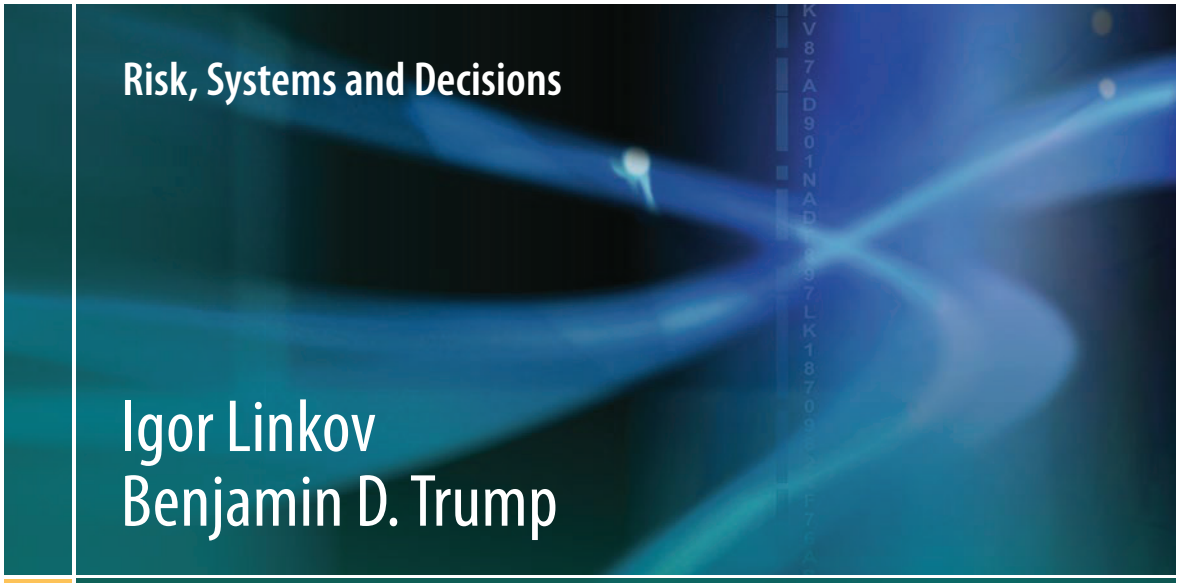

Risk, Systems and Decisions

Igor Linkov
Benjamin D. Trump

The Science and Practice of Resilience

Springer

Risk, Systems and Decisions

More information about this series at http://www.springer.com/series/13439

Igor Linkov • Benjamin D. Trump

The Science and Practice of Resilience

Springer

Igor Linkov
US Army Corps of Engineers
Concord, MA, USA

Benjamin D. Trump
US Army Corps of Engineers
Concord, MA, USA

ISSN 2626-6717 ISSN 2626-6725 (electronic)
Risk, Systems and Decisions
ISBN 978-3-030-04563-0 ISBN 978-3-030-04565-4 (eBook)
https://doi.org/10.1007/978-3-030-04565-4

Library of Congress Control Number: 2018963846

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Foreword

Our world is experiencing critical challenges that affect our everyday life. Severe weather, digital hacking, and infrastructural failure represent just a few of such challenges where a disruption can trigger significant and lasting consequences for stakeholders ranging from local communities to national and international organizations. Even more troublesome is the increasing complexity and range of consequences that these threats produce, including a "butterfly effect" where disruption to one system such as an energy grid can have widespread and disastrous consequences to many others dependent on that resource. These threats, and their impact upon the increasing complexity of our everyday systems, will continue to challenge policymakers and decision-makers to think of more creative and innovative concepts.

Thankfully, our experience and ability to develop innovative concepts will help scientists and policymakers meet the challenges of tomorrow. One of these concepts includes the philosophy and practice of *resilience*, which emphasizes the capacity of our infrastructural, digital, social, environmental, and human systems to recover from disruptions. As the 53rd Chief of Engineers of the United States Army and the Commanding General of the US Army Corps of Engineers (USACE, 2012–2016), resilience was an important philosophy and a practice we sought to apply to various initiatives within the USACE. In this drive to emphasize the concept of resilience, it was important to articulate the need to apply a "systems thinking" approach to complex environments such as watersheds, coastal infrastructure, and storm preparation and response. Such a systems-thinking approach included within an overall focus on resilience will better empower our communities to understand and address the increasingly complex challenges of tomorrow.

This book authored by Dr. Igor Linkov and Dr. Benjamin Trump includes a compendium of research on the subject of resilience, including several projects executed by the US Army Engineer Research and Development Center's Risk and Decision Science Team. Herein, the authors articulate a clear divide between the past focus on "risk management" and "resilience thinking." This "risk management" approach, while helpful in many contexts with well-established and well-researched threat scenarios, does not necessarily address the need to enable systems to *recover from* disruption. Such disruption can arise in various ways, such as low-probability and

high-consequence events as seen in extreme weather demonstrated by Superstorm Sandy on the American Eastern Seaboard or through a chain reaction of complex and cascading events such as the earthquake and subsequent tsunami that triggered the Fukushima Daiichi nuclear disaster in Ōkuma, Fukushima Prefecture, Japan.

Linkov's and Trump's work offers one of the most complete introductory texts on resilience currently available. From general theoretical background to methodological practice and governance, to case study demonstration with real-world data and analytical insight, the book demonstrates the importance of resilience and systems thinking as well as how to actually execute it. This book will be of assistance to anyone interested in learning more about what resilience is, why it is important, and how it can be assessed and implemented in a broad variety of modern infrastructural, environmental, human, and cyber systems.

With increasing uncertainty and complexity in global systems, we must be better prepared to address the role of recovery from disruption as well as the need to address the potential for cascading system failure. Resilience is one such philosophy and methodological approach by which this may be achieved and will complement existing risk assessment and management practices that have been embedded in many modern societies.

Thomas P. Bostick
53rd Chief of Engineers of the United States Army
Commanding General, U.S. Army Corps of Engineers
Washington, DC, USA

Acknowledgment and Dedication

This book could not have happened without the deep support from our many colleagues and friends. This acknowledgment does not do justice to your friendship and contributions to the field of resilience and risk.

Many individuals have inspired our approach on resilience. We would like to thank Dr. Jeffrey Keisler (University of Massachusetts, Boston), Dr. James Lambert (University of Virginia), Dr. Thomas Seager (Arizona State University), and Dr. José Palma-Oliveira (University of Lisbon), who are great friends and trusted colleagues related to resilience theory and practice. Related to network science, we would like to thank Dr. Maksim Kitsak (Northeastern University), Dr. Shlomo Havlin (Bar-Ilan University, Israel), Dr. H. Eugene Stanley (Boston University), and Dr. Alessandro Vespignani (Northeastern University). For their guidance and expertise on resilience as a property of a system, we would like to thank Dr. Craig Allen (University of Nebraska-Lincoln), Dr. Jesse Keenan (Harvard University), Dr. Scott Greer (University of Michigan), Dr. David Alderson (Naval Postgraduate School), and Dr. Stephen Flynn (Northeastern University).

Special thanks are due to past and current members of the Risk and Decision Science Team at the US Army Corps of Engineers who contributed to developing many ideas presented here. Catherine Fox-Lent was tireless in her scholarly and professional work as a civil and environmental engineer and inspired much of the work herein. Dr. Alexander Ganin provided leadership in developing simulations and case studies in network science applications to resilience. We also are very thankful for the scholarly assistance from Dr. Matthew Wood, Dr. Matthew Bates, Valerie Zemba, Dr. Avi Mersky, Margaret Kurth, Dr. Zachary Collier, Emily Wells, Dr. Daniel Eisenberg, Dr. Emanuele Massaro, and Joshua Trump. Additional thanks are due to George Siharulidze, who translated our whiteboard images into beautiful designs and figures published throughout the book.

We are thankful for the leadership of Drs. Beth Fleming and Ilker Adiguzel (Laboratory Directors, Environmental Lab, US Army Engineer Research and Development Center) who allowed us to explore this new and unknown area. We also acknowledge the unprecedented leadership of LTG (ret.) Thomas Bostick, Ph.D., 53rd Chief of Engineers of the US Army Corps of Engineers, who has done

much to advance the study of resilience in civil and environmental engineering within the USACE and nationwide. Funding support is greatly appreciated and acknowledged from several sources over the years, including Drs. Elizabeth Ferguson and Todd Bridges (USACE), Dr. Alexander Kott (Army Research Labs), Dr. Paul Tandy (Defense Threat Reduction Agency), and Dr. Colanda Cato (Army Research Institute for the Behavioral and Social Sciences).

We are grateful to many organizations who actively engaged in promoting resilience. Marie-Valentine Florin and the International Risk Governance Council at the École Polytechnique Fédérale de Lausanne have championed the study of resilience and systemic threats. The Organisation for Economic Co-operation and Development, particularly Gabriela Ramos, William Hynes, Patrick Love, and Stephane Jacobzone, is at the cutting edge of integrating societal and economic resilience in governance. We are thankful for the continued support of the North Atlantic Treaty Organization (NATO)'s Science for Peace Programme, which has funded several workshops on risk and resilience that have allowed us to incorporate an international perspective on the subject through this book. We are also deeply grateful for the time and energy that our NATO workshop participants have given over the years. We are also thankful for the continued engagement and groundbreaking research from the Joint Research Centre (European Commission), the National Institute of Standards and Technology (United States), and the Department of Homeland Security (United States).

Our deepest gratitude is due to all of you for your friendship and support.

This book is dedicated to our sons, Eugene Linkov and Owen Trump. It is our hope that resilience yields a brighter and more promising world for you to explore.

