Preface

Introduction

Several disasters over the past number of years have exposed serious weaknesses and vulnerabilities in the emergency management capabilities within the global communities. Events such as BP Deepwater Horizon Oil spill (2010), Fukushima tsunami and nuclear disaster (2011), earthquake in Haiti (2010), Hurricane Sandy (2013), and Typhoon Haiyan (2013) highlight the devastating effects that man-made and natural disasters have on the population and infrastructure. These examples highlight how 'hyper-risks' emerge from our 'hyper-connected world' [1] pointing to the requirement for enabling resilience to support disaster management. A recent Chatham House report 'Preparing for High-Impact, Low-Probability Events', found that governments and businesses remain unprepared for such events [2]. As described in the Chatham House Report [2], the frequency of 'high-impact, low-probability' (HILP) events in the last decade signals the emergence of a new 'normal'. With regard to the BP Deepwater Horizon Oil spill (2010), the various failures described in the Presidential Report (2011) highlight the lack of a suitable approach for anticipating and managing the inherent risks, uncertainties and dangers associated with deepwater drilling operations, and the failure to learn from previous near misses. Many of the risks that are associated with man-made and natural disasters often arise from unanticipated consequences stemming from interactions within and between different types of systems. Recurrent events, such as flooding, droughts, tornadoes, and even pandemic outbreaks have been shown to have equally serious impacts, raising new questions about how we can 'design' and enable resilience in systems and communities.

Resilience, resilient communities, and resilient livelihoods are becoming a focus of local, regional, national and global governments, and agencies. Researchers along with disaster management agencies are seeking to address the underlying fragilities that turn shocks and stresses into crises and how to enable resilience to support risk, crisis, and disaster management.

Resilience Thinking

Today we see unprecedented interconnectedness and interdependencies at the local and global scale. As described by Sambharya and Rasheed [3] 'risks are rarely confined to a nation, an industry, or a firm. Instead, today's risks are systemic, their contagion rapid, and their consequences devastating and unpredictable. This calls for new approaches to understand measure and respond to risks'. The concept of resilience, in particular associated with disaster risk reduction, has gained significant interest and attention. Within the context of such threats as pandemics, climate change, financial crisis, natural hazards, and technological disasters, resilience thinking has emerged as a concept that recognizes the complex, nonlinear and dynamic properties of interdependent systems (social, political, economic, ecological). "Resilience thinking" supports a systems view of the disaster management domain to reveal new ways of understanding the world and a new approach to managing disasters. The systems lens that supports resilience thinking embraces network analysis to reveal insights into politics, governance, and power relationships that permeate the system as described in Masys [4]. It embraces human, technical, and natural systems as complex entities continually adapting through cycles of change. A resilience thinking approach examines how these interacting systems of people, technology, and nature can be managed to facilitate safety and security.

As part of the Springer book series: *Lecture Notes in Social Networks*, this edited volume: *Disaster Management: Enabling Resilience*, focuses on the contribution of resilience thinking along the following broad themes:

- Urban Domain
- Cyber Domain
- Organizational/Social Domain
- Socio-ecological Domain

This book comprises 15 chapters from leading researchers engaged in resilience thinking within the risk, crisis, and disaster management domain. The chapters present state-of-the-art research on resilience thinking tools, techniques, and applications supported by case studies and computational simulation.

Content

Part I: Introduction

The first two chapters provide a powerful introduction to the notion of resilience within the disaster management domain. The chapter "Resilience Undefined: A Framework for Interdisciplinary Communication and Application for Real-World Problems" by Thomas G. Koslowski and Patricia H. Longstaff describe how resilience scholars from multiple fields continue to look for a universally accepted definition of resilience. But is a universal definition across disciplines possible or

even desirable in the near future? The proposed framework enables a more holistic understanding of the various fields of resilience research and makes communication across several domains more productive by placing the discussions into four types of resilience that are broad enough to facilitate discussion, but specific enough to allow for the translation of resilience into specific policies, practices, and outcomes.

