Universität der Bundeswehr München

Fakultät für Informatik

Dynamic Interdependency Models for Cybersecurity of Critical Infrastructures

Elisa Canzani

Vollständiger Abdruck der von der Fakultät für Informatik
der Universität der Bundeswehr München
zur Erlangung des akademischen Grades eines

Doktor der Naturwissenschaften (Dr. rer. nat.)

genehmigten Dissertation.

Promotionsausschuss

Vorsitzender:	Prof. Dr. Peter Hertling
1. Berichterstatter:	Prof. Dr. Ulrike Lechner
2. Berichterstatter:	Prof. Dr. Stefan Pickl
1. Prüfer:	Prof. Dr. Kristin Pätzold
2. Prüfer:	Prof. Dr. Michael Koch
3. Prüfer:	Prof. Dr.-Ing. Markus Siegle

Die Dissertation wurde am 24.04.2017 bei der Universität der Bundeswehr München eingereicht und durch die Fakultät für Informatik am 21.07.2017 angenommen. Die mündliche Prüfung fand am 15.11.2017 statt.

To my parents and grandparents,
who helped me become the person I am today
and without their teachings and love
none of my success would have been possible.

Ai miei genitori e ai miei nonni,
che mi hanno permesso di diventare la persona che sono oggi
e senza i loro insegnamenti e affetto
nessuno dei miei successi sarebbe stato possibile.

Abstract

Governments have strongly recognized that critical infrastructures (CIs) play crucial roles in underpinning economy, security and societal welfare of countries. The proper functioning of energy, transportation, water plants, telecommunication, financial and other services, is vital for all communities. If a failed infrastructure is unable to deliver services and products to the others, damages may easily cascade into the larger system of interdependent CIs. Understanding such complex system-of-systems dynamics would help to prevent networked CIs from potential catastrophic cascading effects. However, existing security measures to protect a CI from threats and cyberattacks do not usually cross the organization's boundaries.

This research proposes a block building modeling approach based on System Dynamics (SD) to improve the understanding of dynamics of disruptive events in interdependent CI systems. Unlike most of the previous works in modeling and simulation of interdependent CIs, this novel approach accounts for both dynamics within a CI and across CIs while investigating two relevant dimensions of system resilience: operational state and service level. Blocks of models are iteratively developed and assembled together to generate complex scenarios of disruption with the final purpose of simulation-based impact analysis, resilience assessment, policy and risk scenario evaluation. The dynamic interdependency models offer a valuable and flexible tool for predictive analysis to support risk managers in assessing scenario of crisis as well as CI operators towards more effective investment decisions and collective response actions.

Principles of epidemic modeling are used to replicate diffusion and recovery dynamics of CI operations. Hence, SD is combined with a game-theoretic approach to understand "cyber-epidemics" triggered by strategic interactions between attacker and defender. Cyber attack-defense dynamics are modeled as a continuous game of timing to highlight that effectiveness of strategic moves strongly depends on "when to act". The game-theoretic model is applied for the optimization of proactive and reactive defense scenarios. This application demonstrates how the dynamic interdependency models can be used to support strategic cybersecurity decisions within organizations.

Promoting the use of information sharing to improve cybersecurity across organizations, a further application of the dynamic interdependency model represents a relevant contribution to the design of a cyber incident early warning system for CI operators. In accordance with guidelines issued by the European Union Agency for Network and Information Security (ENISA) to identify critical assets and services, the modeling is extended by a perspective of CI operators to demonstrate how it can be used to gain situational awareness in the context of European CIs.

Zusammenfassung

Regierungen und Behörden haben ein Bewusstsein für die entscheidende Rolle von kritischen Infrastrukturen (KIs) für die Aufrechterhaltung von Wirtschaft, Sicherheit und des gesellschaftlichen Wohlergehens von Staaten entwickelt. Die Verfügbarkeit von Energie, Transport, Wasser, Telekommunikation, Finanzdienstleistungen und anderen Dienstleistungen ist für die Zivilgesellschaft von lebenswichtiger Bedeutung. Wenn eine beschädigte Infrastruktur nicht in der Lage ist, Dienste und Produkte für die anderen KIs bereitzustellen, können Schäden leicht auf das größere System von voneinander abhängigen KIs übergreifen. Das Verständnis einer solchen komplexen "System-of-Systems" Dynamik hilft, vernetzte KIs vor möglichen katastrophalen Kaskadeneffekten zu schützen. Bestehende Sicherheitsmaßnahmen zum Schutz einer KI vor Bedrohungen und Cyberangriffen überschreiten jedoch normalerweise nicht die Grenzen der eigenen Organisation.

Die vorliegende Forschung schlägt einen Block-Building-Modellierungsansatz basierend auf System Dynamics (SD) vor, um einen Beitrag zum Verständnis der Dynamik von Störereignissen in voneinander abhängigen KI-Systemen zu leisten. Im Gegensatz zu den meisten vorangegangenen Arbeiten zur Modellierung und Simulation voneinander abhängiger KIs berücksichtigt dieser neue Ansatz sowohl die Dynamik innerhalb einer KI als auch die zwischen mehreren KIs und untersucht dabei zwei relevante Dimensionen der Systemresilienz: Betriebsstatus und Service-Level. Die Modellblöcke werden iterativ entwickelt und anschließend zusammengefügt, um komplexe Störungsszenarien mit dem Ziel der simulationsbasierten Wirkungsanalyse, der Bewertung der Belastbarkeit, der Bewertung von Policies und des Risikoszenarios zu erstellen. Die dynamischen Interdependenzmodelle bieten ein wertvolles und flexibles Werkzeug für die prädiktive Analyse, um Risikomanager bei der Beurteilung von Krisenszenarien sowie KI-Betreiber bei der Auswahl wirksamer Investitionsentscheidungen und kollektiver Maßnahmen zu unterstützen.

Bestimmte Prinzipien der epidemischen Modellierung werden verwendet, um die Diffusions- und Wiederherstellungsdynamik von KI-Operationen abzubilden. Daher wird SD mit einem spieltheoretischen Ansatz kombiniert, um "Cyber-Epidemien" zu verstehen, die durch strategische Interaktionen zwischen Angreifer und Verteidiger ausgelöst werden. Die Dynamik zwischen Cyberangriffen und Verteidigung wird als kontinuierliches Timing Game modelliert, um zu verdeutlichen, dass die Effektivität strategischer Bewegungen stark vom Zeitpunkt des Agierens abhängig ist. Das spieltheoretische Modell wird zur Optimierung von proaktiven und reaktiven Verteidigungsszenarien eingesetzt. Diese Anwendung zeigt, wie die dynamischen Interdependenzmodelle zur Unterstützung strategischer Cybersicherheitsentscheidungen in Organisationen verwendet werden können.

Die weitere Nutzung des dynamischen Interdependenzmodells, die den Informationsaustausch zur Verbesserung der Cybersicherheit in den Organisationen fördert, stellt einen relevanten Beitrag zum Entwurf eines Frühwarnsystems für Cyber-Vorfälle für KI-Betreiber dar. In Übereinstimmung mit den Richtlinien der European Union Agency for Network and Information Security (ENISA) zur Identifizierung kritischer Ressourcen und Dienste, wird die Modellierung um eine Perspektive von KI-Betreibern erweitert, um zu demonstrieren, wie diese Modellierung im Kontext von Europäischen KIs eingesetzt werden kann um das Situationsbewusstsein zu erhöhen.

Acknowledgments

I would like to thank with all my heart my first supervisor, Prof. Ulrike Lechner, who daily mentored me with the right balance between guidance, supervision, and freedom to conduct my research toward the topics of my interest.

Special thanks go to my second supervisor Prof. Stefan Pickl, who first welcomed me at the Univestität der Bundeswehr München and after a 6-month scholarship collaboration proposed to extend my stay in Munich for a PhD program.

In this regard, I express my gratitude to Prof. Renato De Leone from the University of Camerino in Italy, who supported my application for the scholarship that turned out to be the starting point of my extended experience in Germany.

It is my pleasure to acknowledge the roles of Helmut Kaufmann as industrial advisor, who promoted and supervised my work at Airbus Group, and Prof. Margaret Brandeau, who hosted me at Stanford University and continuously encouraged me to pursue my research.

Highly relevant for my career development was the NITIM International Graduate School and its network members, which allowed me growing as researcher through interdisciplinary programs, training activities, and international events.

Last but not least, I would like to thank my lovely family, friends, and colleagues for their daily support, patience, and understanding along this unforgettable and not trivial adventure called “PhD”.

This research has been funded within the Marie Curie Research and Innovation Actions by the European Union Seventh Framework Program FP7/2007-2013 under REA grant agreement No. 317382, project NITIMesr.

Contents

List of Figures

Chapter 1

Chapter 2

Chapter 3

Chapter 4

Chapter 5

Chapter 6

List of Tables

Chapter 1

Chapter 2

Chapter 3

Chapter 4

Chapter 5

Chapter 6

Chapter 1

Introduction

Contributing to the understanding of complex and interdependent dynamics of systems under disruptive events via mathematical modeling and simulation techniques is the main interest of this dissertation.

Among real-world systems, critical infrastructures (CIs) are investigated as particular complex interdependent adaptive systems. It has been widely recognized by governments that the proper functioning of such interconnected cyber-physical systems is vital for all communities and countries. Business operations have come to increasingly rely on information technology (IT). Consequently, cyber attacks represent a major threat to modern infrastructure systems. On this note, Eugene Kaspersky argues that Hackers may have been responsible for many more operational disruptions in CIs than just those cases for which cyber causes were positively identified.

This chapter introduces main concepts and facts in the field of cybersecurity of CIs that motivate and inspire this research work to finally provide a comprehensive outline of the thesis. Section 1.1 presents the basic notions towards the understanding of complexity and interdependency of systems in crisis situations, with a particular attention to interdependent infrastructure systems and related cybersecurity issues.

Among examples of CI disruptions happened over the years, the 2003 US power outage is discussed in Section 1.2 as motivating example for this research. In fact, existing studies on the blackout scenario highlight the lack of comprehensive approaches to capture dynamic relationships between causes and consequences over time in case of disruption in networks of CIs. Section 1.3 highlights the relevance of investigating the CI interdependency problem through the lens of cybersecurity. Section 1.4 frame specific research objectives into the overall challenge of how to model the dynamics of cybercrises affecting CI operations together with the interdependencies between CIs and the impact of interdepenedency on the whole system dynamics.

In Section 1.5, the overall structure of this dissertation is presented according to chapters, content of the chapters, and related author publications upon which chapters are based. Section 1.6 concludes the chapter with further discussions on how this research is conducted, inspired by preliminary work, enriched by training activities, and supported by collaborations with both academia and industry.

1.1 Complex and Interdependent Systems

In a general sense, the adjective “complex” describes a system or component that by design or function or both is difficult to understand (Weng et al., 1999). The difficulty concerns the study of interdependencies between components which constitute the system and determine its global behavior.

(Mitchell, 2006) define a “complex system” as a large network of relatively simple components with no central control, in which emergent complex behavior is exhibited. This means that the global behavior of the system arises from interdependent actions of the simple components, but the mapping from individual actions to interdependent behavior is nontrivial. Here, of key importance is the notion of nonlinearity for which “the whole is more than the sum of the parts”.

In addition to nonlinearity, (Ladyman et al., 2013) provide a list of properties associated with the idea of complex systems. E.g. feedback loop structures, lack of central control, hierarchical organisations, adaptive and self-organizing behaviors, and uncoordinated interactions between elements (i.e. spontaneous order).

Often-cited example of complex systems in nature are the brain, the immune system, biological cells, metabolic networks, and ant colonies In society, complex systems include the Internet and World Wide Web, economic markets, and critical infrastructures.

Traditionally, mathematically oriented sciences such as physics, chemistry, and mathematical biology have focused on the modeling of simpler systems in nature. Then, the rise of the computer has made it possible to make more accurate models of complex systems in modern societies (Mitchell, 2006).

In general, creating a model that accurately predicts the outcomes of the actual system is not possible. However, a model can accurately simulate the processes that the complex system will use in order to create a given output. (National Research Council and others, 2002) argue that awareness of the potential for such models has profound implications for organizational efforts toward homeland security of nations and countries.

As the risk and uncertainty from disruptive changes are increasing, public managers seek methods to improve capabilities of their interdependent organizations to anticipate risk and demonstrate resilience in response to threats (Comfort et al., 2001). On this note, (Coombs, 2012) states that a crisis does not just happen, it evolves. In fact, such complex and interdependent systems drastically change over time in response to stimuli which they undergo during crisis situations. And even small changes or failure in the system can precipitate major displacements through reinforcing feedback processes according to the so-called “butterfly effect” (Faulkner, 2001).

Furthermore, disruptive events are characterized by high threats, short decision time and elements of surprise and urgency. These characteristics highlight the need to develop comprehensive system approaches with predictive functionality which enable to understand highly dynamic environments generated by crisis situations (Simonovic, 2011).

This research particularly focuses on the understanding of interdependencies between complex CI systems and related cybersecurity issues through the strategic use of mathematical modeling and simulation approaches.

Hereafter, the term critical infrastructure (CI) is used according to the following definition given by the EU Council Directive (EU, 2008).

> “CI means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.” (EU, 2008)

The European programme for critical infrastructure protection (EPCIP) discussed by the Council Directive (EU, 2008) is a step-by-step approach to define CIs that concentrates on the energy and transport sectors, asserting the need to include also the information and communication technology (ICT) sector.

The most recent detailed list of CIs and assets of national importance is provided the US National Infrastructure Protection Plan (NIPP)(DHS, 2013) and includes 16 CI sectors as follows:

- Energy,
- Transportation Systems,
- Communications,
- Information Technology,
- Water and Wastewater Services,
- Dams,
- Chemical,
- Nuclear, Reactors, Materials, and Waste,
- Emergency Services,

- Critical Manufacturing,
- Commercial Facilities,
- Financial Services,
- Government Facilities,
- Defense Industrial Base,
- Healthcare and Public Health,
- Food and Agriculture.

The technical report of (Moteff et al., 2004) describes the changes in identifying and defining CIs as the focus of public policy debates shifted from infrastructure adequacy to infrastructure protection. Thereby, it has been widely recognized by governments that CIs play crucial roles in a region's economy, security and societal welfare.

The proper functioning of such complex interdependent adaptive systems is vital for all communities and countries (Rinaldi et al., 2001). If a failed infrastructure is unable to deliver services and products to the others, disruptive effects may easily cascade into the larger system of interdependent CIs. Accordingly, (O'Rourke, 2007) describes CIs as "lifeline systems" which are interdependent primarily by virtue of operational interaction and, in many cases, physical proximity.

For example, after the Hurricane Katrina in 2005 an electric power outage at the pumping stations of the major transmission pipelines led to serious interruptions in supplies of crude oil and refined petroleum (Knabb et al., 2006). Natural hazards include the 1998 Ice Storm in Canada which caused a power outage with greatest societal concern in parts of Ontario, Quebec, and New Brunswick and the Northeastern US (Chang et al., 2007). After the 2016 flood in the German region of Baden-Württemberg, the area-wide supply of electricity and drinking water was interrupted for days and it took several weeks to restore the road network (Laudan et al., 2016).

Worldwide security and economy have been seriously compromised after the 2001 World Trade Center terrorist attack which led to the collapse of the twin towers and damage of numerous other buildings and utilities in the area (Mendonca and William, 2006). The water flooded rail tunnels, a commuter station, and the vault containing all of the cables for one of the largest telecommunication nodes in the world; some boats were dispatched to work as floating ambulances to support emergency services (Ouyang, 2014).

All these different types of extreme events, which highly impacted human lives and costed billions of dollars in economic losses, show the evidence of interdependencies between CIs that may not be visible in normal operations.

As business operations have come to increasingly rely on information technology (IT), modern infrastructures have become increasingly interconnected. Consequently, the risk that even minor disruptions in a single CI can lead to a catastrophic cascade of failures in CI networks is increasing (Buldyrev et al., 2010).

Mostly, the integration of physical systems and processes with networked computing has led to the emergence of a new generation of engineered systems, the so-called cyber-physical systems (Krogh et al., 2008). The worldwide network infrastructure can be seen as a web of interacting cyber-networks (e.g., the Internet) and physical systems (e.g., the power grid). A smart grid is an example of CIs where power grid network and communication network are coupled together for its operational control.

Cyber-physical technologies have been applied to control almost all components of CIs. Consequently, cyber attacks represent a major threat to CI systems. The most famous cyber attack that led to physical damage is the Stuxnet in 2010. The Stuxnet is a malicious computer worm that exploits the programmable logic controllers (PLCs) and supervisory control and data acquisition (SCADA) control systems of the Iranian industrial plant to damage gas centrifuges for uranium enrichment (Langner, 2013).

The CI survey conducted by McAfee Labs (Beek et al., 2016) to assess the eveloving cyber threat landscape confirms that the offensive cyberwarfare may target not only databases and digital infrastructure but also weapons and physical infrastructure. Attackers could attempt to turn off the power or water instead of the Internet. This escalation in vulnerabilities led the 48% of survey respondents to say that it is likely or extremely likely that a cyberattack will take down a CI and provoke loss of human life.

Hence, the time of the fast spreading computer viruses seems to be over. There is an infrastructure to protect from high-impact and silent spreading cyber attacks such as advanced persistent threats (APTs), and there are dynamics of cascading failures between CIs to understand and prevent. It was obvious that increasing mysteries around cyber crises would have been calling for new techniques and methods able to capture dynamics of cyber conflicts. This research work addresses the challenge of how to model the dynamics of cybercrises affecting CI operations together with the interdependencies between CIs and the impact of interdepenedency on disruption spread and recovery dynamics.

In this regard, the cyber security pioneer Eugene Kaspersky argues that hackers may have been responsible for many more operational disruptions in CIs than just those cases for which cyber causes were positively identified (Spiegel Online, 2011). The claim of Mr. Karspersky particularly refers to the 2003 US outage, which is discussed below as a motivating example to investigate the field of cybersecurity of CIs.

1.2 A Motivating Example

On 14 August 2003, the North American power grid experienced its largest blackout ever which provoked tremendous disruptions in parts of Ohio, Michigan, New York, Pennsylvania, New Jersey, Connecticut, Massachusetts, Vermont, and the Canadian provinces of Ontario and Quebec. About 50 million people were affected by the blackout. Even most of the customers got the power successfully restored within hours, some US areas did not have power for two days and in parts of Ontario rotating blackouts occurred for up to two weeks.

System conditions prior to the blackout were in a steady-state. The Northern America Electric Reilability Corporation (NERC, 2015) declared that

- the power system was within the operating limits;
- electricity demands were below record peaks, although high due to high air-conditioning loads typical of warm days in August;
- power transfers were heavy, but not unusual;
- some facilities were out of service for routine maintenance and others have been forced out by an unanticipated breakdown and need for repairs, as on any given day.

Nevertheless, complicate voltage management due to high transfers led to a series of events - electrical, operational, and computer related - causing the power system cascade.

A qualitative analysis on how CIs were directly and interdependently impacted in the Ontario area is reported by Department for Public Safety and Emergency Preparedness in Canada (PSEPC, 2006). The study asserts that the lack of electricity impacted all CI sectors in Ontario. More precisely, the executive summary of (PSEPC, 2006) reports the following information about disruptions of interdependent CIs.

- In **Energy Sector**, most of the power generation, transmission and distribution sources connected with the North American electrical grid were significantly impacted. Power plants took varying amounts of time to resume the production of electricity. Backup generators and fuel supplies were not enough for the maintenance of essential services. Industrial and commercial users made a significant contribution by reducing their electricity consumption. The lack of electricity also compromised the ability of the oil and gas CIs to manufacture or transport its products either via traditional transportation means or by pipeline.

- **Telecommunication** operations of some landline and cellular companies were disrupted, but the whole Canadian telecommunication industry succeeded in maintaining an adequate service level of its telephone networks. The critical situation increased the telecommunication service demand and most wireless services were overloaded during the power outage. Priority access to telephone lines was given to emergency responders. Also, medias employed backup generators to power their production processes and release information to the public.

- As the **Banking and Finance** industry strongly relies on telecommunications, it experienced an immediate degradation of services following the electrical grid collapse. Backup generators and secure network servers allowed most financial institutions to provide at least nominal services on August 15. The power failure had minimal impact on North American market activity because it occurred approximately 15 minutes after trading closed.

- **Food** distribution services were disrupted due to shipping and storage difficulties. Food production operations were reduced to just-in-time delivery of supply and consequently it became extremely vulnerable to any interruptions of supply delivery.

- **Water Services** were adequate for the supplies of treated and potable water throughout the blackout. A number of incidents were reported of waste treatment plants because of the inability to procure chemicals to purify water.

- **Critical manufacturing** chose to shut down completely or reduce the production to scale back power consumption.

- **Transportation Systems** were seriously affected because the blackout occurred during the closure of workplaces across affected areas, compounded the negative effects on transportation networks. The loss of power to traffic lights, electronic highway signs, traffic monitoring stations complicated the rush hours. Delays occurred at bus, rail and airport terminals. Many gas station pumps were inoperable due to interruptions of fuel distribution services.

- **Emergency Services** across the affected areas experienced a dramatic increase of demands which turned into delayed emergency vehicles, backlogged hospitals and difficult communications.

- Some **Nuclear Reactors** remained in standby mode while others had to shut down. Although nuclear reactor operators started slowing the availability of sufficient electricity to meet consumer demand, this did not slow down the restoration of the grid.

- Only essential **Government Facilities** were reported to work on August 15. About 150,000 employees did not report to work for the week of August 18–22. Emergency

> Operations Centres were invoked to offer aid to various CI sectors. Telephone line service of the Canadian government was maintained in order to provide Ontario residents with current information about available provincial services. Government priority was to maintain vital public services such as public health, safety and security, and social and economic welfare.

Beside this comprehensive analysis of interdependencies between CIs, other impacts were reported to be directly related to the power failure. Environmental safety was compromised due to partially treated waste water and hydrocarbons into the atmosphere. And economic impact estimates indicate that the power outage costed between 1 and 2 billion US dollars to Ontario's economy.

Note that data is collected from Canadian and American media reports and cross-sector information sharing with the federal and provincial governments as well as the private sector (PSEPC, 2006).

The qualitative analysis conducted in (PSEPC, 2006) reports the clear evidence of interdependent effects to CIs provoked by the blackout. Quantitative tools to identify existing interdependencies between CIs and quantify magnitude of cascading effects in such interconnected scenarios of disrupition are presented in this work.

Timing is also a relevant issue that needs to be considered in the analysis. The timeline of disruptive events during the US blackout is reported by (ISO, 2005), but it refers to cascading failures in power grids and does not give any information about effects on other infrastructures.

Towards a comprehensive understanding of coupled cause-effect dynamics over time, a relevant question to ask is about causes that actually triggered the power system cascade. Hovewer, technical reports limit the investigation to system conditions prior to the event and provide general recommendations to reduce future outages (Liscouski and Elliot, 2004).

The joint US-Canada Power System Outage Task Force (Liscouski and Elliot, 2004), established after the 2003 blackout, identified the lack of system understanding and loss of situational awareness as major causes of the power outage, followed by poor diagnostic support and inadequate tree trimming. However, the task force which included two phases:

(i) investigate the causes of the outage,

(ii) develop recommendations to reduce the possibility of future outages.

This two-step process adopted in the task force limited the analysis to separated studies on causes and preventive measures.

Also, the research work of (Andersson et al., 2005) identifies the main causes of the blackout with the purpose of improve system dynamic performance. The authors include the lack of reliable real-time data which led to a lack of time to take decisions about mitigation strategies, and the lack of properly automated and coordinated control of response efforts. Practical recommendations and guidelines to prevent from future blackouts on the basis of lessons learned are discussed by (Liscouski and Elliot, 2004).

A different perspective on the 2003 Northeastern blackout was brought to light only seven years later by the cyber security pioneer Eugene Kaspersky. During an interview, Mr. Kaspersky has revealed that the US Northeast blackout of 2003 was most likely caused by a cyber attack (Spiegel Online, 2011). He also suggests that hackers may have been responsible for many more operational disruptions in CIs than just those cases for which cyber causes were positively identified. “We should count on seeing cyber attacks on factories, airplanes and power plants”, the cyber expert said.

However, official reports on the 2003 blackout only indicate the occurrence of two critical cyber threats, the Blaster and SoBig worms, which coincided with the blackout and significantly impacted unpatched corporate networks (PSEPC, 2006).

Overall, the need to improve the system understanding and situational awareness programme via innovative modeling techniques is of interest of this dissertation. Instances that cyber causes have led to physical damages in the case of the 2003 US power outage further motivate this research work towards the domain of cybersecurity of CIs.

1.3 Problem Statement

Studies on the US outage in 2003 (cf. Section 1.2) highlight the lack of proper methods to capture relationships between causes and consequences over time in order to get a proper understanding of dynamics underlying the power blackout.

Governments’ task forces (e.g. (Liscouski and Elliot, 2004)) often limit the analysis to causes of the disaster and preventive measures to avoid similar disruptions in the future. This kind of approaches does not consider that “a problem leads to action that produces a result that creates future problems and actions” (Forrester, 2009).

Also, the relevance of timing is often neglected and information about time components are used in the analysis. E.g. the timeline of initiating events which led to the cascading power outage in interconnected power grids only appears in (ISO, 2005). Vague descriptions of cascading effects into other infrastructures can be found in online available sources (PSEPC, 2006).

Another crucial observation is that technical reports generally describe consequences without linking them to the triggering causes, and viceversa. A special focus is given to the understanding of cascade failures rather than recovery dynamics, while causes are often not deeply investigated. Not surprisingly, cyber causes of the 2003 US blackout have been only identified several years later (Spiegel Online, 2011).

Beside qualitative investigations, quantitative studies mainly focus on a few aspects of the 2003 US outage. E.g., (Haimes, 2015) present an input-output model to assess economic impacts and (Anderson and Bell, 2012) estimate mortality effects in New York city.

Nevertheless, dynamics of blackouts and electric power shortages seem to be relatively well understood on the basis of lessons learned through the years. What is still missing is a comprehensive approach that enables to understand disruptive dynamics affecting interdependent CI systems at both strategic and operational layers in complex scenarios such as autonomous driving or internet of things. New patterns and prospects for crisis managers in the EU are discussed in (Boin et al., 2013).

In general, the lack of available information and relevant data about such critical events represents a major limitation for quantitative research in this field. The body of literature shows however research efforts to study interdependent CIs using modeling and simulation techniques. Based on principles of system-of-systems (Eusgeld et al., 2009), quantitative approaches mainly consider only a few CIs due to the complexity of interdependency modeling, e.g. (O'Reilly et al., 2007). Other studies exclusively refer to IT components of the target infrastructure (Knapp and Langill, 2014).

The state-of-the-art in modeling and simulation approaches for interdependent CI systems highlights the need to integrate different approaches and distinct their responsibilities in a uniform framework (Ouyang, 2014). Further details on existing theories and methodologies are discussed in Chapter 3.

Rather than performing a detailed analysis, (Svendsen and Wolthusen, 2007) argue that exploratory research at a high-level of abstraction is the only way to provide valuable insights to address infrastructure interdependencies. Then, higher level analysis can be used to refine further investigations. This is the rationale behind the exploratory study conducted in this research work to address coupled cause-effect dynamics over time characterizing cybersecurity of CIs.

From a practical perspective, risk managers and decision makers have called for new conceptual frameworks and extended analytical tools to support delicate crisis management processes that take place daily for protecting CIs from vulnerabilities and threats (Kröger, 2008).

When CIs are challenged, national authorities must be able to deal with heterogeneity, multiple and inconsistent boundaries, resilience building, knowledge transfer and other problems that limit the effectiveness of response policies (Hernantes et al., 2013).

During a research seminar organized by the COMTESSA research group in Wildbad Kreuth in 2015, the NATO Branch Head Operational Analysis at Headquarters Supreme

Allied Commander Transformation (HQ SACT) in Norfolk, Johannes de Nijs, said that "decision makers need understanding, not just answers". Arguments on how analysis provides rigour can be found in (De Nijs, 2010).

In reality, complex systems are optimized to be robust against expected failures. However, the main threat is represented by unknown attacks that could cause cascade failures breaking down CIs. CI protection plans need to account for high resiliency with respect to unexpected failures. As companies are expecting more and more cyber incidents with higher and higher costs each year (Ponemon Institute, 2015), CI operators strongly need reliable decision-making supports for more effective IT-strategy investments and more resilient infrastructures.

Together with the evident gap in research method, the need of effective decision support systems which enable practitioners to understand complex dynamics of CI interdependencies in relevant disruption scenarios, and consequently improve the awareness in the decision process, strongly inspires and motivates this research work.

1.4 Research Objectives

This research work takes into account dynamics over time of interdependent CIs under disruptive events, and focuses on the modeling, simulation and analysis of interdependencies between CIs with respect to their operational capability, service availability and resilience to cascading failures.

The main intent is to contribute to the nascent - and rapidly growing - field of cybersecurity of CIs by proposing a set of new instruments and modeling tools to improve the understanding of nonlinear dynamics underlying complex behaviors of interdependent CI systems.

More precisely, research objectives grow iteration by iteration of this design-oriented research (cf. Chapter 3). At first, three building blocks of models are developed to capture relevant aspects of disruption and recovery dynamics within a single CI and across CIs while investigating two dimensions of system resilience: operational state and service level. Questions that can be addressed with the dynamic interdependency models include the following: what are the impacts of a failed CI on other interdependent CIs? How long it takes to get back the system to normal operations? How can cascading effects among CIs be reduced if a CI is down for a certain period of time? How can CIs' capabilities be optimized in order to increase system resilience? How can the risks of CI failures due to demand perturbations be mitigated?