Contents

Part I Foundations of Resilience

1 Risk and Resilience: Similarities and Differences 3

2 Resilience as Function of Space and Time 9
Stages of Resilience 10
Domains of Resilience 12
Risk Versus Resilience: The Difference Between System Hardness and Recovery 15
A Brief Note on the Omnipresence of Uncertainty 17
Similarities and Differences of Traditional Risk Analysis and Resilience Analysis 20
What Does Resilience Bring to the Table of Risk Assessment? 23
Developing Technologies and Resilience 25
Applying a Systems Theory of Resilience 27
Scholarly Views on Resilience: The Opinion of Available Literature 28
Search Methodology 29
Classification Scheme 29
Resilience as Process Versus Ability 30
Results 31
Resilience as a Process Versus Ability 31
Resilience Stages 32
NCO Domains 33
Threat Properties 33
Takeaways from Scholarly Literature 33

3 Panarchy: Thinking in Systems and Networks 35
Introduction 35
Current Practices of Resilience and Potential Limitations with Existing Practice 36
The Dimension of Time and Experiential Learning 37

The Shifting Capacity of a System 38
Developing a Systems Theory of Resilience 38
Be Theoretically Neutral 38
Foster and Apply Systems Theory 39
Adopt a Context-Driven Approach to a Targeted System (Cutter et al. 2008) 39
Apply a Systems-View Rather Than a Situational-View of Risk 41
Operationalizing and Measuring Resilience 41

4 Lessons from History 45
Venice, the Bubonic Plague, and Resilience Thinking: Early Forays to Constructing Communal Resilience 46
Resilience Thinking in Modern Disease Control: Ebola in West Africa 50

Part II Resilience Assessment: State of Science and Governance

5 Resilience and Governance 59
Governance 59
Resilience as a Growing Concept in Literature and Practice 60
Calls for Resilience from Governing Authorities 61
Current Applications in US Regulatory Agencies 65
Resilience as a Driver of Governance in US Regulatory Agencies 68
Applying Resilience Matrices to Individual Organizations: The Case of the Department of the Army 70
Early Discussion of Resilience Within the OECD 73
Critical Challenges for Resilience as a Policy and Governance Philosophy 75
Future and Prospective Applications 79

6 Resilience Quantification and Assessment 81
Generic Frameworks for Resilience Quantification 81
Needed Inputs for Assessment Methods 83
Metrics and Indices 84
A Semi-Quantitative Approach: Resilience Matrix 86
A Quantitative Approach: Network Science 93
Other Possible Methodological Avenues for Assessing Resilience: Preliminary Approaches to Quasi-Quantification 98
The Need to Standardize Methodological Practice for Resilience: Making Resilience Useful for Decision-Makers 99

Part III Resilience Management: State of Practice and Case Studies

7 The State of Practice . . . 105
Public Health and Epidemiological Resilience . . . 106
Macro-Level Physical and Epidemiological Resilience . . . 106
Micro-Level Physical and Epidemiological Resilience . . . 109
Environmental Resilience . . . 110
Architectural Resilience: Theories and Practice . . . 113
Risk and Resilience Within US Building Codes . . . 114
Resilience Assessment for Emerging/Unknown Threats to Architectural Engineering and Design . . . 115
Social Resilience . . . 117
Organizational Resilience: Rulemaking . . . 120

8 Metrics-Based Approaches . . . 125
Coastal and Natural Disaster Resilience . . . 125
Coastal Resilience Case: Jamaica Bay, NY (After Fox-Lent et al. 2015) . . . 129
Appling Matrices to Case Environment: Rockaway Peninsula, New York . . . 131
Energy Delivery and Energy Grid Resilience . . . 139
Example Resilience Matrix for Energy (After Roege et al. 2014) . . . 145
Cybersecurity Resilience . . . 148
Resilience Matrix for Cybersecurity (Based on Linkov et al. 2013b) . . . 152
Psychological Resilience . . . 156
Electrical Engineering . . . 161

9 Applications of Network Science and Systems Thinking . . . 167
Transportation Resilience . . . 167
Efficiency and Resilience Metrics . . . 169
Network Science for Resilience in Epidemic Spread . . . 174
Cyber: Linux Software Network . . . 177

10 Conclusion: Resilience for a Complex World . . . 181

References . . . 185

Index . . . 203

About the Authors

Igor Linkov is the Risk and Decision Science Focus Area Lead with the US Army Engineer Research and Development Center and Adjunct Professor with Carnegie Mellon University. Dr. Linkov has managed multiple risk and resilience assessments and management projects in many application domains, including cybersecurity, transportation, supply chain, homeland security and defense, and critical infrastructure. He was part of several interagency committees and working groups tasked with developing resilience metrics and resilience management approaches, including the US Army Corps of Engineers Resilience Roadmap. Dr. Linkov has organized more than 30 national and international conferences and continuing education workshops, including NATO workshops on Cyber Resilience in Estonia (2018) and Finland (2019), as well as chaired program committee for 2015 and 2019 World Congresses on Risk in Singapore and Cape Town. He has published widely on environmental policy, environmental modeling, and risk analysis, including 20 books and over 350 peer-reviewed papers and book chapters in top journals, like *Nature*, *Nature Nanotechnology*, and *Nature Climate Change*, among others. He has served on many review and advisory panels for DOD, DHS, FDA, EPA, NSF, EU, and other US and international agencies. Dr. Linkov is Society for Risk Analysis Fellow and recipient of 2005 Chauncey Starr Award for exceptional contribution to Risk Analysis as well as 2014 Outstanding Practitioner Award. He is Elected Fellow with the American Association for the Advancement of Science (AAAS). Dr. Linkov has a B.S. and M.Sc. in Physics and Mathematics (Polytechnic Institute) and a Ph.D. in Environmental, Occupational, and Radiation Health (University of Pittsburgh). He completed his postdoctoral training in Risk Assessment at Harvard University.

Benjamin D. Trump is an ORISE Postdoctoral Fellow for the US Army Corps of Engineers and a Postdoctoral Research Fellow at the University of Lisbon, Portugal. He has also held a postdoctoral appointment at the University of Maryland and is a research intern at the Institute of Occupational Medicine in Singapore. Dr. Trump's work focuses on decision-making and governance of activities under significant

uncertainty, such as emerging and enabling technologies (synthetic biology, nanotechnology) and developing organizational, infrastructural, social, and informational resilience against systemic threats to complex interconnected systems. Dr. Trump served as a delegate to assist US presence in OECD's Global Science Forum in 2017 and is the President of the Society for Risk Analysis' Decision Analysis and Risk Specialty Group in 2018–2019. His work has been featured in over 50 peer-reviewed publications, journal articles, and book chapters, including publications in *Nature, Nature Nanotechnology, EMBO Reports, Environmental Science & Technology, Health Policy,* and *Regulation & Governance,* among others. Dr. Trump was also an author of the International Risk Governance Council's *Guidelines for the Governance of Systemic Risks*, as well as their second volume of the *Resource Guide on Resilience*. Dr. Trump is also frequently active with several Advanced Research Workshops for the North Atlantic Treaty Organization's Science for Peace Programme, including his role as a Director of a workshop titled *Cybersecurity and Resilience for the Arctic*. Dr. Trump received his Ph.D. from the University of Michigan's School of Public Health, Department of Health Management and Policy, in 2016. He received an M.S. (2012) in Public Policy and Management and a B.S. in Political Science (2011) from Carnegie Mellon University.

Part I
Foundations of Resilience

Chapter 1
Risk and Resilience: Similarities and Differences

An increasingly globalized world with wide-ranged and uncertain threats to public health, energy networks, cybersecurity, and many other interconnected facets of infrastructure and human activity, has driven governments such as within the United States, European Union, and elsewhere to further efforts to bolster national resilience and security. Resilience analysis has grown in popularity as a mechanism by which states may judge the safety, security, and flexibility of various complex systems to recover from a range of potential adverse events. Preparation for such hazards is generally thought to include measures of both passive and active resilience and have been described as including considerations of necessary actions and risk considerations before, during, and after a hazardous event takes place. Given all of this, resilience is clearly a subject with radical potential consequences in the preparedness of a nation's energy, water, transportation, healthcare, emergency response, communications, and financial sectors to prepare for and recover from external shocks of a significant magnitude.

A 2012 National Academy of Sciences (NAS) report on "disaster resilience" defines resilience as the ability of a system to perfom four functions with respect to adverse events: (1) planning and preparation, (2) absorption, (3) recovery, and (4) adaptation. Nevertheless, quantitative approaches to resilience in the context of system processes have neglected to combine those aspects of the NAS understanding that focus on management processes (i.e., planning/preparation and adaptation) with those that focus on performance under extreme loadings or shocks (i.e., absorption and recovery). Advancing the fundamental understanding and practical application of resilience requires greater attention to the development of resilience process metrics, as well as comparison of resilience approaches in multiple engineering contexts for the purpose of extracting generalizable principles.

A core problem here is that risk and resilience are two fundamentally different concepts, yet are being conflated as one and the same. The Oxford Dictionary defines risk as "a situation involving exposure to danger [threat]," while resilience is defined as "the capacity to recover quickly from difficulties." The risk frame considers all efforts to prevent or absorb threats *before* they occur, while resilience is

I. Linkov, B. D. Trump, *The Science and Practice of Resilience*, Risk, Systems and Decisions, https://doi.org/10.1007/978-3-030-04565-4_1

focusing on recovery from losses *after* a shock has occurred. However, the National Academy (2012) and many others define resilience as "the ability to anticipate, prepare for, and adapt to changing conditions and withstand, respond to, and recover rapidly from disruptions." In this definition, adapt and recover are resilience concepts, while withstand and respond to are risk concepts, thus risk component is clearly added to the definition of resilience. Further, approaches to risk and resilience quantification differ. Risk assessment quantifies the likelihood and consequences of an event to identify critical components of a system vulnerable to specific threat, and to harden them to avoid losses. In contrast, resilience-based methods adopt a "threat agnostic" viewpoint.

We understand resilience as the property of a system *and* a network, where it is imperative for systems planners to understand the complex and interconnected nature within which most individuals, organizations, and activities operate. Risk-based approaches can be helpful to understand how specific threats have an impact upon a system, yet often lack the necessary characteristic of reviewing how linkages and nested relationships with other systems leave one vulnerable to cascading failure and systemic threat. Resilience-based approaches, which inherently review how the structure and activities of systems influence one another, serves as an avenue to understand and even quantify a web of complex interconnected networks and their potential for disruption via cascading systemic threat. Such an approach is one of increasing prominence and focus on the international level, where the need to better protect complex systems from systemic threat becomes a matter not only of whether a system can survive disruption, but importantly in what state would it exist within the aftermath of such a disruption.

There are at least two important obstacles that have inhibited progress in resilience measurement for complex systems. The first of these is the success of quantitative risk assessment as the dominant paradigm for system design and management. In infrastructure and disaster management, pervasive concepts of risk have encroached upon the understanding of resilience. However, resilience has a broader purview than risk and is essential when risk is incomputable, such as when hazardous conditions are a complete surprise or when the risk analytic paradigm has been proven ineffective. Therefore, resilience measurement must be advanced with novel analytic approaches that are complementary to, but readily distinguishable from, those already identified with risk analysis.

The second of these obstacles is the fragmentation of resilience knowledge into separate disciplines, including engineering infrastructure, environmental management, and cybersecurity. This balkanized approach will inevitably fail to meet national resilience goals to manage "all hazards" by supporting only incremental changes to known risks. Such an ambitious policy objective requires a generalizable approach that is both applicable to a diverse array of systems and revealing of their interconnectivity.

Despite the promise of resilience analysis to aid the improvement the safety and security of the variety of industries mentioned, the field remains relatively new to the risk management industry. One recurring complication is the lack of standard-

ization among the field, with practitioners employing a variety of definitions, metrics, and tools to assess resilience in differing applications. Another complication includes the sheer breadth of what resilience analysis may grow to assess, both from the standpoint of methodology and case applications. These issues have motivated us to review resilience and resilience analysis across various fields which make use of its methods in an attempt to offer a snapshot of where the discipline currently stands, how it is deployed in different disciplines, and how it may be improved in a formal and unified manner.

To accomplish this goal, we break down our discussion of resilience into five parts. In Chap. 2, we present a working definition of resilience and separate resilience-based approaches from those grounded in more traditional risk assessment and management. We make use of a young yet burgeoning field of academic inquiry regarding the similarities and differences of traditional risk analysis and the developing field of resilience analysis, with the ultimate goal of identifying those areas where resilience may be viewed as an "extension" of conventional methods. Discussion of whether resilience and risk analysis are competing, conflicting, or complementary processes is not merely an exercise but of importance to the field as a result of existing paradigms of risk management alongside the social science paradigms that compete for funding and attention at the national, state, and local levels for a variety of risk applications (Kasperson 2012). For us, the approaches must be considered complementary, where the benefits and prowess of one can directly benefit the workings of the other.

