas supply shut down because of power outages, frozen equipment, and weather conditions.

Cascading is more common than one might think because CIKR sectors are interconnected in most modern societies. The potential for cascading is exacerbated by optimization and cost-cutting to increase profits and efficiency. The Internet is a classic example. Initially designed to be highly redundant and resilient, the number of servers and routes have consistently centralized for economic reasons. Today's Internet is vulnerable to cascade failures due to reduced servers and links [13].

1.4.3 Terrorism/Extremists

Mohamed Mohamed el-Amir Awad al-Sayed Atta was born in Egypt on 1 September 1968. His strict father demanded his children be educated, so Atta attended Cairo University to study architecture. In 1992 Atta entered the Carl Duisberg Gesellschaft international student exchange program and moved to Germany where he lived in a house provided by a Hamburg couple while attending the Technical University of Hamburg-Harburg, majoring in urban planning. Upon graduating, he worked for Carl Duisberg as a tutor and seminar participant throughout Germany circa 1995–1997 [14].

Atta became more religious and more critical of the Gulf War and US policy in the Middle East while studying and working in Germany. According to the 9/11 Commission Report, Atta expressed anti-Semitic and anti-American sentiment and condemned the "global Jewish movement centered in New York City" that supposedly controlled the financial world and the media. Atta considered New York City the heart of America. If you want to kill America, strike its heart.

Mohammed Haydar Zammar claims he recruited Atta into al-Qaeda. According to the FBI, Atta established the Hamburg cell of the al-Qaeda terrorist network when he moved into an apartment with alleged terrorists Said Bahaji and Ramzi Binalshibh in November 1998. Many other al-Qaeda members lived in the same apartment building, including Marwan al-Shehhi, Zakariya Essabar, Waleed al-Shehri, and others. Twenty-nine men claimed the apartment as home while Atta's name was on the lease, including the 9/11 mastermind Khalid Sheikh Mohammed who repeatedly visited the apartment.

In late 1999 through early 2000, Atta, al-Shehhi, Jarrah, Bahaji, and Binalshibh studied terrorist tactics with Osama bin Laden at Tarnak Farms, near Kandahar, Afghanistan. The CIA observed Atta buying large quantities of chemicals after returning to Germany in 2000. During this time Atta contacted 31 flight schools in the United States regarding flight training. Then he traveled to Prague, stayed overnight, and departed for the United States via Newark, New Jersey. The CIA stopped watching Atta after he entered the United States on 3 June 2000. After all, the CIA does not spy inside of the United States! The CIA's job was done.

Atta and other hijackers in the United States began flight school training in July 2000. He and Marwan al-Shehhi enrolled at Huffman Aviation in Venice, Florida, where both men earned their instrument certificates from the FAA in November. They continued flight training by watching flight deck videos purchased from Sporty's Pilot Shop in Batavia, Ohio. They even practiced flying commercial jets using the Boeing 727 simulator at the Opa-locka Airport near Miami. Atta and Marwan were awarded pilot's licenses on 21 December 2000.

Throughout the summer of 2001, Atta visited Boston, San Francisco, Las Vegas, Spain, and Switzerland, apparently meeting fellow terrorists to plan the 9/11 attacks. In July he met with Binalshibh in Spain, and according to U.S. officials and the Spanish police, Atta drove halfway across Spain to meet with hijackers Wail and Waleed al-Shehri, and Binalshibh. Pere Gomez, manager of Hotel Monica in Spain, said the receptionist on duty refused to rent them a room because she did not like the look of Binalshibh. They later returned and stayed the night. The growing network of hijackers reportedly met al-Qaeda's Spanish point man Imad Yarkas during this trip and coordinated the details of the 9/11 attacks. They ruled out an attack on a nuclear plant and instead decided to hit the World Trade Center.