Thereby, implications for risk managers and decision makers are straightforward. Supported by visualization features of Vensim SD simulation software (Vensim, 2015), the dynamic interdependency models constitute a valuable toolkit that helps CI operators to assess scenarios of disruption, optimize investment decisions, and evaluate collective restoration policies towards more resilient infrastructure systems.

Extending research objectives into the cybersecurity domain, a combination of SD and game theory is adopted to study how operational dynamics of a single CI emerge from strategic interactions between cyber attacker and defender to take over the control of CI operations. The dynamic cyber game model aims at addressing questions like: when must a player act to maximize his benefits? Which are the optimal cyber defense measures with respect to timing? What is the best response against adaptive attackers?

Finally, the dynamic interdependency model is further extended by a perspective of CI operators to demonstrate how it can be used to gain situational awareness in the context of European CIs. The objective is to support CI operators to asses disruption scenarios as well as to collectively identify priorities and coordinate response efforts towards improving cybersecurity across organizations through the strategic use of information systems. E.g. what is the relevant information that operators must share in case of CI disruption? How to assess the disruption magnitude based on the importance of the failed CI operators? How can the design of an early warning system account for interdependency impact analysis?

Model extensions to cyberesecurity issues enable decision-makers to consider both operational and strategic layers in assessing scenario of cascade failures triggered by cyberattacks.

In sum, this dissertation attempts to contribute to methodology by proposing a well-structured modeling process to capture relevant aspects of disruption and recovery phenomena in CI networks through building blocks. Moreover, the application of the modeling approach to support crisis management processes in relevant cyber incident scenarios and use cases demonstrate relevant implications of this research for the practice.

For such a purpose, collaborations with both academia and industry allow establishing solid theoretical foundations as well as dealing with more complex real-world situations. (See 1.6 for further details.)

1.5 Overview of the Thesis

The dissertation is organized as follows (see Figure 1.1). Chapter 2 presents a qualitative literature review that looks for pivotal articles and analyzes models breaking new grounds towards the understanding of complex system dynamics and crisis modeling. More precisely, the review provides mathematical insights emerging from epidemics modeling as well as the description of how epidemic models have been inspiring research in the cybersecurity domain. Then, the state-of-the-art in CI interdependency modeling is introduced with a major emphasis on quantitative modeling and simulation approaches. Overall, research patterns in epidemiology, cybersecurity, and infrastructures' interdependency clearly show similarities and overlaps in methodologies beyond applications. After a brief overview of related works toward the understanding of the cybersecurity landscape, literature findings are discussed with the attempt to guide rational decisions in choosing models for applications into the field of cybersecurity of CIs.

Research design and methodology adopted to conduct this research work are described in Chapter 3. This work is an exploratory study of new fields and domains that follows a design science approach. In particular, the research design is described as an iterative process comprehensive of four main iterations. Also, system dynamics (SD) is introduced as main modeling methodology to capture nonlinear dynamics arising from operational disruptions and cyberattacks to CIs. It follows a description of how SD models are developed within a block building modeling framework which provides a solid structure for the modeling and the analysis of simulation results.

Accordingly, Chapter 4 presents dynamic interdependency models to analyze disruptions in CI networks adopting a block building approach based on SD. This chapter explains how to develop building blocks of models and how to use them to generate scenarios of disruptions in networked CI systems. With a special emphasis on time-dependent dynamics, simulation examples demonstrate the use of dynamic interdependency models for disruption impact analysis and system resilience assessment. On this regard, a further application shows how this modeling approach can be a valuable instrument to support collective policy evaluation of CI operators toward national resilience objectives.

The overall objective of Chapter 4 is to provide insights for potential users of the SD model, such as CI operators that continuously attempt to forecast disruption scenarios and assess risks of failures in interdependent CIs. Further contributions and extensions of the modeling through the use of new technologies and methodologies are presented in Chapters 4 and 5 of this thesis.

Specifically, Chapter 5 combines SD with a game-theoretic approach to investigate cybersecurity dynamics within a single CI. The aim is to understand how strategic behaviors of attacker and defender impact operational performances of the target CI. After a brief survey of existing game-theoretic approaches in cybersecurity of CIs, the dynamic attacker-defender model is presented as continuous game of timing to highlight that the effectiveness of strategic moves strongly depends on when to act. Player strategies are described according to time to attack, time to defend, and thresholds upon which decisions are made over time. Then, a multi-objective optimization of cyber defense policies is conducted to investigate proactive and reactive defense scenarios.

Then, Chapter 6 presents an application of the dynamic interdependency model to the scenario of the project ECOSSIAN (European Control System Security Incident Analysis Network) as relevant contribution to the design of a cyber incident response and early warning system for CI operators in Europe. The interdependency model is extended by a perspective of CI operators in accordance with the work of the European Network Information Security Agency (ENISA). The chapter also presents capabilities of the model to capture dynamic aspects of interdependencies on the basis of environmental, human, economic and other impact factors as well as effects of structured demand patterns for CI services.

Finally, Chapter 7 concludes with an overview of research contributions to theory and practice in the domain of cybersecurity of CIs. Concluding remarks on further applications, usability and flexibility of the dynamic interdependency models presented in this thesis serves as inspiration for future research.

Figure 1.1 depicts the overall structure of this dissertation according to chapters (black dashed boxes), content of the chapters (literature in purple, modeling in blue, and results in orange), and related author publications upon which chapters are based (green labels). Further discussions on research dissemination, collaborations and training activities that supported, enriched and framed this work are presented in the next section.

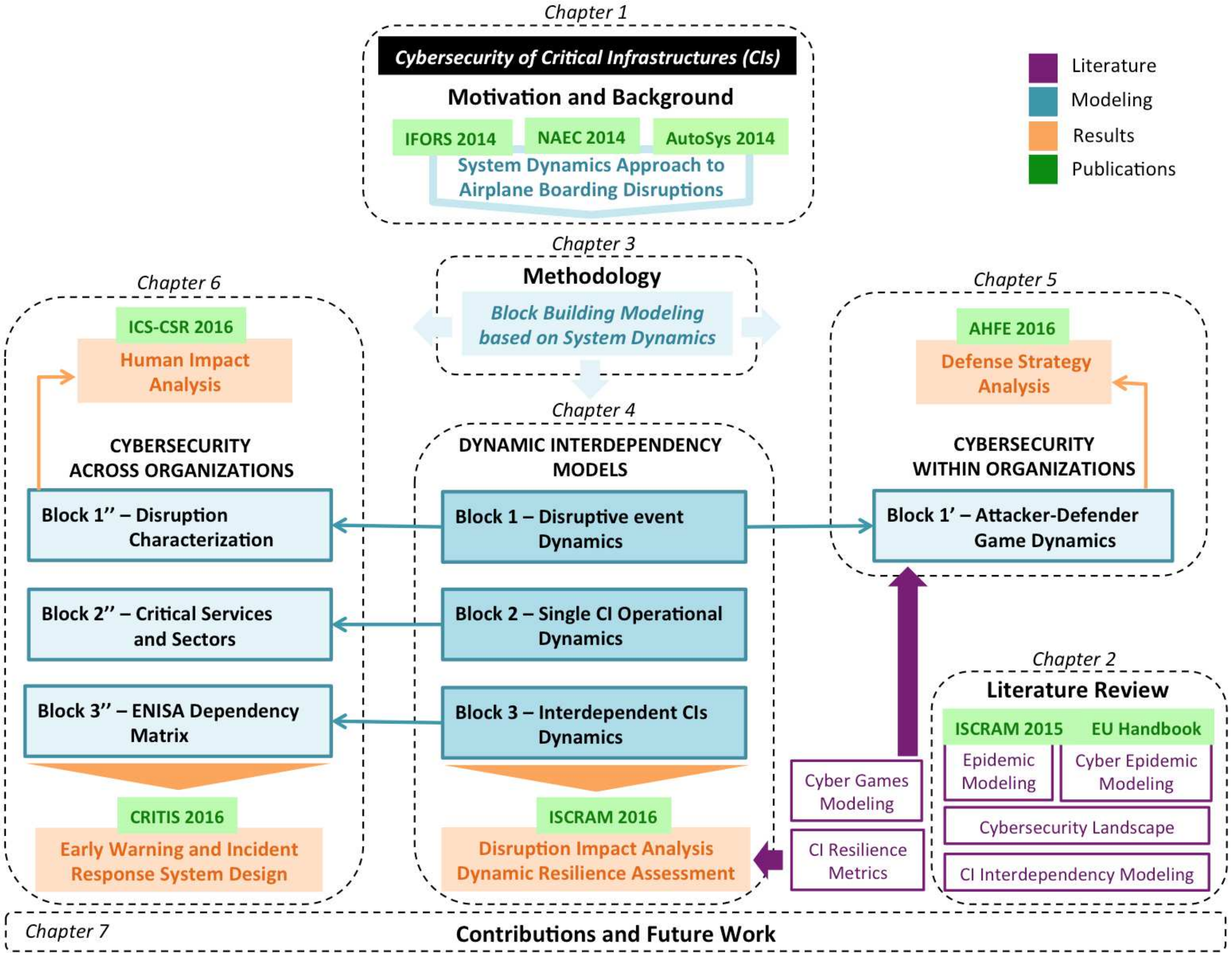

Chapter 1
Cybersecurity of Critical Infrastructures (CIs)
Motivation and Background
IFORS 2014
NAEC 2014
AutoSys 2014
System Dynamics Approach to Airplane Boarding Disruptions
🟪 Literature
🟦 Modeling
🟧 Results
🟩 Publications
Chapter 3
Methodology
Block Building Modeling based on System Dynamics
Chapter 6
ICS-CSR 2016
Human Impact Analysis
CYBERSECURITY ACROSS ORGANIZATIONS
Block 1'' – Disruption Characterization
Block 2'' – Critical Services and Sectors
Block 3'' – ENISA Dependency Matrix
CRITIS 2016
Early Warning and Incident Response System Design
Chapter 4
DYNAMIC INTERDEPENDENCY MODELS
Block 1 – Disruptive event Dynamics
Block 2 – Single CI Operational Dynamics
Block 3 – Interdependent CIs Dynamics
ISCRAM 2016
Disruption Impact Analysis Dynamic Resilience Assessment
Chapter 5
AHFE 2016
Defense Strategy Analysis
CYBERSECURITY WITHIN ORGANIZATIONS
Block 1' – Attacker-Defender Game Dynamics
Cyber Games Modeling
CI Resilience Metrics
Chapter 2
Literature Review
ISCRAM 2015
EU Handbook
Epidemic Modeling
Cyber Epidemic Modeling
Cybersecurity Landscape
CI Interdependency Modeling
Chapter 7
Contributions and Future Work

Figure 1.1: Structure of the PhD thesis

1.6 Publications and Collaborations

This research has been inspired by a preliminary work done by the author between October 2013 and April 2014 in the field of Aviation Management. The author developed a system dynamics (SD) model to analyze the airplane boarding process and evaluate performance of different operational strategies. This six-month research project was funded by a scholarship for post-graduate awarded at the University of Camerino (Italy) to promote a joint collaboration with the COMTESSA research group of Universität der Bundeswehr München, aka UniBw, (Germany). Synergies between the COMTESSA group and the Munich Aerospace Research Network highly motivated this research project.

The author presented the results on *"A System Dynamics Approach to the Airplane Boarding Process"* at the 20th Conference of the International Federation of Operational Research Societies (IFORS 2014) as (Canzani et al., 2014b).

This piece of research facilitated exploring capabilities of advanced SD modeling and simulation techniques to cope with complex feedback structures and nonlinear dynamics underlying operational processes.

From May 2014 the author embarked on her PhD research at UniBw as Marie Curie Research Fellow in the NITIM graduate school, funded by the ITN project on Crisis Management - namely "NITIMesr" - within the European Union Seventh Framework Programme (FP7/2007-2013). The NITIM graduate school is an international network that fosters interdisciplinary research on Networks, Information Technology and Innovation Management. See (NITIM, 2017) for more details.

In the wider field of Crisis Management, personal research interests in understanding dynamics of complex systems via mathematical modeling techniques motivate the use of the SD airplane boarding model as "toy model" to study operational disruptions and interdependency between passengers during the boarding. Considering disruptions caused by the baggage that passengers carry on board, a quantitative analysis of resilience and robustness of the boarding process is performed. Also, a qualitative research on innovative hand-luggage policies applied by airlines highlighted the key role of business strategies for the mitigation of operational disruptions during the boarding process.

Outputs of this research *"Toward Disruptions in the Boarding Process: A System Dynamics approach"* were presented and published by the author in the proceedings of the Networking and Electronic Commerce conference (NAEC 2014) as (Canzani and Lechner, 2014).

With respect to research objectives (cf. Section 1.4), the boarding process represents a motivating example towards the development of valuable tools and instruments to explore the filed of cybersecurity of interdependent CIs by combining qualitative and quantitative approaches that account for both operational dynamics and business strategy implications.

The author supervised two master students at UniBw to conduct a first investigation into the field of IT-security. Information flows characterizing the cyber threat landscape have been investigated. Results of the analysis *"Towards an Understanding of the IT Security Information Ecosystem"* were published in the proceedings of the 7th GI conference on Autonomous Systems 2014 as (Canzani et al., 2014a).

With the attempt to provide solid theoretical foundations to this research work, epidemic modeling have been selected as relevant stream of literature to understand phenomena of spread and recovery dynamics. Accordingly, a paper on *"Insights from Modeling Epidemics of Infectious Diseases – A Literature Review"* was published in the proceedings of the 12th International Conference on Information Systems for Crisis Response and Management (ISCRAM 2014) as (Canzani and Lechner, 2015). This piece of research was further extended towards *"A Review of Epidemics Modeling Approaches to Understand Cyber Crises"*, which is a chapter of the EU Handbook on Networks in Innovation and Crisis Management, deliverable of the NITIMesr project (Canzani, 2016a).

Epidemic models inspired the research towards *"Modeling Dynamics of Disruptive Events for Impact Analysis in Networked Critical Infrastructures"*. This piece of research appears in the proceedings of the 13th International Conference on Information Systems for Crisis Response and Management (ISCRAM 2015) as (Canzani, 2016a). This is cornerstone publication which introduces the block building approach adopted to develop dynamic interdependency models for CIs through SD tools.

Relevant to mention is that the EU doctoral program of the NITIMesr fosters the development of an international open cooperation framework of academics and professionals through specific training objectives, such as doctoral consortia, regional learning circles, and research secondments. Collaborations which enriched and framed theoretical foundations and applications of this work refer to Stanford University and Airbus Group, as affiliated partners of the NITIMesr project.

In particular, the author spent two months (February-March 2016) as visitor research scholar in the department of Engineering and Management Science of Stanford University. This period at Stanford University allows the author to strengthen theoretical foundations of this research through active participation to research seminars of the Center for International Security And Cooperation (CISAC) and the Engineering Risk Research Group (ERRG) as well as semester lectures in Risk Analysis, Health Policy Modeling, and Healthcare Operations Management.

Scientific collaborations and the high-level learning experience of the secondment period in US were inspiring for a research contribution on *"Cyber Epidemics: Modeling Attacker-Defender Dynamics in Critical Infrastructure Systems"*, which appears in the Springer Series on Advances in Intelligent Systems and Computing as (Canzani and Pickl, 2016)

With the intent to apply research findings to scenarios with practical relevance, the author pursued a first research internship at the Cyber Security Research Lab of Airbus Group Innovations from October 2015 to January 2016. The fruitful collaboration has been extended for a second research internship from May 2016 to September 2016.

Airbus Group provided data for validation through use cases and relevant scenarios of interest of the project ECOSSIAN (European Control System Security Incident Analysis Network). The ECOSSIAN aims at the development of an early warning and incident response system for CI operators in Europe. The dynamic interdependency model is extended by a presepective of CI operators, critical services, and sectors to contribute to the design of the ECOSSIAN ecosystem for the purpose of improving situational awareness and response coordination via simulation-based impact analysis.

The author published results on *"Characterizing Disruptive Events to Model Cascade Failures in Critical Infrastructures"* in the proceedings of the 4th International Symposium for Industrial Control Systems & SCADA Cyber Security Research (ICS-CSR 2016) (Canzani et al., 2016), and *"An Operator-driven Approach for Modeling Interdependencies in Critical Infrastructures based on Critical Services and Sectors"* in the proceedings of the 11th International Conference on Critical Information Infrastructures Security (CRITIS 2016) (Canzani et al., 2017).

In sum, dissemination of preliminary research work all along the PhD path targets relevant academic communities in the field of information systems for crisis response and management (e.g. ISCRAM), critical infrastructure security (e.g. CRITIS), and cybersecurity research for both industrial control systems (e.g. ICS-CSR) and human factors (e.g. AHFE). Also, close collaborations with both industry and academia (i.e. Airbus Group and Stanford University, respectively) support the final scope of this design-oriented research to bridge theory and practice (cf. research methodology, Chapter 3).

Other advanced courses and training activities which contributed to strengthen this research work as well as to broaden the author's views are:

- EU Coneeect Training Week 2015 – *Educating Entrepreneurial Educators.* Tel Aviv, Israel.

- IPAM Graduate Summer School Program 2015 – *Games and Contracts for Cyber-Physical Security.* UCLA, Los Angeles, California.

- NATO Graduate Summer School Program 2015 – *Verification and Synthesis of Correct and Secure Systems.* Marktoberdorf, Germany.

- NATO Advanced Training Course 2017 – *Countering ISIS Radicalization Activities through the Cyberspace in the Region of South-East Europe (CIRACRESEE).* Ohrid, Macedonia.

- NITIM programme such as doctoral consortia (Bergamo 2014, Leiden 2014, Belfast 2015, Barcelona 2015, Trondheim 2016, The Hague 2016), career events (Barcelona 2015 and The Hague 2016), and monthly Regional Learning Circles at UniBw.

This research is mostly funded within the Marie Curie Research and Innovation Actions by the European Union Seventh Framework Program FP7/2007-2013 under REA grant agreement No. 317382, project NITIMesr.

Chapter 2

Literature Review

Cybersecurity of critical infrastructures is an extremely important area of research. Complexity and high dynamics arise when studying physical damages and cascade effects between infrastructures, which are increasingly targets of threats and cyberattacks. Understanding, modeling, and analysis of disruptive dynamics of complex systems date back from much older fields, among which epidemiology can be considered the most representative stream of literature. In the wider field of crisis management, epidemiology is a solid research stream that has attracted a wide range of mathematicians and modelers contributing to the understanding of spread and recovery dynamics of infectious diseases the area of public health management.

Over the years, approaches and techniques from epidemics modeling have been adopted to explore diffusion phenomena of networked systems such as social, innovation, and communication systems. In particular, the widely used metaphor of viruses, infections, immunization strategies, and epidemic recovery mechanisms is straightforward in the context of computer security.

Accordingly, this chapter presents a qualitative literature review that looks for pivotal articles and analyzes models breaking new grounds towards the understanding of complex system dynamics and crisis modeling. Structure and objectives of the literature search are presented in Section 2.1. Section 2.2 provides an extensive overview of mathematical insights emerging from epidemiological research patterns, and Section 2.3 discusses how epidemic models have been inspiring research in the cybersecurity domain. The state-of-the-art in CI interdependency modeling is introduced in Section 2.4. A major emphasis is given to quantitative modeling and simulation approaches.

Literature findings are discussed in Section 2.6 with the attempt to guide rational decisions in choosing models for applications into the field of cybersecurity of CIs.

Note that a literature study on mathematical modeling of infectious diseases has been published by the author in (Canzani and Lechner, 2015) and (Canzani, 2016a).

2.1 Structure and Objectives

At large, this research work contributes to better understand complex dynamics of systems in crisis situations through the strategic use of innovative modeling techniques and methodologies. In particular, epidemiology is selected as representative stream of literature which has largely attracted the interest of many modelers and mathematicians aiming at exploring phenomena of spread and recovery dynamics in networked environments.

A review of existing methods and models breaking new grounds in epidemics literature leads to the identification of theoretical foundations of this research work. In fact, modeling epidemic spreads is naturally considered as related field from which to get knowledge about diffusion phenomena such as innovation, social and communication systems. Among the wide range of applications, of particular interest is to investigate how epidemic models have been inspiring research into the cybersecurity domain.

Furthermore, a deep understanding of insights from modeling epidemics of infectious diseases can support the complex modeling of cascading effects, recovery dynamics, and nonlinear relationships between such cyber-physical systems. Thus, mathematical concepts emerging from epidemiological research patterns are solid research pillars towards improving the state-of-the-art on quantitative modeling and simulation techniques in the quite new field of CI interdependency modeling.

Three relevant streams of literature are therefore identified:

- **epidemics modeling**,
- **cyber epidemics modeling**,
- **critical infrastructure interdependency modeling**.

To investigate these fields, an extensive literature review is performed through electronic search of academic databases on the Internet (e.g. Science Direct, Elsevier, Google Scholar, ACM digital library, Springer link etc.).

Guidelines followed to structure the review refer to (Randolph, 2009) and (Webster and Watson, 2002).

Characteristic	**Categories**
Focus	Research outcomes Research methods Theories Practices or applications
Goal	Integration (a) Generalization (b) Conflict resolution (c) Linguistic bridge-building Criticism Identification of central issues
Perspective	Neutral representation Espousal of position
Coverage	Exhaustive Exhaustive with selective citation Representative Central or pivotal
Organization	Historical Conceptual Methodological
Audience	Specialized scholars General scholars Practitioners or policymakers General public

Table 2.1: Cooper's taxonomy of literature reviews (Randolph, 2009)

Table 2.1 shows the Cooper's taxonomy of literature reviews reported by (Randolph, 2009), which helps to characterize the literature search according to focus, goal, perspective, coverage, organization, and audience.

The classification in Table 2.1 is used as reference guide to structure the literature review on the basis of research objectives, which consist in providing new methods and models to improve the understanding of disruption and recovery dynamics in CI systems. First of all, the **focus on theories** is clear to the scope of this work. A review of mathematical theories helps to assess which theories already exist, to what extend they are used, as well as relationships among them.

Selected streams of literature are investigated towards the **identification of central issues**, which are finally discussed and integrated into a big picture to frame the research landscape. Therefore, a qualitative review that looks for **pivotal articles** is conducted through a **neutral representation** of relevant concepts and existing modeling approaches in the fields of epidemics, cyber epidemics, and CI interdependency respectively. In each field, seminal reviews and most cited papers introducing new models are selected and assessed by relevance through a snowball approach until a well-rounded collection of articles is identified.

The literature analysis comprises three main rounds. Each round refers to one of three relevant streams of literature identified above, but they obviously overlap in time as means of a continuous process of literature search.

The first round serves to identify the core building blocks of models and research patterns in epidemiology. Accordingly, the data collection process is done on the basis of specific key words, such as “crisis dynamics”, “crisis modeling”, “epidemic models”, “mathematical epidemiology”, “modeling infectious diseases”, and combinations of them. For this first round, the literature search in academic databases is conducted in September 2014 and the snowballing continued until February 2015.

The second round of literature review is performed to understand how such epidemics models have facilitated research towards the emerging field of cyber crisis modeling. Here, interesting articles are collected using key words related to the cyber world in addition to terms already used in the first round. In particular, a comprehensive body of literature has been identified by combining key words such as “computer” or prefix as “cyber-” with biological-inspired terms (i.e. “epidemics”, “virus”, “immunology”, etc.) and more technical words such as “mathematical modeling”, “crisis dynamics”, and “diffusion process”. The search is conducted in February 2015 and snowballing continued until April 2015. Also, the review is further refined in 2016 for writing the present dissertation.

A third round of literature review refers to modeling approaches in the field of critical infrastructures. A primary research is conducted in parallel to the other two rounds by using the terms “critical infrastructure”, “critical infrastructure protection” and “cyber-physical system” combined with keywords such as “dynamics”, “interdependency”, ”interdependent systems”, ”networks”, “disruption”, “cascade faliure”, “impact anaylsis”, “modeling”, “modeling approaches”, “quantitative modeling”, “simulation”.

Relevant to mention is that the snowballing search in the field of CI interdependency modeling is continually pursued along the research work to update and refine the state-of-the-art, as well as to explore specific research directions through the use of additional keywords such as “system resilience”, “resilience assessment”, “resilience metrics”, “cybersecurity”, “cyberattack”, “attacker-defender dynamics”,“cyber game”, “incident response coordination”, “early warning system”, “cyber-physical system”. Note that this secondary search aims at motivating the use of specific methods (or combinations of them) for applications and extensions of building blocks of models. Reference literature for such purposes is discussed later on in related chapters of this thesis.

The following sections are organized according to the various theories in epidemics, cyber epidemics, and CI interdependency modeling literature. A **conceptual**

organization is characteristic of theoretically-focused review according to (Randolph, 2009). The same author also argues that the primary audience of a dissertation comprises supervisors and reviewers. According to the taxonomy in Table 2.1, the target audience of this literature review refers then to **specialized scholars** who have substantial knowledge of mathematical tools and techniques.

In summary, the literature review starts from mathematical concepts emerging from epidemiological models and moves toward recent studies on modeling cascade failures and cybersecurity of critical infrastructures. The final goal is to provide a reference guide to identify relevant combinations of modeling approaches to address current research gaps in modeling interdependent dynamics of such complex cyber-physical systems.

2.2 Epidemics Modeling

An epidemic is a large and short term outbreak of a disease, and the study of disease occurrence is called epidemiology (Hethcote, 1989). A major concern of epidemiology is to understand transmission characteristics and identify different causes of disease diffusion. The lack of understanding of crucial factors influencing epidemic dynamics of spread often turns into failures of vaccination strategies and inability to quickly respond in case the infection spreads in a population.

The earliest epidemic model was created by Daniel Bernoulli in 1760 (Bernoulli, 1760). He showed through calculations how to increase life expectancy by inoculation against smallpox. However the modern theoretical epidemiology began in the early 1900, when Ronald Ross conducted a mathematical study for the transmission of malaria (Ross, 1911).

Over the years, modelers and mathematicians have been strongly contributing to understand the "persistent threat" of epidemics by developing "more than a thousand and one" models (Hethcote, 1994). This is because the use of mathematical tools to understand high dynamics of crises is particularly relevant when real experiments are not possible such as in case of epidemics.

The valuable contribution of modeling approaches in epidemiology is emphasized by the seminal book of (Brauer and Van den Driessche, 2008):

> "mathematical epidemiology differs from most sciences as it does not lend itself to experimental validation of models. Experiments are usually impossible and would probably be unethical. This gives great importance to mathematical models as a possible tool for the comparison of strategies to plan for an anticipated epidemic or pandemic, and to deal with a disease outbreak in real time." (Brauer and Van den Driessche, 2008)

The comprehensive SIAM review of (Hethcote, 2000) clearly shows that applications of results of epidemics models are significantly behind the mathematical theory rather than modeling specific diseases. However, with exception of the SIAM review, existing literature presents a substantial lack of guidelines which focus on modeling approaches in epidemiology rather than in understanding diffusion dynamics of a particular virus.

This literature review focuses on the identification of epidemiological research patterns, the core building blocks of models, and the questions that they can answer.

More precisely, five core building blocks are identified in epidemics modeling literature:

- *compartmental or deterministic models*,
- *stochastic models*,
- *network models*,
- *spatial models*,
- *computational epidemiology.*

Below, the review of epidemic models aims at exploring mathematical insights emerging from each of the five modeling approaches and is therefore organized accordingly.

Compartmental Models

In mathematical epidemiology, a predominant modeling technique consists in dividing the population into compartments representing the status of individuals with respect to the disease and labeled accordingly. Compartmental models are usually formulated as set of differential equations, which are deterministic. For this reason, compartmental models are also known as deterministic models.

Assuming that the epidemic process is deterministic, the population dynamics is completely determined by its history and the rules describing the model. Thus, questions that can be answered with deterministic models are: will the epidemic outbreak? If an epidemic outbreaks, how many individuals will get infected?

Which are the compartments to consider and how individuals can transfer one to another depend on the type of infection. The simplest case considers the class S of individuals which are susceptible to the pathogen and the class I of infected individuals. Other compartments are included to achieve more realistic results, such as the class R of recovered or removed individuals. See (Hethcote, 2000) for details on the class M of infants born with passive immunity and the class E of exposed individuals who are in the latent period after they get infected.

Flow patterns of individuals between compartments are indicated by the acronyms used for these models. For instance, the SIS model (Susceptible-Infected-Susceptible) indicates that susceptible individuals can get infected and become again susceptible to the pathogen. The SIS model is often used to represent diseases transmitted by bacteria, which usually have no immunity against reinfection.

Relevant to mention is the SIR epidemic model (Susceptible-Infected-Recovered) of Kermack and McKendrick, which represent the earliest milestone work in modern epidemiology (Kermack and McKendrick, 1927). The model assumes that susceptible individuals can get infected and then they die or recover becoming immune to the disease.

Mathematically, the SIR model is formulated as a set of derivatives with respect to time t as independent variable. Let $S(t)$, $I(t)$, and $R(t)$ be the numbers of individuals at time t in the respective classes. McKendrick and Kermack assume the following:

1. Given a population of size N, $S(t) + I(t) + R(t) = N$ at any time t.
2. Let α be the constant contact rate, an average member of the population makes contact sufficient to randomly transmit infection with αN other individuals per unit time.
3. The quantity ${}^{1}/_{\beta}$ is the average infectious period so that infectives leave the class I with a rate of βI per unit time.