In Chap. 3, a chapter coauthored with Dr. José Palma-Oliveira of the University of Lisbon delves further into the relationship between resilience, systems, and panarchy theory. Specifically, this chapter seeks to unpack a potential future direction of resilience thinking and analysis that ties resilience to a systems focus that models interaction effects between various infrastructures, social groups, informational assets, and other critical actors and considerations. As described in Gunderson and Holling (2002), the chapter frames panarchy as the interplay between these various assets and actors. Further, this chapter outlines how modeling cascading effects within this interplay or network is an essential exercise of panarchy-focused resilience thinking, with the ultimate goal of identifying potentially brittle or problematic nodes whose failure could trigger widespread harm to other directly or indirectly connected groups, assets, infrastructures, or other systems and sub-systems in question.

In Chap. 4, we highlight how principles of resilience have been considered and implemented for centuries. Specifically, we discuss how medieval Venice adopted a mixture of risk-based and resilience-based approaches to combat the Black Death in the mid-fourteenth century. Though such measures did not contain the disease to Venice's ports, it did provide a critical departure for Western public health authorities to quarantine and assess the potential for contagion to spread due to international transport of goods and peoples. Lessons from Venice are extended to modern West Africa, which were forced to combat the spread of one of the most destructive breakouts of the Ebola Virus in human history from 2013 to 2016.

In Chap. 5, we discuss the current state of resilience in different US government agencies, as well as internationally, in order to provide discussion of what the field needs in order to mature. Resilience analysis has been discussed as a complement to traditional risk assessment by several federal agencies that seek to apply resilience analysis methodologies to a variety of applications in severe or catastrophic risk. However, such methods have been proposed or deployed in differing contexts with various definitions, which clouds the overall understanding of the concept and its potential to improve conventional risk governance paradigms. Also in this section, we will review the recent history of the calls for resilience analysis by the Obama Administration in its efforts to promote greater resilience to American infrastructure. Where Part I notes similarities and differences between resilience analysis and conventional risk analysis, this section will further delve into the current practices and applications of resilience in order to both discuss how the choice of method can complement or amplify traditional risk assessment methods as well as how a lack of clarity and uniformity in its current status may result in shortcomings or inefficiencies as it grows in the near future. Such an assessment will ultimately help discuss the method's existing issues and shortcomings, which serve as impediments to its maturation and useful deployment in future risk management frameworks.

In Chap. 6, we describe budding methods at resilience quantification, and compare and contrast their prospective advantages and weaknesses. Though resilience analysis has yet to fully mature and develop as a widely utilized methodology, some specific applications have been constructed to demonstrate its future usefulness. These applications are generally case specific, yet reinforce the notion that while resilience thinking may improve conventional methods of risk analysis, the methods of both should be considered complementary. In other words, we intend to show how resilience analysis and traditional risk analysis can be mutually symbiotic when addressing highly uncertain and consequential risk to human and environmental health or financial, industrial, military, and medical assets. Though these early resilience-minded risk management tools are still being developed, their current applications and proposed future use can illuminate where the field may be going, and how it may benefit stakeholders as it matures.

In Chaps. 7–9, we review a variety of resilience analysis cases in fields ranging from energy and cybersecurity to coastal, medical, and psychological resilience. These case studies offer a view of both the wide-ranging appeal of resilience to complement and improve upon existing risk-based approaches, yet also how the method may be transformed and tweaked to fit the needs of some applications that may not be relevant to others. In all cases, high uncertainty is directly connected with the potential for widespread and lasting damage to the given system, which could contribute to highly negative social, economic, and political outcomes on a national level. While many other applications exist for resilience analysis to address risk, these applications represent those fields with the greatest academic attention for the early use of resilience analysis as a method by which to judge risk to an expansive system plagued with high uncertainty and the potential for hazard. These cases represent real-world scenarios, and demonstrate how the methods described in Chap. 6 might be formally used to guide and assess system resilience in a broad diversity of application areas.

Overall, such discussion will help begin the standardization process that resilience needs in order to improve as a broader assessment framework and will help incorporate such methods into the risk manager's toolbox. It is our hope that readers will gain an understanding of how traditional risk and novel resilience are symbiotic rather than methodologically at odds with one another, where the user could choose one or the other based upon the needs of a given situation. With this in mind, we contend that resilience analysis symbolizes the future of high stakes systems-level risk management for a variety of disciplines and industries across the world, where resilience thinking is required for stakeholders to circumvent and actively prepare for global existential events with the capability of drastically impacting the existing environment. While no approach or framework is perfect in the grip of uncertainty, resilience analysis allows its users to position themselves to recover from what otherwise would be a crippling blow to existing capabilities.

Chapter 2
Resilience as Function of Space and Time

As a term, resilience has centuries of use as a descriptor in fields as diverse as military operations, to psychology, to civil and environmental engineering. Its synonyms are vast and varied, ranging from insinuations of toughness to elasticity. While it pulls its roots from these early ideas, the modern application of resilience has centered upon analyzing how systems bounce back from disruption. This seems simple enough at first glance, yet as this book will discuss, the methodological application and analysis of how systems bounce back post-disruption can be quite challenging.

Resilience is a philosophy as much as a methodological practice that emphasizes the role of *recovery* post-disruption as much as *absorption* of a threat and its consequences. Philosophically, this mindset is one that is grounded upon ensuring system survival, as well as a general acceptance that it is virtually impossible to prevent or mitigate all categories of risk simultaneously, and before they occur. Methodologically, resilience practitioners seek to optimize limited financial and labor resources to prepare their system against a wide variety of threats—all the while acknowledging that, at some point in the future and regardless of how well the system plans for such threats, disruption will happen. While the more conventional practice of risk assessment and management is very concerned with accounting for systemic threats, this exercise is typically undertaken on a threat-by-threat basis in order to derive a precise quantitative understanding of how a given threat exploits a system's vulnerabilities and generates harmful consequences. As will be discussed later in this chapter, such an exercise works well when the universe of relevant threats is thoroughly categorized and understood, yet develops limitations when reviewing systemic risk to complex interconnected systems. Building from this limitation, resilience complements traditional risk-based approaches by reviewing how systems perform and function in a variety of scenarios, agnostic of any specific threat.

The key question that resilience practitioners seek to answer is "how can I make sure my system performs as optimally as possible during disruption, and recovers quickly when disruption does occur" (Fig. 2.1)? This question is particularly salient for the study of complex systems, where large organizations like hospitals rely upon

I. Linkov, B. D. Trump, *The Science and Practice of Resilience*, Risk, Systems and Decisions, https://doi.org/10.1007/978-3-030-04565-4_2

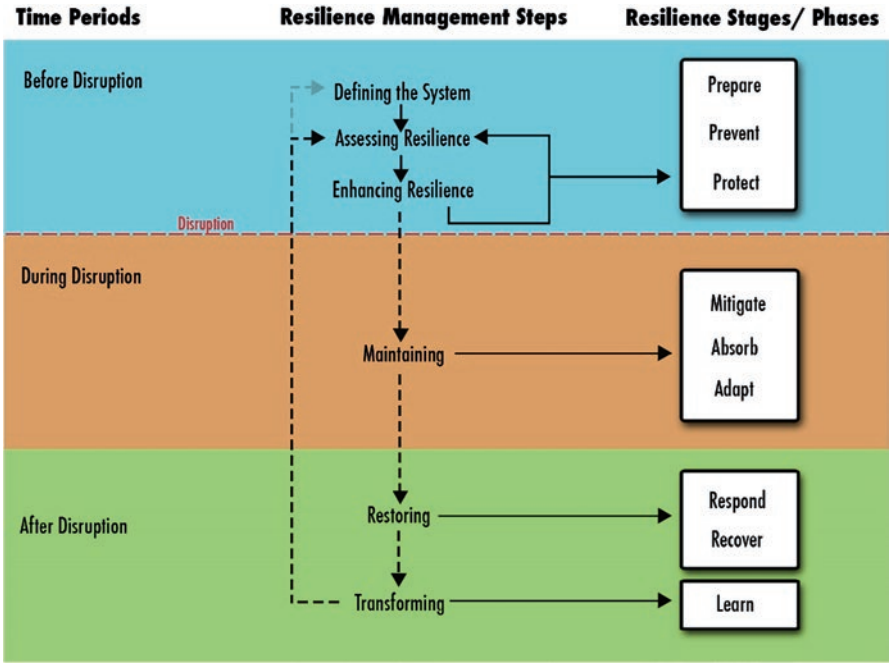

Fig. 2.1 Role of resilience in systems, emphasizing importance of combating disruptions

the smooth operation of various connected systems and sub-systems to function properly (i.e., the energy grid, secure and efficient information systems, simplified patient intake, medical supply chains, and various others). Resilience is also an important question to tackle threats of very low probability yet disastrous consequences, where no clear strategy exists to mitigate or prevent such threats from happening in the first place. Regardless of the situation to which it is applied, resilience requires one to think in terms of how to manage systemic, cascading threats, where a disruption to one sub-system can trigger dramatic changes to other connected systems. This is a complex task with few formalized answers, yet a helpful beginning is to operationalize resilience in a meaningful and methodological focus.

A central theme of this book is the need to understand resilience as a function of both *time* and *space.* We emphasize these considerations due to the multi-temporal and cross-disciplinary view by which one must review systemic threats.

Stages of Resilience

With respect to time, resilience of a system is less of a singular moment when a disruption incurs losses, but is instead a process of how a system operates before, during, and after the threat arrives. No single definition has been formalized in this

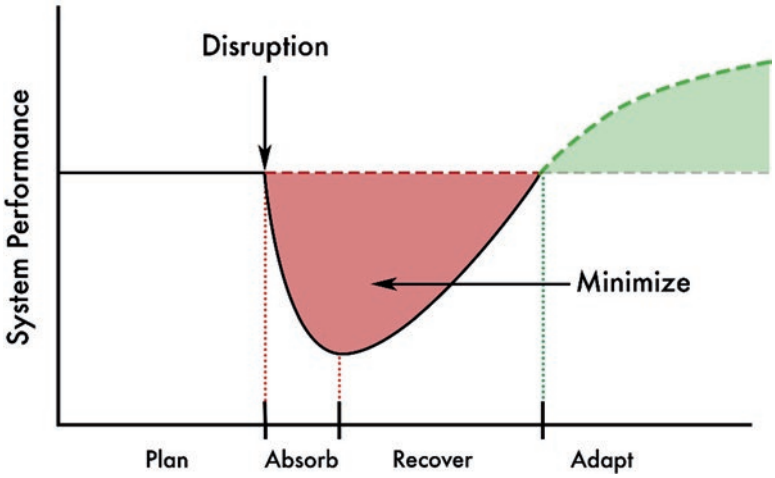

Fig. 2.2 Stages of resilience as proposed by NAS

area, yet the National Academy of Sciences' 2012 report on Disaster Resilience describes resilience as how a system plans and prepares for, withstands and absorbs, recovers from, and adapts to various disruptions and threats (Fig. 2.2) (NAS 2012). In this approach, system resilience is an ever-changing activity whereby a system's core functions are constantly shifting to deal with threats.