The day before 11 September 2001, Atta collected al-Omari from the Milner Hotel in Boston and drove to a Comfort Inn in Portland, Maine, where they spent the night in room 232 only to return back to Boston the following morning. Authorities speculate that this maneuver was designed to avoid strict security checks at Logan Airport in Boston. At 6:45 a.m. on 11 September, Marwan al-Shehhi called Atta to confirm that the attacks were ready to begin.

The plane departed Boston with 81 passengers at 7:59 a.m. At 8:24 a.m. air traffic controllers heard a voice believed to be Atta's saying, "We have some planes. Just stay quiet and you will be OK. We are returning to the airport. Nobody move, everything will be OK. If you try to make any moves, you'll endanger yourself and the airplane. Just stay quiet...". Atta is believed to have been the pilot of the plane when it crashed into the north tower of the World Trade Center 23 minutes later at 8:46:40 a.m.

Everyone on the planet remembers 9/11, when a group of terrorists attacked the United States using commercial airliners as weapons. Whenever terrorism is discussed, most people think of the 9/11 terrorists. But terrorism is a narrowly defined act committed by non-state actors:

> **Terrorism**: The threatened or actual use of illegal force and violence by a non-state actor to attain a political, economic, religious, or social goal through fear, coercion, or intimidation.

Data collected since 1970 suggests that most terrorist attacks are for political purposes and not to damage critical infrastructure. With the exception of cybercrime, acts of terror are narrowly focused and declining. Summarizing[25]:

- The highest proportion of unsuccessful attacks since 1970 occurred in 2011 – four out of nine recorded attacks were unsuccessful.
- From 2001 to 2011 California (40) and New York (19) experienced the most total terrorist attacks against the US homeland.
- The three cities in the United States that experienced the most attacks from 2001 to 2011 were New York City (12), Washington, DC (9), and Los Angeles (8).

25 https://www.theguardian.com/news/datablog/2013/apr/17/four-decades-us-terror-attacks-listed-since-1970#data.

- The most common weapons used in terrorist attacks in the United States from 2001 to 2011 were bombs (53% of all weapons used) and explosives (20% of all weapons used).
- For the period from 2001 to 2011, biological weapons were tied with firearms as the third most common weapon used in terrorist attacks (both represented 8% of all weapons used). This is due to the anthrax attacks in October 2001.
- From 2001 to 2011, the most common targets of terrorists in the United States were businesses (62 attacks), private citizens and property (59 attacks), and government (43 attacks).
- The three terrorist organizations with the largest number of attacks on the United States from 2001 to 2011 were the Earth Liberation Front (50), the Animal Liberation Front (34), and al-Qaeda (4).

Physical attacks with costly consequences aimed at infrastructure are rare [15]. The number of attacks since 1970 has steadily declined as well as the number of human casualties. Eighty-nine percent of all deaths due to terrorist attacks in the United States during this time period were caused by the 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City (5%) and the 11 September 2001 attacks (84%). More than 90% of all attacks that targeted critical infrastructure were nonlethal, compared to just over 80% of attacks that did not target critical infrastructure. In contrast, 15% of attacks that did not target critical infrastructure resulted in a single death compared to 5% of attacks that did target critical infrastructure.

Statistically, physical attacks on CIKR obey what is called a long-tailed distribution, see Figure 1.6. By long-tailed, we mean that the distribution rapidly declines as the number of deaths or targets increases. The distribution is skewed to the left with highly likely events of low consequence and rare events of high consequence.