Erik Hollnagel (well known through his contributions to resilience engineering) in his chapter "Disaster Management, Control and Resilience", looks at disaster management as a form of safety management, using the perspective of resilience engineering. In safety management, control can be lost by not being ready to respond, by having too little time, by lacking knowledge of what is going on, or by lacking the necessary resources. To maintain control unsurprisingly requires the converse of these conditions. Resilience engineering looks at how systems can sustain required operations under both expected and unexpected conditions by adjusting its functioning prior to, during, or following changes, disturbances, and opportunities. To do so requires the abilities to respond to what happens, to monitor the situation, to learn from what has happened, and to anticipate what may happen. The same type of analysis can be applied to disaster management, to better understand how it succeeds.

Part II: Urban Domain

The part on Urban Domain resilience comprises four insightful chapters. Oliver Chikumbo, Steve Lewis, Hugh Canard, and Tony Norris in their chapter entitled "Futuristic Smart Architecture for a Rapid Disaster Response" describe how the ability to control and contain an unexpected disaster event such as a bushfire or flooding in real-time is fraught with logistic and planning challenges. Information is difficult to assimilate both from structured and unstructured data that may be collected in real time—unreliability of mostly unstructured data from social media and mobile devices, though extremely helpful, can make it difficult to deploy needed help/assistance in time. Also when part of the infrastructure is destroyed that normally is relied on for collecting structured data, the situation can even make it harder for ad hoc planning specifically targeted at saving lives first. In such situations, a combination of unstructured data that carries uncertainties and limited structured data from infrastructure that might still be working after/during a disaster event can be used to the best of advantages and still enhance the control process to better achieve desired outcomes: i.e., real-time event monitoring through real-time limited and high uncertainty data; filtering unstructured data through crowd sourcing, not only for reliability but sometimes for language translation as well; short-term predictions of anticipated changes from already existing interoperable simulation models, using the limited structured data from infrastructure that might be still standing following a disaster; and all this with the aim of appropriate, timely responses to saving lives in a rapidly evolving environment. A generic management framework designed to be used during a "phase transition" between pre- and post events, and characterized by the interoperability of distributed simulation models, and the collection and sharing of structured and unstructured data via cloud services and "connected devices", is essential for the consistent provision of highly effective responses. Chikumbo et al. explores this

framework from a science and innovations perspective, advocating "antifragility" for emergency response system designs. For antifragility systems, failures do not stand for a breakdown or malfunctioning of normal system functions, but rather represent the adaptations necessary to cope with the real-world complexity through the management of "robustness trade-offs" as it occurs in dynamic and real-world contexts.

The chapter entitled "Building in Resilience: Long-term Considerations in the Design and Production of Residential Buildings in Israel" by M. Sever, Y Garb, and D. Pearlmutter develop ideas from previous work regarding architectural awareness of earthquake resistance. They introduce three levels of integration needed when designing for resilience: (1) integration in multidisciplinary design teams; (2) integration in the design process, i.e., integrated design or co-design, and (3) integration of long-term and short-term considerations. The aim of this chapter is to examine barriers to the integrated design of resilient buildings by looking at disincentives for nonlinear co-design processes along the extended building supply chain.

In their chapter "Urban Resilience and Sustainability: The Role of a Local Resilience Forum in England", Julie Fisher, Ksenia Chmutina, and Lee Bosher argue that the urban environment is prone to impacts of hazards, threats, and major accidents. In light of this it is crucial to plan, design, build, manage, and operate urban environment in a resilient and sustainable manner. The compatibility and conflict between resilience and sustainability has received increasing attention in recent years in academic literature, however, its application on local and national levels has not yet been widely attempted. The Local Resilience Forum (LRF) is an important mechanism for facilitating the complex multi-stakeholder interactions required to deliver urban resilience in England, however, sustainability does not appear to be a priority. This study explores how emergency planning and the design of the built environment can further both agendas. A range of promising practices was found that potentially could not only increase the resilience of, but that are also integral to the sustainability of the built environment.

Alexandra JaYeun Lee delves into the world of wicked problems and complexity in her chapter "Wicked Problems Framework: Architectural Lessons from Recent Urban Disasters". Urban issues such as informal settlements, poverty, and overcrowding, are merely the physical symptoms of deep systemic issues beyond the control of planners and architects alone, and hence, are 'wicked'. Rittel, a thought leader of design thinking, coined the expression "Wicked Problems" in 1973 to describe the complex issues of society situated in the real world that cannot be solved using rationality alone. In fact, such issues need transdisciplinary understanding and action to optimize decision-making based on multiple viewpoints and methods of inquiry.