Most conventional, risk-based approaches emphasize the plan/prepare and withstand/absorb phases to identify, assess, and prevent/mitigate threat (Linkov et al. 2018a, b, c). Regardless of whether a specific threat is considered, these stages focus upon (a) identifying and interpreting signals associated with threats to a system, (b) exploring the structure and connections that a system has with others, and (c) identifying strategies that preserve a system's core capacity to function regardless of the disruption that occurs (Patriarca et al. 2018; Park et al. 2013). Signals include statistics and other information that might indicate a pending systemic threat, i.e., early reports of new and virulent disease as an indicator of a pending epidemic and public health crisis (Scheffer et al. 2012). Signal detection is a difficult and recurring task, but can be the only avenue to better understand the variety of systemic threats that may arise at different points in the future. Likewise, mapping of the various connections and dependencies within one's system can help identify critical functions that, if taken offline, could generate cascading systemic failure.

If possible, system preparation and absorption of threat is accomplished via a prevention-based approach where a threat is avoided altogether. However, when this is not possible, emphasis is placed upon the capacity of a normatively beneficial system to avoid total collapse. This can be accomplished by "graceful degradation," where the core operations of a system are prioritized over non-essential services for as long as possible. By limiting the extent and scope of disruption to a system, it becomes easier to keep system functions online. Often, this is accomplished by "hardening" different functions of a system so that they will not break under pressure.

While the plan/prepare and absorb/withstand stages are important to help a system address systemic threats before they occur and as they arise, resilience approaches also must place importance upon how a system performs after the threat has arrived. This includes (1) recovery and (2) adaptation. Recovery includes all efforts to regain lost system function as quickly, cheaply, and efficiently as possible, while adaptation centers upon the capacity of a system to change and better deal with future threats of a similar nature. Recovery and adaptation serve as the particularly novel additions by resilience to the broader fields of risk analysis, assessment, and management, and force stakeholders to account for percolation effects due to disruptions. The role of adaptation and recovery is discussed throughout this book as a primary point of focus for any resilience analyst, where a system with a robust capacity for recovery can efficiently weather serious disruptions that would otherwise break even the most hardened of system components.

Domains of Resilience

Outside of the NAS' stages of resilience, the spatial component of resilience requires one to consider how a disruption to one system can trigger consequences in others—including those that have indirect or inapparent linkages to the disrupted system.

Alberts and Hayes (2003) identify four different Network-Centric Operation (NCO) domains important to a system's agility, or what Alberts later defines as "the ability to successfully effect, cope with, and/or exploit changes in circumstances" (Alberts and Hayes 2006). While early in scope, this effort at resilience thinking is intended to force its users to consider the wide breadth of characteristics and decision inputs that may factor into system performance. Each domain is impacted in a different yet equally important manner when a critical or disruptive event arises, and success in one domain may not guarantee the same outcome in other areas. Additionally, it is important to note that the greatest resilience and the ability to recover from adverse events is achievable only when all domains are considered and resolved in a resilience analysis policy problem. These domains include (Hayes 2004; Alberts 2007):

1. Physical: sensors, facilities, equipment, system states, and capabilities
2. Information: creation, manipulation, and storage of data
3. Cognitive: understanding, mental models, preconceptions, biases, and values
4. Social: interaction, collaboration and self-synchronization between individuals and entities

These domains are important to decision-making for complex systems in general and resilience in particular (Roege et al. 2014; Collier and Linkov 2014). The physical domain represents where the event and responses occur across the environment and is typically the most obviously compromised system in the midst and aftermath of an external shock or critical risk event. Elements here can include infrastructural

characteristics ranging from transportation (roads, highways, railways, airports, etc.) to energy or cyber networks that deliver services to public and private entities alike (DiMase et al. 2015). As such, the physical domain of resilience thinking generally includes those infrastructural factors that are most directly impacted by a hazardous event, where the other domains include outcomes and actions that are a response to damage to physical capabilities and assets. Threats to such infrastructure can range from environmental (i.e., a catastrophic storm) to anthropological (i.e., terrorist violence or military attack). In this domain, the objective of resilience analysis is to bring the infrastructural or systems asset back to full efficiency and functionality for use by its original owner or user.

The information domain is where knowledge and data exists, changes, and is shared. Such elements here can include public or private databases, which are increasingly under potential attack from private hackers and other aggressive opponents (Osawa 2011; Zhao and Zhao 2010). Another growing target for information domain-type risks includes stored online communications and e-mails, which if acquired by a nefarious third party could generate individual embarrassment or even national security risks (Murray and Michael 2014; Berghel 2015; Petrie and Roth 2015). Where such attacks are a growing reality in the Information Age (Kaur et al. 2015), adequately protecting against such risks and bolstering information systems to be resilient and robust under attack is of paramount importance to government agencies and private companies alike (Lino 2014). For this domain, the objectives of resilience management are to prepare information assets for a variety of potential attacks while also assuring that such systems will react quickly and securely to such threats in the immediate aftermath. In this way, risk preparedness, risk absorption, and risk adaptation make information and cybersecurity resilience a growing priority for a variety of governmental and business stakeholders (Linkov et al. 2013a; Collier et al. 2014; Björck et al. 2015).

The cognitive domain includes perceptions, beliefs, values, and levels of awareness, which inform decision-making (Linkov et al. 2013a; Eisenberg et al. 2014). Along with the social domain, the cognitive domain is the "locus of meaning, where people make sense of the data accessed from the information domain" (Linkov et al. 2013a). Such factors are easy to overlook or dismiss due to a reliance upon physical infrastructure and communication systems to organize the public in response to a disaster, yet such perceptions, values, and level of awareness of publics to strategies to overcome shocks and stresses are essential to the successful implementation of resilience operations (Wood et al. 2012). In other words, without clear, transparent, and sensible policy recommendations that acknowledge established beliefs, values, and perceptions, even the best-laid plans of resilience will fall to disrepair. A robust accounting for the cognitive domain is particularly important for instances where policymakers and risk managers may have a disconnect with the local population, such as with international infrastructure development projects of health-based interventions. For such cases, sensible and common sense policy solutions to the policymaker or risk manager may be assumed to be robust, yet rejected by locals as contrary to established custom or practice.

The social domain represents interactions between and within entities involved. The social domain also provides an area to which careful attention should be paid in overall community resilience. Social aspects of society have impacts on physical health (Ebi and Semenza 2008). For example, individuals or communities can have better recovery in the face of epidemic when they also have strong social support and social cohesion. The social domain also ties into the information domain in regard to trust in information. When the community does not trust the source of information, they often do not trust the information or have to take the time to verify it, leading to a need for community engagement by the authority or organization to increase their social relations and therefore trust within the community (Longstaff 2005).

While the physical and cognitive domains gain a lot of attention in both overall resilience and hazard-specific resilience, the information domain is of great importance for overall functioning. In more than just health events, information has a huge impact on citizen response (Crouse Quinn 2008). Not all individuals understand and interpret information the same way. This leads to a need for attention to be paid on how to get information out effectively and in a timely fashion during a crisis. Information is important to more than just the citizens, however. Adequate information is crucial in real time for authorities to make informed and appropriate decisions (Hsu and Sandford 2010). As important as information is, however, it is equally important to account for the role of human decision-making. Specifically, human interpretation of data is important as raw numbers can be misleading if not considered in context of a given environmental setting or policy application. This ties back into needing to disperse tailored information for understanding that places data pertinent to a threat in a manner that is not convoluted for its recipient. How authorities and citizens handle information should be evaluated with careful consideration for the communities being discussed.

Social resilience within this context may apply to societies and communities of various size, ranging from local neighborhoods and towns to more regional or national governments. For smaller communities, organizations, and businesses, discussions of resilience may center on the ability of local governments and set communities to address long-term concerns such as with the impact of climate change (Berkes and Jolly 2002; Karvetski et al. 2011), ecological disasters (Adger et al. 2005; Cross 2001), earthquakes (Bruneau et al. 2003), and cybersecurity concerns (Williams and Manheke 2010), as well as other man-made hazards such as transnational wars, civil wars, terrorism, migration, and industrial hazards. For larger communities and governments, such concerns are similar yet often more complex and varied in nature, where they involve hundreds to potentially thousands of stakeholders and include the interaction of various infrastructural systems.

These domains often overlap and exist in all systems, such as for messages from the information domain to be shared, infrastructure in the physical domain or interactions in the social domain must support dissemination. At its core, a focus upon domains ensures that a policymaker or risk manager acquires a holistic understanding of their policy realm, and is able to understand how a shock or stress could trigger cascading consequences that were previously difficult to comprehend. For example, the collapse of Lehman Brothers triggered a worldwide economic recession in 2008 due to the inherent interconnectivity of various economic and financial systems at that time.

Risk Versus Resilience: The Difference Between System Hardness and Recovery

Resilience as a formal method and disciplinary practices lacks the rich and extensive history as complementary practices of risk analysis. Despite the lack of any formal definition or methodological practice, the role of resilience in economic, infrastructural, environmental, and social policy is a topic of growing interest and equally rising uncertainty. Though it is ultimately the responsibility for high-level policymakers and other key stakeholders to define and scope the practice of resilience, this book offers one view that frames resilience as a differing yet complementary process to conventional risk assessment and management.

Risk analysis has decades of history as a collection of tools dedicated to espousing and managing risk—generally through some synthesis of the threat in question, the vulnerability of a system to that threat, and the consequences should the threat arise. In this way, risk-based assessment and management approaches emphasize the capacity of a system to *absorb* and *withstand* specific threats. Such an approach is battle tested in various application areas and performs admirably in situations of high clarity and robust opportunities to acquire data related to situational risk.

For government projects and interests, risk analysis, including risk assessment and management, involves the systematic review of various infrastructural, environmental, and organizational factors to identify potential areas where risk could arise (National Research Council 1983; Linkov et al. 2005). This exercise has multiple purposes, including (1) to identify and understand those areas where a certain hazard is most likely to arise, (2) to gauge some value of the likelihood of this negative event from occurring, (3) to understand the consequences if this risk would actually occur, and (4) to provide some alternative policies or actions that could mitigate or prevent such a scenario. Different tools provide a qualitative and/or quantitative algorithm that addresses these needs, ranging from an unstructured ad hoc qualitative panel discussion to a fully quantitative and reductive decision model to assess expected losses in the form of financial, infrastructural, or human casualties.

In such an environment, the outcome of a risk is both uncertain and meaningful to the relevant stakeholder. Risk presents the potential for both direct (i.e., human health hazard) and indirect loss (reduction in reputation), and retains an element of unpredictability that makes many risks difficult to fully prepare for over any time frame or even to predict the full vector of risks that may arise. An additional concern is the availability of resources to protect against risks, where policymakers are required to conduct resource maximization exercises to best prepare various assets for a universe of future risk events with limited annual budgets. Ultimately, this means that the potential for some future hazard must be tolerated due to a lack of resources or general inability to resolve the weakness that permits a negative outcome. By and large, risk assessment exercises require the prevention and mitigation of the most consequential and likely risk firsts, where more minor externalities and very low-probability, high consequence events are, respectively, given less emphasis for risk preparation and mitigation. Of course, this exercise is at the discretion of

the stakeholder, where stakeholders and key decision-makers will have to decide how to optimize limited funds and available manpower to achieve the greatest risk preparation possible.