Under these assumptions, the SIR model is formulated as follows:

$$\begin{cases} \dfrac{\mathrm{d}}{\mathrm{d}t}S(t) = -\alpha\dfrac{I(t)S(t)}{N} \\ \dfrac{\mathrm{d}}{\mathrm{d}t}I(t) = \alpha\dfrac{I(t)S(t)}{N} - \beta I(t) \\ \dfrac{\mathrm{d}}{\mathrm{d}t}R(t) = \beta I(t) \end{cases} \tag{2.2.1}$$

The non-linear system in (2.2.1) can be seen as initial value problem with

$$S(0) = S_0 \geq 0, \tag{2.2.2}$$

$$I(0) = I_0 \geq 0, \tag{2.2.3}$$

$$R(0) = R_0 \geq 0. \tag{2.2.4}$$

The assumptions of homogeneous uniformly mixing population (1.), contact rate proportional to the population size (2.), and exponentially distributed recovery rate (3.) are unrealistic. Nevertheless, important conceptual results can be deduced from this simple model.

The SIR model is successful in predicting the behavior of epidemics ff applied to many recorded cases of infection. In fact, the so-called McKendrick-Kermack threshold theorem states that an infection outbreaks if and only if the basic reproduction number is bigger than 1. The basic reproduction number, R_0, is the average number of secondary infections produced when one infected individual is introduced into a fully susceptible population. In other terms, McKendrick and Kermack prove that the no epidemic occurs for $R_0 < 1$, while the epidemic affects a substantial fraction of the population when $R_0 > 1$. The case of $R_0 = 1$ corresponds to the endemic state, for which the disease is maintained in a population (Kermack and McKendrick, 1932).

The SIR model assumes recovered individuals get permanent immunity to the disease. If recovered individuals can become again susceptible to the disease, they are reintroduced into the compartment S. This situation corresponds to the SIRS epidemic model, in which individuals can transfer from class R to class S at rate γ due to immunity loss.

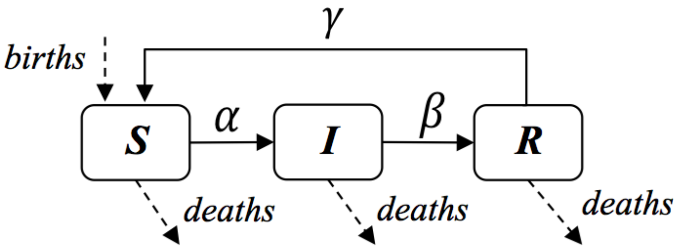


Figure 2.1: Transfer diagram for the SIRS model

Figure 2.1 depicts the transfer diagram of the SIRS compartmental model. Note that there is a inflow of new born individuals to the class S and outflows of dead people from any compartments. This is because demographic effects cannot be ignored when the time scale of the disease spreads is not much faster than the timescale of births and deaths. Thus, the McKendrick and Kermack assumption of homogeneous uniforming mixing community can be removed by taking into account a varying population size. The so-called “vital dynamics” is discussed for the SIS and SIR epidemic models in (Hethcote, 1989).

Demographic models describe changes in birth and mortality rates according to the age distribution of the total population over time. In fact, age-structure is a main focus of vaccination programs because risks of infection is often related to age. Age-dependent mixing models include both time t and age a as independent variables to define the force of infection (Anderson, 1991).

(Anderson, 1991) highlight how the McKendrick and Kermack threshold theorem plays a crucial role for subsequent developments in the study of epidemic dynamics. The authors remove the assumption of constant contact rate and describe various types of heterogeneity in the processes that determine transmission between infected and susceptible individuals. This is a relevant concept to model sexual-transmitted diseases, such as HIV and AIDS.

Early studies on how the variability in sexual activity influence the magnitude of epidemics refer to (Hethcote and Yorke, 1984) and (May and Anderson, 1987). A comprehensive review of deterministic models for HIV and AIDS transmission dynamics is given by (Akpa and Oyejola, 2010). (Akpa and Oyejola, 2010) conclude that such epidemic models provide valuable insights on average epidemic behavior at the population scale with no much data required. However, deterministic models do not take into account random variables and uncertain risk factors.

Stochastic Models

Stochastic epidemic models represent a major generalization of deterministic epidemic models. They incorporate randomness and uncertainty in parameter values and the final number of infectives. More precisely, the response variables are a family of random variables indexed by time so that the epidemic is basically a stochastic process.

Additional questions can be addressed with stochastic models; for example, what is the probability of a major outbreak? Stochastic effects also play a crucial role in questions of recurrence and extinction of infections (Isham, 2008). That is, under what conditions does a small initial number of initial infectives invade an almost entirely susceptible population? And if it does so, when does the infection persist and become endemic?

In mathematical terms, stochastic models are formulated as Markov chains which enable to consider bias and standard errors in parameter estimation from real data of the disease spread.

The simplest stochastic epidemic model was formulated by Lowell Reed and Wade Frost in 1928 in a series of lectures (unpublished). The Reed-Frost model describes the evolution of an infection by generations t which independently infect each susceptible individual with some probability p. Then, infected individuals constitute generation $t+1$ and individuals in generation t are removed from the epidemic process.

While the Reed-Frost model is a discrete-time model, later studies refer to continuous time stochastic models. A survey on stochastic epidemic modeling is (Britton, 2010). The author proposes the stochastic counterpart of the SIR epidemic model of (Kermack and McKendrick, 1927).

In general, the stochastic SIR model assumes a population of size N such that $S + I + R = N$ is constant at any time and (S_t, I_t, R_t) is the current state at time t. In a stochastic terms, an infection corresponds to the simultaneous transitions $S \to S-1$ and $I \to I+1$. In the time interval $[t, t+\Delta t]$, the probability of an infection is $\alpha^{SI}/_{N}\Delta t+o(\Delta t)$. (See (Greenwood and Gordillo, 2009) for more details).

Assuming that infected individuals recover with rate β, the probability for a recovery, i.e. $I \to I-1$ and $R \to R+1$ in $[t, t+\Delta t]$, is $\beta I \Delta t + o(\Delta t)$. Because $R = N - S - I$, it is enough to consider the process (S_t, I_t). Hence, the probabilities of an infection and of a recovery during the time interval $[t, t + \Delta t]$ are as follows:

$$P((S_{t+\Delta t}, I_{t+\Delta t}) - (S_t, I_t) = (-1, 1)) = \alpha \frac{S_t I_t}{N} \Delta t + o(\Delta t), \tag{2.2.5}$$

$$P((S_{t+\Delta t}, I_{t+\Delta t}) - (S_t, I_t) = (0, 1)) = \beta I_t \Delta t + o(\Delta t), \tag{2.2.6}$$

with the complementary probability

$$P((S_{t+\Delta t}, I_{t+\Delta t}) - (S_t, I_t) = (0, 0)) = 1 - \left(\alpha \frac{S_t}{N} + \beta \right) I_t \Delta t + o(\Delta t). \tag{2.2.7}$$

This model is known as the *general stochastic epidemic* introduced by (Bartlett, 1949). The epidemic process is described by stochastic equations in which increments S_t and I_t can be expressed as their expected values plus a sum of centered increments. In formulas,

$$\Delta S = S_{t+\Delta t} - S_t = -\left(\alpha \frac{S_t I_t}{N} \right) \Delta t + \Delta Z_1, \tag{2.2.8}$$

$$\Delta I = I_{t+\Delta t} - I_t = \left(\alpha \frac{S_t I_t}{N} - \beta I_t \right) \Delta t - \Delta Z_1 + \Delta Z_2, \tag{2.2.9}$$

where ΔZ_1 and ΔZ_2 are conditionally centered Poisson increments.

Dropping the terms ΔZ_1 and ΔZ_2 and if Δt goes to zero in Equations (2.2.8) and (2.2.9), the resulting system of ordinary differential equations defines a deterministic model. Note that the solution of the deterministic equations is not simply the mean of the stochastic process as consequence of the non-linearity of the transition rates of the stochastic model. Nevertheless, the deterministic solution is a good approximation to the stochastic mean of a major outbreak when N is large. Comparisons between stochastic and deterministic models can be found in (Allen and Burgin, 2000).

With a major focus on AIDS/HIV, further discussions on continuous time stochastic epidemic models can be found in (Isham, 2008). The author investigates the effects of population heterogeneity on patterns of spread and persistence of sexually-transmitted disease. Also, (Wai, 2000) conducts a comprehensive study on stochastic epidemic modeling for HIV pathogenesis.

Compartmental models assume a fully mixing population can be extended to stochastic variants which consider a random mixing population weighted by sexual activity. However, (Anderson, 1991) states that this is still a crude assumption; more realistic epidemic models would need to identify “who mixes with whom”. This issue turns into a call for the use of networks in epidemiology.

Network Models

In real life, an infected individual does not have the same probability to infect all the others. Effects of age structure and population turnover in the contact rate have been considered by both deterministic and stochastic models. However, all traditional epidemic models lack of a network topology to characterize different types of individuals according to social, behavioral, and other factors (Newman, 2002).

Three comprehensive review works are selected (i.e. (Keeling and Eames, 2005), (Danon et al., 2011), and (Kuperman, 2013)) to provide an overview of research patterns and modeling efforts to explore the links between network theory and epidemiology.

The science of networks has its grounds in the fields of graph theory and social science. Social network analysis studies how connections among individuals change according to the rule of social dynamics (Morris, 1993). The mathematical description of network structures and proprieties is the main focus of graph theory (Erdös and Rényi, 1959). In graph theory a network is defined as set of “nodes” connected by “edges”, while social literature refers to “actors” and “relations”between actors. Basically, the same idea is transferred to epidemiology by defining a network of “individuals” and “contacts” between them. Overall, mathematical epidemiology combine the formalism of graph theory and concepts of social science to study contact dynamics.

The recognition that connections between individuals, which allow an infectious disease to propagate, naturally define a network traces back to mid-1980s with the rise of AIDS/HIV worldwide. Pioneering studies in this context were done by (Klovdahl, 1985) and (May and Anderson, 1987).

First examples on how to use mathematical concepts and observations of social behavior to generate contact networks are provided by (Anderson, 1991). The idea is to describe the population mixing through an adjacent matrix P with mixing probabilities $p(i, j)$, which describe the proportion of the contacts of an individual i with an individual j. Elements of the matrix P are subject to the following constraints:

$$0 \leq p(i,j) \leq 1, \tag{2.2.10}$$

$$\textstyle\sum_i p(i,j) = 1, \tag{2.2.11}$$

$$p(i,j) = p(j,i). \tag{2.2.12}$$

The proprieties 2.2.10 and 2.2.11 follow by definition of probability. The third propriety 2.2.12 states that connections are symmetric, i.e. the infection can pass either ways across a contact. (Anderson, 1991) prove how distribution of sexual activity change over time according to the mixing matrix P under different constraints (random, preferred, and complex choice mixing).

This theoretical result on sexual mixing networks highlights the important role of network structure to understand epidemic dynamics. However, approximations are still far from real mixing among individuals and it often refers to relatively small-scale communities.

With the attempt to describe the real diffusion dynamics of a disease, researchers gather data with three main techniques (Mossong et al., 2008):

- *Infection tracing* to build a tree-like network consisting of all the directional links from infected individuals to whom they transmitted the disease.
- *Contact tracing* to identify a contact network by tracing all potential relationships between individuals.
- *Diary-based tracing* to gather detailed information by recording contacts real-time.

An alternative source of information comes from the recorded movements of individuals. Experiments to model movement networks are currently conducted to model movement of individuals in airline transportation networks (Hufnagel et al., 2004), movement of dollar bills to infer people (Brockmann et al., 2006), and movement of livestock (Robinson et al., 2007). Nevertheless, trying to trace a real contact network requires deep knowledge at individual level and difficulties arise therefore during the data collection process.

As the lack of proper information turns into several limitations of the network being sampled, researchers construct network simulators to match available data with observed social characteristics (e.g. (Halloran et al., 2002)).

Rather than simulated networks, epidemiologists observed that theoretical constructs are needed to identify network structures and proprieties. Mathematically, network epidemic models refer to the "neighborhood" of each individual (i.e. a node) as the set of contacts (i.e. edges) that the individual has. The size of such neighborhood is the "degree" k (i.e. number of contacts that an individual has). The "degree distribution" is defined as a set of probabilities $P(k)$ that a node chosen at random will have degree k. The degree distribution $P(k)$ captures heterogeneity in individuals' potential to become infected and cause further infections. In particular, $P(k)$ influences the recovery in a way that breaks the classical result of Kermack and McKendrick on epidemic thresholds in particular cases.

On the basis of the seminal SIAM review of (Newman, 2003) on structure and proprieties of complex networks, (Danon et al., 2011) describe fundamental network measures in epidemiological context. Relevant to mention are the n-th moment of $P(k)$, distance between nodes, betweenness centrality, and clustering coefficient. In particular, clustered networks formalize the notion of "communities" which are groups of highly connected individuals in a population. Although a few studies focus on community structures, they have high impact on the transmission process. In epidemiology, (Newman, 2003) analyze the concept of community in terms of modularity measure. Computer science literature presents the conductance as valuable measure for cluster structures in large networks (Leskovec et al., 2009).

With respect to network topology, (Newman, 2002) states that the standard SIR epidemic model can be solved on a large variety of networks. (Keeling and Eames, 2005) shows this result for five common families of epidemic networks.

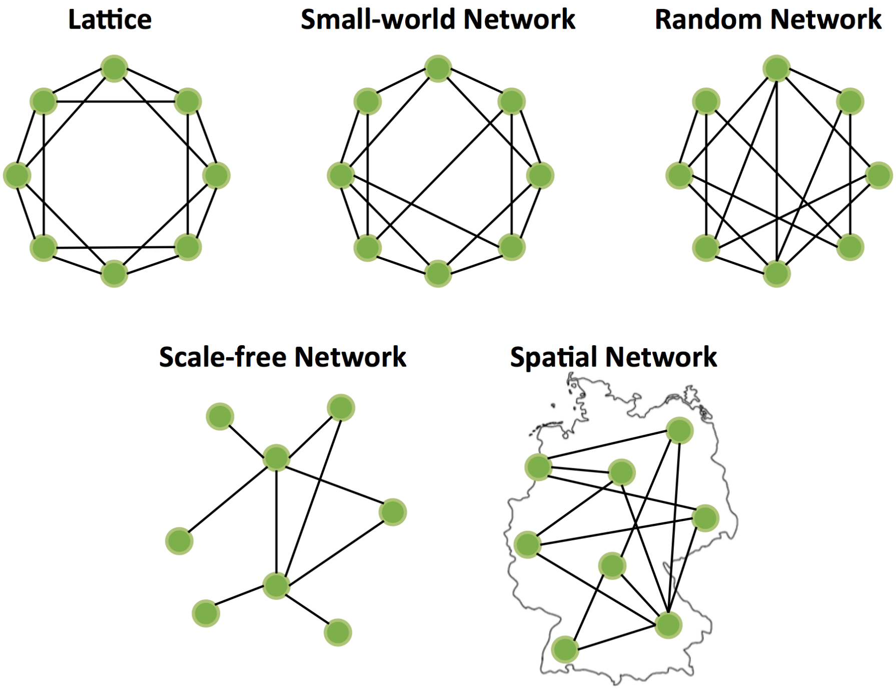


Figure 2.2: Five families of networks used in epidemiology.

Figure 2.2 illustrate the most common types of networks used in epidemiology.

Lattices are networks in which only short-range interactions are possible because the neighbor of each node is reduced to the adjacent nodes. They are usually represented as 2-dimensional grids which define the position of individuals and contacts are localized in space. Such networks are homogeneous at individual level and highly clustered because of the localized nature of connections. The lattice based SIR models have threshold conditions for which the epidemics can just remain localized around the initial focus or turn into a pandemic, similar to, e.g., forest fire models.

A *small-world network* is a mathematical graph in which most nodes are not neighbors of one another, but most nodes can be reached from every other node by a small number of steps. The concept of "small-world" was introduced in 1967 by (Milgram, 1967) to describe topological characteristics of social relationships and communities. In fact, changes in the social topology lead to dramatic changes in behavior of epidemics (Kuperman, 2013). (Watts and Strogatz, 1998) introduce a method to construct networks that mimic features of social architecture by randomly adding long connections to a lattice. The degree of disorder is defined by a rewiring parameter that ranges from 0 to 1, which correspond to lattice and random network respectively. As the rewiring parameter increases, the system transits from an endemic state to periodic oscillations in the number of infectives.

Random networks are the other extreme of the rigid lattice structures. They lack of clustering and have short path lengths. Connections are randomly distributed and the spatial position of individual is not considered. A pioneer work on random graphs refers to (Erdös and Rényi, 1959). The so-called Erdös-Rényi (ER) graphs are built from a set of nodes connected at random with probability p, which is independent from any other contact. The degree disribution $P(k)$ is binomial and it can be approximated by Poisson distribution when the number of node is large. Newman [25] has shown a different approach using In alternative, a generating function method can be used to construct random networks with arbitrary $P(k)$ (Newman, 2002).

Scale-free networks provide a means to achieve extreme levels of heterogeneity, in which some individuals are highly connected (i.e. the so-called "super-spreader") while others almost isolated. A scale-free network can be constructed with the Barabási-Albert (BA) algorithm (Barabási and Albert, 1999), starting from a core of nodes and dynamically adding new individuals (one node at each step) through a connection mechanism that replicates the choice rules of social contacts. The scale-free degree distribution $P(k)$ follows a power law distribution. In a later application of scale-free models to the Internet topology, (Pastor-Satorras and Vespignani, 2001) demonstrate the absence of epidemic threshold for epidemics solved on scale-free networks.

Spatial networks are graphs generated according to the spatial location of all individuals. Therefore, lattice and small world networks are particular cases of spatial networks. Starting from a set of locations, individuals are connected with a probability given by a connection kernel that usually decays with the distance. Spatial networks generally have a reasonably high degree of heterogeneity and an approximately Poisson degree distribution $P(k)$.

Researchers in social networks are interested in a particular class of network models: the *exponential random graphs*. A characteristic of such models is that the probability of connection between two nodes is independent of the connection between any other pair of distinct nodes. Hence, using Markov Chain Monte Carlo techniques to generate a range of plausible networks, information on network structures can be collected even if the complete network is unknown (Strauss and Frank, 1986).

The majority of the studies on epidemic networks focuses on static networks, in which all edges remain unchanged over time and have equal weight. However, magnitude and duration of contacts are time-dependent factors in real transmission networks. Such dynamics have long-term impacts on real epidemic networks. How to capture the structure of such *dynamic networks* is a substantial challenge of epidemiological modeling.

Towards dynamic networks, *co-evolutionary or adaptive networks* consider the dynamics of social links to determine the epidemic behavior. The idea behind is to model the interplay of two different dynamics with competitive effects, that is epidemics and social reactions to epidemics (Gross et al., 2006). For example, if susceptible individuals learn about the existence of infectious individuals, the first try to avoid the latter. Another example is the case of health policies which promote the isolation of infectious individuals. (Risau-Gusman and Zanette, 2009) show that is possible to completely eliminate a disease by breaking links between susceptible and infective individuals and connecting then each susceptible to a new random neighbor. Hence, contact switching is an effective control strategy in real epidemic outbreaks.

Spatial Models

Spatial Epidemiology is the description and analysis of heterogeneity of infectious diseases. As scientific discipline, it dates back to 1930s, when the parasitologist Pavlovsky used the concept of "landscape epidemiology" to gather three simple observations: diseases are geographically limited, spatial variation lies on physical and biological changes of condition, and these conditions can be mapped to predict disease risk and incidence.

First mathematical insights to the wide field of spatial epidemiology are given by those network formulations that account for spatial location of individuals, i.e. spatial networks (and lattice and small-world networks as particular cases) However, (Kuperman, 2013) argue that is still unclear if such simple formulation can be truly representative.

A review of major approaches used for mapping spatiotemporal dynamics is provided by (Ostfeld et al., 2005). The authors distinguish between models that are spatially implicit and explicit. A promising bridge between ecology and epidemiology seems to be exactly the impacts of landscape structure on epidemiological processes, which (Ostfeld et al., 2005) claim being often neglected so far.

Recent advances in spatial modeling mainly depend on developments of geographical information systems (GISs) and remote sensing to record spatial distribution data (Carroll et al., 2014). An overview of terms and tools for spatial analysis in epidemiology is provided by (Rezaeian et al., 2007). (Lawson, 2013) argue that spatial epidemiology is more important now than ever, with modern threats such as bio-terrorism making such analysis even more complex.

Computational Epidemiology

Research in epidemiology is moving from analytical methods to computer simulation techniques and advanced modeling tools to capture complex dynamics of infectious diseases. *Computational Epidemiology* aims at creating synergies between biology and computer science for a better understanding of epidemics. (Goodman and Meslin, 2014) present a comprehensive overview of best practices and challenges on the use of IT tools in epidemiology.

In general, it has been widely recognized that epidemic spreads do not depend just on the bacteriological nature of pathogens. Transmission dynamics of infectious diseases arise from characteristics of each individual, the social context, policy structures and logistical factors. Multi-level factors characterizing the complex ecology of epidemics are described by (Swarup et al., 2014). With a special focus on human and social factors, (Funk et al., 2010) present a review of studies on how to model the influence of human behavior in epidemic diffusion.

Computational epidemiology represents a challenge domain for multiagent systems and this turns into a call for new technologies and simulation tools able to embed such dynamic complexity into models. Arguments for such methodological shift to complex systems in epidemiology can be found in (Galea et al., 2010).

According to (Luke and Stamatakis, 2012), the major modeling paradigms for system science methods in public health are:

- **Network Analysis**,
- **System Dynamics**,
- **Agent-based Modeling**.

Network Analysis is a research method that lays the foundations in a number of different disciplines and mathematical insights have been presented above (see network models). The development of advanced software for network analysis led to the use of the new science of networks in almost every area of science. However, epidemiologists and other experts in the field do not usually have the mathematical background to understand theories behind such technical tools. User-friendly approaches are largely developed in the context of System Dynamics and Agent Based modeling.

System Dynamics (SD) is a methodology to study the complex behavior of systems (organizational, social, etc.) as result of flows (of people, information, money, etc.) and accumulation of flows that change over time in accordance with interaction of variables within nonlinear feedback loops. SD models are built using simulation software that allows decision-makers to analyze what-if scenarios and evaluate recovery and vaccination strategies in case of epidemics. References on background and opportunities of SD modeling for Public Health can be found in (Homer and Hirsch, 2006). Relevant to mention is that SD offers a continuous-time domain of variables to get an aggregated view of the system behavior through a set of differential equations underlying the model. Differently, Agent-Based models the real world as a set of behaviors of agents.

Agent-Based modeling (AB) is a decentralized and interaction-oriented modeling approach. This means that infection dynamics are the result of a variety of events determined by the behavior of single individuals (i.e. agents). (Patlolla et al., 2006) survey of the state-of-the-art in AB modeling to empathize its unique features for coping with the emerging area of Computational Epidemiology. Comparisons of SD and AB simulation models applied to epidemics can be found in (Bagni et al., 2002).

A fourth computational approach refers to the so-called *Synthetic information methods*. Synthetic information methods are sophisticated agent based models able to provide realistic approximations by combining multiple data sources that cannot be gathered through surveys or other methods. In this direction, (Marathe and Ramakrishnan, 2013) developed the Synthetic Information Environments (SIEs) approach, that consists of four components: statistical models of the host population (i.e. synthetic population), activity based models of the social-contact network, disease-progression models, and models for evaluating interventions and individual behavioral adaptions.

2.3 Cyber Epidemics Modeling

Many researchers attempt to understand complex phenomena of different natures by leveraging on lessons learned from biological systems. As any complex system, biological systems are dynamic, evolving, self-organized, highly complex, and continuously adapting to an ever-changing environment. Therefore, analogies with biological concepts are extremely helpful in understanding complexity and uncertainty of other system in crisis situation.

At large, this section aims at emphasizing research efforts that focus on drawing the parallel between biology and the virtual world. In the specific case of epidemics, models of transmission of infectious diseases have been inspiring and highly contributing to understand newer, but not less dangerous, crisis situations such as the spread of computer virus and related cybersecurity problems. The abstraction from details of biological pathogens makes it possible to apply these models into disparate fields. A pioneering example is the close collaboration between sociologists and epidemiologists in Social Network Analysis (Morris, 1993). In the context of Computer Science, (Meisel et al., 2010) present a comprehensive taxonomy of studies in which biological concepts are successfully applied to computer networking.

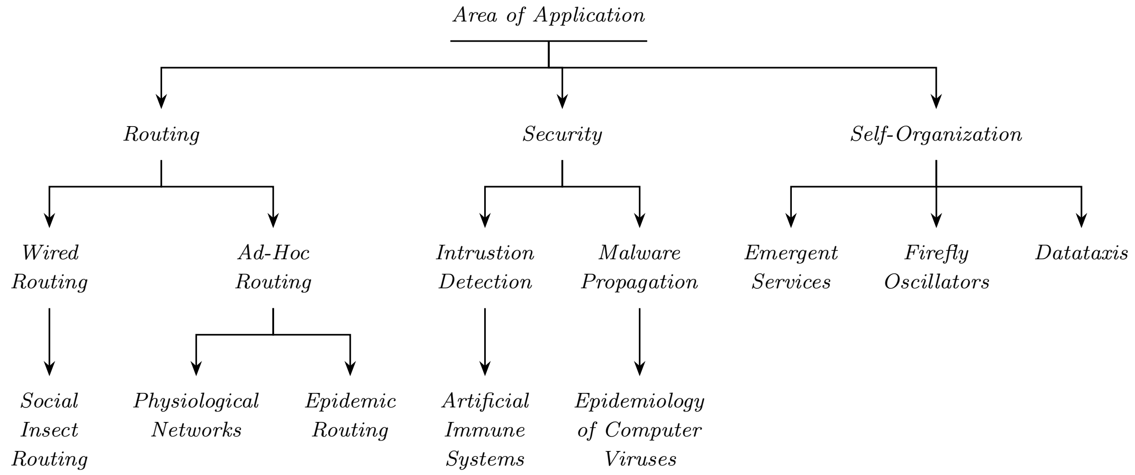


Figure 2.3: Taxonomy of computer network research inspired by biology (Meisel et al., 2010)

Figure 2.3 illustrates the classification of research programs in life sciences organized by respective areas of application in computer network research.

Concerning *computer routing*, literature shows relevant applications of the so-called "epidemic algorithms" to the spread of desirable information through wireless and mobile ad-hoc networks. An example is the epidemic routing for MANET networks (Vahdat and Becker, 2000). Other research works use the concept of *self-organization* of "cyberentities" with biologically inspired proprieties to build distributed systems. An example is the pioneering work by (Wang and Suda, 2001). The authors describe the Internet architecture as a set of interconnected nodes (i.e. cyber entities) with different capabilities to provide a service to the users, and characterized by bio-life cycles of reproduction, dead, and mitigation across the network topology.

In line with the objectives of this dissertation, of particular interest is to explore how epidemiology is applied to the field of *computer security*. See (Meisel et al., 2010) for further references on biological applications to computer network routing and self-organization.

(Meisel et al., 2010) define the application of epidemiology to malware propagation and intrusion detection in computer networks as the strongest of all the biological connections. First pioneering efforts to draw parallels between epidemics and the spread of computer viruses refer to (Murray, 1988). Later, two researchers of IBM (Kephart et al., 1993) model the spread of computer viruses on networks as SIS epidemic model. The authors demonstrate the high impact of network topology on dynamics of spread by studying different directed-graph models in which susceptible nodes become infected only if there is a connecting edge from any infected node to the susceptible ones. In 1993, experts of IBM (Kephart et al., 1993) provide the first detailed description towards constructing a theory for computer security based on epidemiological concepts.

Nevertheless, (Pastor-Satorras and Vespignani, 2001) argue that the widely used SIS epidemic models of computer virus are very instructive but not completely adequate to represent the real phenomena. Analyzing real data of computer viruses infections, (Pastor-Satorras and Vespignani, 2001) model the Internet topology with the particular class of scale-free networks. A very surprising result of their study is the absence of an epidemic threshold and associated critical behavior on scale-free networks. Such epidemiological framework changes many conclusions of the traditional threshold theory of (Kermack and McKendrick, 1927), and it contributes to understand particular diffusion phenomena of social, biological and communication systems.

The rapid growth of computer networks led to higher complexity of network structures as well as an increasing number of sophisticated computer viruses spreading on such computer networks. Epidemiological approaches are adapted to "cyberepidemics" modeling with little modification and much success (Meisel et al., 2010). For instance, (Zou et al., 2002) use the SIR epidemic model to analyze the Code Red worm propagation. The SAIR model, proposed by (Piqueira and Araujo, 2009), is a modified version of the deterministic SIR epidemic model that includes the antidotal population compartment A, to study the network operational state and its recovery time when subject to perturbations. (Yang and Yang, 2012) study stochastic SLBS models, which consider infected computers divided in two classes on the basis of different probabilities to get treatment, i.e. breaking-out computers B, and latent computers L. The SEIQRS model analyze the effect of quarantine Q, on recovered nodes R (Mishra and Jha, 2010).

Beyond theoretical results, engineering approaches are used to demonstrate the accuracy of analytic results through experiments on real and synthetic networks, see e.g. (Wang and Chakrabarti, 2003). The authors propose the epidemic threshold as function of a single parameter, named the eigenvalue, which define the virus propagation proprieties.

According to the taxonomy in Figure 2.3, there is another stream of literature on computer security that focuses on malware detection and prevention rather than modeling the diffusion process. First research efforts in "computer immunology" refer to (Forrest et al., 1997). The author describes an artificial immune system comprehensive of three standard phases occurring in both biological and cyber systems: infection, recognition, and destruction of the virus. These basic functions correspond to the description of an ideal Intrusion Detection System (IDS), which was then designed and implemented by (Kephart, 1994) for the first time.