Many of the 'wicked' attributes of society are amplified in a state of chaos such as in urban disasters, and this chapter argues that the wicked problems framework can lead to alternative visions through democratic, transdisciplinary design strategies. The Rittelian framework is still relevant in today's complex societies, particularly in community development projects. This chapter presents some of the key findings from three post-disaster case studies, tracing some of the successful design decisions that were made by local stakeholders with and sometimes without architects.

Part III: Cyber Domain

The pervasiveness and impact of cybercrime on national and global systems is significant. Chris Johnson in his chapter "Architectures for Cyber-Security Incident Reporting in Safety-Critical Systems" highlights how cyber-attacks can have a devastating impact on safety-critical systems. The increasing reliance on mass market Commercial Off-The Shelf (COTS) infrastructures, including Linux and the IP stack, have created vulnerabilities in applications ranging from Air Traffic Management through to Railway signalling and Maritime surveillance. Once a system has been attacked, it is impossible to demonstrate that malware has been completely eradicated from a safety-related network. For instance, recent generations of malware use zero day exploits and process injection with command and control server architectures to circumvent existing firewalls and monitoring software. This creates enormous problems for regulators who must determine whether or not it is acceptably safe to resume operations. It is, therefore, important that we learn as much as possible from previous cyber-attacks without disclosing information that might encourage future attacks. This chapter describes different architectures for encouraging the exchange of lessons learned from security incidents in safety-critical applications.

Building upon the insights emerging from Chris Johnson's chapter, Anthony J. Masys presents "The Cyber Ecosystem-enabling Resilience Through the Comprehensive Approach". The pervasiveness of the global cyber infrastructure is instrumental for economic prosperity and national security. Helbing [1] poignantly argues that 'Globalization and technological revolutions are changing our planet. Today we have a worldwide exchange of people, goods, money, information, and ideas, which has produced many new opportunities, services, and benefits for humanity. At the same time, however, the underlying networks have created pathways along which dangerous and damaging events can spread rapidly and globally'. With this in mind comes the realization that '…most cyber infrastructure is not secure and is vulnerable to attacks from malicious actors potentially leading to failure of critical infrastructure, exploitation of sensitive information, and loss of intellectual property' [5] .

The challenge in dealing with such cyber threats stems from the fragmented and disconnected approaches and solutions which as noted by Pawlak and Wendling [6] '…are driven by policy, legal, or technological considerations and as such rarely include all stakeholders: public administration, businesses, citizens, the research community or relevant international players'. To address the pervasiveness and severity of the cyber threats requires an approach that recognizes the cyber security risks from a 'systems perspective' recognizing the complex interdependencies between the physical, human, and informational domains [7–9]. This chapter approaches this 'complexity' dilemma through the application of systems thinking and the comprehensive approach [7, 8].

Part IV: Organizational/Social Domain

The organizational and social domains are explored in a number of chapters. In the Chapter entitled "Enabling Resilience: An Examination of High Reliability Organizations and Safety Culture Through the Lens of Appreciative Inquiry"

Jerson Wattie and Anthony J. Masys focus on shaping a safety culture through the strength-based approach of appreciative inquiry. Dulac [10] argues that complex socio-technical systems have a tendency to slowly drift from a safe state toward a higher risk state, where they are highly vulnerable to small disturbances whereby seemingly inconsequential events can precipitate an accident. Recent socio-technical disasters such as the 2011 Fukushima Nuclear accident, 2010 Deepwater Horizon accident and 2005 refinery explosions at BP's Texas City all highlight major disasters in which a safety culture was not working. Many industries around the world are showing an increasing interest in the concept of 'safety culture' as a means of reducing the potential for large-scale disasters, and accidents associated with routine tasks [11]. Traditional root cause methods of analysis examining safety culture apply a deficiency model in which problems are identified to support corrective action and transformational change. Within this paradigm one asks: "What are the problems?", "What's wrong?" or "What needs to be fixed?". Here we introduce a paradigm shift from a deficiency-based approach to a strength-based approach through the advent of "Appreciative Inquiry" (AI). The Appreciative Inquiry model is based on the assumption that the questions we ask will tend to focus our attention in a particular direction. Appreciative Inquiry stands out as a methodology that can facilitate examination and 'construction' of safety culture. As a high engagement, strength-based approach to organizational change, AI focuses on aligning strengths of the organization with opportunities, aspirations and desired results, and transforming goals into action fostering organizational learning at its core. Drawing upon the literature on AI, High Reliability Organizations and safety culture, this chapter presents appreciative inquiry as a tool-set to facilitate structured analysis and construction of the qualities of a safety culture of excellence to support a High Reliability Organization.