Along with considerations of outcomes, uncertainty, and overall risk tolerance, stakeholders and policymakers are required to consider the passage of time. While predicting what will happen tomorrow is already an inaccurate science, accounting for risk over the course of years or decades can quickly become an impractical task without some mechanism for decision support. Such an exercise includes the assessment of an assortment of political, social, and industrial preferences. Shifting societal preferences alongside the degradation of infrastructure 5, 10, 20, or more years into the future only increases the uncertainty of the hazards posed by external shocks to environmental, industrial, commercial, and cyber systems. Conventional risk assessment attempts to account for these issues by advising for protection against the most egregious and harmful hazards over the extended term. However, the recommendations given are generally the reflection of an intransigent system with fixed preferences, and may not provide a clear or optimal path to recover from serious adverse events that may dramatically alter or damage a given system.

Ultimately, most applications of risk analysis focus upon system preservation based upon its capacity to prevent or mitigate risk by withstanding and absorbing a specific threat or a collection of threats. This conclusion is generally a logical one—we tend to want to prioritize our resources to address the problems that we know we have—particularly those in the near future. While such an approach addresses many of the challenges facing most individuals and organizations today, risk-based approaches that emphasize withstanding or absorbing specific threats to specific systems are less effective at addressing problems of high complexity or high uncertainty. Simply put—a differing approach is likely needed to address subjects with greater uncertainty, be they "known unknowns" or even "unknown unknowns."

Resilience analysis fundamentally maintains much of the same philosophical background as traditional risk assessment, but resilience analysis additionally delves into the unknown. Resilience thinking requires its practitioners to ponder potential future threats to system stability and develop countermeasures or safeguards to prevent longstanding losses, not just direct losses from historical threats. Resilience analysis maintains one primary difference in its focus on outcomes, where practitioners are directly concerned for the ability of the impacted organization, infrastructure, or environment to rebound from its external shock. In other words, where traditional risk assessment methods seek to mitigate and manage hazards based upon a snapshot in time, resilience analysis instead seeks support system flexibility and ultimately offers a "soft landing" for the organization or structure at hand (Fig. 2.3). Simply put, resilience analysis is the systematic process to ensure that a significant external shock—e.g., climate change to the environment, hackers to cybersecurity, or a virulent disease to population health—does not exhibit lasting damage to the efficiency and functionality of a given system. This elegant philosophical difference is complex yet necessary to meet the growing challenges and uncertainties of an increasingly global and interconnected world.

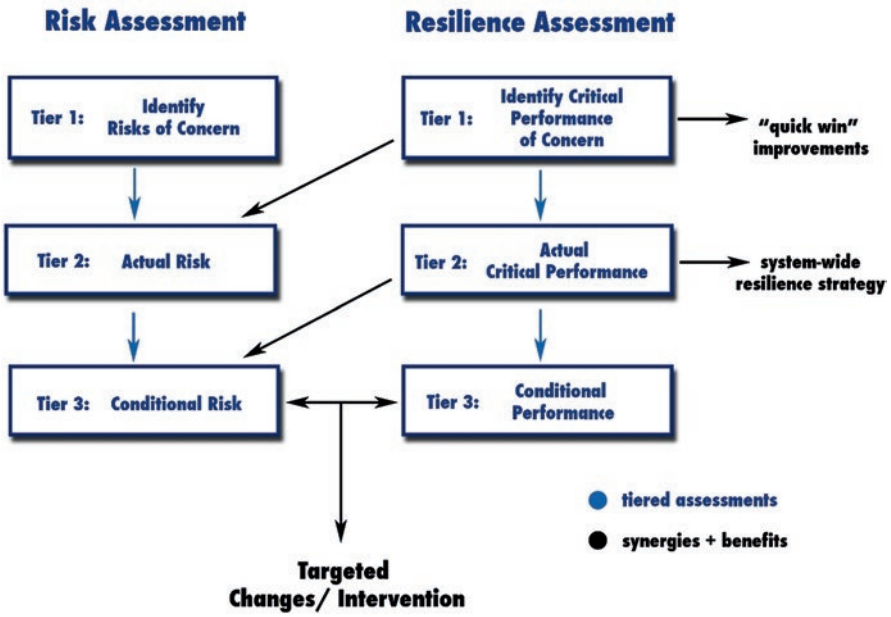

Fig. 2.3 Differentiating risk-based and resilience-based methodologies and philosophies

This section will include both an introductory review of resilience analysis and how it compares and contrasts with existing risk analysis and management tools. In discussing the calls for resilience analysis, we will consider the activities and needs of individual US government agencies. Next, we will discuss those shortcomings in conventional risk analysis methods that could be filled by resilience analysis, along with any existing impediments or resistance to adopting this growing methodology. As such, this chapter will provide the groundwork to understand the benefits of resilience analysis in the risk management toolbox alongside those stakeholders who have already called for its development and use.

A Brief Note on the Omnipresence of Uncertainty

This chapter has already touched on a key ingredient of any risk calculation—uncertainty. Regardless of how familiar a situation or condition seems, from driving a car on a familiar road to purchasing food at a local grocery store, a certain degree of uncertainty exists regarding the potential for success or injury for a given activity. It plagues individual and systemic activities alike, injecting the possibility of negative outcomes (however slight) that may arise in the midst of certain actions or behaviors. In a general sense, uncertainty is omnipresent in all elements of daily life, with individuals and systems making either deliberate or subconscious

cost-benefit calculations to decide on future actions. In most daily decisions and circumstances, a reliance upon past experience and historical information is adequate for an ad hoc decision-making exercise, and formal decision tools and support systems are not needed.

However, uncertainty within systems-level activities is particularly worrisome for both traditional risk managers and now resilience analysts due to the ability of unanticipated negative outcomes with widespread effects to cause extensive, costly, and lasting damage. In such circumstances with "high uncertainty"—or the potential for costly and systems-wide risk—ad hoc decision-making and past experience is neither a sufficient means of risk judgment nor generally an acceptable business practice for virtually any industry. Instead, relevant managers make use of formalized algorithms, decision aids, and decision support systems to address all critical elements of an activity at hand. One example is supply chain management, where a risk assessor would seek to list all of the potential problems that could arise within each life cycle stage of production and address the likelihood of these threats arising, without limiting him or herself to only events that have happened in the past. For less uncertain and lower risk activities, these decision support activities may be relatively simple to perform, such as mapping or thought exercises by a few directly involved decision-makers.

For more complex risks, high uncertainty may be mitigated by the deployment of redundancies to reduce potential harms as well as data-gathering efforts to gain more information regarding the risk's likelihood of occurrence and magnitude if realized. In such an environment of high uncertainty, the decision aids are likely to be more rigorous, such as with the use of formalized decision software or extensive information-gathering activities to unveil a more accurate cost-benefit trade-off for a given scenario. However, Kasperson and Berberian (2011) note that such activities may not always yield more beneficial or certain outcomes; instead the risk assessor may encounter still further risks that had not yet been considered (Kasperson and Berberian 2011). Per Kasperson, situations of extensive and deep uncertainty may be initially addressed by several strategies, including:

1. *Delay.* Where possible, delaying potential action to gain additional information regarding a particular action can reduce the spectrum of potential plausible outcomes. An active approach here would be to make use of a Value of Information method (Keisler et al. 2014). Decision-makers may assess the possible costs of delaying to acquire improved information for a particular situation. Where costs of risk-based interventions are outweighed by the benefits, delaying action is an optimal course to follow (see, for example, similar declarations for synthetic biology governance described in the President's Commission on the Study for Bioethical Issues in 2010 which described the need for synthetic biology to mature before establishing new governance priorities or regulatory requirements upon the field's development; PCSBI 2010).
2. *Prioritize.* While a system may be faced with a slew of complex uncertainties in a given decision problem, not all uncertainties are likely to generate similar levels of risk or hazard. In other words, actively "ranking" perceived uncertainties

based upon their understood importance to the eventual consequence can serve as an iterative method to deploy limited resources in order to meet the most egregious and harmful risks currently known. This process has been standardized by a variety of US government agencies such as the US National Research Council, which provides guidelines for risk analysts to follow when prioritizing risks according to perceived hazards to stakeholders.

3. *Broaden Knowledge Base.* It is highly likely that others have encountered a risk profile similar to the one a given risk analyst faces. Thinking outside the box, or upon the risk and policy situations that risk practitioners in other fields and industrial sectors have been forced to address, can serve as a method to acquire additional information on the likelihood of certain outcomes. Such an activity can help decision-makers by pointing out those choices or options that are fully dominated by others, effectively reducing the number of possible paths forward.
4. *Precautionary Principle.* The precautionary principle is discussed with the introduction of a new product or process whose ultimate effects are disputed or unknown (Sandin 1999; Kriebel et al. 2001). As a risk management philosophy, this is as highly conservative mentality falls within *preventative anticipation* and *safeguarding of environmental space*. Within such an arrangement, regulators and risk managers are required to prepare for and protect against risks from uncertain or unknown technological developments until more evidence is available to facilitate their risk assessment (O'Riordan 1994; Origgi 2014). This option requires risk assessors to identify hazards of catastrophic or permanent damage (Whiteside 2006). For such scenarios, the deployment of cost-effective activities and options to prevent or reduce such harms should not be delayed due to limitations in available scientific knowledge. Instead, a traditional risk assessor advocates for active steps in order to mitigate and manage these potentially catastrophic risks, despite the uncertainties. Resilience analysis may insert an additional dimension to address such catastrophic yet uncertain risks, with particular focus on the ability of the targeted system or activity to rebound fully and quickly if such a hazard should arise.
5. *Adaptive Management.* In situations where various and deep uncertainties cannot be mitigated or managed in a systematic way, an adaptive management process advocates for a "trial and error" approach that evolves over time based upon lessons learned and information gained (Pahl-Wostl 2007; Linkov et al. 2006). While not available or ethical for all applications in all industries, this option allows a risk analyst to acknowledge the difficulty in finding the perfect policy option for a risk portfolio without some experimentation and trials.

While other options exist for risk analysts to address system complexity and associated uncertainties, these represent the traditional cache of options that analysts of various industries may deploy. For conventional risk analysis, these efforts represent the gold standard of how to proceed in the face of high uncertainty and potentially heightened risk, with different tools and decision support systems to help guide stakeholders and practitioners as they follow one or more of these policy options. Rather than fully advocate for a new set of procedural options, resilience

analysts can make use of this existing framework, yet adapt it to a different understanding of risk outcomes where priority is placed upon the ability of a system or activity to quickly rally from an adverse event to full functionality. Ultimately, uncertainty about the potential and magnitude for risk is what drives risk and resilience analysis and makes this work beneficial and necessary for a variety of disciplines and potentially high risk activities.