Similarly, modeling insights of immunization and vaccination strategies of infectious diseases are also applied to epidemiology of computer viruses. E.g., (Madar et al., 2004) analyze the effects of random, acquaintance, and targeted vaccinations on epidemic dynamics by solving the SIR model on complex networks, in particular, scale-free networks (that is the Internet topology, see (Pastor-Satorras and Vespignani, 2001)).

Thus, the same concepts are used by (Huang, 2012) to evaluate new security policies for eradicating computer viruses in networks. Emphasizing limitations of analytical approaches, (Wang et al., 2000) propose a simulation study to investigate effects of random and selective immunization on different network topology. (Fu et al., 2008) introduce other immunization schemes on scale-free networks with nonlinear infection dynamics.

Overall, literature shows that security threats in networked systems arise many issues that epidemiology has encountered and resolved. Nevertheless, it was only 1998 when a major expert of the IBM research group emphasized the existence of open problems and announced that evolving technologies would have generated a plenty of new problems to solve in the field of computer security (White, 1998).

Biological epidemics modeling provides solid research pillars to study complex phenomena of spread and recovery in networked systems. However, a lot of work needs to be done to understand dynamics of complex cyber crises daily affecting critical infrastructures.

2.4 Critical Infrastructure Interdependencies

As business operations have come to increasingly rely on information technology (IT), modern infrastructures have become increasingly interconnected. Consequently, the risk that even minor disruptions in a single CI can lead to a catastrophic cascade of failures in CI networks is increasing (Buldyrev et al., 2010).

Increasing is also the attention posed by governments on CIs and their interdependencies. This stimulates many researchers to develop innovative approaches for the identification, description, and modeling of such interdependencies between CIs. (Rinaldi et al., 2001) argue that an infrastructure cannot be considered as system isolated from other CIs because interactions with the environment extremely determine the CI. First definitions of dependency and interdependency between CIs are then provided as follows.

> "A *dependency* is a linkage or connection between two infrastructures, by which the state of one infrastructure influences or is reliant upon the state of the other."

> "An *interdependency* is a bidirectional relationship between two infrastructures in which the state of each infrastructure influences or is reliant upon the state of the other."

In general, researchers use either dependency and interdependency to describe the concept of direct link from an infrastructure to another according to specific criteria, e.g. (Porcellinis et al., 2008),(Nieuwenhuijs et al., 2008). (Note that the notation adopted in this dissertation refers to *interdependency* as the direct link from an infrastructure to another, while the term *dependency* is used when the direct link is within the same CI).

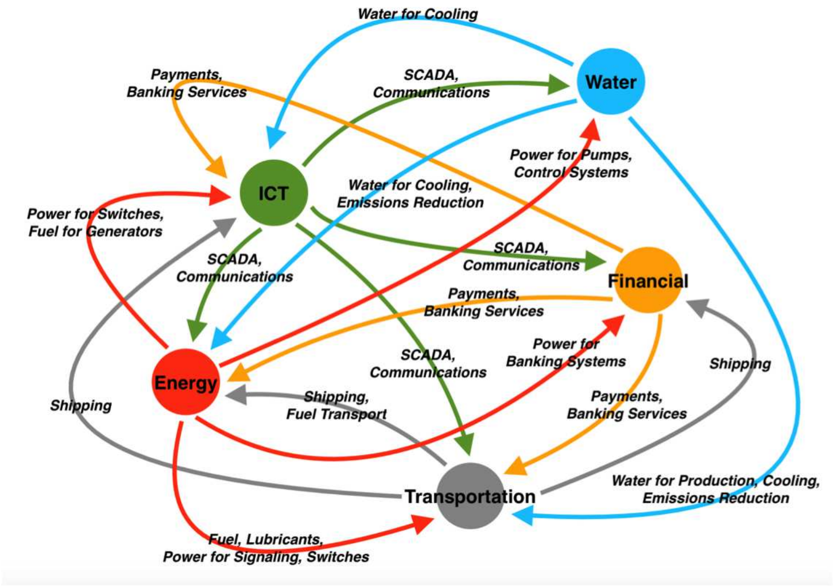


Figure 2.4: Example of qualitative description of interdependencies (Canzani, 2016b) - Adapted from (Rinaldi et al., 2001)

Adapted from (Rinaldi et al., 2001), Figure 2.4 gives an idea of the qualitative characterization of direct interdependencies on the basis of products and services that CIs provide to each other.

Beyond pioneering works (e.g. (Rinaldi et al., 2001)) that mainly refer to conceptual studies that illustrate the complexity of modeling CI interdependencies, later research efforts focus on "the next step" of determining metrics and mathematical frameworks to quantify impacts of cascades among CIs (Zimmerman and Restrepo, 2006).

The comprehensive review of (Ouyang, 2014) defines the CI interdependency modeling as an immature, but rapidly growing, discipline. A major problem is the lack of publicly available data about CIs, which compels researchers to perform qualitative as opposed to quantitative analyses (e.g. (Popescu and Simion, 2012)). Recently, the understanding of CIs as "system of systems" (Eusgeld et al., 2011) and "network of networks" (Gao et al., 2014) leads to deeper quantitative investigations of dependencies within a CI and interdependencies across CIs. However, the complexity of interdependency modeling often limits many studies to consider only a single infrastructure (O'Reilly et al., 2007) or a few of them (Eusgeld et al., 2009).

Overall, qualitative approaches provide insightful characterizations of CI interdependencies which guide further research towards a quantitative understanding of cascade effects across CIs. It follows a review of the literature on qualitative and quantitative approaches to CI interdependencies, with a special emphasis on modeling and simulation techniques.

2.4.1 Qualitative Approaches

Conceptual frameworks aim at identifying and defining CIs and their interdependencies. The seminal work of (Rinaldi et al., 2001) introduces a taxonomy that frames in six “dimensions” the major aspects of interdependencies as follows.

- **Types of interdependencies**, classified in *physical*, *cyber*, *geographic*, and *logical* interdependencies based on their own characteristics and effects on infrastructure agents.

- **Infrastructure environment**, that is the framework in which operators establish goals, define their businesses, and make decisions in accordance with *economic*, *social*, *legal concerns, public policy*, *government decisions*, *technical* and *security issues.*

- **Coupling and response behavior** among CIs in case of perturbations, characterized by a certain *degree* and *order* of coupling, *linearity* or *complexity* of the interactions.

- **Infrastructure characteristics**, such as *spatial* and *temporal scales* emerging from CI components, *operational* and *organizational factors* that depend on the role of a specific CI.

- **Types of failures**, which help to determine the damage propagation based on the nature of disruptions (i.e. *cascading*, *escalating*, or *common cause* failures).

- **State of operation**, which is a function of interrelated factors and system conditions at any point of time.

These dimensions offer valuable insights to raise a wide number of research questions, empathizing that researchers must cope with the complexity of CI interdependencies in the attempt to solve open issues. The need of a new conceptual framework and extended analytical tools is discussed in (Kröger, 2008). Recently, (Popescu and Simion, 2012) identify new criteria to define CI interdependencies. A summary of interdependency types defined by different scholars and their evidence is provided by (Ouyang, 2014).

Beyond academic papers, a valuable source of qualitative studies refers to governmental reports describing strategies to protect CIs. For example, the U.S. Department of Homeland Security periodically issues a National Infrastructure Protection Plan (NIPP) to define sector specific strategies as well as nation resilience objectives (see e.g. (DHS, 2009) and (DHS, 2013)). In Europe, the work of ENISA highly contributes to the development of a unified EU framework for CI operators based on critical services and sectors (ENISA, 2014).

Despite detailed descriptions of CI protection strategies and ambitions of coordinated response among national CIs and across boarders, governments do not address modeling and simulation approaches to support decision-making processes in such technical reports.

2.4.2 Quantitative Approaches - Modeling and Simulation

A recent review of modeling and simulation approaches to evaluate interdependent infrastructure systems is conducted by (Ouyang, 2014). The author categorizes existing approaches into six types as shown in Table 2.2.

Table 2.2 presents a comparison of modeling and simulation approaches used to explore the CI interdependency according to how many input data are needed and whether it is easy to get access to them. This is because the relevance of a quantitative modeling approach also depends on the availability of data which are necessary to run simulation and then conduct a proper analysis of simulation results. The number of articles found in literature provides insights on the maturity level of each methodology: few prototype applications if less than 5 articles and with successful real-world applications in case of more than 20 publications. Finally, approach contributions to specific aspects of the concept of resilience are highlighted. Note that definitions and further reference literature on CI resilience are discussed in Chapter 4.

Studies that analyze data of historical crisis situations and expert experience refers to **empirical approaches**. (McDaniels et al., 2007) propose an empirical framework to quantify societal interdependent disruptive effects in CIs on the basis of societal impacts. The framework is also applied to analyze the North American blackout in 2003. An other example of database accounting for interdependent failure incidents in European CIs is (Luiijf et al., 2008).

Although empirical approaches support the identification of significant failure patterns and empirically-based risk analyses, the results highly depend on empirical data collected and may not give good prediction for disasters of different nature. More general insights towards the quantification of interdependency indicators are provided by CI expert surveys (see, e.g., (Laugé et al., 2015)), but it is still a challenge of how to associate this empirical indicators with simulation models.

A modeling paradigm which is widely used to analyze the the complexity of CIs is **agent-based (AB) modeling**. This is a bottom-up approach which assumes that complex dynamics arise from single interactions among CI components (i.e. agents of the system). Many national laboratories uses agent-based approaches to develop decision-making tools for CI operators, such as the CIMS (Critical Infrastructure

Modeling Approach	**Sub-approach**	**Quantity of Input Data**	**Accessibility of Input Data**	**No. of Articles**	**Resilience Improvements (sample)**
Empirical		Medium, Large	Medium	$5-20$	Restoration, Backup
Agent-based		Large	Small	> 20	Stakeholders Knowledge
System Dynamics		Medium, Large	Medium	> 20	Management
Economic Theory	Input-Output	Medium	Large	> 20	Backup, Restoration, Cascade Prevention
	Computable General Equilibrium	Large	Medium	5-20	Absorptive capacity, Restoration
Network Theory	Topology-based	Small, Medium	Medium	> 20	CI topology
	Flow-based	Large	Small	> 20	Communication Channel, Sensor network
Others	Hierarchical holographic	Large	Small	< 5	Management
	High level architecture	Large	Large	< 5	Resistant, Absorptive, Restorative Capacities
	Petri-Nets	Medium, Large	Medium	$5-20$	Cascade Prevention
	Dynamic Control System	Medium, Large	Small	< 5	Comm. Systems, Cascade Prevention
	Bayesian network	Medium, Large	Small	< 5	Comm. Systems, Cascade Prevention

Table 2.2: Classification of modeling and simulation approaches compared from several criteria - Adapted from (Ouyang, 2014)

Modeling System) framework proposed by the Idaho National Laboratory (Dudenhoeffer et al., 2006).

AB approaches enable to analyze scenarios with all interdependency types among CIs via discrete-event simulations. However, quality of results strictly depend on agent behaviors which are often difficult to model due to the lack of available data.

As opposed to AB modeling, **system dynamics (SD) based methods** adopt a top-down approach to explore interdependent complex adaptive systems such as CIs. SD models are stock-and-flow diagrams which capture the aggregated system behavior through nonlinear feedback loops. Causes of disruptions, what-if scenarios, and effects of policy and design are analyzed via continuous time simulations. For instance, (Karaca et al., 2015) study the sustainability of a combined water and energy infrastructures. (Vugrin and Camphouse, 2011) focus on CI resilience assessment through control design.

A successful application of SD to study CIs is the CIP/DSS (Critical Infrastructure Protection/Decision Support System) simulation tool built in a joint collaboration of several national laboratories (Brown et al., 2004). Relevant to mention is the application of the CIP/DSS to a specific scenario of epidemic outbreak (Fair et al., 2007). The US government, through the National Infrastructures Simulation and Analysis Centre (NISAC), collects data of all US infrastructures for a detailed analysis using multiple modeling approaches (Brown, 2007). However, most of NISAC activities are not publicly available. Data access problems and the inability to analyze topology changes and component-level dynamics are major limitations of SD approaches.

Input-output models are the most popular **economic theory based approaches** used to model CI interdependencies. The main characteristic of economic input-output flow models is to connect the inability of CIs to produce as planned (i.e. inoperability) with demand perturbations (Haimes et al., 2005). A pioneering work is the Leontief input-output inoperability model (IIM) proposed by (Haimes and Jiang, 2001).

Input-output models are formulated as system of linear equations that describes flows of commodities among CIs and often do not consider the time-dependence. Linearity of relationships between CIs and absence of time components are limitations which can be overcome with the economic theory of *computable general equilibrium* (CGE). E.g. (Rose and Liao, 2005) perform a CGE analysis of economic resilience in case of water service disruptions.

An intuitive way to cope with CI interdependency is to use concepts of **network theory**. Single CIs can be seen as networks, where nodes are different components of the CI (e.g. (Nistor et al., 2017) conduct a network analysis of the transportation network). Similarly, interdependencies between CIs can be described by networks in which each node represents a CI (e.g. the network flow model proposed by (Holden et al., 2013)). In general, modeling criteria for interdependent networks of CIs account for infrastructure topologies (*topology-based methods*) or services delivered by CIs (*flow-based methods*).

When considering topological features and node heterogeneity, CIs performance in case of disruptive events can be evaluated by using different metrics such as number of failed nodes, path length, connectivity loss, redundancy ratio and clustering (Dueñas-Osorio et al., 2007). Time-dependent characteristics of the nodes, such as duration of CI unavailability and lost service hour, can be modeled to analyze system-level functionality (Johansson and Hassel, 2010). However, topology-based methods fail in providing information about flow performance of CIs.

Flows of commodities between CIs are captured by the so-called network flow models. For instance, (Oh et al., 2010) propose a disaster impact analysis based on two measurement factors: level of service and level of inter-relationship. The first assesses the damage of the disrupted infrastructure; the latter identifies how industries depend on adjacent infrastructure for sustaining their activities. However, network flow models do not consider dynamics within a single node (i.e., the CI). Studies based on network flow principles often consider a limited number of CIs due to the complexity of modeling detailed operation mechanisms of each infrastructure. An example is the connectivity model proposed by (Svendsen and Wolthusen, 2007) to capture production and consumption of power grid, telecommunication, and gas infrastructures.

Similar to network based approaches, *Petri-Nets* (PN) modeling allows to represent the network of CIs in terms of places, transitions, and mapping functions between them. Interdependencies are then simulated as flow of 'tokens' through the network (Beccuti et al., 2012). Probability of cascade failures can be modeled with *Bayesian Networks* (BN), but BN approaches only provide a static model of the system at each time instant (Di Giorgio and Liberati, 2011). Of interest is the work of (Eusgeld et al., 2011), which builds on the concept of "system-of-systems" by introducing a *high level architecture* (HLA) to model the layered structure of CIs (from the single CI to the system of CIs). Other approaches are *dynamic control system theory* (DCST) and *hierarchical holographic modeling* (HHM), which are difficult to apply due to their mathematical complexity. See (Ouyang, 2014) for more details on these approaches.

Extended reviews with technical details on applications and existing modeling and simulation tools to analyze interdepedencies of CIs systems are provided by (Pederson et al., 2006) and (Yusta et al., 2011).

2.5 Cybersecurity Landscape

In recent years, computer security research communities have made clear that "the threat landscape is an extremely fast-moving environment. It is essential for our society to be prepared and for our businesses, governments and research institutions to innovate faster than criminals and other actors with malicious intents" (Choo, 2011).

This is because hackers proved to have a high degree of success in exploiting Industrial Control Systems (ICSs), which are the hardware and software packages that control and monitor physical CIs like power plants, factories, and city infrastructure (Magazine, 2016). The Stuxnet attack is one of the most famous example of cyber threats that target ICSs and was responsible for causing substantial damage to the Iranian nuclear program (Zetter, 2014).

Intel Security experts argue that one of the biggest challenges in protecting infrastructures is having to cover any possible attack vector while attackers only need to find one week point (Intel Security, 2015). In order to develop effective responses, Scott Brandt (CIO and director of IT, Texas Office of the Secretary of State) suggests that organizations must partner to coordinate security awareness plans rather than solely implementing technology solutions in the network perimeter (Brandt, 2016).

Recent studies and tools to improve the understanding of such extended cyber threat surface refer to:

- **Threat analysis**,
- **Threat modeling**,
- **Traffic network analysis**,

Expert of IBM define a cyber threat analysis as the process of matching the knowledge of internal and external information vulnerabilities of an organization to real-world cyber attacks (Ayoub and Richmond, 2016). At large, this approach is part of the cyber risk assessment procedure described by (SANS, 2002). Sandia Laboratories present a framework for comprehensive threat analysis in the energy CI that includes the identification of adversary characteristics, adversary intent, and possible attack vectors (Duggan and Michalski, 2007). The final purpose of threat analysis is to provide a means for mitigation strategies and best practices on how to maximize CI protection.

In Germany, the Federal Office for Information Security (BSI, which stands for Bundesamt für Sicherheit in der Informationstechnik) is responsible for providing standards for the implementation of basic IT protection, management systems, risk analysis, and business contiunity management (BSI, 2017). A comprehensive overview of IT-security concepts, procedures and protocols in the German context is provided by (Eckert, 2013).

At the EU level, of particular interest are standards and guidelines issued by the European Network Information Security Agency (ENISA) towards the definition of cybersecurity (ENISA, 2015), analysis of threat landscape (ENISA, 2016c), cost of cyber incidents in CIs (ENISA, 2016a), and cyber crisis cooperation among Member States (ENISA, 2016b).

As support for the qualitative analysis, threat models have been developed to better explore attack vectors through different techniques. The most popular method is the use of attack trees, which are conceptual diagrams describing possible attack patterns to exploit system vulnerabilities. Details on threat modeling can be found in the seminal book of (Shostack, 2014). The author states that, as discipline, “threat modeling is the use of abstractions to aid in thinking about risks”.

Cyber security situational awareness is also improved via traffic network analysis tools. Latest advances are online interactive maps of cyber threats (Kaspersky, 2017) and connected devices (Shodan, 2017). More precisely, Shodan is the first search engine to find specific types of computers connected to the Internet using a variety of filters. Kaspersky developed a cyberthreat real-time map that depicts malware epidemics in real time, which allows comparing different types of cyberthreats and their distribution worldwide.

Beyond modeling, analysis, and monitoring the threat surface, relevant contributions by cyber security providers concern malware prevention, with a particular focus on advanced persistent threats (APTs). APTs are silent and sophisticated attacks which target machines of specific persons or organizations to steal confidential data. An example is the specific mitigation program against APTs promoted by Kaspersky Lab researchers. They claim that prevention is significantly more effective and more cost-efficient than remediation after an attack. The so-called proactive strategies against APTs are discussed in (Juuso and Takanen, 2012). Further details on cybersecurity countermeasures are discussed in Chapter 5.

2.6 Literature Findings

Three streams of literature have been selected and analyzed to provide solid theoretical foundations for this research. One of them is the well-established field of epidemiology, which offers valuable insights on how to model complex phenomena of spread and recovery dynamics.

The complexity of epidemic modeling increases from compartmental SIR models to social network models which account for relations among individuals as crucial factor to understand epidemic dynamics. Traditional mathematical models are then supported by comuputer simulation techniques and multi-method approaches to explore relevant impacts of heterogeneity on disease spreads.

Among the wide range of applications of epidemic models to disciplines showing biological analogies, mathematical insights from epidemic modeling allow cybersecurity research to quickly move one step ahead. Literature shows that the new persistent threat of computer security has a lot in common with issue that epidemiology has encountered and resolved. Nevertheless, days of modeling spread of computer viruses are gone and recent works on cybersecurity modeling rarely mention their epidemiological roots.

It was only 1998 when a major expert of the IBM research group announced that the evolving technology would have generated a plenty of new problems to solve in the field of computer security (White, 1998). Modern cyberthreats include highly targeted but slowly spreading malware that causes physical damages as, e.g. Stuxnet, and targeted attacks as ransomware and APTs.

As business operations have come to increasingly rely on information technology (IT), modern infrastructures have become increasingly interconnected. Security experts continuously claim the lack of comprehensive methods to cope with this extended threat surface that goes far beyond organizations' boundaries. Research efforts need to be done towards the understanding of such cyber-physical systems, cascading effects between CIs, operational disruption dynamics triggered by cyberattacks, their impacts on business and viceversa.

The investigation of the young body of literature in CI systems points out that existing qualitative and quantitative approaches provide an understanding of the complexity characterizing interdepedencies between CIs. However, applications of modeling and simulation techniques usually focus on few aspects of the CI interdependency problem. The widely used agent-based or network models often refer to one infrastructure or a portion of them. A comprehensive modeling and analysis framework is more desired for applications (Ouyang, 2014).

Overall, research patterns in epidemiology, cybersecurity, and infrastructures' interdependency clearly show similarities and overlaps in methodologies beyond applications. Thus, epidemics modeling consitutes an old - but still open - research domain from which to get mathematical insights and valuable research leads to explore disruptive dynamics and effects of recovery strategies in the relatively new field of cybersecurity of CIs.

Chapter 3

Research Design and Methodology

This chapter describes key mechanisms and processes adopted to conduct the research. This work is an exploratory study of new fields and domains, and it adopts a design science approach following the works of (Hevner and Chatterjee, 2010) and (Baskerville et al., 2009). In this work, the research design can be seen as an iterative process comprehensive of four main iterations. In each research iteration, the focus of modeling and the data used in simulations are different. Iteration by Iteration, modeling techniques are combined together to emphasize different aspects of the dynamics of interdependent CIs.

System dynamics (SD) theory is introduced as main modeling methodology and perspective to capture nonlinear dynamics arising from operational disruptions and cyberattacks to CIs. Dynamic models are then iteratively extended combined together through a block building modeling process. Further discussions concern the rationale behind block building approaches based on SD.

The chapter concludes with an overview of the building blocks of models developed in this work, with a special emphasis on the overall research framework which provides a solid structure for the modeling and the analysis of simulation results.

3.1 Design-oriented Research

In line with research objectives (cf. Chapter 1), a design-oriented approach is selected to conduct an exploratory study of new fields and tools. In fact, the production of new knowledge is one of the major characterizing elements of design-oriented approaches.

Another fundamental challenge of design science is to bridge practice and theory by combining theoretical developments with problem-solving research (Holmstr et al., 2009). This is of particular relevance when academic research interests do not seem to coincide with managerial practices, such as in the field of IT-security.

On the basis of (Hevner, 2007) and (Baskerville et al., 2009), the research design adopted in this work can be described as an iterative process to continuously explore and update research foundations. The goal is to get a better understanding of the state-of-the-art, and to provide then new valuable outcomes iteration by iteration. The final artifact is a set of models and modeling instruments to cope with real-world dynamics.

This iterative process of learning and developing allows to constantly question the research and explore new research directions on the basis of previous research findings. Each iteration includes both qualitative and quantitative approaches to understand, model, and analyze highly dynamic environments.

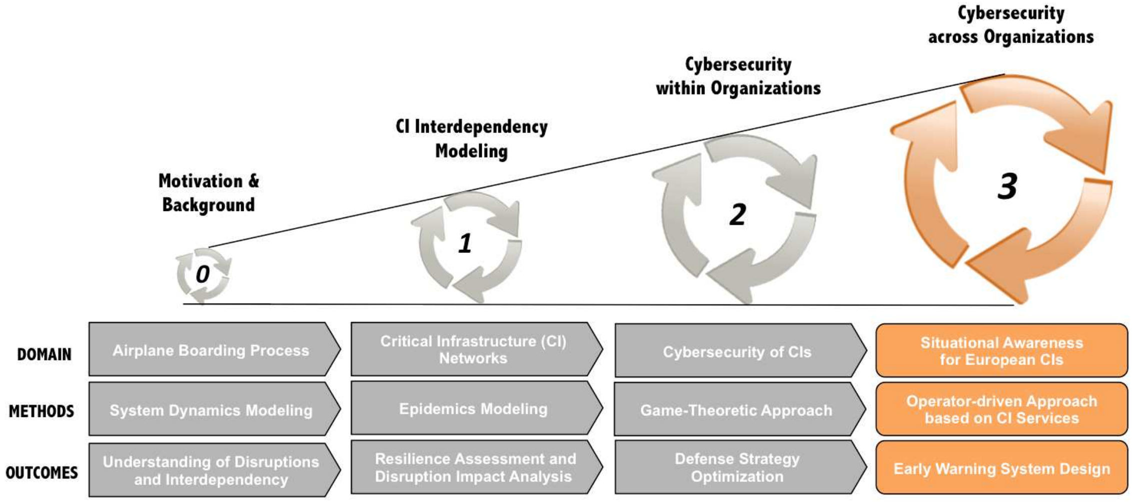

Cybersecurity across Organizations
Cybersecurity within Organizations
CI Interdependency Modeling
Motivation & Background
0
1
2
3
DOMAIN
METHODS
OUTCOMES
Airplane Boarding Process
Critical Infrastructure (CI) Networks
Cybersecurity of CIs
Situational Awareness for European CIs
System Dynamics Modeling
Epidemics Modeling
Game-Theoretic Approach
Operator-driven Approach based on CI Services
Understanding of Disruptions and Interdependency
Resilience Assessment and Disruption Impact Analysis
Defense Strategy Optimization
Early Warning System Design

Figure 3.1: Research iterations

The research design comprehends four main iterations as depicted in Figure 3.1. At large, all iterations aim at developing models which capture disruptive behaviors and dynamics of crisis situations. Application domains, the focus of modeling, and the data used in modeling and simulations are different.

Substantially, each iteration "prepares the ground" for the next one. All the knowledge achieved through previous iterations are used, enriched, and extended in next iterations. This leads to a structured research development process that ranges from theoretical foundations (grey iterations in Figure 3.1) to real world applications (orange iteration in Figure 3.1). Hence, the design-oriented research pattern evolves trough iterations and grows in terms of research relevance and complexity due to combined explorations of new fields and techniques.

In Figure 3.1, the labels underlying each iteration describe the respective application domain, the methodology used, and final outcomes. In line with the rationale behind exploratory studies (Holmstr et al., 2009), the methodology adopted in one iteration is also used in next iterations in combination with new methods to explore more complex dynamics. Also, iteration outcomes provide solid pillars upon which to base further research and therefore extend the body of knowledge through iterations.

More precisely, **iteration 0** refers to the preliminary work done with SD modeling to understand operational disruptions and interdependency between passengers during the airplane boarding process.

Based on literature review findings (cf. Chapter 2), **iteration 1** adopts principles of epidemics modeling to study disruptions and interdependencies in a different application domain which refer to networks of critical infrastructures. Simulation analysis aims at evaluating resilience and disruption impacts.

Iteration 2 builds on the modeling of the previous iteration to explore cybersecurity aspects of CIs by combining game theoretic approaches with SD. Outcomes concern the optimization of defense strategies when the CI is targeted by cyberattacks.

Finally, a real-world application of dynamic interdependency models is presented in **iteration 3**. As contribution to coordination response and situational awareness programs in Europe, the modeling is extended by a perspective of CI operators and the critical services they provide one another. The SD model contributes to the design of an early warning and incident response system for European CIs.

Note that iterations of this design-oriented research overlap with the thesis structure (cf. Figure 1.1). The iteration 0 corresponds to motivation and background discussed in Chapter 1. Contributions to the field of cybersecurity of CIs, i.e. iterations 1, 2, and 3, are presented in Chapters 4,5, and 6 respectively.

3.2 System Dynamics Theory

The theory of dynamical systems represents a major modeling paradigm to investigate coupled dynamics of cybersecurity of CIs over time.

In the attempt to turn the application of engineering concepts to organizational policy studies, Jay W. Forrester defines **system dynamics (SD)** as

> “the study of information-feedback characteristics of industrial activity to show how organizational structure, amplification (in policies), and time delays (in decisions and actions) interact to influence the success of the enterprise” (Forrester, 1961).

After first pioneering SD modeling and simulation efforts to study business and industrial problems (Forrester, 1961), Forrester extends the application of SD to the analysis of world growth dynamics (Forrester, 1971). Other application fields refer to urban, social, ecological, and all types of systems characterized by complex structures and nonlinear processes which make it difficult the use of analytical methods.

As a discipline, SD builds on principles of *General Systems Theory* of (Von Bertalanffy, 1950) and *Systems Thinking* of (Senge, 1990).

In a mathematical perspective, general systems theory is originally defined as

> “the scientific exploration of “wholes” and “wholeness” which, not so long ago, were considered to be metaphysical notions transcending the boundaries of science” (Von Bertalanffy, 1950).

The process of understanding and studying real-world systems as a whole is then supported by principles of systems thinking, for which

> “a system isn’t just any old collection of things. A system is an interconnected set of elements that is coherently organized in a way that achieves something” (Meadows and Wright, 2008).

Thinking in systems is a perspective which enables to recognize that repeated events or patterns derive from systemic structures which, in turn, derive from mental models (Monat and Gannon, 2015).

Such mental models belong to the same class as the computer models used in SD. (Forrester, 2009) argues that SD builds two-way communication between mental models and simulation models, in the sense that a SD model is often built from assumptions made by the mental models. Then, a computer simulation enables to determine the complex behavior resulting from the system structure.

Hence, SD modeling and simulation is used to understand the behavior of complex systems over time when the natural learning process is too long and complex for the human mind.

