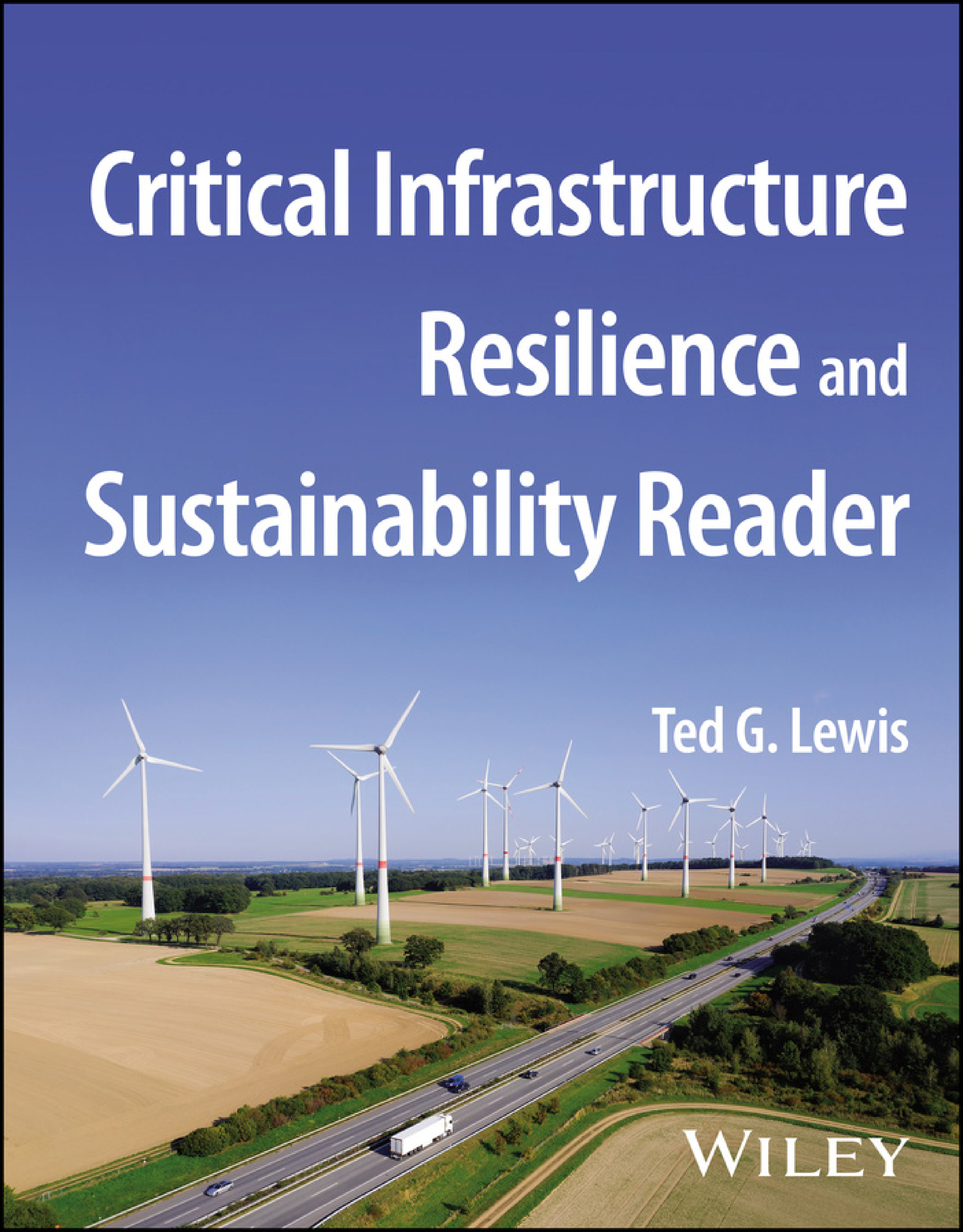
Critical Infrastructure Resilience and Sustainability Reader

Ted G. Lewis



WILEY

Critical Infrastructure Resilience and Sustainability Reader

Critical Infrastructure Resilience and Sustainability Reader

Ted G. Lewis
Naval Postgraduate School (ret.)
Montery, California, USA

WILEY

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Further, readers should be aware that websites listed in this work may have changed or disappeared between when this work was written and when it was read. Neither the publisher nor authors shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic formats. For more information about Wiley products, visit our website at www.wiley.com.