Similarities and Differences of Traditional Risk Analysis and Resilience Analysis

In reviewing the similarities and differences of the two philosophical approaches, it is necessary to consider the philosophical, analytical, and temporal factors involved in each method's deployment (Aven 2011). Philosophical factors include the general attitude and outlook that a risk or resilience analyst holds while exploring and understanding risks. Analytical factors include those quantitative models and qualitative practices deployed to formally assess risk. Temporal factors include the time frame over which risk is traditionally considered. Overall, consideration of these and other factors will demonstrate that while resilience analysis does differ somewhat from traditional risk assessment and management, resilience thinking is highly compatible with existing methods and is synergistic with traditional risk analysis approaches.

Philosophically, risk and resilience analysis are grounded in a similar mindset of reviewing systems for weaknesses and identifying policies or actions that could best mitigate or resolve such weaknesses. Risk is the operative term for both steps—the analysis and the management planning, and the overall goal is to lessen as much as possible the damages that could accrue from a hazardous external shock or other undesirable event. As such, a practitioner's focus is on identifying and categorizing those events that could generate hazardous outcomes to humans, the environment, or society in general (i.e., commerce, infrastructure, health services), and then identifying countermeasures to meet such hazards.

However, risk and resilience contrast philosophically on two key measures—how to understand and assess uncertainty and how to judge outcomes of hazardous events (Scholz et al. 2012; Fekete et al. 2014; Aven and Krohn 2014). For the former, a traditional risk analyst approach would seek to identify the range of possible scenarios in either an ad hoc or formalized manner, and to develop protections against them based upon the event's likelihood, consequences, and availability of funding to cover an array of issues for a given piece of infrastructure or construct. In this way, conventional risk assessors generally construct a "rigid" framework of protections, fail-safe mechanisms, and/or response measures to protect against and respond to adverse events. Such a framework has its benefits, but as we discuss in the next section, such a rigid and inflexible risk philosophy can hinder event response efforts to rebound from severe or catastrophic events that were outside of the prevention and protection plan.

Resilience fundamentally provides the groundwork for a "soft landing" and expeditious recovery, or the ability to reduce harms while helping the targeted system rebound to full functionality as quickly and efficiently as possible. This is consistent with The National Academy of Sciences (NAS) definition of resilience as noted above, which denotes the field as "the ability to plan and prepare for, absorb, recover from, and adapt to adverse events" (NAS 2012). While this difference may appear subtle, it carries a significantly different operating statement than risk, such that resilience analysts focus more on "flexibility" and "adaption" within their targeted systems. This differs from the conventional "one-size-fits-all" approach commonly deployed by traditional risk analysis and assessment, which instead seeks to identify a system that is fail-safe in nature yet inherently rigid. Such approaches can take many forms, including establishing a system less prone to disruption or structuring a system that can expeditiously recover from disruption with minimal loss of time (Fig. 2.4).

However, the intrinsic uncertainty within the world and the various actors and forces that work in it make it significantly unlikely that such an inflexible system would prevent all risk in the long run, or would adequately protect against severe

Fig. 2.4 Various permutations of system response to disruption. Top-left includes no system resilience with maximal loss from disruption. Top-right includes expeditious recovery from disruption with minimal time loss. Bottom-left includes minimal loss of disruption, yet extended time required for recovery. Bottom-right represents a system with maximal resilience, including minimal loss of system function via disruption and minimal time required to recover any lost functionality

events that could cause lasting and sweeping damage to society and the environment. This is particularly true for low-probability events (Park et al. 2013; Merz et al. 2009), which have a significant chance of being written off in a traditional risk assessment report as being excessively unlikely enough to not warrant the proper resources to hedge against. This is an accepted practice and the result is termed "residual risk."

The comparisons between traditional risk analysis and resilience analysis are less understood and developed due to the relatively brief time that resilience assessment has been employed, yet it is possible to derive some understanding based upon the philosophical frameworks that each applies to the understanding risk. Both approaches permit the use of both quantitative data and qualitative assessment, which allows for greater overall flexibility in applications ranging from the more well-known to the highly uncertain and futuristic. Such information is generally integrated into an index or algorithm in order to translate the findings into a meaningful result for the risk analyst, who is then able to offer either an improved understanding of the real hazards that certain risks pose against targeted infrastructure and/or an improved review of which alternative actions or policy options may be taken to mitigate the harms presented by such risks.

Quantitative data may be derived from engineering tests in the field or computer-based modeling results, where policymakers and stakeholders are able to view and assess the likelihood and consequence of certain risks against identified anthropologic or natural infrastructure. Likewise, qualitative assessment is generally derived from meetings with subject experts, community leaders, or the lay public, and can be recorded a variety of applications for more streamlined assessment such as with content analysis. In most cases, it is optimal to include both sources of information due to the ability of quantitative field data to indicate more accurate consequences and likelihoods of hazard alongside qualitative assessment's ability yield greater context and breadth to possible risks. However, it is often not possible for both sets of information to be generated either due to a lack of reliability within qualitative sources of assessment or a dearth or quantitative data (due to concerns of ethical experimentation, the extreme rarity of a situation to be studied, and/or cost and time), leaving policymakers and stakeholders to make the best of what is available to them. This is universally true for both traditional risk analysis and its fledgling partner in resilience analysis and is likely to be the case for any resilience assessment methodology to be developed in the future.

However, frameworks of risk and resilience have also begun to indicate some early differences in quantification and assessment. While we will discuss this later in Chaps. 5 and 6, it is worth noting now that resilience quantification is less mature than its peer in traditional risk assessment. Nonetheless, several quantitative, semi-quantitative, and qualitative approaches have been proposed and deployed to measure systemic resilience at local, national, and international levels for a variety of cases, all of which seek to improve systemic or infrastructural response to a catastrophic event (generally low-probability, high consequence "disasters"). Such approaches could be relatively simplistic such as with a qualitative classification system to somewhat more complex as with resilience matrices or highly complex

network analysis, where the availability of information and user needs will determine the level of sophistication chosen. Despite these differences, however, resilience thinking and analysis will be similarly dogged by the potential for "garbage-in, garbage-out" analysis, and so resilience practitioners must be vigilant and robust in their use of relevant and valid quantitative data or qualitative information for whichever risk classification they employ (Hulett et al. 2000).

Temporally, traditional risk and resilience analysis are required to consider the immediate term risks and hazards that have the potential to arise and wreak havoc upon an infrastructural system (Hughes et al. 2005). Both engage in exercises that identify and chart out those potential dangers that threaten to damage the infrastructure in question. This exercise can range from being unstructured and ad hoc to organized and iterative, yet ultimately any analyst must develop a series of threats or hazards that can have some measurable impact upon natural or man-made structures. These hazards are then reviewed based on their likelihood of occurrence and consequences on arrival, which is another iterative process. Lastly, risk analysts are required to assess the immediate aftermath of the various adverse events that were initially identified, and gain a greater understanding into how different components of infrastructure may be damaged and what the consequences of this may be.

While not necessarily universally true, resilience analysis begins to differ in use of timescales from its risk counterpart due to two major factors: its focus on more temporally distant and minute risks with severe consequences, and its review of the time frame and resources needed for the impacted infrastructure to regain full functionality. Traditional risk analysis *can* be used to perform these functions well with a detailed analysis and a skilled analyst, yet this is not necessarily the prime focus of the overall risk analytic effort. Instead, a traditional risk analysis project constructs the ideal set of policies that, given available money and resources, would offer the best path forward for risk prevention, mitigation, and eventual management. In this case, longer term and lower probability risks are often neglected in favor of more intermediate and likely dangers, with only limited emphasis or focus on the push for infrastructural and organization resiliency and in the face of more distant threats. In this way, traditional risk assessment may not accurately or adequately prepare for those low probability yet high consequence events that dramatically impact human and environmental health or various social, ecological, and/or economic infrastructure that has become ubiquitous within modern American life such as contaminated water supplies, toxic spills, extreme precipitation or storm surge, and earthquakes.

What Does Resilience Bring to the Table of Risk Assessment?

Traditional risk analysis and resilience analysis certainly have their differences, yet overall they must be considered complementary approaches to resolve similar problems. Resilience analysis may not necessarily replace traditional risk analysis, but it certainly can improve for implications research and risk management protocols in a variety of cases. This is particularly true for the case of low-probability, high

consequence risks of the distance future, such as those associated with climate change, large-scale cybersecurity threats, or severe weather events on the coasts.

In the risk management paradigm, more focus on these extreme events would require more protective and preventive infrastructure which would be very costly. The goal of the resilience paradigm is not only to prevent what is preventable in a cost-effective way, but also improve the impacted individual or system's ability to "bounce back" to complex or extreme events, or reduce the time and resources necessary to repair the impacted infrastructure back to normal operating procedures. Though not universally true, resilience management *may* afford policymakers and stakeholders a greater upfront defense against system endangering hazards (Sikula et al. 2015).

In this way, resilience analysis adds in a different viewpoint that traditional risk analysts may miss the ability to understand just how an organization or infrastructural system is able to rebound from a massive external shock. While it is impossible to fully predict a highly uncertain and infinitely diverse future, a robust resilience analysis can offer greater organizational and societal preparation and more resilient protocols that, if adhered to, can reduce harms received by infrastructure systems and improve the functionality of the system in the midst of the ongoing crisis. While such events are rare in number, several have been experienced in recent memory, ranging from the September 11th terrorist attacks to the Fukushima Daiichi nuclear disaster in 2011, making such assessment both a realistic and highly useful tool to minimize unnecessary losses to infrastructure, capital, and most importantly, human well-being.

This perspective is of critical importance for policymakers with limited financial, labor, and infrastructural resources to protect against a wide universe of threats. For example, if the US government had an unlimited amount of funds to protect its coastlines against severe weather like hurricanes, it would develop and maintain infrastructure capable of withstanding the severity of a Category 5 storm. However, this is an entirely unrealistic and unacceptable policy outcome, where government funds must also address a broad range of other unrelated issues. As such, funds are optimized and allocated in a manner that the most cost-effective level of protection is generated (i.e., a Category 2 or 3 hurricane, depending upon historical trends and regional vulnerability to such threats). Further protection might help protect against more serious levels of threats, yet the risk-reduction return would eventually reach diminishing marginal returns—whereby a dollar invested in system hardness yields a gradually shrinking level of risk protection (Fig. 2.5).

Resilience-based approaches complement risk-based policies by optimizing resources in a manner that prepare systems for a broad variety of threats. As noted above, this is accomplished by identifying interlinkages and interdependencies within and between systems, and taking steps to prevent the potential for cascading failure to degrade or destroy the capacity for a system to function during and after a disruption has occurred. This helps optimize funds dedicated to protect systems against threats, where rather than hardening a system to a specific set of threats with scarce resources, some of those funds are allocated to help the system more efficiently recover from disruption when a broader variety of disruptions occur.