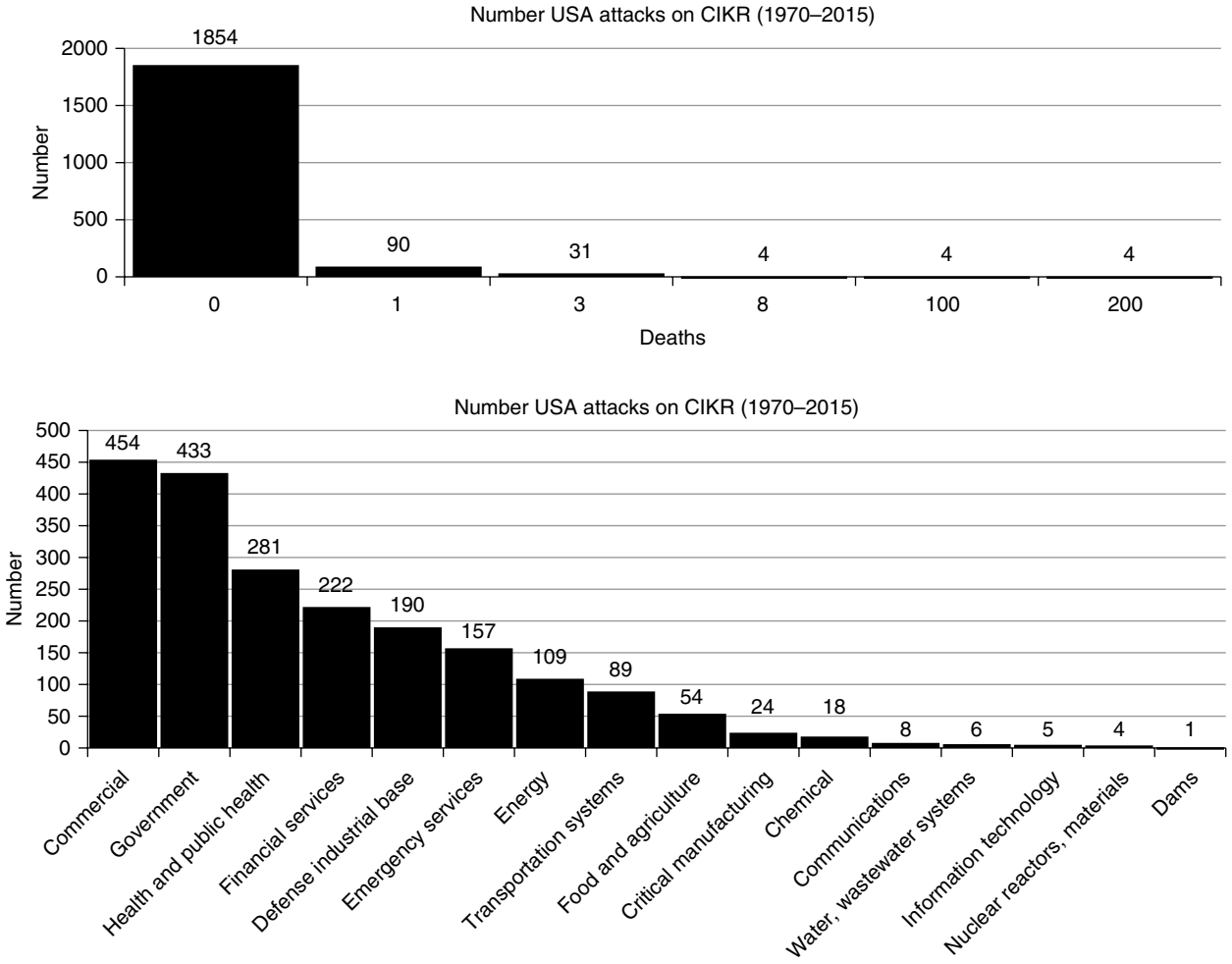

Figure 1.6 CIKR attack statistics are long-tailed – most attacks result in one death, most targets are in the commercial and government sectors, and most are bombings.

By far the preferred weapon used in an attack is a bomb. Neither the attacks nor the weapons used are random. Therefore, aggregation of results in terms of average value is meaningless. Instead, one has to study the distributions as illustrated.