Library of Congress Cataloging-in-Publication Data applied for:
ISBN: 9781394179527 (PB); 9781394179534 (ePDF); 9781394179541 (epub)

Cover Design: Wiley
Cover Image: © Bim/Getty Images

Set in 9.5/12.5pt STIXTwoText by Straive, Pondicherry, India

Contents

Preface *xiii*

1 **The Challenge** *1*
1.1 The Evolution of Critical Infrastructure Protection *2*
1.1.1 In the Beginning *2*
1.1.2 Natural Disaster Recovery *4*
1.1.3 What Is Critical? *5*
1.1.4 Public–Private Cooperation *7*
1.1.5 Federalism: Whole of Government *8*
1.2 Defining CIKR Risk and Resilience *11*
1.2.1 Risk Strategy *12*
1.2.2 Resilience Strategy *13*
1.2.3 Sustainability Strategy *14*
1.2.4 The Four Horsemen *15*
1.3 Weather/Climate Change/Global Warming *16*
1.3.1 The Carrington Event *17*
1.3.2 Black Bodies *18*
1.3.3 The Lightening Rod *19*
1.4 Consequences *20*
1.4.1 Accidents/Aging/Neglect *21*
1.4.2 The Report Card *21*
1.4.2.1 The Domino Effect *22*
1.4.3 Terrorism/Extremists *22*
1.4.4 Cyber Exploits/Criminals *25*
1.4.4.1 Black Hats *25*
1.4.4.2 Cybercrime Pays *26*
1.4.5 The Soft War *27*
1.4.6 Cyberattacks and CIKR *27*
1.5 Discussion *29*
References *29*

2 **What is a Catastrophe?** *30*
2.1 Theories of Collapse *31*
2.1.1 Normal Accident Theory (NAT) *32*
2.1.2 Punctuated Equilibrium Theory (PET) *33*
2.1.3 How Uncertain are Avalanches? *33*
2.1.4 Self-Organized Criticality *35*
2.2 Complex Systems Theory *36*
2.2.1 Tragedy of the Commons (TOC) *36*
2.2.2 Paradox of Enrichment (POE) *38*
2.2.3 Competitive Exclusion Principle (CEP) *41*

2.2.4 Paradox of Redundancy (POR) *43*
2.3 General Systems Theory *43*
2.3.1 Emergence *43*
2.3.2 Self-Organization *44*
2.3.3 Preferential Attachment *44*
2.4 Vulnerable Industrial Commons *46*
2.4.1 TOC Failure *46*
2.4.2 POE Failure *47*
2.4.3 CEP Failure *47*
2.4.4 POR Failure *47*
2.5 Resilience Versus Sustainability *48*
2.5.1 Black Swans *48*
2.5.2 Catastrophe's Long Tail *49*
2.6 Discussion *49*
References *49*

3 Energy Transition *51*
3.1 A Sector Under Transition *51*
3.2 Energy Fundamentals *52*
3.2.1 Understanding Units and Measures *53*
3.2.2 Consumption *54*
3.3 Regulatory Structure of the Energy Sector *55*
3.3.1 Evolution of Energy Sector Regulation *55*
3.3.2 Energy Pipeline Regulations *55*
3.3.3 The Energy ISAC *56*
3.4 Legacy Fuels *56*
3.4.1 Coal *57*
3.4.2 The Rise of Oil and the Automobile *57*
3.4.3 Natural Gas Middlemen *58*
3.4.4 Nuclear Fuel *58*
3.5 Legacy Energy Infrastructure *61*
3.5.1 Oil Refineries *61*
3.5.2 Oil Transmission and Distribution *62*
3.5.3 Oil Storage *63*
3.5.4 The Natural Gas Supply Chain *64*
3.5.5 The Critical Gulf of Mexico Cluster *65*
3.5.6 Critical Refineries *65*
3.5.7 Critical Transmission Pipelines *66*
3.6 Renewables *66*
3.7 Solar – Photovoltaic (PV) *67*
3.7.1 Wind *67*
3.7.2 The Hydrogen Circle *68*
3.7.3 Others *69*
3.8 Batteries and Reservoirs *70*
3.8.1 Modern Batteries *70*
3.8.2 Grid Scale Storage – LDES *71*
3.9 Discussion *71*
References *72*