On the other hand, these novel benefits do not immediately mean that resilience analysis is an all-around improvement over conventional risk analytic methods. For traditional risk analysis, risk planning is a multistage effort that requires significant

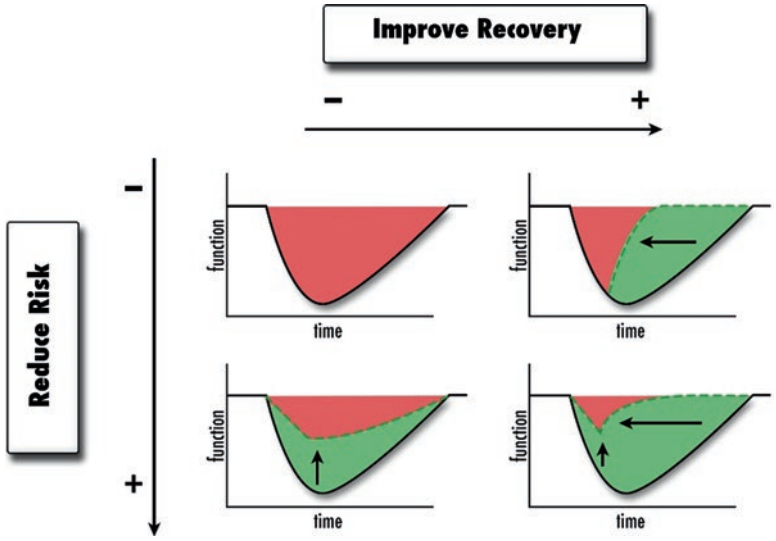

Fig. 2.5 Diminishing marginal returns for "buying down risk"

preparations for hazardous events prior to their occurrence. Resilience analysis follows this same paradigm, where the integration of risk perception (the active identification of risk and hazard in the midst of uncertainty), risk mitigation (steps taken to reduce harms before they occur), risk communication (the need for a clear and meaningful discourse on the seriousness of risk to the general population), and risk management (post hoc measures to address a realized hazard) collectively guide any risk or resilience effort. In this way, resilience analysis *is* far more than a focus on rebounding from a serious risk event, but rather a series of similar steps as with conventional risk analysis that has its own angle on how to best prepare for such hazards.

Additionally, resilience analysis may not significantly improve existing risk analysis protocols for events with fewer systemic and enduring hazards. This is due to the relative degree of higher complexity of resilience analysis thinking and methods, where less severe hazards and more mundane uncertainties are better served by conventional methods that adequately assess perceived cost and benefits for a given action. In this way, the improvements that resilience analysis brings to the table of conventional risk management are particularly applicable to high uncertainty events with the potential to yield cascading effects, rather than through more well-characterized and described activities, actions, and externalities.

Developing Technologies and Resilience

One emerging idea in the field of resilience is the use of smart technologies. Smart systems use connected technology (sensors, monitors, data recorders) to aggregate and analyze data continuously and in real time. Smart systems go under names such

as "internet of things," "automated control," and "wearable tech." Some smart systems often feed all information to a single command site, allowing for rapid decision-making and adaptive control by a manager in response to a disruption in the system. Other smart systems utilize built-in algorithms for decision-making to bypass the human component altogether. Smart technologies can greatly enhance the resilience capacity by detecting emergent behavior and preempting a disruption, by reducing the time needed to assess the degree of loss following a disruption, and/or by permitting adaptive response to a range of situations. Algorithms are great for systems that experience regular, predictable, and manageable disruptions such that an appropriate response can be coded into the artificial intelligence unit. Centralized command structures are useful for responding to emerging and unpredictable threats. Critical infrastructure systems may employ a combination of the two and even minor losses in the system can have consequences for human life safety.

The flip side of enhanced system operability via smart technology is the introduction of additional vulnerabilities. Unintentional events such as electrical outages or software failures can take the entire system offline, destroying both the ability to monitor and the ability to interact with the system (Fig. 2.6: Marchese and Linkov 2017). Many systems can still be evaluated and managed by hand, but this process becomes inefficient after it is supplanted by regular use of smart technologies. Furthermore, the greater connectivity increases vulnerability to intentional

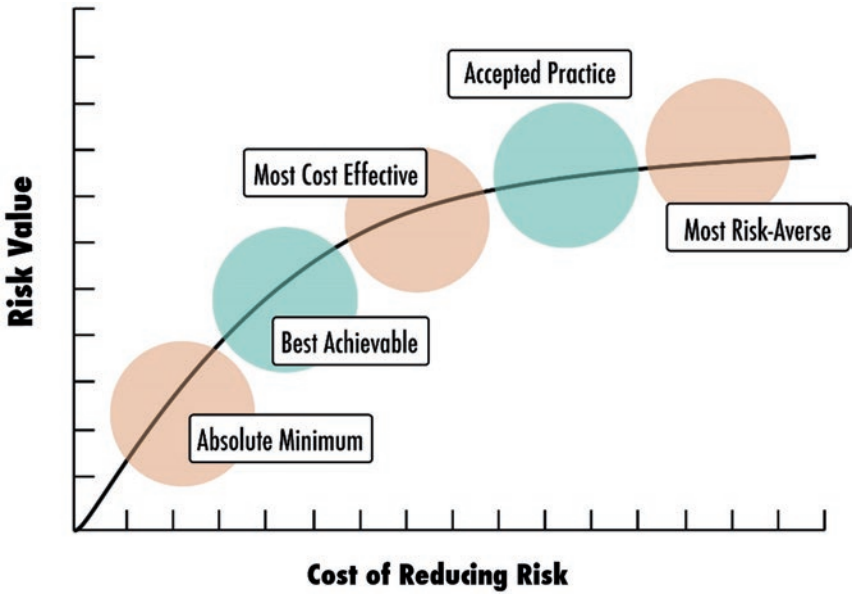

Fig. 2.6 Difference between resilient digital systems and "smart" digital systems as reproduced from Marchese and Linkov (2017). Resilient systems are illustrated as having less efficiency and greater redundancy, while smart systems are illustrated as having greater efficiency yet more substantial risk and function loss from targeted system disruption of certain system functions

attacks where the system can be hacked and used to cause intentional disruption or destruction, or simply to gather proprietary or for-official-use-only data. Smart technologies can vastly increase the efficient operation of a system, but smart and resilient are not always synonymous. Smart technology is being integrated into modern system faster than the potential consequences can be analyzed, thus careful consideration of the trade-offs of investing in smartness for resilience should be undertaken.

Applying a Systems Theory of Resilience

A further feature of resilience thinking that will be discussed throughout this book includes how resilience requires a *systems theory* to effectively operationalize and implement in a meaningful manner. Within such a theory, resilience is used to model and explain the interaction of systems between one another as well as within its own interconnected sub-systems. Given the high uncertainty and inability to fully predict or even characterize the wide universe of shocks and stresses that may challenge a given system over time, we argue that a systems theory serves as a beneficial resilience framework as it helps focus upon a given system functionality, agnostic of any given shock or stress. In other words, such a systems approach to resilience seeks to look internally at the structure and interrelationships of systems to review how impact or change to one node of a system generates cascading effects, in various degrees, to other directly and indirectly connected nodes.

As will be argued in Chap. 5, such a systems theory outlines (1) the need to understand how a given organization, asset, or infrastructure (herein defined as "system") interfaces with other systems in a complex environment, (2) the need to understand the composition of a given system to unpack its various sub-systems that influence its behavior or activity, and (3) the need to review how the impact of one system or a system's sub-systems can generate a cascading effect that, in a manner similar to the "domino effects" or "butterfly effects" described by Jervis (1998) and Holbrook (2003), can trigger substantial and potentially permanent shifts in the composition, activity, and status of various other connected systems. Within such a systems-focused approach to resilience thinking, we argue that it is essential to gain understanding of how these cascading events can trigger systemic change within and between systems.

This notion is highlighted in discussions of panarchy theory (Walker et al. 2004; Garmestani et al. 2008; Berkes and Ross 2013). Panarchy theory includes considerations of how systems interact with each other, and how a change in one can induce effects upon various others. Rather than seeking to categorize and analyze a wide universe of potential threat scenarios, a panarchy-driven system focus of resilience instead seeks to characterize the relationship within and between *systems* in order to identify areas that should be improved due to the strong cascading impact that their failure may have upon other connected systems and sub-systems.

Scholarly Views on Resilience: The Opinion of Available Literature

Resilience research to date has been narrowly focused on specific threats, asking questions to the effect of "how do we make a coastal community resilient to a hurricane?" or "how do we make a city resilient to earthquakes?" (Adger et al. 2005; Cimellaro et al. 2010). This attention to specific threats severely limits the alternatives considered downstream in the analysis process and therefore has potential to reduce the capacity to be resilient against other threats. Instead, resilience research should focus on maintaining the critical functions provided by a system and how a system may prepare, absorb, respond, or recover from an unknown hazard that may threaten the system's ability to function as recommended by the National Academy of Sciences. By looking at resilience as a goal of maintaining holistic system function as opposed to point-responses to address specific vulnerabilities, one gains a big picture view—a view that shows the overlapping nature of these hazards as pieces of a larger assessment protocol. When viewed as an overall function, increasing the community resilience as a whole may become an easier and more uniform task.

To gain a greater perspective on current activity and research in the field of resilience thinking, we conducted a preliminary literature review on the subject and its various topics of discussion. Specifically, this literature review attempts to identify principles of resilience from the physical health literature that can be abstracted to other domains.

We chose physical health resilience as the focus of this review for several reasons. The first is pragmatic. As indicated above, most current work on resilience has been contextualized for specific threats, with resilience to physical health representing one of the larger areas of inquiry. In addition, a review of the physical health literature allows us to study the processes that give rise to resilience at different timescales. Some diseases spread quickly and require a rapid response, e.g., the H1N1 epidemic of 2009 in North America. In contrast, diseases like HIV/AIDS persist in populations and require management and long-term planning. A resilient system should be able to respond to threats at both timescales.

Resilient systems should also be able to respond to an array of threat types, whether they occur naturally like influenza, or are engineered with adversarial intent like anthrax. Looking at resilience through the lens of physical health provides another piece of this larger tool-kit to increase community resilience as a whole. Knowing what a community has in resources to combat a health incident and how they will react can enable community planners and responders to better handle the incidents. For instance, knowing how a community could interpret information and in turn change their behavior in an epidemic could inform how best to distribute that information. Additionally, understanding the current state of how physical health and resilience have been conceptualized and how they have been studied present key pieces to understanding the role health plays in both individual and community resilience.

The goal was to conduct a review of resilience literature in the context of human physical health, identifying aspects of the definition to provide an expanded

understanding of how it fits in the larger picture of individual and community resilience and to aid in future decisions to increase resilience for any defined system. Two key aspects of human physical health highlight its importance in the field: timescale properties and potential adversarial nature of health threats. Threats to human physical health can happen quickly and require immediate response or they can persist over time. Health can also be threatened in adversarial ways, through chemical, biological, radiological, nuclear, and high yield explosives (CBRNE) attacks.

Search Methodology

Articles were identified primarily from Web of Science (WOS) and PubMed databases. The search was time scoped to include papers from 2000 to 2016. Initially, 12 queries were run in each database, resulting in a total of 3535 articles. PubMed articles were further filtered to include government publications, guidelines, introduction journal articles, journal articles, meta-analyses, and reviews, and exclude clinical trials and non-human studies. Micro-level experiments make up many clinical trials, and clinical trials do not mimic community resilience. Human health, instead of non-human, was the primary focus because of the ability to observe both physical and psychosocial aspects of resilience. As the goal was to look at physical, not mental, health, articles pertaining mainly to mental health were excluded. Two PubMed queries with high total numbers of articles were specifically revised to exclude mental health and psychology with the intention of decreasing the number of articles focused on solely those two areas, bringing the revised number of articles to 1146. Duplicate articles were removed, retaining 744 articles.