The dynamic of the system is described as a number of interacting feedback loops and delay structures. Real-world processes are represented in terms of

- **stocks** (or “levels”), which are the variables representing the system at a given time and can be imagined as accumulation of data or materials (e.g. knowledge, people, money, information);
- **flows** (or “rates”) between stocks, which are actions regulating the rate-of-changes of stocks, i.e data or materials going in and out of the stocks;
- **auxiliary variables**, which are information determining the values of the flows;
- **feedback loops**, which are closed-path structures connecting stocks and flows.

Note that the feedback is a transmission of information about the state of a stock to other parts of the system, and it can be direct or indirect due actions of other variables (Landriscina, 2013).

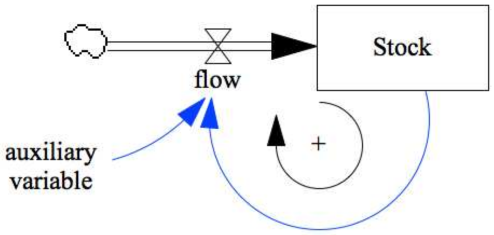


Figure 3.2: The basic elements of system dynamics

Figure 3.2 shows the basic elements of SD modeling and the feedback structures within which all change occur and decisions are made. Blue connectors represent the information arrows which generate reinforcing (+, positive effect on stocks) or balancing (−, negative effect on stocks) feedback loops. Stocks are represented as rectangles and flows as valves on the arrows regulating the input-output data or materials of stocks. Note that clouds represent the sources and sinks for the flows in case they originate or end outside the model boundary.

Stock and flow diagrams have a precise and unambiguous mathematical meaning. Stocks accumulate or integrate their flows. The variation of a stock can be formulated as differential equation, and the value of a stock at any time is obtained by integrating the differential equation itself.

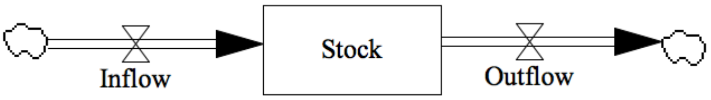


Figure 3.3: General stock-and-flow structure

Accordingly, the general stock-and-flow structure in Figure 3.3 can be described by differential and integral equations, respectively, as follows.

$$\frac{d(Stock)}{dt} = Inflow(t) - Outflow(t), \tag{3.2.1}$$

$$Stock(t) = Stock(t_0) + \int_{t_0}^{t} [Inflow(s) - Outflow(s)]ds. \tag{3.2.2}$$

Graphical representation of SD models makes it easy to evaluate policies also for those who do not have a mathematical background. This research work shows both stock-and-flow representations and mathematical equations underlying them.

The general SD modeling method consists in

(i) building the causal structure of the system by using basic elements to be visually combined in a diagram, and

(ii) using equations and rules to describe the causal relationships among these elements.

SD modeling approaches are used for framing, understanding, and capturing complex behavior of real-world systems over time in terms of stocks and flows, internal feedback loops and delays. In contrast to other simulation approaches such as agent-based or discrete-event simulation, SD abstracts from single events and entities and takes an aggregate view concentrating on policies (Borshchev and Filippov, 2004).

Items in the same stock are indistinguishable and without any individuality. This means that the modeler must think in terms of global structural dependencies and provide accurate quantitative data for them, especially when adopting high levels of abstraction to understand nonlinear dynamics of complex systems such as interdependent CIs.

The literature review in Chapter 2 reveals that SD approaches are already used in the field of CI protection. Existing applications mainly aim to provide support for CI management with a special emphasis on policy modeling (Ouyang, 2014). This research work adopts a different perspective by modeling the operational dynamics within a CI and across interdependent CIs. Then, combinations of SD with other modeling approaches such as network theory and game theory support the analysis of effects of cyber defensive strategies on CI operations as well as the evaluation of protection policies and coordinated response efforts.

Further details on SD theory can be found in the seminal book of (Sterman, 2000).

3.3 Block Building Modeling Approach

Simulation models represent a major advance in the understanding of complex systems. However, the field of simulations often lacks of frameworks to streamline the key processes of systems modeling (Carvalho et al., 2011).

In the context of SD, a five-steps modeling process is presented by (Sterman, 2000) to build consistent models from scratch. The five-steps modeling process guides the modeler from the qualitative understanding of the system to quantitative policy analyses. With respect to the model development, (Sterman, 2002) emphasizes the need to ensure that the modeling purpose must be to solve a problem and not simply to model a system. The model should simplify the system to a point where the model replicates a specific problem. In other terms: understanding first, but the goal is improving the system.

In general, there are different ways to develop SD models (Sterman, 2001). Of particular interest is the **block building modeling approach**, which is a structured process to develop the final model by integrating the dynamics of several models, i.e. building blocks. (Watson et al., 1998) highlight arguments for the so-called "building-block hypothesis", which appeals to the notion of problem decomposition and the assembly of solutions from sub-solutions.

Overall, the rationale behind block building approaches is to focus on relevant dynamics underlying complex systems and model them in different steps. This allows to break the complexity of the system into building blocks of models, which are then assembled together during the modeling process.

Block building modeling has been already applied in literature. For instance, (Milo et al., 2002) presents simple building blocks of complex network. In the context of SD, (Hines et al., 1996) conducts a comprehensive work which describes the so-called "molecules of structures" for SD models.

This research work applies a block building modeling framework based on SD. A series of simple blocks of models are developed to replicate relevant dynamics of the system. Following an iterative model development scheme (Keating, 1998), these basic blocks are iteratively combined together and extended to generate complex disruption scenarios of interdependent CIs for the purpose of simulation-based impact analysis, dynamic resilience assessment, and policy evaluation.

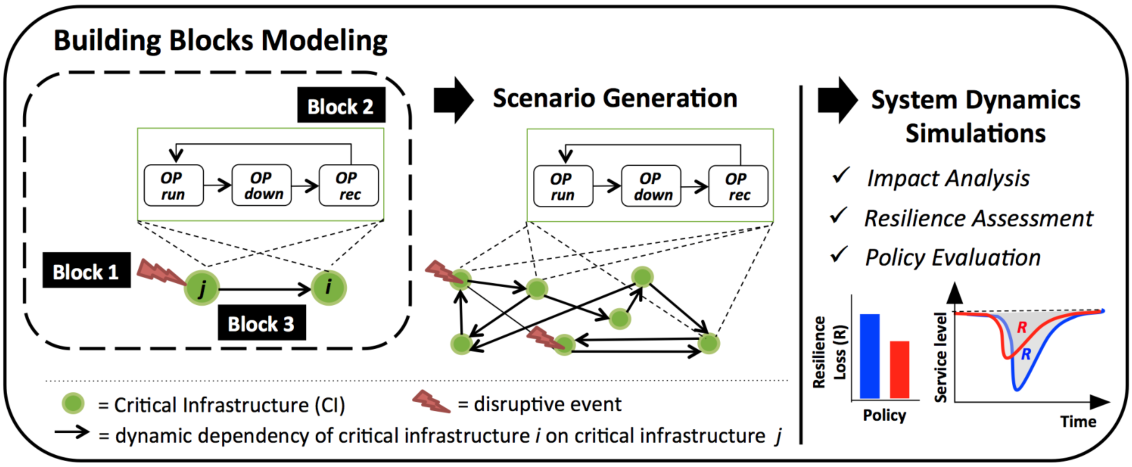


Figure 3.4: Block building modeling framework

Figure 3.4 describes the block building modeling framework based on SD. It starts with the development of three building blocks:

- **Block 1** replicates a general disruptive event according to the magnitude and time-dependent aspects of the disruption;
- **Block 2** models internal dynamics of a single CI as a function of its operational state depending on the ratio of running, down, and recovered operations over time;
- **Block 3** quantifies the dynamic interdependencies between CIs based on the level of service that CIs are able to provide one another over time.

Secondly, these basic building blocks are used for the generation of disruption scenarios of CIs (cf. Figure 3.4). At the network level, infrastructures (nodes of the network) to consider in the scenario must be identified and modeled according to their own operational dynamics (Block 2). Dynamic interdependencies (edges) between CIs (nodes) are identified and quantitatively characterized (Block 3). Disruptive events in one or more CIs are thus modeled according to the crisis scenario of interest (Block 1).

Finally, SD simulations (cf. Figure 3.4) allow to analyze disruptive impacts, assess dynamic resilience, and evaluate policies in the networked system of CIs.

Note that block building modeling approach is applied as an iterative process (cf. Section 3.1), and the modeling framework is extended through research iterations. In particular, Figure 3.4 refers to building blocks developed in the first iteration (see Chapter 4). The second research iteration (see Chapter 5) introduces a further building block which replaces the general disruptive event (Block 1) with a game theoretic model to capture complex cyber attack-defense dynamics over time, i.e. **Block 1'**.

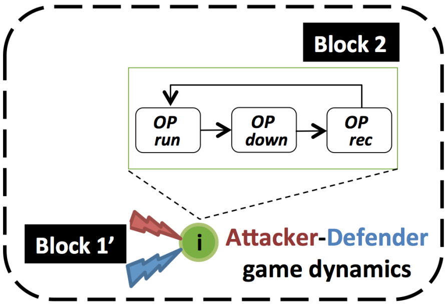


Figure 3.5: Extension of the block building modeling framework in Figure 3.4

Figure 3.5 gives an idea of how Block 1 is replaced by Block 1', extending the block building modeling framework in Figure 3.4. The aim of this building block is to explore disruptive dynamics in an infrastructure when the trigger event is a cyber attack. In this case, operational dynamics of the target CI emerges from attacker and defender strategic behaviors during the cyber conflict.

The third iteration (see Chapter 6) further extends the modeling towards a complex scenario of situational awareness of CI operators in the context of European CIs. For such purpose, **Block 1" Block 2"**, and **Block 3"** are developed as characterization of the three basic building blocks in Figure 3.4.

3.4 Simulation software and input data

Several commercially available programs facilitate the development of continuous SD simulation models. In this research work, Vensim SD simulation software (Vensim, 2015) is used for modeling and simulation purpose.

Simulation graphs are obtained with Vensim Personal Learning Edition (Vensim PLE, Version 6.2, Copyright 1988-2013 Ventana Systems, Inc.). Optimization and sensitivity analysis are done with Vensim Decision Support System Edition (Vensim DSS Version 5.11a for Macintosh, Copyright 1988-2010 Ventana Systems, Inc.).

A further note concerns the availability of quantitative data in the field of CIs. Approaches to investigate CI interdependencies tend to perform qualitative as opposed to quantitative analyses, or rely on limited or artificial data (cf. literature in Section 2.4.1). This is because operators prefer not to share confidential information about their infrastructure when a disruptive event occurs.

In order to preserve model applicability, this work aims at developing quantitative models to analyze CI interdependencies that do not require sensitive data on specific CI components. The choice of the level of abstraction is made on the basis of recommendations given by the CI operators partners of the ECOSSIAN project. Accordingly, input parameters of the dynamic interdependency models use publicly available data collected by (Laugé et al., 2015) in a survey of CI experts and operators.

Also, modeling assumptions are made on the basis of information available on the Internet. This means that model characterization is mainly based on technical reports and guidelines downloaded from official websites of organizations and research institutions (e.g. ENISA, IBM, etc.).

Chapter 4

Dynamic Interdependency Models

Governments have strongly recognized that CIs play crucial roles in economy, security, and societal welfare of nations. Due to the increasing interdependencies of modern infrastructures, the risk that even minor disruptions in a single CI can lead to a catastrophic cascade of failures in CI networks is very high.

This chapter presents a dynamic interdependency model to analyze disruptions in CI networks adopting a block building approach based on system dynamics (SD). In line with the block building modeling process (see Figure 3.4), the chapter starts with the analytical description of the three building blocks of models which have been iteratively developed and embedded together to understand the dynamics of disruptive events (Section 4.1), operations in a single CI (Section 4.2), and interdependencies across CIs (Section 4.3).

Section 4.5 explains how to build CI interdependency models with SD tools and therefore generate scenario of single or multiple disruptions in networked CI systems. With a special emphasis on time-dependent dynamics, simulation and analysis of example scenarios demonstrate how to use the method to assess disruption impacts (Section 4.6) with the purpose of estimating magnitude of cascading effects and providing insights for risk assessment.

Section 4.7 provides an overview of definitions existing metrics for system resilience, and it explains how to assess time-dependent resilience using the dynamic interdependency models. On this regard, a further application shows how this modeling approach can be a valuable instrument to support collective policy evaluation of CI operators toward national resilience objectives.

Note that the author published a preliminary version of the interdependency model in (Canzani, 2016b).

4.1 Block 1: Disruptive event dynamics

This building block defines a function, $d(t)$, to replicate a general disruptive event according to relevant characteristics for risk assessment. With regard to temporal aspects, a disruption occurs at time t_d (i.e. *disruption time*) and lasts for a particular length of time (*disruption duration*, ΔT_d). As disruptions can lead to different damages depending on their nature, the disruptive event has a certain magnitude (*disruption magnitude*, m_d) varying between 0 (no disruption) and $m_{d_{Max}}$ (entire infrastructure breakdown).

Figure 4.1 illustrates the input parameters characterizing a disruptive event in the interdependency model.

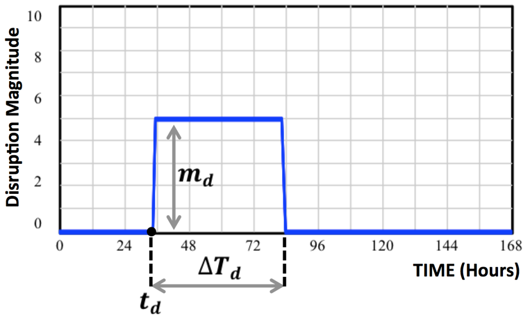


Figure 4.1: Example of disruption function

Mathematically, the disruption function $d(t)$ is defined as follow:

$$d(t) := \begin{cases} m_d, & \text{if } t_d \le t \le t_d + \Delta T_d, \\ 0, & \text{otherwise.} \end{cases} \tag{4.1.1}$$

Note that SD simulation tools offer a range of predefined functions to stress the system behaviour. The PULSE function is used to replicate the disruptive event. In Vensim, the PULSE function provides a pulse of height 1.0 starting at time t_d and lasting after time units ΔT_d. Therefore, the disruption function $d(t)$ corresponds to the magnitude factor m_d multiplied by the PULSE function.

4.2 Block 2: Operational dynamics of a single CI

While modeling approaches based on network theory are excellent for analyzing interconnectivity of a huge number of CIs, they fail in considering the internal dynamics of a single node of the network (i.e. one single infrastructure). In line with principles of system-of-systems (Eusgeld et al., 2011), this building block attempts to characterize the dynamics of operations in every single CI before dealing with interdependencies across CIs.

The relevance of considering the operational dynamics of each CI in the system relies on the fact that operational processes of any infrastructure may be compromised by

- **direct effects** of disruptions within the CI itself, and also
- **indirect effects** (or **cascading effects**) of operational disruptions in other CIs that must provide critical services for the correct functioning of its internal processes.

Inspired by previous investigation in epidemic modeling literature (Canzani and Lechner, 2015) to understand phenomena of propagation and recovery dynamics, the compartmental structure of the SIRS epidemic model (see literature review in Chapter 2) is used to describe the operational dynamics of a single CI.

Hereafter, let i denote any infrastructure in the networked system of $i = 1 \dots n$ infrastructures. Then, $OP^i_{run}(t)$, $OP^i_{down}(t)$, and $OP^i_{rec}(t)$ define respectively *running operations*, *down operations*, and *recovered operations* of the infrastructure i at time t.

Let n^i_{OP} be the *number of total operations.* At any time t,

$$OP^i_{run}(t) + OP^i_{down}(t) + OP^i_{rec}(t) = n^i_{OP} \tag{4.2.1}$$

An ideal state should have all CI operations are available to run, that is $OP^i_{run}(t) = n^i_{OP}$ at any time t. However system capabilities may change when disruptive events occur in the networked system of CIs as described above. This means that $OP^i_{run}(t)$ can be disrupted with a certain rate $\alpha^i(t)$ (*breakdown rate*) and get out of service, i.e. $OP^i_{down}(t)$. In this case, CI operators must intervene to repair down operations, so that $OP^i_{down}(t)$ move into $OP^i_{rec}(t)$ with rate $\beta^i(t)$ (*repair rate*). Recovered operations, $OP^i_{rec}(t)$, are finally restored back to function at rate $\gamma^i(t)$ (*service restoration rate*).

The operational dynamic of the single CI over time is described as a system of differential equations as follows.

$$\begin{cases} \dfrac{\mathrm{d}}{\mathrm{d}t}\big(OP^i_{run}(t)\big) = -\alpha^i(t)\Big(\dfrac{OP^i_{run}(t)}{n^i_{OP}}\Big) + \gamma^i(t)OP^i_{rec}(t) \\ \dfrac{\mathrm{d}}{\mathrm{d}t}\big(OP^{\mathrm{1}}_{down}(t)\big) = \alpha^i(t)\Big(\dfrac{OP^i_{run}(t)}{n^i_{OP}}\Big) - \beta^i(t)OP^i_{down}(t) \\ \dfrac{\mathrm{d}}{\mathrm{d}t}\big(OP^i_{rec}(t)\big) = \beta^i(t)OP^i_{down}(t) - \gamma^i(t)OP^i_{rec}(t) \end{cases} \tag{4.2.2}$$

Given an initial ideal state $OP^i_{run}(t) = {n_{OP}}^i$ in (4.2.1), the dynamic behavior starts at the moment of time when the CI is affected by direct or indirect damages of disruptions i.e. the breakdown rate $\alpha^i(t) \neq 0$ in Equation (4.2.2). Considering the CI as independent and isolated system, disruptive dynamics would only be triggered by disruptive events $d(t)$ that directly affect system operations (cf. Section 4.1), i.e.

$$\alpha^i(t) = d(t) \tag{4.2.3}$$

However, the bigger system of interdependent CIs must be considered to understand how functionalities of a CI strongly depend on the ability of other CIs to provide critical services. Fur such a purpose the next section aims at modeling effects of cascades between CIs.

Note that, on the basis of the above considerations, this chapter focuses on the breakdown rates while assuming constant average rates for $\beta^i(t) = \beta_0$ and $\gamma^i(t) = \gamma_0$. Different assumptions will be made in the application of the modeling approach to specific scenarios of cyber attacks in CIs (cf. Chapter 5).

4.3 Block 3: Dynamics of Interdependent CIs

Interdependency across CIs is a major concern when assessing the potential risk of CI disruptions. This third building block serves to capture dynamics of cascading effects that may occur in interdependent CIs when one or more of them are disrupted. In particular, dynamic performances of the system arise from two relevant dimensions of system resilience (see (Sterbenz et al., 2013)), i.e.

- **CI operational state**, which assesses effects of operational disruptions;
- **CI service level**, which determines if operational disruptions make the infrastructure unable to provide services to other CIs.

Accordingly, interdependencies are based on current operational capabilities of CIs to provide services that are critical for the correct functioning of other CIs. More precisely, a CI is fully able to provide service only if it is able to provide an amount of services that (at least) meet the demand. For example, a power plant may have some generators not fully operative, but the load of electricity generated can still match electricity demands of other CIs.

Note that the term “service” also refers to products, commodities, and all critical needs that CIs must deliver one another.

Let $C^i(t)$ be the current capability of infrastructure i at time t. $C^i(t)$ is defined as the ratio between the stock of running operations and the maximum capability of the CI. That is

$$C^i(t) := \frac{OP^i_{run}(t)}{C^i_{Max}}, \tag{4.3.1}$$

where the maximum CI capability C^i_{Max} corresponds to the total number of operations n^i_{OP} previously defined in Block 2 (cf. Section 4.2). The rationale behind is straightforward, as capabilities of a system depend on its available operations. According to the definition of $C^i(t)$, a CI is able to work at maximum capability at time t if and only if all operations are available to run, i.e. $OP^i_{run}(t) = C^i_{Max}$. In this case, the CI is said to be in its “normal operational state”.

Let $D^i(t)$ be the demand for critical services and products that infrastructure i has to deliver to others CIs. More precisely, $D^i(t)$ is a fraction (in percent) of the maximum capability of CI operations at time t, i.e. the CI operational level required to match market demand. For example, transportation infrastructures usually work at maximum operational level during daily peak hours when people come and go from work.

Note that, for demonstration purpose, scenario simulations presented later on in this chapter assume an average demand $D^i(t) = D^i_{Av}$. Effects of demand perturbations in simulation results are discussed in Chapter 6.

Then, a new control variable service provided $S^i(t)$ is defined to assess the level of service that the infrastructure is able to provide based on its current capability and demand for that service. Mathematically,

$$S^i(t) := \begin{cases} 1, & \text{if } C^i(t) \geq D^i(t), \\ \dfrac{C^i(t)}{D^i(t)}, & \text{otherwise.} \end{cases} \tag{4.3.2}$$

Note that $S^i(t)$ varies over time between 0 (no service provided) and 1 (if current operational capability allows the CI to deliver an amount of service that at least matches the demand). Thus far, Block 3 builds on Block 2 to capture dynamic relationships between operations and services of a CI with respect to the demand factor. Dynamic interdependencies among CIs are then modeled as function of the ability of CIs to provide critical services to each other over time.

4.3.1 Direct and indirect interdependencies

Every infrastructure needs products and services from other infrastructures to maintain its normal operational state. However, the complexity of such interdependent mechanisms makes it difficult to assess the ways in which CIs depend on each other. Qualitatively, two types of interdependencies are identified:

- **direct interdependencies**, and
- **indirect interdependencies**.

Note that in other research works they often correspond to first-order and higher-orter of dependencies respectively (see, e.g., (Laugé et al., 2015)). Figure 4.2 illustrates an example of direct and indirect dependencies between Water, Energy, and Financial CIs.

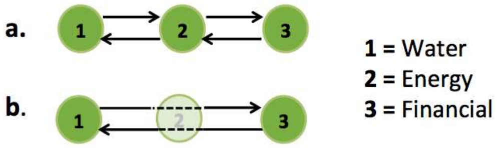


Figure 4.2: Direct and indirect interdependencies

Figure 4.2 (a) depicts direct interdependencies. The Financial CI directly depends on power services for banking systems provided by the Energy CI, and in turn the Financial CI provides payment and banking services to the Energy CI. Also, the Energy CI needs water for cooling systems of power plants from the Water CI while the latter receives power for pumps and control systems from the Energy CI.

Figure 4.2 (b) shows indirect interdependencies between Water and Financial CIs through direct dependencies on the Energy CI. This means that, although financial services do not directly depend on water infrastructures, damage effects of a disruption in the Water CI may cascade into the Financial CI due to service disruptions of the power plant that will not be able to provide electricity without adequate water resources for its cooling systems.

4.3.2 Interdependency matrix

Complexity of non-linear interactions between CIs make it difficult to provide a quantitative assessment of all types of interdependencies. Nevertheless, CI operators are able to understand the effects on their own infrastructures if they would not receive products and services from each of the other CIs. With the objective to assess magnitude of such direct interdependencies, a **weighted connection matrix** (or **interdependency matrix**) $E = \{e_{ij}\}$ is defined. The matrix E has the following proprieties:

(i) the weights $0 \leq e_{ij} \leq e_{Max}$ assess magnitudes of direct dependence of i on j on a scale of 0 (no dependence) to e_{Max} (highly dependent);

(ii) $\forall i = j$, $e_{ij} = 0$ since the dynamics within a CI is modeled in Block 2;

(iii) $\exists i \neq j$, $e_{ij} \neq_{ji}$, i.e. direct interdependency of a CI on services of another CI does not implies the opposite and, in case it exists, magnitudes can be different.

This research work uses publicly available data of a latest survey of CI operators (Laugé et al., 2015) to set values of the interdependency matrix $E = \{e_{ij}\}$, $0 \leq e_{ij} \leq 5$, as shown in Table 4.1.

e_{ij}	*Failed j*						
Effect on i	Energy	Telecom	Water	Financial	Transport	Health	Food
Energy	-	2.67	0.83	0.17	1.17	0.50	0.00
Telecom	0.86	-	0.57	1.00	1.00	0.14	0.14
Water	1.33	1.00	-	0.00	0.00	0.00	0.00
Financial	2.67	2.33	0.00	-	1.00	0.00	0.00
Transport	2.40	2.40	0.60	1.00	-	0.00	0.00
Health	1.40	2.20	0.20	1.40	1.40	-	0.00
Food	2.89	1.67	1.22	1.11	1.11	0.78	0.60

Table 4.1: Quantitative assessment of direct interdependencies between CIs (Laugé et al., 2015)

The questionnaire of (Laugé et al., 2015) asked CI experts from several countries to score on a scale of 0 (no effect) to 5 (high effect) the magnitude of effects on their infrastructure i if another infrastructure j would be non-operational for less than two hours. Final values were obtained by averaging individual scores provided by CI operators of each of the eleven infrastructures considered in the survey.

Note that the choice of input data for E is made according to simulation time scale (hours). Then, the SD model dynamically calculates magnitudes of direct and indirect dependencies over the time horizon. Furthermore, different disruptions of different duration and magnitudes may provoke cascading effects across CIs depending on their ability to deliver services over time as described below.

4.3.3 Cascading Effects

Let J_i be the set of infrastructures j that have to provide services to infrastructure i for its correct functioning, i.e.

$$j \in J_i \quad \text{if and only if} \quad e_{ij} \neq 0. \tag{4.3.3}$$

Critical services $S^j(t)$, for $j \in J_i$, influence the nonlinear breakdown rate $\alpha^i(t)$. This means that inadequate level of services $S^j(t)$ may trigger disruptive dynamics of operations in i. Mathematically,

$$\alpha^i(t) = \sum_{j \in J_i} \frac{e_{ij}\big(1 - S^j(t)\big)}{|J_i|} \tag{4.3.4}$$

In Equation (4.3.4), the cardinality of J_i serves as normalization and each weight $e_{ij} \in E$ assesses the magnitude of cascade effects of a failed infrastructure j on i. By definition of J_i,

$$e_{ij}(1 - S^j(t)) = 0 \quad \text{if and only if} \quad S^j(t) = 1. \tag{4.3.5}$$

Therefore, impacts of operational disruptions in any infrastructure $j \in J_i$ may cascade into infrastructure i with a magnitude e_{ij} only if service interruptions occur in j. In this case, operations of infrastructure i break down due to lack of those critical resources that cannot be provided by j.

Assuming that infrastructure i is also directly affected by a disruptive event $d(t)$ (see Block 1, Section 4.1), the breakdown rate $\alpha^i(t)$ is the sum of both dependency on other CI services and disruption components. That is

$$\alpha^i(t) = \sum_{j \in J_i} \frac{e_{ij}\big(1 - S^j(t)\big)}{|J_i|} + d(t) \tag{4.3.6}$$

Note that disruption functions are additive terms in Equation (4.3.6). This means that disruptive events can be simulated in one or more infrastructures occurring at the same or different time. This is key to the generation of a wide range of scenarios through the block building modeling approach.

4.4 Implementation with Vensim

Simulation scenarios are implemented with Vensim SD simulation software by integrating one another the building blocks of models. Figure 4.3 illustrates an example of SD stock and flow model that refers to two generic infrastructures i and j, such that j is disrupted and i depends on services provided by j (i.e. $j \rightarrow i$).

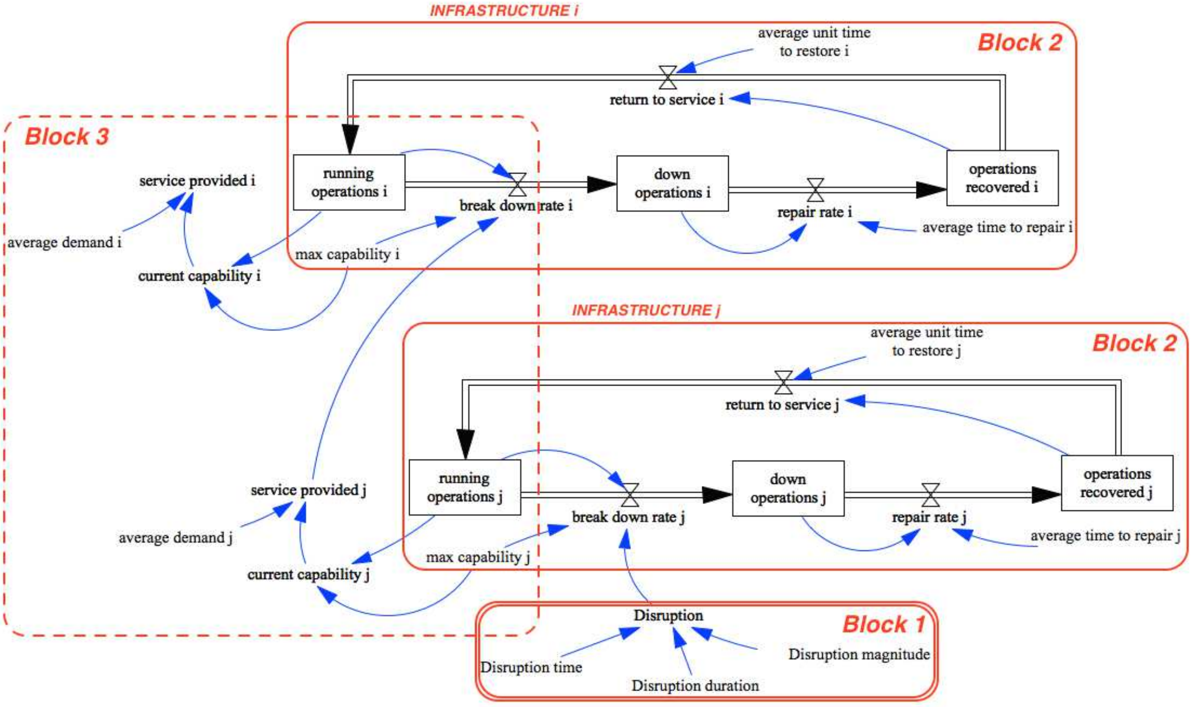


Figure 4.3: SD stock-and-flow diagram of integrated building blocks

4.5 Scenario Generation and Simulation

Using the three building blocks of models, the **scenario generation process** is done in three simple steps as follows.