4 The Vulnerable Powergrid *73*
4.1 What Is the Grid? *74*
4.2 The North American Grid *76*

4.2.1 Grid Structure *77*
4.2.2 ACE and Kirchhoff's Law *78*
4.2.3 Anatomy of a Blackout *78*
4.3 Threat Analysis *80*
4.3.1 Attack Scenario 1: Disruption of Fuel Supply to Power Plants *80*
4.3.2 Attack Scenario 2: Destruction of Major Transformers *81*
4.3.3 Attack Scenario 3: Disruption of SCADA Communications *81*
4.3.4 Attack Scenario 4: Creation of a Cascading Transmission Failure *82*
4.4 From Death Rays to Vertical Integration *83*
4.4.1 Early Regulation *83*
4.4.2 Deregulation and EPACT 1992 *85*
4.4.3 Electricity Sector ES-ISAC *85*
4.5 Out of Orders 888 and 889 Comes Chaos *86*
4.5.1 Economics Versus Physics *88*
4.5.2 What Increases SOC? *89*
4.5.3 NIMBY Versus Environmentalism *90*
4.5.4 A Change of Heart *91*
4.6 The Architecture of Twenty-First Century Grids *91*
4.6.1 The Future Is Storage *92*
4.6.2 SOC Is Reduced *94*
4.6.3 Economics of Electrification *95*
4.7 Discussion *96*
References *96*

5 Water and Water Treatment *97*
5.1 A Vanishing Resource *97*
5.1.1 From Germs to Terrorists *98*
5.1.2 Safe Drinking Water Act *99*
5.1.3 The WaterISAC *100*
5.2 Foundations: SDWA of 1974 *101*
5.3 The Bio-Terrorism Act of 2002 *102*
5.3.1 Is Water for Drinking? *103*
5.3.2 Climate Change and Rot – The New Threats *103*
5.4 The Architecture of Water Systems *104*
5.4.1 The Law of the River *105*
5.4.2 Resiliency of Water Pipeline Networks *105*
5.5 Hetch Hetchy Water *106*
5.5.1 Risk Analysis *108*
5.5.2 Resilience Analysis *108*
5.6 Threat Analysis *108*
5.6.1 The Rational Actor *109*
5.6.2 Hetch Hetchy Threat Analysis *109*
5.6.3 Chem-Bio *109*
5.6.4 Earthquakes *110*
5.7 Water Resilience *110*
5.7.1 Save the Pineapple Express *110*
5.7.2 Gray Water *112*
5.7.3 Desalination *112*
5.7.4 Exemplar Israel *113*
5.8 Discussion *113*
References *113*

6 Transportation Renewed *114*
6.1 Transitioning a Vast and Complex Sector *114*
6.1.1 Government Leads the Way *115*
6.1.2 Safety and Security *115*
6.2 Roads at TOC Risk *116*
6.2.1 The Road to Prosperity *119*
6.2.2 Economic Impact *120*
6.2.3 The National Highway System (NHS) *120*
6.2.4 The Interstate Highway Network is Resilient *121*
6.2.5 The NHS is Safer *121*
6.2.6 The Future is Electric *122*
6.3 Rail and Railroads *122*
6.3.1 Birth of Regulation *123*
6.3.2 Freight Trains *125*
6.3.3 Passenger Rail *126*
6.3.4 Terrorist Target Passenger Trains *127*
6.3.5 Economics of Rail *127*
6.4 Air Transportation *129*
6.4.1 Resilience of the Hub-and-Spoke Network *130*
6.4.2 Security of Commercial Air Travel *132*
6.4.3 How Safe and Secure is Flying in the United States? *134*
6.4.4 Drones *134*
6.4.5 eVTOLs *135*
6.4.6 Commercial Airline Impact on Global Warming *135*
6.5 Discussion *135*
References *136*