Remaining articles were filtered based on relevancy to literature review goals by screening titles and abstracts. Relevant articles involved community resilience, individual resilience as a smaller part of the community, public health emergencies, communicable diseases, and/or physical health. Excluded articles that were deemed not relevant from visual inspection (623) contained the following content: psychological/mental-health focus, wet-lab or micro-level scientific studies, non-human studies, non-health disasters, and non-communicable diseases. The number of relevant articles totaled 121. Of those articles deemed relevant, only 104 articles (86.0%) were available through Google Scholar and the Duke University library system.

Classification Scheme

Nine criteria were used to code the 104 articles in the query. The articles were coded on process versus ability, overall functioning, article type, classification level, resilience stage (NAS 2012), NCO domain (Linkov et al. 2013a; Alberts and Hayes 2003), and threat properties, which included disease presence, transmission type, and CBRNE.

Resilience as Process Versus Ability

The articles were coded on whether or not they contained explicit definitions of resilience. Once these definitions were recorded, each definition was coded on whether it described a process or ability. The reason for this coding was that processes tended to imply a continuum of resilience, while ability tended to imply a dichotomy. A definition that encompassed a process was defined as implying a system dynamic that moved the system towards improved resilience. Keywords for a defining resilience as a process were process, function, develop (a capability, for example), overcome (something), or endure. A definition that laid out resilience as ability implied that a system either had or lacked some component. Keywords indicating ability included ability, capability, capacity, and construct.

- *Overall functioning.* The articles were classified on whether or not the concept of resilience presented in the paper represented an idea applicable to other areas of resilience.
- *Article type.* The article types were broken down into review, theoretical, and empirical. Articles could only be coded as one article type.
- *Classification level.* The classification levels were individual, community (county or smaller), and societal (larger than county). When coding by classification levels, articles that provided a look at multiple levels were coded by their largest level; for example, if an article looked at individual and community resilience, the article was coded as community.
- *Resilience stages.* The papers were classified into the four defined stages of resilience, with the option to be classified in more than one stage. The categories were presented as: plan/prepare, absorb, recover, adapt.
- *NCO Domains.* Articles were also coded on what NCO domain of resilience they fell into, again allowing multiple classifications. The domains, as described earlier, were:
  - Physical
  - Information
  - Cognitive
  - Social
- *Threat properties.* In addition to many other features, articles were coded on different aspects of physical health. These aspects were disease presence, or the nature in which the disease exists in the system, and transmission type, or how the disease spreads within the system. These coding criteria allow a better view of natural features of the diseases being discussed. Since some papers did not address specific diseases or the diseases addressed did not fit into specific categories, each coding measure had other/unspecified as an option.
  - Disease Presence:

    Persistent (chronic): Diseases in article last an extended period of time in a community (HIV/AIDS)

Sporadic (acute): Disease in article are periodic and spread quickly through a community (Influenza)
Other/Unspecified: No mention of specific disease in article or no specified/known time course

– Transmission type:

Human-Human: Transmissible from humans to other humans (STDs)
Animal-Human: Transmissible from animals to humans (Avian Flu)
Vector-borne: Spread via an arthropod vector such as a mosquito or tick (malaria, dengue fever)
Other/Unspecified: No mention of specific disease in article or no known transmission type

Coding articles on whether or not they related to CBRNE (Chemical, Biological, Radiological, Nuclear, and Explosive) events as termed by the Department of Defense Dictionary of Military and Associated Terms provided another interesting facet to the research (Joint Publication 1-02). CBRNE coding was included due to the nature of the threats because they are not necessarily naturally dispersed and thus may be handled in different fashions. The anthrax attacks of 2001 demonstrate this. In this case, anthrax was sent through the mail system, an unnatural method of delivery that lead to a broader chain of potential exposure than simply coming into contact with anthrax since it does not spread human-to-human. CBRNE events are adversarial and intentional or unnatural events.

Results

Resilience as a Process Versus Ability

Each of the 104 articles was coded based on described criteria, and the counts were analyzed for each coding criteria. In total, just over half provided an explicit definition of resilience (53.8%). For many of the papers without an explicit definition, the word resilience was used without a definition or the concept was discussed but not explicitly stated. Of those definitions, 46.4% were classified as process and 53.6% as ability, respectively (Fig. 2.1).

Just over half of the articles (59 of 104, or 56.7%) conceptualized resilience in a fashion applicable to research areas beyond just physical health. Some of these papers presented broad constructs not focused solely on improving physical health resilience, but also on community resilience as a whole. Alternatively, others looked at physical health as a smaller piece of the larger picture of community resilience.

The papers were divided by their publication year and display a left-skewed distribution (Fig. 2.2). The majority of the articles (87.5%) are from 2007 to present. Most articles were reviews (39.4%) or empirical (37.5%), while considerably fewer were theory (23.1%). Many of the review articles looked retrospectively at past

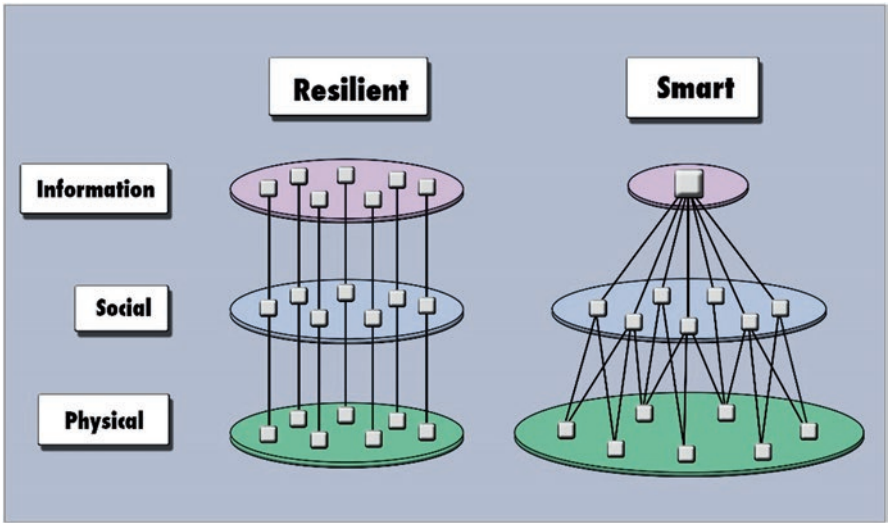

Fig. 2.7 Accounting for uncertainty in the decision-making process

incidents and literature to which the concept of resilience was applicable. The empirical articles often involved surveys about perceptions and preparedness to real or hypothetical situations or implementation of a framework or training for a specific scenario.

Each article was assigned a classification level for the sample size being examined. Nearly two-thirds (62.0%) of all articles involved community level analysis or review. A small number of articles (14.0%) looked solely at the individual level, while some expanded beyond to the community by placing emphasis on society (24.0%; Fig. 2.7). Many of the community level articles focused on counties or neighborhoods, while the societal articles tended to discuss nations as a whole or regions of a nation.

Resilience Stages

A majority of articles (85.6%) involved the plan/prepare resilience stage, specifically. Absorb and adapt were given much less attention at 19 (18.2%) and 20 (19.2%) papers, respectively, while recovery only appeared in 12 (11.5%) papers (Fig. 2.4). It should be noted that articles could be placed in more than one stage; overall 31% of articles fell into more than one resilience stage.

NCO Domains

The NCO domains were more evenly distributed. However, many papers (81.7%) fell into multiple categories. The physical and cognitive domains occurred most often at almost equal counts (68.3% and 70.1%, respectively), while the information domain and social domain occurred less often (44.2% and 55.7%, respectively). Of the articles coded for infrastructure under the physical domain, many dealt with the concept of communications infrastructure to ensure that all members of society receive appropriate information in the event of a crisis. Others discussed the need for adequately prepared hospitals, i.e., hospitals that could handle both in-patient and out-patient services at high levels of demand during a health incident.

Threat Properties

Just under half (49%) of the papers addressed a specific disease (Fig. 2.6a). Of the 51 papers that addressed a specific disease presence timescale, 47.1% addressed a disease that persists in the population, which was very often HIV/AIDS. The remaining (52.9%) articles addressed diseases that occurred sporadically in the population, such as influenza and SARS. Of the 57 that addressed specific disease transmission types, most articles (71.9%) included diseases with human-to-human transmission, while fewer featured animal-to-human transmission and vector-borne diseases (12.3% and 15.8%; Fig. 2.6b). Eleven of the 104 papers were classified as specifically pertaining to CBRNE research.

Takeaways from Scholarly Literature

From the results several features become prominent. Of the articles queried, a large proportion was published from the year 2007 onward. Several events around that time likely contributed to this increase in publications. The destruction and lack of resilience during Hurricane Katrina in 2006 probably had some influence on this. Furthermore, 2009 saw the onset of H1N1 that many feared would be a great pandemic, and again likely contributed to the trend.

Researchers defined resilience as a process versus ability fairly evenly. However, this definition should move more towards a process as research continues to expand. Resilience is not a static component of a system; it can always be improved. Thus, a process more easily defines the idea of continually improving resilience. Focusing on resilience as ability limits the continuum that resilience exists on because all systems are resilient to some degree. Resilience does not simply disappear when a system fails, it instead decreases; as the system recovers and adapts, its resilience increases. Resilience can be viewed as the process of maintaining

effective functioning before and during and event and altering it to be better maintained for the future after the event (Linkov et al. 2013a). Moving towards overall functioning instead of point-specific functioning in system resilience also advances the idea of a process. Looking at a community's resilience to point-specific hazards may be easily defined by ability; it is either resilient to an event or it is not. However, when looking at the whole of a community's resilience, a process viewpoint supports the idea of overall functioning because it is many pieces integrating to define the system. A community may be less functional in one area than another, but overall the process viewpoint provides some level of overall resilience for the community and building up general services resources instead of hazard-specific ones.

The results show a heavy emphasis placed on the plan/prepare stage. Looking for proactive solutions to problems often lends itself to this focus. Even when articles do focus retrospectively on an event, they often address failures in situational handling and suggest better ways to handle a similar event in the future, providing some sense of plan/prepare through assessment of the systems current state. Plan/prepare provides an easy facet to focus on due to the concept of hardening. Hardening often becomes confused with resilience because a system becomes more resistant to failure; however, resilience provides a dynamic function in which the system absorbs and comes back from near failure, whereas hardening does not provide that flexibility. While planning and preparing for disasters provides an important piece of resilience, the other areas need more recognition. This presents a difficult task when trying not to focus on specific hazards because research on absorb, recover, and adapt often focus retrospectively and provide suggestions for the future. However, coming up with a system of metrics to evaluate how well a system handles the different stages of resilience could increase the ability to adjust those areas.

This background, and review of scholarly literature, offers an idea of how resilience has developed and evolved in its early years of modern use as a tool and philosophy. As will be seen in the following chapters, the application of resilience requires detailed consideration of how it interacts with existing governance structures, methodological tools, and application areas in order to understand whether and to what extent resilience-based approaches can be beneficial for pertinent stakeholders.