1.4.4 Cyber Exploits/Criminals

Like a thief in the night, Code Red entered through an open door – port 80 – the same door used by browsers to access web pages from anywhere in the world. But it wasn not looking for personal information – at least not yet. Named Code Red by eEye Digital Security employees Marc Maiffret and Ryan Permeh, who were drinking Code Red Mountain Dew when they first detected it, the software *worm* sent copies of itself to thousands of randomly generated Internet addresses as it blazed a trail through the Internet. It jumped from computer to computer using the oldest cyber trick in the book – the *buffer overflow exploit*. Posing as data, buffer overflow allows malicious code into your computer so a hacker can take control. In this case, the impostor "data" would initiate a *distributed denial-of-service* attack (DDOS) on the White House of the United States.

Silently and secretly, Code Red spread to other computers for 20 days, lying dormant inside of Microsoft's Internet Information Server until a certain time and date, when all copies simultaneously attacked www.whitehouse.gov. The force of this malicious program was multiplied by infecting not just one, but nearly 400,000 unsuspecting "*zombie*" computers before lashing out. Like a torrent of water released by a collapsing dam, millions of messages rushed toward the servers located in Washington DC. Only this torrent wasn't water. It was pure software – ones and zeros – that leapt from machine to machine much like the spread of a modern Black Plague. Code Red flooded the www.whitehouse.gov servers with a torrent of meaningless data.

Code Red recruited thousands of innocent and unsuspecting computers along its swath. The unsuspecting participants – called *zombies* – became unwilling co-conspirators in a crime of national scope. Zombie computers form a kind of network – a *botnet* – for the purpose of massively attacking a single target. Botnet zombies derive their power from numbers: at a prespecified date and time, the entire botnet of zombies floods the victim's computer with half-completed requests for attention. But once they get the victim's attention, they ignore it!

1.4.4.1 Black Hats

Black Hats are malicious hackers – people who break into networks for the purpose of doing harm. They use a variety of tools and techniques to perpetrate cyberattacks known as *exploits*. *Script Kiddies* are amateurs, but Black Hats are serious criminals. They are also very clever and often border on genius. Perhaps this is one reason they are drawn to cybercrime – to commit a serious cybercrime you have to be seriously clever. In some cases, Black Hats establish their reputation through crime but earn their fortunes through honest security work at reputable Internet companies. When this happens, Black Hats become White Hats.

DDOS attacks like Code Red are the oldest of all known cyber exploits. Robert Tappan Morris first demonstrated the basic technique, while a student at Cornell University in 1988. At the time, his father, Robert Morris was a NSA scientist working on cybersecurity! The Morris Worm was the first computer worm set free in the *wild*, as hackers say, and the first to get out of control. Morris claims he was trying to see how large the Internet was by tracking where his worm went. Unfortunately, the Morris Worm rendered more than 6000 machines unusable.

Pioneer Morris invented the first *worm* – a malicious program that travels on its own. Viruses have been around longer, but they require human intervention because viruses travel with humans. For example, a virus might jump from one computer to another via a shared disk drive or other storage device that is moved from one computer to another by a user. A worm, on the other hand, spreads clandestinely through the Internet, via email attachments, web pages, etc.

Morris was also the first person prosecuted under the 1986 Computer Fraud and Abuse Act. He was convicted and sentenced to three years' probation, required to perform 400 hours of community service, and fined $10,000. But his story did not end there. Like many hackers, Morris went on to become one of the foremost computer network researchers in the country.

He cofounded and sold a company named Viaweb to Yahoo for $48 million in 1995. Yahoo renamed it Yahoo Store. Later he earned a Harvard PhD in 1999. Today he is a tenured professor of Computer Science at the MIT Computer Science and Artificial Intelligence Laboratory researching network architectures.[26] His friend and co-entrepreneur partner Paul Graham says, "Robert is never wrong."[27]

---

26 www.itsecurity.com.

27 http://en.wikipedia.org/wiki/Robert_Tappan_Morris.