Simon Bennett describes in his chapter "Unintended Consequences. What Lessons Can Risk-Managers Learn from the Use of Armed Remotely Piloted Vehicles for Counter-insurgency in Pakistan?" how actions have intended and unintended consequences, some of which are functional, some not. The CIA's drones-first Pakistan counterterrorism strategy is used to illustrate how a well-intentioned policy may generate adverse outcomes sufficient to undermine that policy. The adverse outcomes (in Merton's argot 'latent dysfunctions') generated by the CIA's counterterrorism strategy may be so numerous and grave as to undermine the War on Terror. Adverse outcomes include collateral damage, radicalization, destabilization, and diplomatic schism. Several lessons are drawn. For example, the latent dysfunctions can undermine, if not fatally compromise, purposive action. It is far from certain that the CIA's drones-first counterterrorism strategy is making a net contribution to the War on Terror. Latent dysfunctions could render the War on Terror a zero-sum game. The author concludes that a timely response to contra-indications (Langer's 'mindfulness' and Toft's 'active learning') makes policy success more likely. Inhibitors to mindfulness include ignorance, prejudice, dogma, groupthink, and collective amnesia.

In the chapter "*Extra-fragile* in Disaster: People with Disabilities in a Bombarded Zone", Rita Sever describes how although some guidelines and manuals support the specific inclusion of people with disabilities in emergency considerations, most programs focus on disability as a cross cutting issue, or on protecting people with disabilities as a vulnerable group, rather than on the specifics of inclusion and overcoming barriers. There is little evidence that these guidelines are used to any effect with people with disabilities.

In emergencies, handicapped people may encounter particular difficulties that make the general facilities and assistance inaccessible to them. At the same time, services that usually cater to their special needs also suffer damage and become less effective or even unavailable. The social and personal supports that surround people with disabilities are fragile and appear to be particularly susceptible to the type of disruption that disasters incur.

This is what was happening in Israel in summer 2006. The existing public services were inadequate for people with disabilities living in the bombarded North which became a disaster zone, and third sector organizations stepped in to fill the void. A program was created by NGOs to respond to a deluge of requests for assistance from people with disabilities living in their communities within the disaster zone.

The research presented in this chapter is a mixed-methods case-study that studied this program. It is based on documentary material, program records, in-depth interviews with the partners and staff members of the program, and a survey of a representative sample of people with disabilities who requested assistance from the project. In addition to complementing findings of other researches, this study has unveiled some of the problems and dilemmas encountered by the project and has highlighted several issues that have not gained ample consideration, if at all, in the existing literature on disaster management and planning for resilience: unintended consequences of the participatory approach; managing and coordinating volunteers; and the double jeopardy of people with physical or mental disabilities who are also culturally and/or linguistically different from the mainstream population.

In the chapter "Disaster Management: Enabling Resilience" Regan Potangaroa, Happy Santosa, and Suzanne Wilkinson looks at one way to possibly measure resilience as a first step toward perhaps managing it. This issue of metrics seems to be at the core of the resilience discussion. The approach discussed uses a Quality of Life (QoL) Tool that was theoretically adapted for its application in the field.

In the chapter "Defining and Negotiating a Shared Responsibility for Disaster Resilience", Bede Wilson applies Cultural Theory to examine how the community of Springbrook, Australia, defines and negotiates a shared responsibility for disaster resilience. The influence of this process on the community's disaster management plan is also assessed. The Springbrook example shows that initiatives that promote mutual understanding of world views are an effective way to develop disaster resilience. Through deliberation these world views may form alliances that address the limitations of any single approach. Such alliances are both exclusive

and temporary however, suggesting that a broader range of initiatives, rather than broader participation itself, is required to support widespread and sustained resilience.