(i) The first step is the identification of infrastructures (*nodes of the network*) to consider in the interdependent system, which are modeled according to their internal operational dynamics (Block 2).

(ii) Then, direct interdependencies (*edges of the network*) across CIs are identified and quantitatively characterized through the weighted connection matrix (Block 3).

(iii) Lastly, disruptive events in one or more CIs are modeled to generate different scenarios of crisis (Block 1).

Once created the scenario of interest, SD simulations allow to analyze impacts of disruption, assess dynamic resilience and evaluate policies in the networked system of CIs. Arguments for the use of scenario-generation methods to forecast possible futures in decision-making contexts are discussed in (Banuls and Turoff, 2011). The authors integrate Delphi method and Cross Impact Analysis to describe possible scenarios of interdependent events. This thesis uses data gathered from experts in (Laugé et al., 2015) as input parameters with the purpose of illustrating model applications to assess hypothetical scenarios using SD simulations.

4.5.1 Scenario generation example

The first step to generate scenarios is defining which are the infrastructures to consider, i.e. the nodes of the network. This example considers a scenario with five CIs: Water, Energy, Financial, Telecom, and Transport.

Obviously, these infrastructures are not independent systems. The normal operational state of each CI depends on the ability of other CIs to provide critical services. In line with the second step of the scenario generation process, this means that the edges of the network must be identified. Figure 4.4 depicts direct interdependencies between CIs with respect to services they provide to each other.

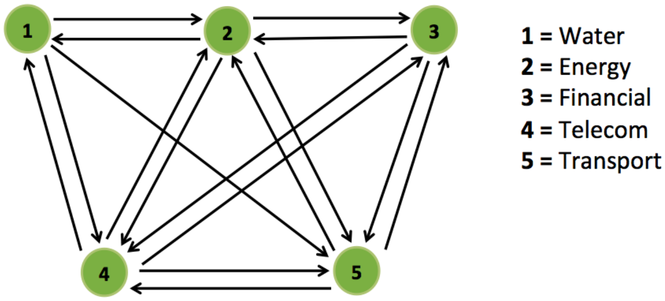


Figure 4.4: Example of scenario

For a better understanding of which kind of interdependencies the directed edges in Figure 4.4 refer to, Table 4.2 provides a qualitative characterization of such interdepedencies between the five CIs on the basis of the seminal work of (Rinaldi et al., 2001).

Then, the interdependency matrix provides a quantitative assessment of such interdependencies. (See Section 4.3.2 for details on the interdependency matrix). According to data in Table 4.1, the interdependency matrix that corresponds to the scenario example in Figure 4.4 is as follows.

$$E = \{e_{ij}\} = \begin{bmatrix} 0 & e_{12} & e_{13} & e_{14} & e_{15} \\ e_{21} & 0 & e_{23} & e_{24} & e_{25} \\ e_{31} & e_{32} & 0 & e_{34} & e_{35} \\ e_{41} & e_{42} & e_{43} & 0 & e_{45} \\ e_{51} & e_{52} & e_{53} & e_{54} & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1.33 & 0 & 1.00 & 0 \\ 0.83 & 0 & 0.17 & 2.67 & 1.17 \\ 0 & 2.67 & 0 & 2.33 & 1.00 \\ 0.57 & 0.86 & 0.71 & 0 & 1.00 \\ 0.20 & 2.40 & 0.60 & 2.40 & 0 \end{bmatrix} \tag{4.5.1}$$

Finally, one or more disruptive events over time can be modeled in any infrastructure to generate different disruption scenarios. Figure 4.5 depicts two disruptive events (red thunderlights), in Energy and Telecom respectively, that are considered in the next subsection as example of disruption scenario simulation.

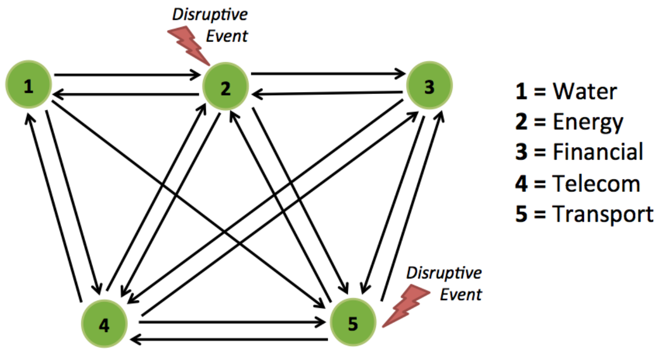


Figure 4.5: Example of scenario with multiple disruptions

Infrastructure	*depends on*	*Description of critical services provided*
Water	Energy	Power for pumps, control systems
	Telecom	SCADA, communication services
Energy	Water	Water for cooling, emission reduction
	Financial	Payments, banking services
	Telecom	SCADA, communication services
	Transport	Shipping, fuel transport
Financial	Energy	Power for banking systems
	Telecom	SCADA, communication services
	Transport	Shipping
Telecom	Water	Water for cooling
	Energy	Power for switches, fuel for generators
	Financial	Payments, banking services
	Transport	Shipping
Transport	Water	Water for production, cooling, emission reduction
	Energy	Fuel, lubricants, power for signaling, switches
	Financial	Payments, banking services
	Telecom	SCADA, communication services

Table 4.2: Qualitative assessment of direct interdependencies

4.5.2 Simulation of Single and Multiple Disruptions

With the purpose of demonstrating the applicability of the modeling approach, this section presents a comparison of different disruption scenarios obtained by simulating the scenario example in Figure 4.5.

In particular, simulations consider the following disruptive events:

Disruptive Event	*Disruption Time*	*Disruption Duration*	*Disruption Magnitude*
(d_1) in Transport CI	$t_{d_1} = 24$ hours	$\Delta T_{d_1} = 48$ hours	$m_{d_1} = 10$
(d_2) in Energy CI	$t_{d_2} = 96$ hours	$\Delta T_{d_2} = 20$ hours	$m_{d_2} = 80$

Table 4.3: Characterization of disruptive events

With the two disruptive events described in Table 4.3, three different disruption scenarios are generated in the networked system of five CIs:

- **Scenario 1:** single disruption in the Transport CI (d_1),
- **Scenario 2:** single disruption in the Energy CI (d_2),
- **Scenario 3:** multiple disruptions as combination of previous scenarios (d_1 and d_2).

Each scenario is simulated over 2 weeks time period with an hourly time scale (i.e. *INITIAL TIME* $= 0$ and *FINAL TIME* $= 336$ hours).

For convenience, every infrastructure i has the maximum operational capability $C^i_{Max} = 100$ operations. The average demand is then assumed being 90% of the maximum capability, i.e. $D^i_{Av} = 90\%$. Also, the system of CIs is in its normal operational state before a disruptive event triggers the nonlinear dynamics, that is $OP^i_{run}(t) = C^i_{Max}$ per $t < t_{d_1} < t_{d_2}$.

Simulation outputs in Figures 4.6, 4.7, and 4.8 show dynamics of running operations $OP^i_{run}(t)$ (in percent, graphs on left) and service provided $S^i(t)$ (in percent, graphs on right) over time for Scenario 1, 2, and 3 respectively.

It follows the description and simulation analysis of the three disruption scenarios.

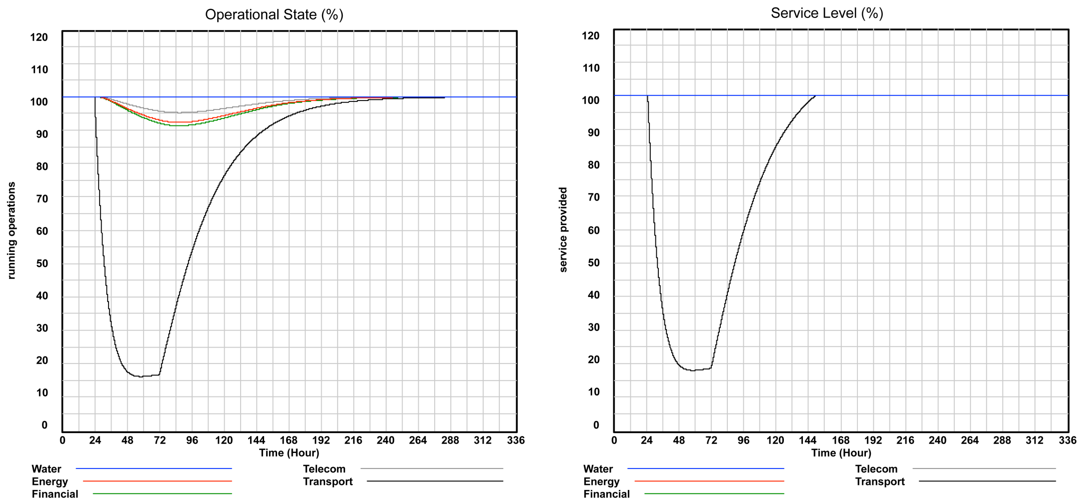


Figure 4.6: Transport disruption (Scenario 1)

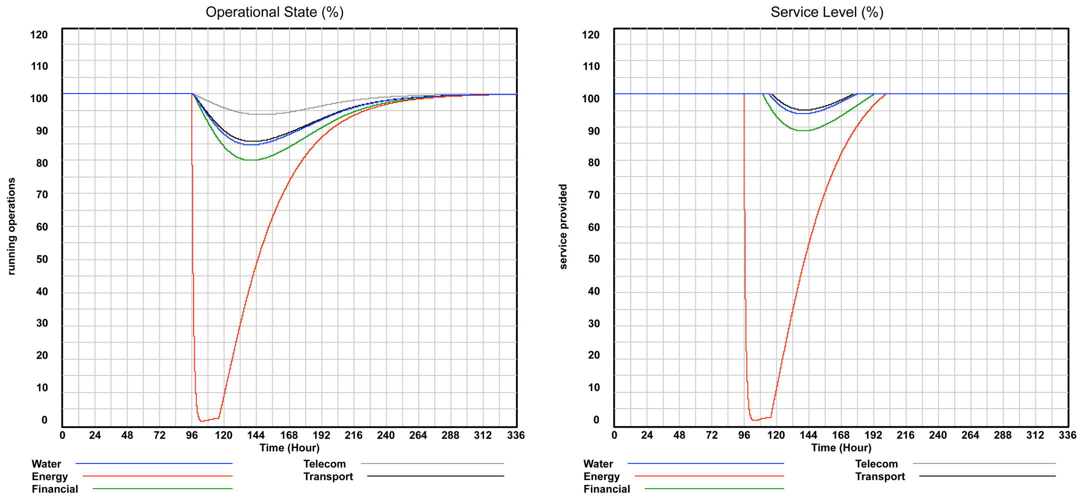


Figure 4.7: Energy disruption (Scenario 2)

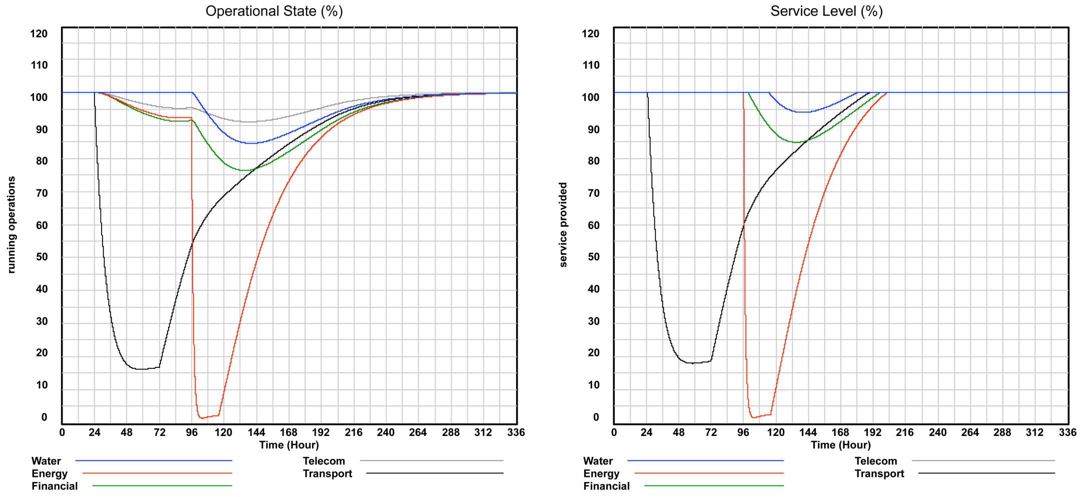


Figure 4.8: Transport and Energy disruptions (Scenario 3)

Scenario 1

According to Table 4.3, after one day of simulation time, a disruption of relatively low magnitude affects the Transport CI and it lasts two entire days. It may be the case of a bridge collapsing due to a natural hazard. The collapse interrupts the usual route of thousand daily vehicle trips, creating higher congestion and consequent opportunity losses.

In Figure 4.6, operational performances of the transportation network drastically decrease and the level of service drops down with a minimum peak of about 20%. More than one week is needed to restore the normal operational state in the Transport CI. Reshaped travel patterns has longer travel distance and generate significant costs. It turns into difficulties for shipping operations (i.e. Telecom CI), the supply of gas stations (i.e. Energy CI), and so on. Nevertheless, Energy, Water, Telecom, and Financial infrastructures can still fully satisfy the service demands although their operations get partially damaged.

Scenario 2

This scenario refers to a disruption in the Energy CI of very high magnitude occurring after 4 days (simulation time) and lasting one and a half days (cf. Table 4.3). A power outage may leave a critical area in the dark, without electricity. It leads to operational breakdowns of financial operations and telecommunication systems that strongly rely on electric power. Lack of signals could be the cause of tremendous crashes in the transportation system, and water pumps need power too.

Accordingly, simulation graphs in Figure 4.7 show that effects of the outage cascade into other CIs provoking up to 20% of operational disruptions. In Water, Transport, and Financial infrastructures, minor service interruptions start between one and two days after the disruptive event occurs. The Telecom CI does not shows service unavailability. This is because telecommunication systems have more effective backup power sources such as standby generators to prevent such cascading failures.

Scenario 3

Scenario 3 assumes that a power outage occurs after the bridge collapse by combining disruptions in Energy and Transport CIs of the two previous scenarios. Of interest is to demonstrate how coupled dynamics of disruptive events impact on system performances at operational and service levels.

Although Scenario 1 shows that the collapse of a bridge may not provoke service interruptions in the bigger system of CIs, the impacts can be catastrophic if a power outage occurs while the Transport CI is recovering from that crisis situation.

Comparing the Scenario 3 (Figure 4.8) with Scenario 1 and 2 (Figures 4.6 and 4.7 respectively), it is clear that the Transport CI needs longer to recover internal operations due to the outage. In fact, the lack of electric power complicates the restoration of transportation network services. While service interruptions of the Transport CI lasts about 5 days in Scenario 1, it takes more than 7 days in Scenario 3. Also banking, shipping and telecommunication operations are longer affected In case of multiple disruptions. The Financial CI results the infrastructure most affected by cascade effects in the three scenarios.

In general, performances of single CIs can be compared to analyze cascading effects under different disruption scenarios. To clarify this concept, simulation graphs in Figure 4.9 show how changes in recovery times strongly depend on different disruptions occurring over time. The charts plot operational dynamics of the CIs not directly affected by disruptive events in the three scenarios discussed above (i.e. Telecom, Financial and Water CIs).

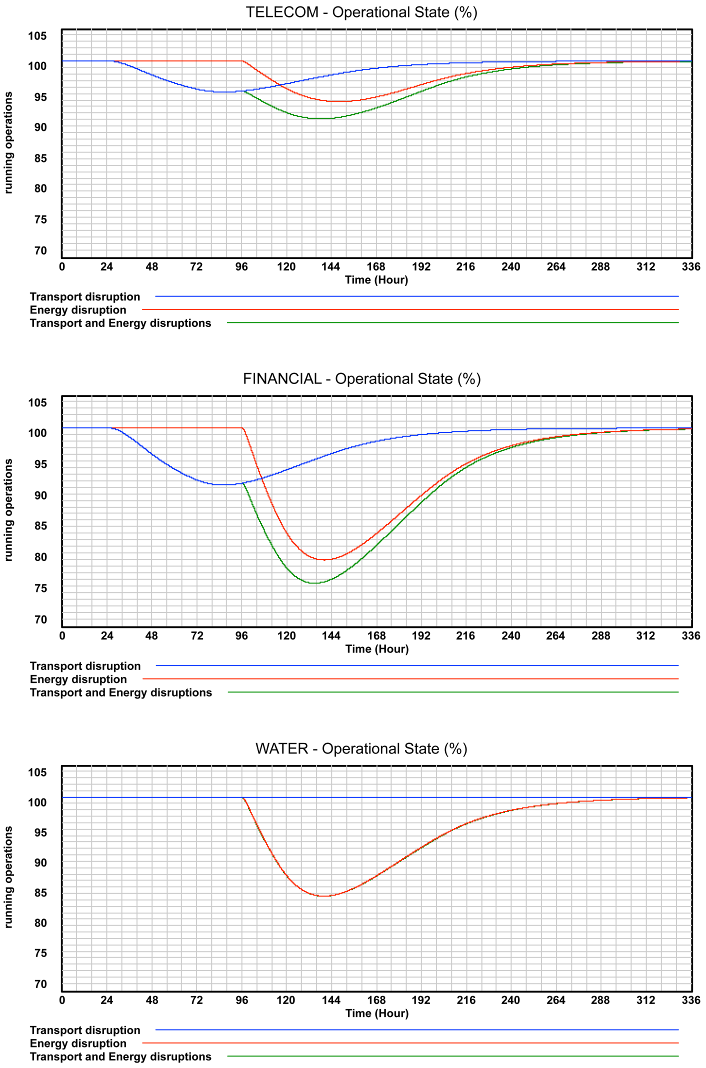


Figure 4.9: Operational performance of single CIs under different disruption scenarios

4.6 Disruption Impact Analysis

This section demonstrates how the dynamic interdependency models can be used to assess disruptive impacts and risk scenarios with respect to relevant components of disruptive events, such as magnitude and time duration.

First, a simulation-based impact analysis is conducted to investigate the effects of disruptions with different magnitude. Cascade effects between CIs are analyzed at both operational and service levels. Then, multivariate sensitivity simulations are implemented in Vensim to provide insights for risk assessment. The automated sensitivity analysis allows exploring patterns of cascade effects according to distributed input parameters.

Note that simulation results in this section refer to disruptive scenarios generated in the simple network of three CIs depicted in Figure 4.10.

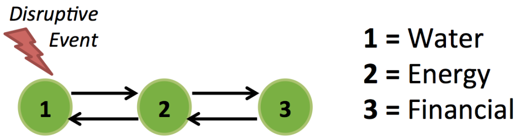


Figure 4.10: Simple disruption scenario for impact analysis

The scenario considers Water, Energy, and Financial CIs; and different kinds of disruption are simulated in the Water CI. The interdependency matrix that corresponds to the disruption scenario in Figure 4.10 is as follows (cf. Table 4.1).

$$E = \{e_{ij}\} = \begin{bmatrix} 0 & e_{12} & e_{13} \\ e_{21} & 0 & e_{23} \\ e_{31} & e_{32} & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1.33 & 0 \\ 0.83 & 0 & 0.17 \\ 0 & 2.67 & 0 \end{bmatrix} \qquad (4.6.1)$$

Note that direct and indirect interdependencies between Water, Energy, and Financial CIs are qualitatively described in Section 4.3.1.

4.6.1 Effects of Disruption Magnitude

The simulations consider a disruption $d(t)$ of two days, $\Delta T_d = 48$ hours, occurring in the Water CI at simulation time $t_d = 24$ hours. Then, disruption impacts and cascading effects are analyzed for different values of the magnitude m_d.

For convenience, infrastructures $i = 1, 2, 3$ have the maximum operational capability $C^i_{Max} = 100$ operations. The average demand D^i_{Av} is then assumed being 90% of C^i_{Max}. Also, the system of CIs is in its normal operational state before the disruption, i.e. $OP^i_{run}(t) = C^i_{Max}$ per $t < t_d$.

In Figures 4.11, 4.12, and 4.13 below, simulation graphs show dynamics over time of running operations $OP^i_{run}(t)$ (in percent, graphs on left) and service provided $S^i(t)$ (in percent, graphs on right) in case of $m_d = 0.4$, $m_d = 10$, and $m_d = 40$, respectively. Note that simulations run over 2 weeks time period with an hourly time scale (i.e. *INITIAL TIME* $= 0$ and *FINAL TIME* $= 336$ hours).

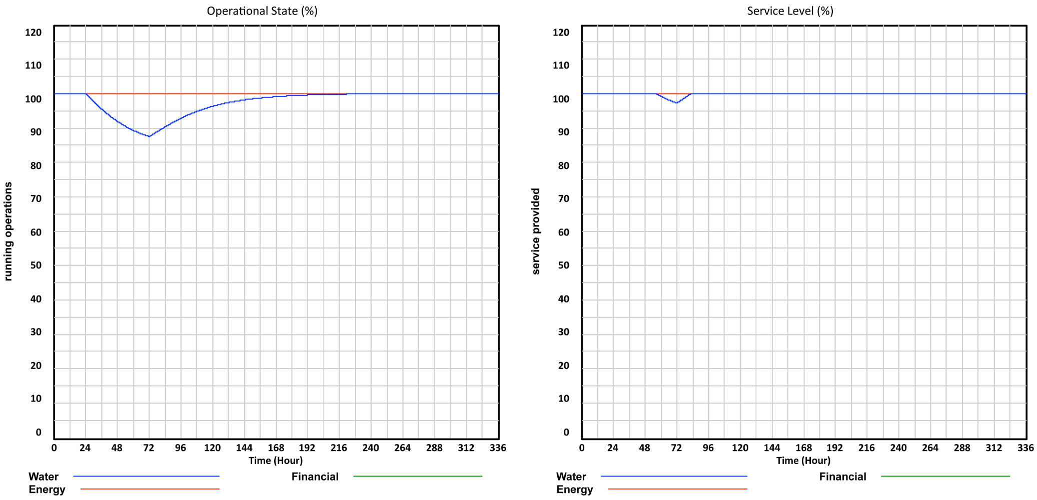


Figure 4.11: 2-days Water CI disruption with $m_d = 0.4$

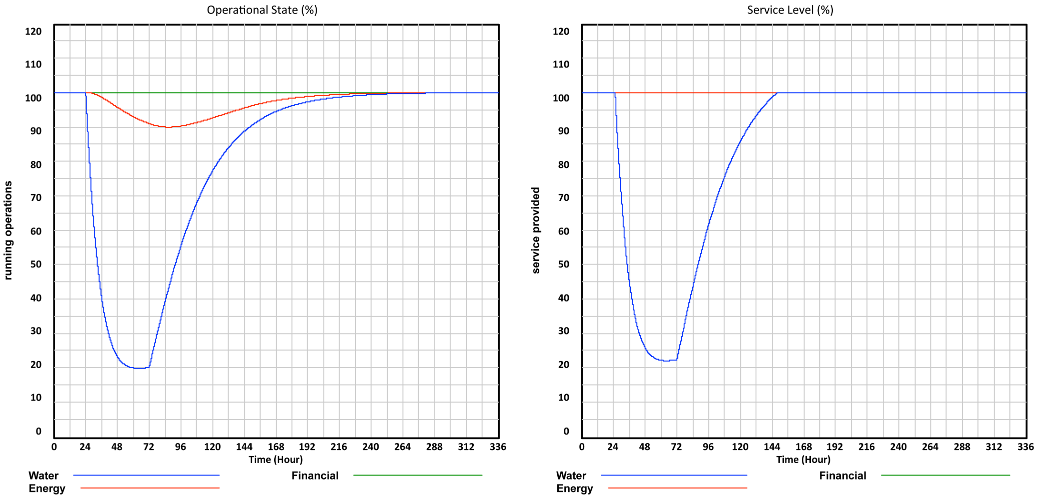


Figure 4.12: 2-days Water CI disruption with $m_d = 10$

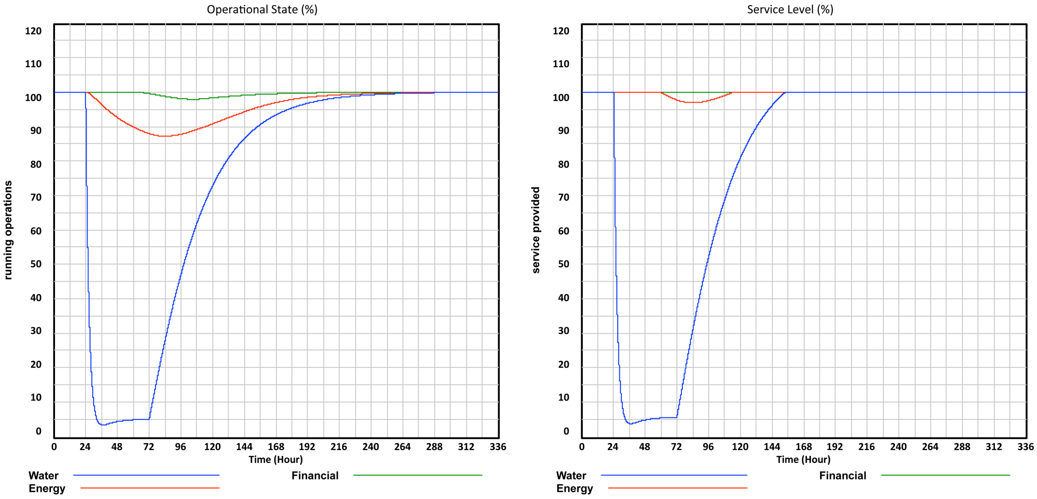


Figure 4.13: 2-days Water CI disruption with $m_d = 40$

In Figure 4.11, up to 15% of water distribution operations (down peak value of the blue line, graph on left) are down due to two days disruption with very low magnitude ($m_d = 0.4$). Recovery actions require a substantially long time so that, one and a half days after the disruptive event happens, also Water CI services loose 5 % of availability for almost one day (blue line, graph on the right). Nevertheless, the system absorbs the damage before it cascades into Energy and Financial CIs. This means that the Water CI is still able to provide a level of service that meets the demand.

The same scenario is simulated after increasing the value of disruption magnitude to $m_d = 10$ in Figure 4.12. About 80% of critical water operations are disabled due to the disruptive event, and this leads to serious service interruptions of the Water CI. Consequently, power plants are temporarily unable to receive water for system cooling such that Energy CI operational capabilities decrease to 90 % (red line, graph on left). Despite damage effects due to direct dependency on the disrupted Water CI, the Energy CI remains able to fully provide services and therefore disruptive effects do not impact operations and services of the Financial CI (green lines).

Finally, Figure 4.13 shows output graphs replicating a Water CI disruption of magnitude $m_d = 40$. In this case, direct interdependencies between the disrupted Water CI and Energy CI have higher impacts on both operational and service dynamics of power plants and generators. Water operations and services are completely down for 2 days before recovery actions are taking place. From the disruption time, the entire system of CIs needs more than 5 days to provide an adequate level of services (graph on the right) and up to 10 days to completely recover all operations (graph on left). Immediately after the event occurs, the Energy CI starts losing its operational capabilities up to 85 % (red line on left). One and a half days after the disruption, also power generation services get interrupted at about 5 % (red line on the right). Damage effects cascade also into the Financial CI: operational performance decreases over time for about 3% after 2 days the disruption occurs (green line, graph on left). Banking and payment services can still be fully provided (green line, graph on left).

This scenario demonstrates that high-magnitude operational disruptions in the Water CI can have indirect impacts on financial services even do the Financial CI does not rely on services provided by the Water CI (cf. Section 4.3.1).

The impact analysis explores how cascading failures propagate over time through a networked system of CIs due to magnitude of direct and indirect dependencies between CIs. The simulation example considers the effects of disruptive magnitude m_d. Similarly, the analysis can be conducted by varying the disruption duration ΔT_d to demonstrate the ability of the dynamic interdependency model to capture time-dependent aspects.

Note that so far model development and findings implementation adopted a deterministic perspective. Nevertheless, a SD model is an excellent tool for analyzing system behavior under a wide variety of parametric assumptions (Arthur and Robert, 1996).

This section demonstrates how such analysis can be done manually through simulations of specific scenarios of interest. Beside best case, worst case, and most likely scenarios, next section demonstrates how Vensim tools can be used for a more comprehensive exploration through repeated simulations in which magnitude and duration of disruptions are automatically changed for each simulation according to a given range of uncertainty in parameter values.

4.6.2 Insights for Risk Assessment

Identification, evaluation, and estimation of the level of risks involved in a crisis scenario, require tools for the comparison of risks against benchmarks or standards and the determination of an acceptable level of risk. Within the entire process of risk management, operators of CIs must undertake risk assessment procedures to answer questions such as: what can go wrong? What is the likelihood that it would go wrong? What are the consequences? What is the time frame? (Haimes, 2015).

This section aims at showing how to use the dynamic interdependency model and Vensim SD tools towards providing insights for risk assessment procedures.