1.4.4.2 Cybercrime Pays

Morris avoided serving time, but 16-year-old Jonathan James achieved a small amount of fame as the first juvenile to serve prison time for hacking. He targeted high-profile organizations like NASA and the Department of Defense. According to the Department of Justice, James cracked into NASA computer systems and downloaded the International Space Station's control software worth $1.7 million. NASA was forced to shut down its computer systems at a cost of $41,000. When caught, James claimed the exploit helped him study C programming and observed that the NASA code was "crappy" and hardly worth $1.7 million. He was banned from recreational computer use and eventually served six months in prison for violation of parole. James' ambition after getting out of jail was to start a computer security company and get rich the old-fashioned way – by earning it.

Adrian Lamo – the *homeless hacker* – cracked computer systems at The New York Times, Yahoo, Bank of America, Citigroup, and Microsoft. Lamo, a Colombian-American who lived in Wichita, Kansas, was once nicknamed the "homeless hacker" because he would drift across the United States on Greyhound buses, finding shelter with friends or in vacant buildings. Lamo would find flaws in his victim's information technology security, exploit them, and then tell the companies about their vulnerabilities. For example, he broke into the New York Times internal network to look at personal information such as social security numbers. He may have pioneered another racket: a decade later, cyber extortion is big business. Modern Black Hats extort World Wide Web companies by promising to *not* attack their sites in exchange for money.

He is perhaps best known for high-profile hacks of companies like Microsoft, and later for turning in Chelsea Manning after receiving leaked classified documents from her. Manning gave Lamo classified video allegedly showing a 2009 air strike in Afghanistan that killed nearly 200 civilians.

Lamo was eventually caught and ordered to pay approximately $65,000 in restitution and sentenced to six months of home confinement plus two years of probation. After his probation expired on 16 January 2007, Lamo began working as an award-winning journalist and public speaker. He was working for a threat analysis company in Sacramento, California in 2009, according to his online bio. He died in 2010 at the age of 37.

Perhaps the best-known Black Hat is Kevin Mitnick – the self-proclaimed "hacker poster boy." The Department of Justice described him as "the most wanted computer criminal in United States history." Mitnick may have benefitted from overly exuberant publicity from two movies: *Freedom Downtime* and *Takedown*. Like traditional wiseguy gangsters, Mitnick began his career as a small-time thief, hacking the Los Angeles bus-ticketing system for free rides. Then he dabbled in *phone phreaking* – manipulating the telephone system to make free long-distance calls. His online bio says, "[My] hobby as an adolescent consisted of studying methods, tactics, and strategies used to circumvent computer security."[28]

Mitnick was eventually caught and convicted of breaking into the Digital Equipment Corporation's computer network and stealing software. He served five years – about eight months of it in solitary confinement. He became a computer security consultant, author, and speaker, appearing on 60 minutes, The Learning Channel, Court TV, Good Morning America, CNN, and National Public Radio. He is the author of two books: *The Art of Deception* (2002) and *The Art of Intrusion* (2005).

Dark Dante, who is Kevin Poulsen in real life, worked for SRI International by day and hacked by night. His most famous hack won him a brand-new Porsche. Each week the Los Angeles radio station KIIS-FM ran a "Win a Porsche by Friday" contest. The station awarded a $50,000 Porsche 944 to the 102nd caller following a preannounced sequence of songs. When the song sequence triggered the calling frenzy, Poulsen took over the station's phone system, blocked out all other callers, made call number 102, and drove away with the prize!

Poulson worked as a White Hat for the government but was drawn to the dark side as his skill and fame spread. In another telephone exploit Dark Dante crashed the phone lines of the TV show Unsolved Mysteries after his photo appeared on the show. More seriously, he hacked into the FBI database containing wiretap information – perhaps to punish the FBI. Law enforcement dubbed him "the Hannibal Lecter of computer crime."[29] When captured, authorities found so many hacking devices they said Poulsen put James Bond to shame. After a 17-month pursuit, Poulsen was captured in a supermarket and served 51 months in jail and was ordered to pay $56,000 in restitution.