7 Supply Chains *137*
7.1 The World is Flat, but Tilted *139*
7.1.1 Supply Side Supply *140*
7.1.2 The Father of Containerization *140*
7.1.3 The Perils of Efficient Supply Chains *141*
7.2 The World Trade Web *144*
7.2.1 WTW and Economic Contagions *145*
7.2.2 Resilience Failures *147*
7.3 TWIC *148*
7.3.1 MSRAM *148*
7.3.2 PROTECT *150*
7.4 Sustainable and Resilient Supply Chains *151*
7.4.1 Greening of Ships *151*
7.5 Are Supply Chains Secure? *151*
7.5.1 Encapsulation Works *152*
7.5.2 Who Owns the Trusted Path? *152*
7.6 Discussion *152*
References *153*

8 Communications and the Internet *154*
8.1 Early Years *156*
8.1.1 The Natural Monopoly *157*
8.1.2 The Communications Act of 1996 158
8.2 Regulatory Structure *158*
8.2.1 The Most Important Person in Modern History *159*

8.2.2 The First (Modern) Critical Infrastructure *159*
8.3 The Architecture of the Communications Sector *160*
8.3.1 Physical Infrastructure *161*
8.3.2 Wireless Networks *163*
8.3.3 Extra-Terrestrial Communication *163*
8.3.4 Land Earth Stations *165*
8.3.5 Cellular Networks *165*
8.3.6 Cell Phone Generations *166*
8.3.7 Wi-Fi Technology *166*
8.4 Risk and Resilience Analysis *167*
8.4.1 Importance of Carrier Hotels *168*
8.4.2 The Submarine Cable Network *169*
8.4.3 HPM Threats *169*
8.4.4 Cellular Network Threats *170*
8.4.5 Physical Threats *171*
8.5 The Monoculture Internet *171*
8.5.1 The Internet Self-Organized *172*
8.5.2 The Original Sins *173*
8.5.2.1 The DNS *174*
8.5.2.2 More Original Sin *175*
8.5.3 The Hierarchical Internet *176*
8.5.4 Too Many Open Ports *177*
8.6 Internet Governance *177*
8.6.1 IAB and IETF *178*
8.6.2 ICANN Wars *179*
8.6.3 ISOC *180*
8.6.4 W3C *180*
8.6.5 Internationalization *181*
8.6.6 Regulation and Balkanization *182*
8.6.6.1 Rise of Regulation *182*
8.6.6.2 Criticality of the Internet *183*
8.7 Green Communications *183*
8.7.1 Solar Computing *183*
8.7.2 Quantum Communications *184*
8.7.3 Adiabatic Logic *184*
8.8 Discussion *184*
References *185*

9 Cyber Threats *186*
9.1 Threat Surface *188*
9.1.1 Script-kiddies *191*
9.1.2 Black Hats *191*
9.1.3 Weaponized Exploits *192*
9.1.4 Ransomware and the NSA *193*
9.2 Basic Vulnerabilities *194*
9.2.1 The First Exploit *195*
9.2.2 TCP/IP Flaws *196*
9.2.3 Open Ports *198*
9.2.4 Buffer Overflow Exploits *199*
9.2.5 DDoS Attacks *200*
9.2.6 Email Exploits *201*
9.2.7 Flawed Application and System Software *201*

9.2.8 Trojans, Worms, Viruses, and Keyloggers *202*
9.2.9 Hacking the DNS *203*
9.2.10 Hardware Flaws *203*
9.2.11 Botnets *204*
9.3 Cyber Risk Analysis *205*
9.3.1 Kill Chain Approach *206*
9.3.2 Machine-learning Approach *206*
9.4 Analysis *207*
9.5 Discussion *208*
References *208*

10 Social Hacking *209*
10.1 Web 2.0 and the Social Network *211*
10.2 Social Networks Amplify Memes *213*
10.3 Topology Matters *215*
10.4 Computational Propaganda *217*
10.5 Beware the Echo Chamber *218*
10.6 Big Data Analytics *219*
10.6.1 Algorithmic Bias *220*
10.6.2 The Depths of Deep Learning *221*
10.6.3 Data Brokers *221*
10.7 GDPR *222*
10.8 Social Network Resilience *223*
10.9 The Sustainable Web *224*
10.9.1 The Century of Regulation *225*
10.9.2 The NetzDG *225*
10.10 Discussion *226*
References *227*