Part V: Socio-Ecological Domain

Socio-ecological resilience is addressed by Michael R. Czaja in his chapter "Wildland Fire Management: Movement Towards Enabling Resiliency?". Wildfires in the western US are changing. Research suggests they are expanding in size and duration. The results include civilian and firefighter fatalities, record destruction and damage to homes and infrastructure, and increasing costs to agencies responsible for fire management. Two developments within the framework of wildland fire management suggest potential movement toward enabling resiliency. One of these is development of the National Cohesive Wildland Fire Management Strategy. The other is a state-level initiative, Colorado's Task Force on Wildfire Insurance, and Forest Health. A goal of both processes is to seek methods which allow human populations and infrastructure to withstand a wildfire without loss of life and property. One implication will be how these initiatives enable resiliency within the larger subject of disaster management. Another will be to potentially apply this type of strategy development and working group methodology to other appropriate fields of disaster management.

In the chapter "Vulnerabilities and Co-evolutionary Dynamics in Morelia Michoacan, Mexico: A Case Study" L. Aguilar-Armendariz and A.N. Martinez-Garcia suggests that human populations' vulnerability to environmental hazards relates to sustainability and complexity sciences, given the global, multi-disciplinary, and dynamic nature of the issues currently faced by humanity. Among the human population affected by environmental disasters (being of hydrometeorological, geological, biological, technological, and even socioeconomic nature), the poor are usually the most affected (BID 1999, UNDP 2004). Not only the lack of basic infrastructure, education, goods, and services make the human poor more vulnerable to disasters, poverty issues also hinder the response of governments after each event. Human populations' vulnerability to environmental hazards can be understood as a dynamical process among physical, economic, ecologic, and sociocultural factors. Depending on the dynamic outcome among them, these factors either contribute or hinder human societies' sustainability. The case study for this chapter is Morelia, which is the capital city of Michoacan State, Mexico. The city had 729,279 residents in 2010, and it is vulnerable to extreme rainfall events, which result in flooding of given areas of the city every raining season. There are also geological fault lines where inhabited sections of the city have been constructed. This study considers social, economic and ecological variables, using metadata from the National Institute of Geography and Statistics (INEGI 2000, 2005, 2010) and the National Council for the Assessment of Social Development Policies (CONEVAL, 2010) of Mexico.

Collectively, the chapters present the reader with a broad overview of resilience thinking across the Urban Domain, Cyber Domain, Organizational/Social Domain, and Socio-ecological Domain. It advances our understanding and state of the art

regarding resilience within the risk, crisis, and disaster management domain and lays the foundation for continued exploitation and development of resilience thinking tools and techniques.

References

1. Helbing D (2013) Globally networked risks and how to respond. Nature 497: 51–59
2. Lee B, Preston F, Green G (2012) Preparing for high-impact, low-probability events: lessons from eyjafjallajokull. A Chatham House Report, London
3. Sambharya RB, Rasheed AA (2012) Global Risk in a changing world: new paradigms and practice. Organizational Dynamics 41:308–317
4. Masys AJ (2012) The emergent nature of risk as a product of 'heterogeneous engineering': A relational analysis of the Oil and Gas Industry safety culture. In: Bennett S (ed) Innovative thinking in risk, crisis and disaster management, Gower Publishing, UK
5. Kelic A, Collier ZA, Brown C et al (2013) Decision framework for evaluating the macroeconomic risks and policy impacts of cyber attacks. Environ Syst Decisions 33:544–560
6. Pawlak P, Wendking C (2013) Trends in cyberspace: can governments keep up? Environ Syst Decisions. 33:536–543
7. Masys AJ (2014) Critical infrastructure and vulnerability: A relational analysis through actor network theory. In Masys AJ (ed) Networks and network analysis for defence and security. Springer Publishing
8. Masys AJ (2014) Dealing with Complexity: thinking about networks and the comprehensive approach. In Masys AJ (ed) Networks and network analysis for defence and security. Springer Publishing
9. Collier ZA, Linkov I, Lambert JH (2013) Four domains of cybersecurity: a risk-based systems approach to cyber decisions Environ Syst Decisions 33:469–470
10. Dulac N (2007) A framework for dynamic safety and risk management modelling in complex engineering systems. Ph.D. Dissertation, MIT, Cambridge, MA
11. Cooper MD (2000) Towards a model of safety culture. Saf Sci 36:111–136

http://www.springer.com/978-3-319-08818-1

Disaster Management: Enabling Resilience
Masys, A.J. (Ed.)
2015, XVI, 338 p. 45 illus., 33 illus. in color., Hardcover
ISBN: 978-3-319-08818-1