Like so many other Black Hats, Poulsen got off easy, leveraged his expertise to get a lucrative job after serving time, and achieved more celebrity than notoriety.[30] Poulsen became a senior editor for Wired News, specializing in cybercrimes and the people who do them. His most prominent article exposed 744 sex offenders for exploiting MySpace profiles. It seems that our society rewards genius even when it leads to a life of crime. Who says crime does not pay?

---

28 http://mitnicksecurity.com/media/Kevin_Mitnick_Bio_BW.pdf.

29 http://library.thinkquest.org/04oct/00460/poulsen.html.

30 https://www.wonderslist.com/top-10-black-hat-hackers.

1.4.5 The Soft War

Cyber exploits are not all done by freelance Black and White Hats. Governments are getting into the business from the offensive side. In May 2007, US President Bush authorized the NSA to launch cyberattacks on the cellular phones and computers operated by insurgents in Iraq to coordinate roadside bombings. The insurgents were recording the strikes and then posting the videos on the Internet to recruit followers.[31] More interesting, however, was the way the American forces used cyber exploits to deceive the insurgents. By hacking into their network and sending messages to the unwitting insurgents, the Americans led the insurgents into a trap set by waiting U.S. soldiers. Cyber exploits in the virtual world can have serious consequences in the real world.

These military hacks were partly responsible for the success of the 2007 surge in Iraq. They allowed military planners to pinpoint and kill the most influential leaders with minimal collateral damage. But using this technology on the battlefield is more significant than Black Hat hacking because it introduces a new weapon into modern warfare. In fact, the war in Iraq was as much about psyops and cyber countermeasures as it was about bombs and IEDs.

The commander of coalition forces in Iraq – General Petraeus – believes in cyberwarfare. Testifying before Congress in September 2007, the General said, "This war is not only being fought on the ground in Iraq but also in cyberspace." The Defense Department's Cyber Command's job is to defend military computer networks as well as go on offense and attack the enemy's network infrastructure. But the United States is not the only country to go on the cyber offensive. In addition to traditional hot wars, nations are now ramping up to fight *soft wars*.

In August 2008, a dispute between the Russian Federation and neighbor Georgia over a region called South Ossetia located on the border between Georgia and Russia initiated a vigorous and effective cyber exploit designed to augment physical conflict between Russian and Georgian military forces. The strife began when Georgian forces launched a surprise attack against South Ossetia separatist forces on 7 August. On 8 August, Russia responded by sending troops into Georgian territory, which Georgian authorities viewed as Russian aggression against Georgia.

Cyberattacks were launched against a large number of Georgian government websites prior to the physical attacks. The exploits primarily defaced public websites and denied service to a number of other sites. Attacks lasted from two to six hours, and damages were relatively low. In some cases, websites were disabled for days following the disruptive attacks.

At first, it appeared that Russian forces were behind the cyberattacks. Later, it was discovered that the attacks were carried out by Black Hats – perhaps located in Russia, but not necessarily supported by the Russian military. Research suggests that the Russian government also did nothing to stop the attacks coming from Russia. It is impossible to trace the DDOS attacks to their origin because the botnet used zombies. Apparently, the aim of the attackers was to block governmental operations and discredit the Georgian government. Georgia's government was unable to get its point of view out to the rest of the world.

Strategies like President Bush's authorization of *information warfare* against Iraqi insurgents can also backfire and get out of control much as Morris's Worm did. For example, military planners rejected a proposed cyberattack on Iraq's banking system because those networks were connected to banks in France. An attack of global proportions might take down the entire banking system! A global cyber contagion may be easier to start than to stop.

These examples illustrate how assaults on the information infrastructure of companies and countries are tools for both good and evil. Criminals use exploits for fame, financial gain, or mischief. Countries use exploits for political and psychological offenses. Some experts claim that terrorist groups such as al-Qaeda purposely do not try to destroy the Internet because they benefit from it too!