11 Banking and Finance *228*
11.1 The Financial System *231*
11.1.1 Federal Reserve Versus US Treasury *232*
11.1.2 Operating the System *233*
11.1.3 Balancing the Balance Sheet *233*
11.1.4 Paradox of Enrichment *234*
11.2 Financial Networks *235*
11.2.1 FedWire *235*
11.2.2 TARGET *236*
11.2.3 SWIFT *236*
11.2.4 Credit Card Networks *237*
11.2.5 3-D Secure Payment *237*
11.3 Virtual Currency *238*
11.3.1 Intermediary PayPal *238*
11.3.2 ApplePay *239*
11.3.3 Cryptocurrency *239*
11.3.3.1 Nakamoto's Revenge *240*
11.3.3.2 Double Spend Problem *240*
11.3.3.3 Crypto Challenges *241*
11.4 Hacking a Financial Network *242*
11.5 Hot Money *244*
11.5.1 Liquidity Traps *244*
11.5.2 The Dutch Disease *245*

11.6 The End of Stimulus? 246
11.7 Fractal Markets 246
11.7.1 Efficient Market Hypothesis (EMH) 247
11.7.2 Fractal Market Hypothesis (FMH) 248
11.7.3 Predicting Collapse 248
11.8 The Threat is Existential 250
11.9 Discussion 250
References 250

12 Strategies for a Changing World 251
12.1 Whole of Government 252
12.2 Risk and Resilience 253
12.3 Complex and Emergent CIKR 255
12.3.1 Communications and IT 255
12.3.2 Internet and Cybersecurity 256
12.4 Surveillance Capitalism 256
12.5 Industrial Control Systems 257
12.6 Global Pandemics 257
12.7 Transportation and Supply Chains 258
12.8 Banking and Finance 258
12.9 An Integrated Infrastructure Strategy 259
12.9.1 What to Do? 259
12.9.2 The Plan 260
12.9.3 Issues 260
12.10 Discussion 261

Index 262

Preface

I wrote this book as a companion to the third edition of *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*, 2020. It is intended to be a more casual compendium suitable for the curious reader interested in the broad issues of critical infrastructure rather than a formal and rigorous textbook. I hope the reader agrees.

During the 20-year evolution of critical infrastructure studies, from the fear of terrorism, to the daunting problems of cybersecurity, and finally to the challenges of rouge nation-states and domestic terrorism, infrastructure became a national security concern for an entirely different reason – climate change. The world is now facing an existential crisis posed by the byproducts of the industrial revolution – pollution. We have come to the end of the 150-year trail. Now it is time to address the challenge of climate change precipitated by pollution. There is simply too much greenhouse gas (GHG) being emitted into the atmosphere and too much pollution (plastics, etc.) spewing into our water and soil. We are in danger of extinction by our own hands!

As it turns out, most of the problem lands squarely on critical infrastructure systems. According to the US EPA, in 2020, the United States emitted nearly six billion metric tons of GHGs. Carbon dioxide accounted for the largest percentage (79%), followed by methane (11%), nitrous oxide (7%), and other GHGs (3%). Total US emissions for 2019 totaled 6558 million metric tons of CO_2 and net emissions, taking sinks into account, totaled 5769 million metric tons of CO_2 equivalent. Greenhouse gases are emitted by all sectors of the economy, including electric power (25% of total), transportation (29%), industry (23%), residential and commercial (13%), and agriculture (10%).[1]

While all sectors emit GHG, it is interesting to note that a handful of critical infrastructure sectors account for the majority of emissions: electric power, transportation, and agriculture combined account for nearly two-thirds! Thus, the problem may be manageable by addressing a rather narrow – but large – segment of the economy. This is the good news. The bad news is that it is an enormous challenge to turn around such a large entrenched ship!

My strategy is to advocate for circular economics in each of the main sectors that contribute the most to climate change. Circular economics is the economics of recycling and reusing materials and processes. It involves the use of renewable energy to power the planet and greater efficiencies in production, transportation, and consumption. I show that in each instance it is possible to turn the tide by carefully thinking about how to "recycle" and replenish the Earth's assets while at the same time building on the ever-expanding need for energy, transportation, and agriculture.