In particular, multivariate sensitivity simulations (MVSS) are used to support the understanding of the potential range of behaviors the model can generate. MVSS are often labeled Monte-Carlo simulations (Daryanani, 2002) and allows generating dynamic confidence intervals for trajectories of variables in the SD model (Sterman, 2000).

In MVSS, uncertainty is represented by treating model parameters as statistical distributions instead of constants. Vensim provides several distributions for this purpose.

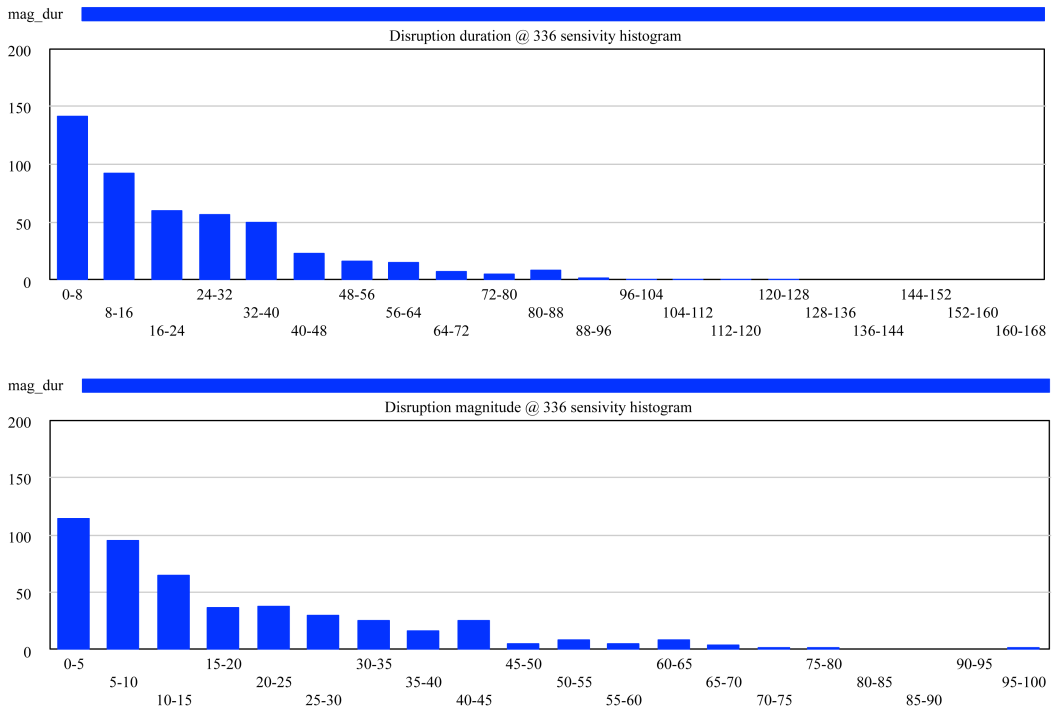


Figure 4.14: Exponentially distributed input parameters (500 samples)

Figure 4.14 illustrates random exponential distributed input parameters for magnitude and duration of the disruptive event in the simple scenario of networked CIs in Figure 4.10. In Vensim, the predefined distribution RANDOM EXPONENTIAL *(min,max,shift,stretch)* draws a number on a specified range between min and max from an exponential distribution that starts at 0 and has mean 1. Before the value is returned it is multiplied by a stretch that stretches to the right the distribution by decreasing its value, and then a shift is added to it to determine the beginning of the distribution with respect to the right of the origin.

Histograms in Figure 4.14 show how 500 samples are distributed according to

- a disruption duration distribution for ΔT_d between 0 and 168 hours stretched by 24 hours and with no shift;
- a disruption magnitude distribution for m_d between 0 and 100 stretched by 20 and with no shift.

These assumptions rely on CI experts data in (Laugé et al., 2015), confirming that infrastructures usually suffer short-duration failures, and overall no longer than two weeks service downtime. Also, empirical data on low probabilities of huge catastrophic events in CIs can be found in (Luiijf et al., 2008). However, assumptions only serve to run simulations with the purpose of demonstrating applicability of the dynamic interdependency model; therefore they do not limit further model application to different scenarios.

Note that MVSS are run over 2 weeks time period with an hourly time scale (i.e. *INITIAL TIME* $= 0$ and *FINAL TIME* $= 336$ hours).

Given the plausible range of uncertainty for disruption input parameters in Figure 4.14, the simulated levels of CI running operations over time are no longer numbers. The outcome variables of CI running operations are described by distributions of values.

Sensitivity graphs in Figure 4.15 show the entire range of outcomes for running operations of Water, Energy, and Financial CIs with different confidence bounds. Results are obtained by running the model 500 times for a given noise seed and using specified values for each parameter all at once (i.e. multivariate testing).

Note that different colors indicate the percentage of outcomes that fall within the different sub-ranges. Given a kind of uncertain disruptions in the Water CI, the estimated low peak (in percent) for the operational state of the Energy CI might be 87 % of running operations with 95 % of confidence bounds ranging from 86 % to 88 % (blue area, middle graph in Figure 4.15). Thus, there is only a 5% chance that the true value lies outside of this range. In this range of scenarios, water disruptions may cascade into the Financial CI leading up to 3 % of operational capability loss with 95 % of confidence bounds (blue area, bottom graph in Figure 4.15).

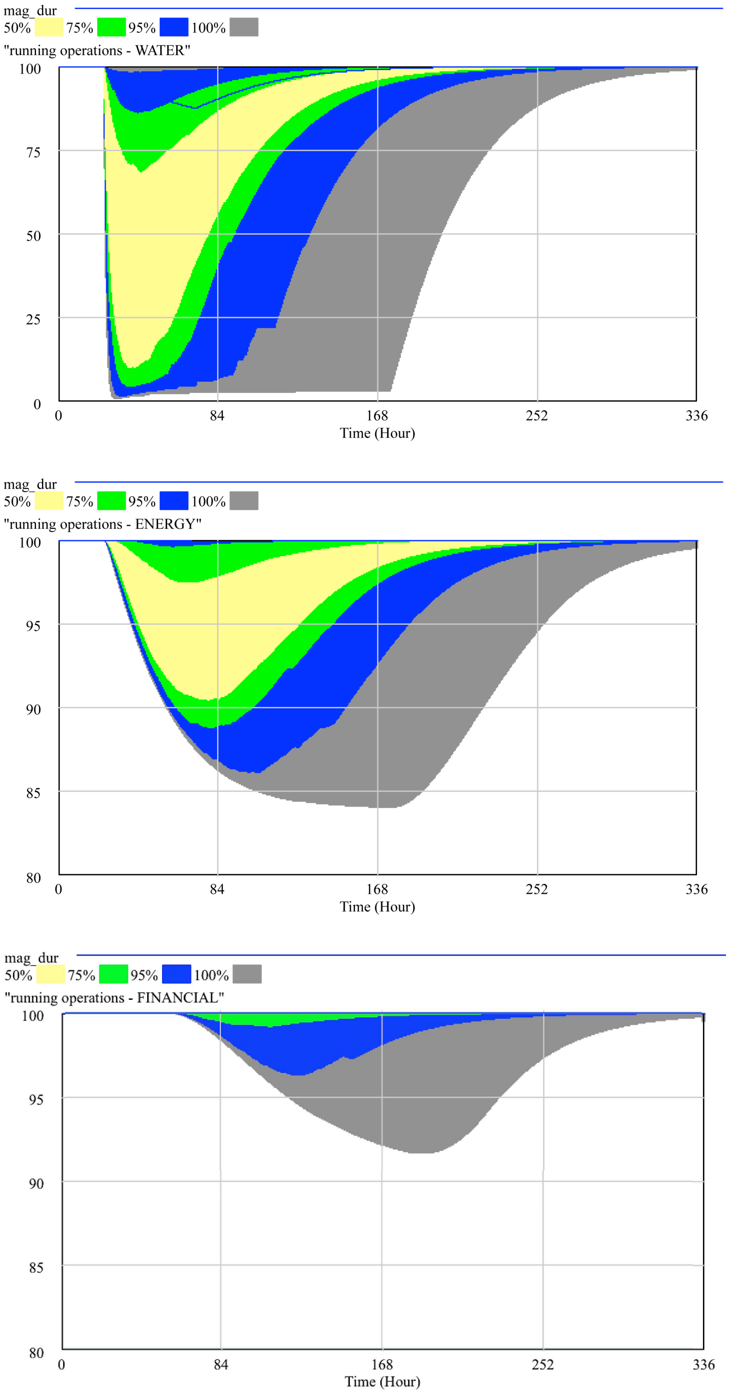


Figure 4.15: Sensitivity graphs with confidence bounds

In sum, conducting a parametric sensitivity testing in the interdependency model provides information on the distributions of magnitude of cascade effects which strongly influence risk managers' decisions in determining an acceptable level of risk which complies with benchmarks and CI security standards.

4.7 Dynamic Resilience Assessment

Resilience of CIs is a common main objective of governments and authorities worldwide. The US National Infrastructure Advisory Council (NIAC) states that

> "resilience is the ability to reduce the magnitude, impact, or duration of a disruption. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event." (Berkeley and Wallace, 2010)

Toward the definition of a long-term and systematic approach to build resilience of vulnerable countries and communities, the European Commission defines resilience as

> "the ability of an individual, a household, a community, a country or a region to withstand, cope, adapt, and quickly recover from stresses and shocks such as violence, conflict, drought and other natural disasters without compromising long-term development." (EU, 2012)

Despite there is no unique insight about how to define resilience, the common use of this term emphasizes the propriety of a system to "bounce back" to normal conditions after a situation of crisis. A latest review of definitions and metrics of system resilience is (Hosseini et al., 2016). The authors identify four main domains in which the concept of resilience is applied: organizational, social, economic, and engineering. Note that also (Francis and Bekera, 2014) present a similar classification of resilience definitions from different disciplinary perspectives in the specific context of infrastructure systems.

After a brief overview of existing metrics for resilience assessment, this section introduces the dynamic interdependency model as potential instrument to support dynamic resilience assessment of CI networks. This means that resilience components of every CI are considered with respect to the bigger system of CIs to support collective policy evaluation toward national resilience objectives.

4.7.1 Existing Metrics

With a special focus on engineering fields (of which infrastructure systems can be considered a subdomain), (Hosseini et al., 2016) conduct a literature review of papers published from 2000 and 2015 that are relevant to modeling and measuring resilience. They classify resilience assessment methodologies as follows:

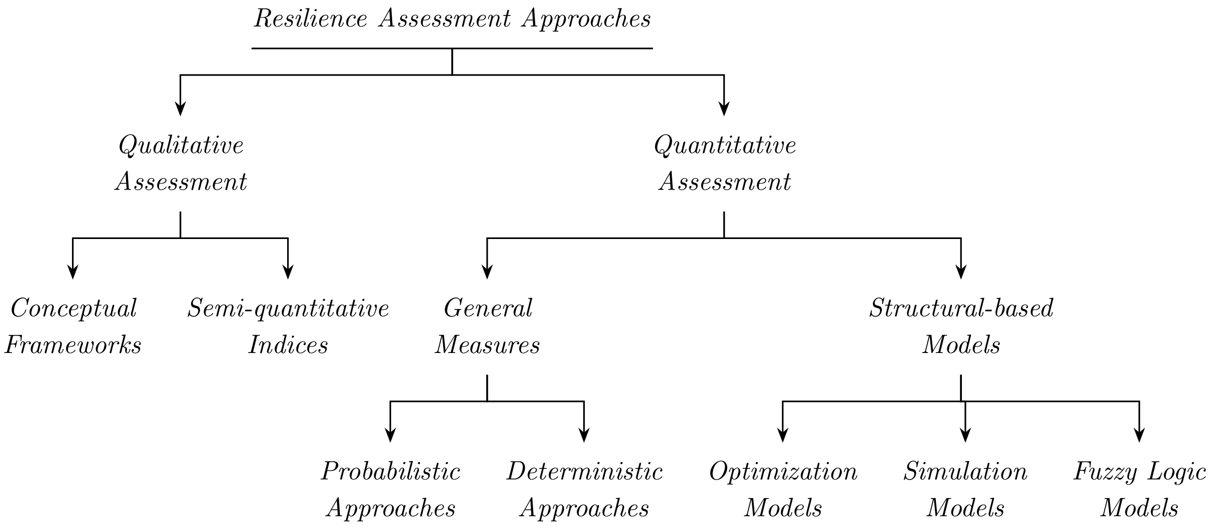


Figure 4.16: Classification of resilience assessment approaches (Hosseini et al., 2016)

Qualitative methods focus on describing qualitative aspects of resilience and providing best practices trough conceptual frameworks (see e.g. (Labaka et al., 2013) and (Kahan et al., 2009)).

Relevant to mention is the conceptual framework proposed by (Sterbenz et al., 2010) for resilience and survivability of communication networks. Conceptual insights of the so-called ResiliNet framework (Sterbenz et al., 2010) have been later developed by the same author in (Sterbenz et al., 2013) toward a comprehensive methodology to quantify resilience on the basis of two relevant dimensions: the operational state and service level. More precisely, it considers that operations are affected by perturbations and such operational disruptions may provoke degradation of service capabilities. Thus, evaluation of resilience is done through a mapping between network operation and service.

In accordance with the classification of resilience assessment methods (cf. Figure4.7.1), **quantitative approaches** can be subdivided in generic measures (that do not consider the system structure in evaluating system performance) and structure-based models.

Structure-based models often refers to resilience measures for supply chains, communication, transportation, or organization networks, in which the infrastructure structure is a relevant characteristic. For instance, the work of (Sterbenz et al., 2013) belongs to the category of structured-based simulation models as they use a combination of topology generation, analytical, simulation and experimental emulation techniques to improve resilience of the Internet.

Beside simulation models, structured-based approaches also comprehend optimization models (e.g. (Faturechi et al., 2014) for resilience of airport pavement networks) and fuzzy logic models (e.g. (Azadeh et al., 2014) in the context of a petrochemical plant).

A special emphasis on network-based components of resilience and its relevant metrics is given in (Barker et al., 2013).

General quantitative approaches are called deterministic if do not consider uncertainty in the metric, they are probabilistic (or stochastic) otherwise. Each of these two categories can be further classified with respect of time dependent aspects. More precisely, resilience can be measured in terms of

- **static resilience**, which is the amount by which a system is able to avoid the maximum impact; or
- **dynamic resilience**, which is the speed at which the system recovers from a disruption over time.

Differences between static and dynamic resilience are discussed by (Pant et al., 2014) in the context of economic systems. An example of static quantification of resilience is (Rose, 2009), which measures the changes in economic performance regardless of time components.

This thesis focuses on dynamic resilience, which considers time-dependent aspects of system recovery capabilities. Accordingly, (Pant et al., 2014) defines dynamic resilience in the context of the speed of system recovery: a more resilient system is the one able to recover faster from a disruptive event. In addition to recoverability, resilience can be quantified on the basis of two other capacities such as absorptive capacity and adaptive capacity (Francis and Bekera, 2014). The latter propose a resilience metric based on these three characteristics to describe system resilience in terms of proportions of initial system performance.

A widely used deterministic framework to assess dynamic resilience is the so-called "resilience triangle" of (Bruneau et al., 2003). The resilience triangle measures loss of resilience by the size of the expected degradation in system quality over time (that is, recovery time). In particular, (Bruneau et al., 2003) argue that

> "resilience can be understood as the ability of the system to reduce the chance of a shock, to absorb a shock if it occurs (abrupt reduction of performance) and to recover quickly after a shock (reestablish normal performance)".

This definition relies on three proprieties of dynamic resilience. They are as follows:

- *Robustness*, which refers to the ability of a system to withstand a given level of stress or demand without functionality losses;
- *Redundancy*, that is the ability to satisfy functional requirements in crisis situations;
- *Rapidity*, i.e. the ability to timely recover functionality in order to contain losses.

In (Bruneau and Reinhorn, 2007), the authors identify a fourth characteristic to expand the resilience concept in 3-dimensions: the resourcefulness, which is the ability to establish priorities during the recovery actions.

4.7.2 Measuring Resilience in Dynamic CI Networks

Considering CI performance at operational and service levels over time, the dynamic modeling approach developed in this thesis suits a wide range of existing metrics for resilience analysis. For example, operational state (i.e. $OP^i_{run}(t)$) versus service level (i.e. $S^i(t)$) can be plotted as the two relevant dimensions to quantify system resilience identified by (Sterbenz et al., 2013).

In this section the resilience triangle (Bruneau et al., 2003) to quantify the loss of resilience R_i in a single infrastructure i based on its ability to provide services $S^i(t)$ (in percent), overtime. Mathematically we have

$$R_i = \int_{t_i}^{t_f} [100 - S^i(t)]\, dt, \tag{4.7.1}$$

where t_i is the initial time in which the system starts to loose service capabilities and t_f is the time in which the service disruption is fully recovered. Figure 4.17 illustrates the triangle area (in grey) corresponding to the loss of resilience R_i.

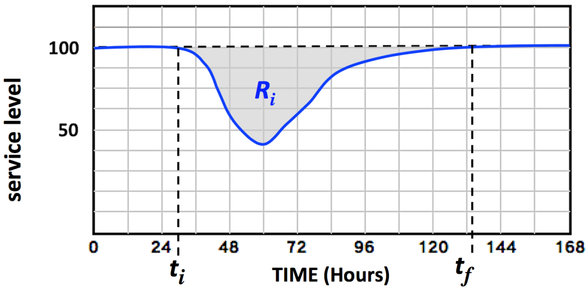


Figure 4.17: Loss of resilience R_i for infrastructure i (Bruneau et al., 2003)

The objective is now to calculate total resilience losses of the bigger system of networked CIs, given a measure for the loss of resilience of single nodes (CIs). Of relevance is to observe that all CIs are critical by definition, but some of them are more critical than others. This means that governments should consider different criticality of infrastructures to prioritize protection plans.

Hence, the importance of a CI is defined accounting for magnitudes of effects that its failure would provoke on other CIs of the system. Considering the weighted connection matrix E, the importance I_j of infrastructure j is given by the sum of magnitudes of effects $e_{ij} \in E$ that a failure of j would provoke to any other infrastructure i (in the networked system). That is,

$$I_j = \sum_i e_{ij}, \quad e_{ij} \in E. \tag{4.7.2}$$

Given a network of $1, 2, \ldots, n$ infrastructures, the system resilience loss R is calculated as the average of resilience loss of single CIs weighted by their relative importance in the system. In formula

$$R = \frac{I_1 R_1 + I_2 R_2 + \cdots + I_n R_n}{R_1 + R_2 + \cdots + R_n}. \tag{4.7.3}$$

After briefly explaining the steps of the policy evaluation process in Section 4.7.3, these resilience metrics are applied in the simulation example in Section 4.7.4 to evaluate policy scenarios using the dynamic interdependency models.

4.7.3 Policy Evaluation Process

The 2013 US National Infrastructure Protection Plan (NIPP) (DHS, 2013) aims at collectively guide national efforts to manage risks to the critical infrastructures of the nation. The US government argues that CI operators must consider national resilience objectives in assessing capabilities of their infrastructure.

Accordingly, a policy evaluation process is defined to describe how to use the interdependency model to support coordination among CI operators towards a collective policy assessment. The four-steps process is as follows.

1. First, a disruption scenario is generated using the building blocks (cf. Section 4.3).
2. Then, the policy of interest must be implemented as part of the initial model setting (i.e. by defining specific values for max CI capabilities, demands factors, etc).
3. A dynamic resilience metric is adopted to conduct the analysis of the simulation scenario (the resilience triangle in this thesis). Here the goal is to quantify first losses of resilience in each CI (node of the network) over time, resilience losses of the entire network of CIs is then calculated according to the importance of each CI in the scenario.
4. The steps above are therefore repeated for different model settings (policies) in order to identify the most effective policy by comparison of resilience analysis results.

Note that effective policies are those which minimize system resilience losses for a specific scenario of disruption. Below, a simulation example demonstrates how to apply this process to evaluate effectiveness of policy investments in CI capabilities with respect to a specific scenario of disruption.

4.7.4 Simulation Example: CI Capability Investments

Figure 4.18 depicts the disruption scenario considered in this example. Concerning interdependencies, transportation systems provide shipment services for both Energy and Financial CIs while receiving fuel, lubricants and power for control systems from the Energy CI and payment services from the Financial CI. Also, the Transport CI needs water for cooling, production and emission reduction of vehicles. Other direct interdependencies between the Water, Energy and Financial CIs are qualitatively described in Section 4.3.1.

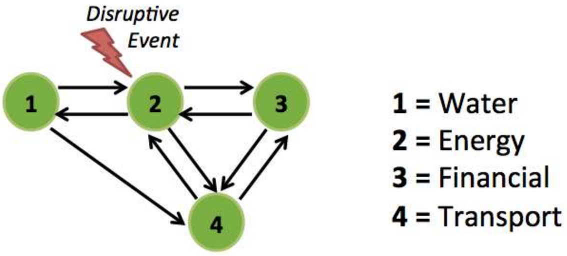


Figure 4.18: Disruption scenario example for policy evaluation.

The following weighted connection matrix quantifies the direct dependencies shown in Figure 4.18.

$$E = \{e_{ij}\} = \begin{bmatrix} 0 & e_{12} & e_{13} & e_{14} \\ e_{21} & 0 & e_{23} & e_{24} \\ e_{31} & e_{32} & 0 & e_{34} \\ e_{41} & e_{42} & e_{43} & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1.33 & 0 & 0 \\ 0.83 & 0 & 0.17 & 1.17 \\ 0 & 2.67 & 0 & 1.00 \\ 0.20 & 2.40 & 0.60 & 0 \end{bmatrix} \tag{4.7.4}$$

The importance of the Water, Energy, Financial, and Transportation CIs with respect to the scenario is obtained by summing up values in every column of the matrix E, i.e.

$$I_1 = 1.03, \quad I_2 = 6.40, \quad I_3 = 0.77, \quad I_4 = 2.17. \tag{4.7.5}$$

The disruption scenario simulates a power blackout $d(t)$ of high magnitude $m_d = 70$ occurring at simulation time $t_d = 24$ hours and lasting half a day, i.e. $\Delta t_d = 12$ hours.

The government wants to invest in a policy that reduces potential system damages due to such operational failures in the Energy CI by increasing capabilities of other CIs (i.e. Water, Financial, and Transportation) by a total of 20%.

The government may decide to increase Transportation CI capabilities by 20%, or perhaps invest 10% in the Water CI and 10% in the Financial CI. The objective is to find the policy that minimizes network resilience losses by optimal allocation of the limited resources. Note that for convenience the model assumes that the increase of capability in any CI has the same cost per unit, different assumptions can be made to consider budget allocation.

In particular, the following list of policies is considered for the analysis.

Scenario	Policy (*% increase of CI capabilities respect to the baseline scenario*)
A	10% Water and 10 % Financial
B	10% Water and 10 % Transport
C	10% Financial and 10 % Transport
D	20% Transport
E	20% Water
F	20% Financial

Table 4.4: Policy scenarios with different allocation of CI capability investments

For $i = 1,2,3,4$, the baseline scenario assumes maximum capabilities of each CI $C^i_{Max} = 100$ operations and average demand for CI services is $D^i_{Av} = 90\%$ of C^i_{Max}.

For each of the policy scenarios in Table 4.4, the SD model is simulated to calculate the resilience loss of single CIs and then system resilience loss R as described in Section 4.7.2. Simulation results are shown in the left chart of Figure 4.19.

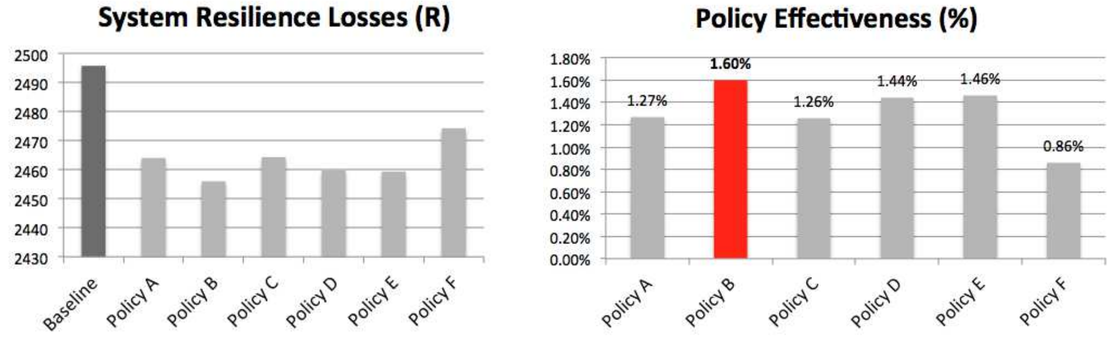


Figure 4.19: System resilience losses for policy scenarios of Table 4.4 (chart on left) and effectiveness of policy investments with respect to the baseline scenario (chart on right).

In Figure 4.19, the chart on left shows system resilience losses for the baseline scenario (dark grey column) and the different policies (light grey columns). The chart on the right shows effectiveness of each policy compared to the baseline disruption scenario (i.e. with no investments). By increasing both Water and Transport CI capabilities of 10%, Policy B (red column) improves system resilience by 1,6% and it results the most effective strategy according to initial goals of the analysis.

Observing the results of the policy evaluation, the worst system performance is obtained by investing all the 20% in capabilities of the Financial CI. This is not surprising since the Financial CI is also the infrastructure with “lowest importance” ($I_3 = 0.77$) in the network of CIs. However, fully investing in the Transportation CI (Policy D), which is the “most important” infrastructure ($I_4 = 2.17$) considered in the policy scenarios, does not lead to the best system performance.

Simulation suggests that balancing increases of both Transport and Water CI capabilities can better reduce cascading effects of half-day Energy CI disruptions into the system of CIs. In fact, investments in power generators to improve operational capabilities of transportation systems and water distribution pumps are both relevant for the maintenance of the vital societal functions in case of power outages.

Prioritization of capabilities among CIs is a complex process that requires a careful analysis of complex system dynamics of disruptions. The above example demonstrates how the dynamic interdependency modeling approach can support the identification of such priorities for more effective investments in CI capabilities.

In line with the purpose of the 2013 US National Infrastructure Protection Plan (NIPP) (DHS, 2013) to guide the national effort to manage risks to the nation’s critical infrastructures, the interdependency model developed in this thesis can help CI operators to collectively identify priorities, articulate clear goals, mitigate risk, and measure progress toward national resilience objectives.

4.8 Brief Summary

This chapter introduces a block building modeling approach based on system dynamics (SD) to understand complex dynamics of disruptive events in CI networks. Inspired by the structure of compartmental epidemic models, blocks of models are developed to capture different aspects of both micro (single CI) and macro (across CIs) dynamics in such complex system of systems. Scenarios of single or multiple disruptions in interdependent systems of CIs are build using the SD building blocks of models. Accordingly, resilience of every CI is evaluated with respect to the bigger system of CIs.

Hence, building blocks are primarily used to generate disruption scenarios with the purposes of simulation-based impact analysis and dynamic resilience assessment. Simulation examples illustrate the effects of disruption magnitude on dynamics of cascading effects, the impact analysis can be also conducted by varying the disruption duration, or even both magnitude and time duration of disruptive events.

Toward investigating dynamic resilience, a further application shows how to evaluate effectiveness of policy investments in CI capabilities. SD simulations are run to measure system resilience under different policy scenarios to reduce effects of power outage. Findings highlight the relevance of recognizing interdependencies among CIs in planning for business operations.

The dynamic interdependency models can be also used to provide insights for risk assessment. In particular, a simulation example demonstrate how to apply the SD model to assess magnitude of cascading effects in different risk scenarios using SD sensitivity analysis tools.

The overall objective is to provide insights for potential users of the dynamic interdependency models, such as CI operators that continuously attempt to forecast scenarios and assess risks of failures in interdependent CIs. Flexibility and potentials of the modeling approach allow to a number of other applications. Further contributions and extensions of the modeling through the use of new technologies and methodologies are presented as research iterations in the following chapters of this thesis.

Chapter 5

Cybersecurity within Organizations

Cyber attacks are increasingly becoming the cause of operational failures in critical infrastructures (CIs). Decision support tools must consider both operational and strategic layers to assist in understanding nonlinear dynamics of such complex cyber-physical systems.

This chapter builds on the modeling of Chapter 4 to explore disruptive dynamics of CI operations when the trigger event is a cyberattack. The aim is to understand how strategic behaviors of attacker and defender impact operational performances of the target CI. Thereby, a novel combination of system dynamics (SD) with a game-theoretic approach is used to investigate cybersecurity dynamics within a single CI.

Section 5.1 provides a brief overview of existing game-theoretic approaches in cybersecurity of CIs. Particularly inspired by the *FlipIt* game (Dijk et al., 2013), emphasis is given to temporal dynamics of the players who compete to gain the control of CI operations through asynchronous decision making. In addition, the cyber game accounts for resources and capabilities of the players, i.e. thresholds upon which decisions are made over time.

Therefore, Section 5.2 introduces the dynamic attacker-defender model as continuous game of timing to highlight that the effectiveness of strategic moves strongly depends on when to act. The cyber game dynamics is investigated for scenarios with stealthy adaptive attackers and observable periodic defenders, which is the most common case in reality. While in the *FlipIt* game a player can fully take over the resource instantly, in the dynamic attacker-defender model interdependent player strategies are modeled according to time needed to attack, time needed to defend, and players' thresholds. A graphical representation of the model using Vensim stock-and-flow diagrams is provided in Section 5.3. The final goal to conduct a multi-objective optimization of cyber defense policies using SD tools (Section 5.4). Accordingly, the chapter concludes with a simulation analysis of optimized proactive and reactive defense scenarios to demonstrate how the model can support cybersecurity within organizations (Section 5.5).