In any case, offensive and defensive exploits are not unlike hurricanes. They are virtual storms blowing through cyberspace. While Internet storms may be caused by humans instead of Mother Nature, they also take on characteristics of natural catastrophes. They are unpredictable, extreme, and rare.

1.4.6 Cyberattacks and CIKR

Cyberattacks are asymmetric – they are inexpensive to build and buy but capable of causing great financial harm. It only takes knowledge of the Internet and coding skills to build a malicious worm, virus, or botnet. Moreover, off-the-shelf malicious code is available for purchase over the web! Anyone can buy one and unleash an exploit on the global Internet. The number of exploits, and cost of recovery, is growing exponentially, see Figure 1.7.

---

31 http://www.itsecurity.com.

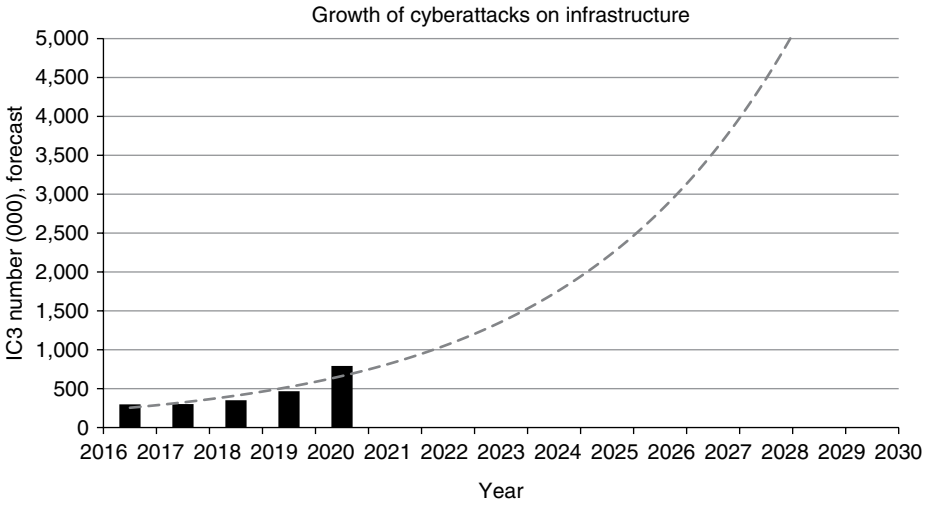

Figure 1.7 Cyberattacks are on the rise, and the forecast is not getting better. Globally, exploits cost trillions of dollars per year.

The most famous exploit against infrastructure so far is *Stuxnet* – the worm that took down Iran's nuclear processing centrifuges in 2009.[32] The Stuxnet worm spread via USB drives that had to be inserted into a control system computer in order to spread.

> **Stuxnet** is a computer worm, reportedly developed and launched by the United States and Israel, that specifically targets programmable logic controllers (PLCs) that control the automation of electromechanical processes, such as those used for centrifuges. It is considered to be the first cyber weapon used in the world due to its ability to cause physical destruction and the first known malware designed to infect industrial control systems (ICS). Stuxnet is typically introduced to a network via an infected USB drive and contains three modules: a worm that executes the main payload, an LNK file that automatically executes the propagated worm copies, and a rootkit that hides all malicious files and processes to evade detection. The worm propagates across the network searching for Siemens Step 7 software on computers controlling PLCs. Once the targeted machine is found, the malware injects the rootkit onto the PLC and Step 7 software, modifies the code, and sends commands to the PLC while displaying normal operation system information to the end user. Stuxnet was used specifically to target centrifuges at Iran's uranium enrichment facility outside Natanz, Iran. It manipulated valves on the centrifuges, increasing and decreasing their speed, putting additional pressure on them, and ultimately damaging the machines until they no longer functioned.
>
> Stuxnet found the controlling software for the centrifuges, seized control, and manipulated the speed of the centrifuges. The malware forced the centrifuges to spin very fast for 15 minutes and then return them to normal speed. Within five months of the attack, the excessive speed changes caused the machines to break, resulting in the loss of about 1,000 centrifuges.
>
> Unfortunately, Stuxnet was unintentionally unleashed in the wild, reportedly, when one of the engineers at an infected facility connected his work laptop to his home network. It infected many more machines than originally intended.