We are now at the stage of development where it is entirely possible – even profitable – to implement circular economics in every sector. Within the United States, we are on the verge of a 10–20-year revision of the most critical of all infrastructures – energy, transportation, and agriculture. This will have a ripple effect on adjacent infrastructure systems such as water and water systems, banking and finance, supply chains, and cybersecurity.

Circular economics requires different thinking. In particular, we must concern ourselves with externalities like the impact of dumping industrial byproducts into the river and pumping byproducts of industrial processes into the air. What once was "free," is no longer free. These externalities must be paid for or eliminated. For example, petroleum-powered automobiles produce CO_2, which is no longer free. It extracts a price in terms of global warming, illnesses, and social unrest. And while the solution is to electrify transportation, electrification is not free, either. Electrification creates a long supply chain, each stage at which, there is an opportunity to adopt a circular economy – or not! This is the central theme of resilience and sustainability.

[1] https://www.c2es.org/content/u-s-emissions.

The passage of the Inflation Reduction Act (IRA) commits the United States to billions of dollars to address aging infrastructure systems, signals the beginning of the Great Sustainability Movement, and accelerates the transition to resilient and sustainable infrastructure systems. It will unfold dramatically over the following years and be characterized by sorely needed resilience – the ability to absorb and recover from faults – and sustainability – a property of infrastructure that allows it to operate and last for an indefinite length of time.

Second, the threat posed by cybercriminals will only intensify as ultra-sophisticated technologies such as artificial intelligence (AI), machine learning (ML), and large language models (LLM) become commonplace. Abuse of social networks and online interaction pales compared with the potential abuses of these powerful technologies. Ultimately, they must be tamed by regulation, but that will not stop criminals and enemies of the state from using them. We must prepare ourselves by mastering and taming cybersecurity. Hence, the emphasis of this edition of critical infrastructure protection is on cybersecurity as well as resilience and sustainability.

The theme of this edition is resilience and sustainability in the age of existential risk due to climate change. The opportunity is in the Great Sustainability Movement of revising critical infrastructures for the twenty-first century and beyond.

Ted G. Lewis
March 2023

1

The Challenge

CHAPTER MENU

1.1 The Evolution of Critical Infrastructure Protection, 2
1.1.1 In the Beginning, 2
1.1.2 Natural Disaster Recovery, 4
1.1.3 What Is Critical?, 5
1.1.4 Public–Private Cooperation, 7
1.1.5 Federalism: Whole of Government, 8
1.2 Defining CIKR Risk and Resilience, 11
1.2.1 Risk Strategy, 12
1.2.2 Resilience Strategy, 13
1.2.3 Sustainability Strategy, 14
1.2.4 The Four Horsemen, 15
1.3 Weather/Climate Change/Global Warming, 16
1.3.1 The Carrington Event, 17
1.3.2 Black Bodies, 18
1.3.3 The Lightening Rod, 19
1.4 Consequences, 20
1.4.1 Accidents/Aging/Neglect, 21
1.4.2 The Report Card, 21
1.4.2.1 The Domino Effect, 22
1.4.3 Terrorism/Extremists, 22
1.4.4 Cyber Exploits/Criminals, 25
1.4.4.1 Black Hats, 25
1.4.4.2 Cybercrime Pays, 26
1.4.5 The Soft War, 27
1.4.6 Cyberattacks and CIKR, 27
1.5 Discussion, 29
References, 29

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.

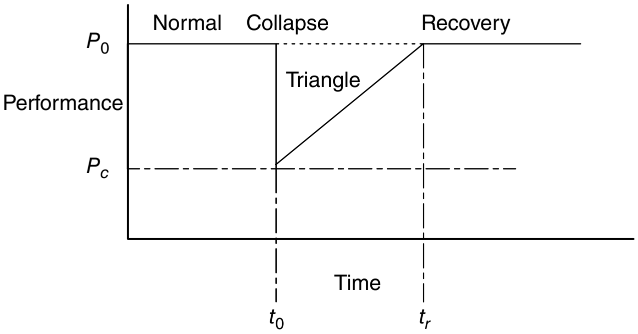


Figure 1.1 A resilience triangle is formed by a collapse followed by gradual recovery.

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.