While typical attacks on infrastructure do not result in deaths, the cost of recovery may be large due mainly to labor. The exception, of course, is ransomware, in which the threat actors encrypt files and then blackmail system owners and operators to pay a ransom to unlock their encrypted files. More on this in subsequent chapters.

32 https://www.cyber.nj.gov/threat-center/threat-profiles/ics-malware-variants/stuxnet.

1.5 Discussion

The following are offered as thought-provoking questions to stimulate discussion.

A. The DHS has an evolving strategy that changes relatively quickly as compared to other government 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 is not 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 DHS employed 225,000 people in 2019 and consumed nearly $50 billion. Is it worth it? What are the alternatives?
F. The characterization of threat as the four horsemen may be too simplistic. What is the advantage – and disadvantage – of focusing on these versus the full list provided by DHS?
G. Is the heavy focus on sustainability and resilience in the face of extreme weather and climate change justified? Is the emphasis on cybersecurity also emphasized? What happened to the concern for terrorists and terrorist attacks?
H. Is the extreme rise in gun violence in America a concern for sustainability and resilience of CIKR? Are the two related?

References

1 Marsh, R.T. (1997). Critical foundations: protecting America's infrastructures. The Report of the President's Commission on Critical Infrastructure Protection, October 1997.
2 Department of Homeland Security (2003). The National Strategy for the protection of critical infrastructures and key assets, February. www.dhs.gov.
3 The Whitehouse (2003). Homeland security presidential directive/Hspd-7. 17 December 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. http://www.sandia.gov/CasosEngineering/resilience_assess_framework.html.
5 Lewis, T.G. (2014). *Book of Extremes*. Springer. pp. 183.
6 Trenberth, K.E., Fasullo, J.T., and Kiehl, J. (2009). Earth's global energy budget. *Bulletin of the American Meteorological Society* 90 (3): 311–324.
7 National Research Council (2008). *Severe Space Weather Events: Understanding Societal and Economic Impacts: A Workshop Report*. Washington, DC: The National Academies Press. http://www.nap.edu/catalog.php?record_id=12507.
8 U.S. EPA (2021). Inventory of U.S. greenhouse gas emissions and sinks: 1990–2019. https://www.epa.gov/sites/default/files/2021-04/documents/us-ghg-inventory-2021-main-text.pdf.
9 Earthobservatory. Global warming. https://earthobservatory.nasa.gov/features/GlobalWarming.
10 Hansen, J., Sato, M., Kharecha, P., and Von Schuckmann, K. (2011). Earth's energy imbalance and implications. *Atmospheric Chemistry and Physics* 11 (24): 13421–13449.
11 Hansen, J., Sato, M. and Ruedy, R. (2012). Perception of climate change. *Proceedings of the National Academy of Sciences* 109(14726–14727): E2415–E2423. doi:https://doi.org/10.1073/pnas.1205276109.
12 ASCE (2021). Infrastructure policy & planning: ASCE's 2021 report card marks the nation's infrastructure progress. https://www.asce.org/publications-and-news/civil-engineering-source/civil-engineering-magazine/issues/magazine-issue/article/2021/03/asce-2021-report-card-marks-the-nations-infrastructure-progress.
13 Lewis, T.G. (2015). Why physical cyber security is broken. *Ubiquity*, 24 August 2015.
14 Lewis, T.G. (2011). *Bak's Sand Pile*, 382. Agility Press.
15 Miller, E. (2016). *Terrorist Attacks Targeting Critical Infrastructure in the United States, 1970–2015*. College Park, MD: START.