Note that this work has been published by the author in (Canzani and Pickl, 2016).

5.1 Game-theoretic Approaches

Game theory is the study of mathematical models of conflict and cooperation between intelligent rational decision-makers (Myerson, 2013). It assumes that human interactions have the characteristics of a game. Originally used in economics, game theory is a powerful tool to support policy optimization in a wide range of applications. Obviously, the type of game must be chosen according to the problem of interest. Figure 5.1 illustrates a taxonomy of games given by (Roy et al., 2010).

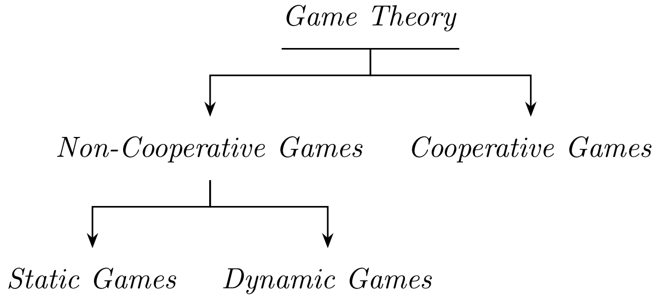


Figure 5.1: Classification of games (Roy et al., 2010)

A **non-cooperative game** is a game with competition between players with opposite objectives, as opposed to **cooperative games**. Conflicting behavior of players can be studied in one or more stages over time. **Static games** are one-shot games in which all players simultaneously decide their plan of action (i.e. their strategy). In **dynamic games**, players can choose their moves in different stages.

In the field of cyber security, existing game-theoretic research falls under non-cooperative games. In particular, game theory has been largely used to understand the nature of cyber conflicts: attacker and defender interact with the attempt to maximize their intended objectives (Roy et al., 2010). In particular, game-theoretic approaches can provide valuable insights to support cost-benefit analysis (Manshaei et al., 2013). An application to malware proliferation prevention is (Spyridopoulos et al., 2013).

Attacker and defender modeling is also applied to the analysis of critical infrastructures (see, e.g., (Ten and Manimaran, 2010)). (Backhaus et al., 2013) highlight how interactions between attacker and system operator strongly depends on the design of cyber-physical network infrastructures. (He et al., 2012) model probabilities of successful attacks in both cyber and physical spaces as functions of the number of components that are attacked and defended. A survey of game theory for energy systems can be found in (Bosetti et al., 2014).

However, many of the existing models do not consider the relevant component of timing. See, for example, the robust optimization model for resource allocation of defensive budget proposed by (Zhuang and Nikoofal, 2012).

Concerning the relevant component of time, a branch of the game theory literature that accounts for time-dependent aspects refers to the the so-called ”games of timing” (Radzik, 1996). The focus of this studies is on ”when” the player should act to get an advantage over the opponent, rather then ”how much” to invest or ”what” strategy must be selected among the possible options.

Of particular interest is the *FlipIt* game (Dijk et al., 2013), a two-player non-cooperative game with continuous timing and asynchronous decision-making. In *FlipIt*, attacker and defender compete to control a critical resource. Players can make a move at any time to take over the control of the resource. Their objective is to maximize the fraction of time they are in control of the resource.

The classification of games in Figure 5.1 can be further extended on the basis of information available to the players. A game is called **perfect information game** if each player is aware of the moves of all other players, **imperfect information game** otherwise. A **complete information game** is a game in which every player knows strategies and payoffs of all players in the game, but not necessarily the moves. If at least one of the player is not aware of possible strategies and payoffs of adversaries, it is an **incomplete information game**.

Thus, different scenarios can be generated with *FlipIt* depending on which kind of information are known to the players. For instance, advanced persistent threats (APTs) benefit from advanced system knowledge to launch zero-days attacks. APTs are often silent and not immediately detected by the system administrator. (Zhang et al., 2014) use *FlipIt* to investigate such scenarios of stealthy attacks and observable defenses. (Nochenson et al., 2013) conduct a behavioral investigation of *FlipIt* through an experiment with 300 participants by changing the information that a player has available when the game starts. Other applications of *FlipIt* to system security can be found in (Bowers et al., 2012).

Beyond two-player attacker-defender games, a survey of interdependent security information games can be found in (Laszka et al., 2014). Example of game theoretic approaches in heterogeneous networks are in (Chen and Leneutre, 2009) and (Hernández et al., 2013).

5.2 Block 1’: Attacker-Defender Dynamic Model

In the first implementation of the model in Chapter 4, disruptive events are modeled with a general pulse function that considers the disruption magnitude, its duration, and time in which the disruption occurs (cf. Block 1 in Section 4.1). If such disruptive events are triggered by cyberattacks, operational dynamics of the target CI emerges from strategic interactions between attacker and defender. With the purpose of understanding specific cybersecurity dynamics in CI systems, a new SD building block (Block 1’) is developed to replace the general disruptive event (Block 1) with a game theoretic model that replicates the cyber conflict. In Chapter 3, Figure 3.5 illustrates how the block building modeling framework (cf. Figure 3.4) is extended with Block 1'.

The combination of SD and Game Theory allows to capture complex attack-defense dynamics over time. In particular, operational dynamics within a single CI (Block 2) are influenced by strategic behaviors of the players in the cyber game (Block 1'). Towards a multi-layer approach to security of cyber-physical systems, the two building blocks are integrated to understand interdependent dynamics of

- the **operational layer**, i.e. dynamics of operations in a single CI (Block 2); and
- the **strategic layer**, i.e. the attacker-defender game dynamics (Block 1').

Different from existing game theoretic-approaches that bound the cybersecurity issue into budget allocation and optimization problems (cf. Section 5.1), a special emphasis is given to time-dependent aspects to highlight that effectiveness of strategic choices to maximize benefits also depends on when to act.

Inspired by the *FlipIt* game (Dijk et al., 2013), interactions between players are modeled as a continuous game of timing with asynchronous decision making that suits the SD simulations. Assuming that players compete to gain the control of the infrastructure over time, the attacker aims at breaking down CI operations while the defender tries to restore them back to function. In *FlipIt* (cf. Section 5.1), a player can fully take over the resource instantly by making a move. However, in reality attacker and defender need time to perform their actions. The cyber game proposed in this thesis avoids such limitation by considering a further time component, which is the time players need to fully take over the control of CI operations.

In particular, the dynamic attacker-defender model considers scenarios with

- **stealthy adaptive attacks**, and
- **observable periodic defenses**.

This means that the defender does not know attacker moves and adopts a regular periodic defense strategy for checking and patching the system. On the other side, the attacker has information about the defender moves and decides when to exploit vulnerabilities on the basis of defender moves and system state (i.e., security level of the target CI). A similar scenario with stealthy attacks and observable defenses is discussed by (Zhang et al., 2014), but the authors do not consider adaptive attackers in their work.

5.2.1 Attacker and Defender Thresholds

Effectiveness of attacker and defender strategies also depends on their resources, skills, motivation, knowledge and budget. In the model, such player characterization corresponds to thresholds upon which decisions are made over time.

Let $l(t)$ be the *security level* of the CI. At any time t, $l(t)$ indicates the level of system security on a scale of 0 (fully vulnerable) to 1 (not vulnerable, that is the ideal case). Values of player thresholds are defined in the same scale of 0 to 1 as follows:

- *Attack Threshold*, T_A, s.t. successful attack if and only if $l(t) \leq T_A$;
- *Defend Threshold*, T_D, s.t. $l(t) \geq T_D$ at any time t (security policy).

In other words, the cyber activist is able to identify and successfully exploit system vulnerabilities up to a certain level of system security (i.e. T_A). However, he cannot launch more sophisticated attacks to vulnerabilities above such threshold, i.e. vulnerabilities unknown to the attacker. The IT administrator uses available cybersecurity resources and tools to protect the CI system and guarantee a minimum level of system security (i.e. T_D). This means that the defender is able to resolve those vulnerabilities that are known to him, and update the system so that the security level does not go below the threshold value. Obviously the defender is unable to protect the CI against attacks to vulnerabilities which are unknown to him, but he can periodically check the system to detect silent attacks (if any).

Given these assumptions, two possible cases of scenario are represented in Figure 5.2.

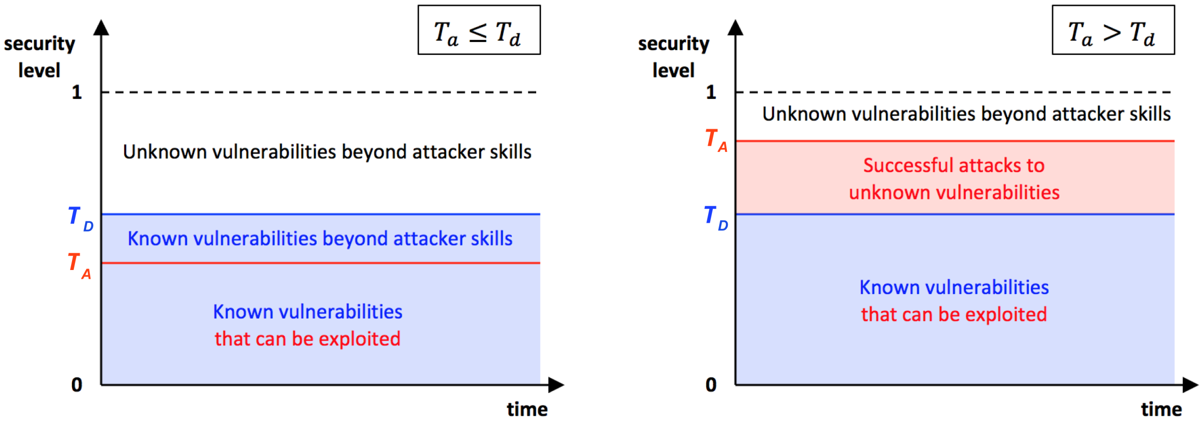


Figure 5.2: Scenarios generated by relationships between attacker and defender thresholds

Figure 5.2 on left shows that the attacker cannot take over the control of the system if the security level over time is always higher than the attack threshold, i.e. $T_A < T_D$. In this case the attacker would only identify those vulnerabilities for which patching measures are available to the defender. Figure 5.2 on the right illustrates the case in which the attacker is stronger than the defender ($T_A \geq T_D$), and therefore he can launch zero-days exploits to vulnerabilities unknown to the IT-administrator.

5.2.2 Cyber Game Dynamics

The game is simulated over a fixed time period $[t_0, t_f]$. As in reality IT-components degrade over time, the model assumes that the CI security level decreases according to a *security loss factor*, s_{loss} s.t. $0 \leq s_{loss} \leq 1$. Changing the value of s_{loss}, game dynamics can be simulated under different risk scenarios: the bigger s_{loss} is, the quicker the security level decreases over time.

Hence, defense moves aim at periodically bringing up to 1 the degraded security level $l(t)$ through system checking, patches and updates. The *defender periodic strategy* $S_D(t)$ is modeled as periodic function varying over time from T_D (minimum security level according to available security measures) to 1.

Let n_D be the *number of defender moves* available to the defender over the fixed simulation time period $[t_0, t_f]$. The period p of the periodic strategy $S_D(t)$ is calculated by equally distributing the moves along the game, i.e.

$$p = \frac{t_f - t_0}{n_D}.$$

Note that the bigger the number of moves is, the shorter the period of the periodic defense strategy is because the game is simulated over a fixed time interval. Therefore, n_d can be also referred as the *frequency* of moves in $S_D(t)$.

Finally, the *defender periodic strategy* $S_D(t)$ is defined as follows.

$$S_D(t) =: \max\left(T_D, 1 - \frac{t \mod p}{p \cdot n_D \cdot (1 - s_{loss})}\right). \tag{5.2.1}$$

As the periodic strategy ranges between T_D (lowest security level of the strategy) and 1 (ideal case of a fully secure system), S_D takes the maximum between T_D and the periodic construct which replicates effects of defense moves over time. The periodic construct is obtained with the function $t \mod p$ that returns, at any time t, the reminder of the ratio between the current time t and the period p i.e. a number between 0 and p. This number is normalized between 0 and 1 by dividing by a factor p. The term $n_D \cdot (1 - s_{loss})$ serves to control the slope between periods (defense moves) based on the security risk scenario. As the system security level decreases within period lengths (time between system updates), "$1 - \mod$" is taken in 5.2.1. Note that MODULO and MAX are predefined functions in Vensim DSS.

The *FlipIt* game assumes a player can fully take over the resource (CI) instantly. This unrealistic assumption is removed by distinguishing between player strategy and actual control. The *defender control* $D_{ctrl}(t)$ is modeled with a SMOOTH function in Vensim to delay the strategy $S_D(t)$ by the time the defender needs to check the system and take back its control, i.e. the *time to defend*, Δt_D. In formula,

$$D_{ctrl}(t) =: \max\big(0, f_{smooth}(S_D(t), \Delta t_D)\big). \tag{5.2.2}$$

Note that in 5.2.2 the maximum is taken to guarantee non-negativity of $D_{ctrl}(t)$.

Figure 5.3 clarifies differences between defender strategy and his actual control of the system. It also highlights that $S_D(t)$ has a linear decrease between defense moves determined by s_{loss}. The output graph in Figure 5.3 refers to a game simulated over 3-month time period for a low-risk scenario $s_{loss} = 0.3$ with monthly defenses ($n_D = 3$), $T_D = 0.7$ and $\Delta t_D = 24$ Hours.

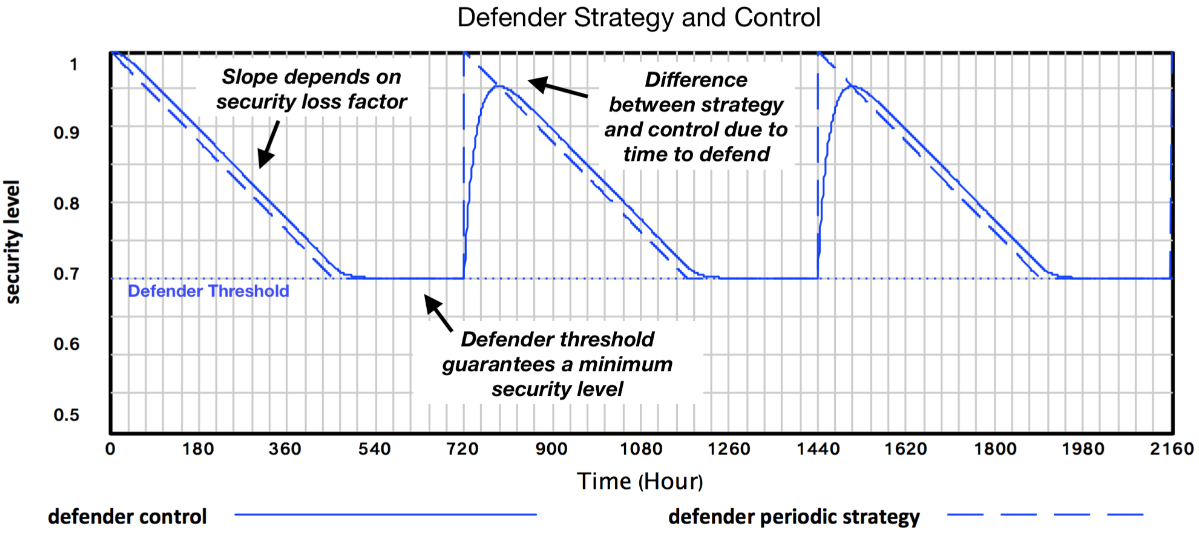


Figure 5.3: Difference between defender strategy and actual control

Defense strategy and system degradation over time follow such dynamics until an attacker identifies the target CI and starts observing the system to take over the control of CI operations. In modeling, this moment of time is defined as the *targeted system time*, t_{target}; Obviously, attacker-defender dynamics start at $t \geq t_{target}$.

While the defender is periodically updating and checking the system, the adaptive attacker observes what the defender is doing and launches successful attacks as soon the security level $l(t)$ is lower than the threshold T_A.

Note that the system security level clearly depends on defender policy and actions over time. Thus, $l(t) := D_{ctrl}(t)$ by definition. This means that the *attacker adaptive strategy* $S_A(t)$ consists of learning defender moves and attack it every time that his threshold is above the current defender control $D_{ctrl}(t)$. Mathematically,

$$S_A(t) := \begin{cases} 1, & \text{for all } t : D_{ctrl}(t) \leq T_A, \\ 0, & \text{otherwise.} \end{cases} \tag{5.2.3}$$

In Vensim, the attacker strategy $S_A(t)$ is modeled with a STEP function that, within a cycle IF THEN ELSE, provides an input of height 1 at every time t s.t. $D_{ctrl}(t) \leq$

T_A. In fact, this condition implies that the attacker can successfully exploit system vulnerabilities. As for the defender, also the attacker needs time to perform his actions and take over the control of the CI. Similar to $D_{ctrl}(t)$, the *attacker control* $A_{ctrl}(t)$ is defined by smoothing $S_A(t)$ for the *time to attack* Δt_A.

$$D_{ctrl}(t) =: \max\big(0, f_{smooth}(S_A(t), \Delta t_A)\big). \tag{5.2.4}$$

Figure5.4 gives an example of strategic dynamics of attacker and defender competing to control the CI over time. The output graph in Figure 5.4 refers to a game simulated over 3-month time period for a low-risk scenario $s_{loss} = 0.3$. The system is protected with monthly defenses ($n_D = 3$), $T_D = 0.7$, and $\Delta t_D = 24$ Hours. Successful exploits are launched by a sophisticated attacker with $T_A = 0.9$ and $\Delta t_A = 24$ Hours.

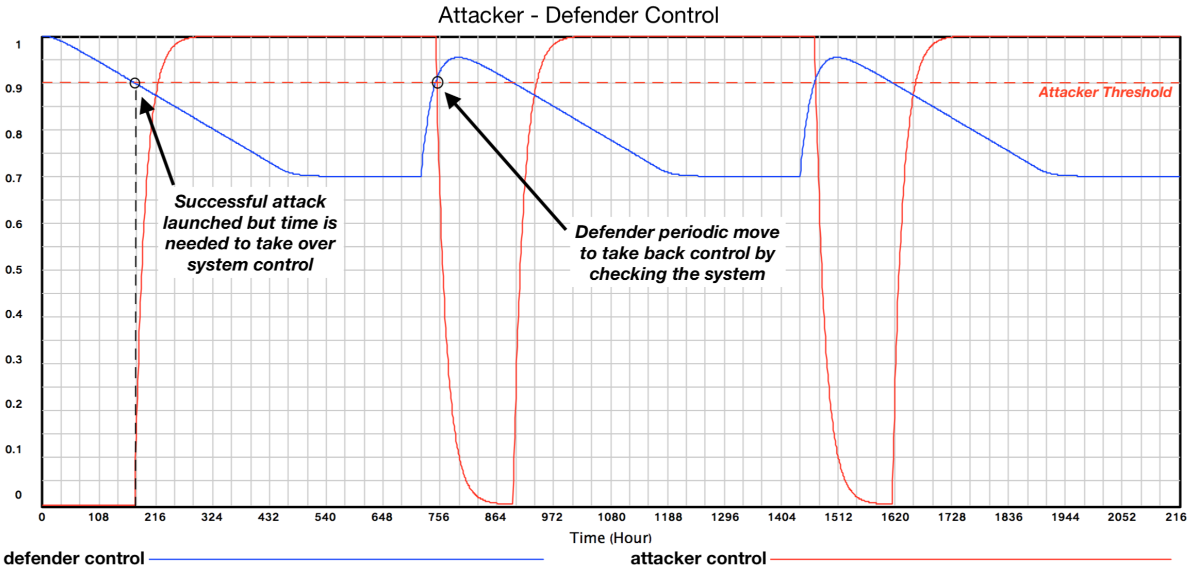


Figure 5.4: Attacker-defender control dynamics

Once defined strategies of attack and defender during the game, benefit of players depends on:

(i) the fraction of time they are in control of CI operations, and

(ii) portions of total CI operations they control over time.

Note that (ii) assumes that the control of CI operations does not "flip" instantly between players, such as in the *FlipIt* game, but time is needed to gain it. Accordingly, *total gain* of each player is defined as cumulative control of CI operations over time as follows.

$$G_A(t) = \int_{t_0}^{t_f} A_{ctrl}(t)dt, \qquad G_D(t) = \int_{t_0}^{t_f} D_{ctrl}(t)dt. \tag{5.2.5}$$

Gains of attacker and defender are the result of strategic decisions made over time that affect operations of the target infrastructure. Mathematically, operational and strategic layers are combined in the following system of differential equations.

$$\begin{cases} \dfrac{\mathrm{d}}{\mathrm{d}t}\big(OP_{run}(t)\big) = -\alpha(t)\Big(\dfrac{OP_{run}(t)}{n_{OP}}\Big) + \gamma(t)OP_{rec}(t) \\ \dfrac{\mathrm{d}}{\mathrm{d}t}\big(OP_{down}(t)\big) = \alpha(t)\Big(\dfrac{OP_{run}(t)}{n_{OP}}\Big) - \beta(t)OP_{down}(t) \\ \dfrac{\mathrm{d}}{\mathrm{d}t}\big(OP_{rec}(t)\big) = \beta(t)OP_{down}(t) - \gamma(t)OP_{rec}(t) \end{cases} \tag{5.2.6}$$

Note that the system in Equation (5.2.6) corresponds to the system in Equation (4.2.2) in Chapter 4 describing the operational dynamics of a general infrastructure i. Similarly, $OP_{run}(t) + OP_{down}(t) + OP_{rec}(t) = n_{OP}$ at any time t.

In Chapter 4, the main focus is on the breakdown rate of running operations, $\alpha(t)$; while assuming constant rates to repair and restore operations ($\beta(t)$ and $\gamma(t)$ respectively). In the dynamic game model, the attacker attempts to break operations down influencing $\alpha(t)$, while $\beta(t)$ changes according to defender moves to gain system control and recover disrupted operations. These rates depend on player benefits and time needed to make attack and defense moves respectively, i.e.

$$\alpha(t) = \frac{G_A(t)}{\Delta t_A}, \qquad \beta(t) = \frac{G_D(t)}{\Delta t_D}. \tag{5.2.7}$$

Recovered operations are restored back to function with constant rate, i.e. $\gamma(t) = \gamma_0$.

For convenience, the system in Equation (5.2.6) is written in a compacted form as follows.

$$\begin{cases} \dfrac{\mathrm{d}}{\mathrm{d}t}\big(OP_{run}(t)\big) = -\Phi_\alpha(t) + \Phi_\gamma(t) \\ \dfrac{\mathrm{d}}{\mathrm{d}t}\big(OP_{down}(t)\big) = \Phi_\alpha(t) - \Phi_\beta(t) \\ \dfrac{\mathrm{d}}{\mathrm{d}t}\big(OP_{rec}(t)\big) = \Phi_\beta(t) - \Phi_\gamma(t) \end{cases} \tag{5.2.8}$$

In accordance with SD terminology, equations in (5.2.8) describe the variation of stocks (OP_{run}, OP_{down}, OP_{rec}) over time as sum of outflows (negative terms in (5.2.6)) and inflows (positive terms in (5.2.6)). Namely, they are the *flow of operation breakdown* $\Phi_\alpha(t)$, the *flow of operation recovery* $\Phi_\beta(t)$, and the *flow of operation restore* $\Phi_\gamma(t)$.

The implementation of the stock-and-flow model using SD tools is illustrated below.

5.3 Implementation with Vensim

After the analytical description of the attacker-defender dynamic model, Figure 5.5 clarifies how Block 1’ and Block 2 are integrated with Vensim to capture interdependent dynamics of strategic and operational layers.

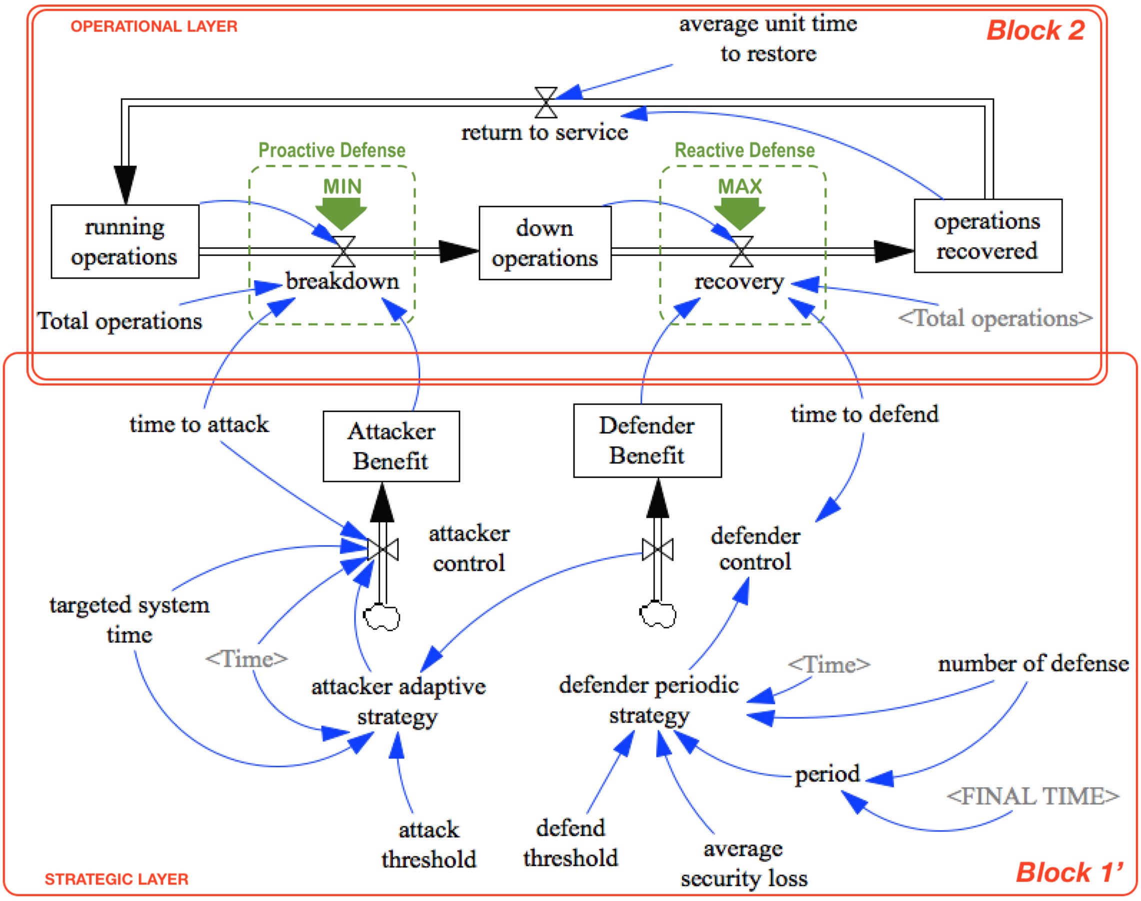


Figure 5.5: SD stock-and-flow diagram of the dynamic attacker-defender model

The green dashed boxes in Figure 5.5 show the optimization objectives for proactive and reactive defenses. Details and application of the model to defense strategy optimization are discussed in the next section.

5.4 Defense Strategy Optimization

This section describes how to test effectiveness of proactive and reactive defense strategies using the dynamic attacker-defender model. In particular, the analysis refers to

- **proactive defenses**, which are those security resources dedicated to the prevention of expensive damages that will likely occur if such preventive measures are not taken; and
- **reactive defenses**, that refer to recovery plans in place to respond to business losses caused by successful cyber attacks when proactive approaches either were not effective or did not exist.

The optimization of such defense strategies is done with respect to specific attack scenarios. Thus, as model input parameters it must be defined:

- how fast security decreases over time by choosing a value for the security loss factor s_{loss}, $0 \leq s_{loss} \leq 1$; and
- attacker skills, resources, and capabilities determined by attack threshold T_A and time needed to perform the attacks Δt_A.

Given the security risk scenario and the adaptive attacker, the objective is to find the optimal combination of factors representing defender periodic strategies (i.e. n_D, T_D, and Δt_D) such that best operational performances are obtained in the CI system (cf. equations in 5.2.8).

With respect to the system of differential equations in (5.2.8), optimization of proactive strategy corresponds to minimizing the flow of operation breakdown, i.e. $\Phi_\alpha(t)$. In particular, note that minimizing $\Phi_\alpha(t)$ is equal to maximize $-\Phi_\alpha(t)$. Optimizing reactive strategy means maximizing the flow of operation recovery $\Phi_\beta(t)$. In terms of the SD model, see green dashed boxes in Figure 5.5.

In reality, organizations invest in both proactive and reactive defenses by allocating the cybersecurity budget in different ways. Therefore, the defender payoff function considers a weighted combination of proactive and reactive strategies by introducing a *weighting factor* c s.t. $0 \leq c \leq 1$ that allows emphasizing different aspects of the cybersecurity policy. The *policy payoff function* is as follows:

$$c(-\Phi_\alpha(t)) + (1-c)(\Phi_\beta(t)). \tag{5.4.1}$$

Therefore, proactive and reactive optimization problems are reduced to a unique maximization problem that accounts for mixed defense strategies. This means that the IT administrator may decide whether to give more importance to proactive or reactive defense by adjusting the weighting factor c. Note that $c = 1$ corresponds to a fully allocation of the budget for proactive defense, while $c = 0$ for reactive defenses in **??**.

In Vensim DSS, policy optimization tools are used to perform the nonlinear multi-objective optimization that accounts for the complex system dynamics of both strategic and operational layers captured by the SD model. In line with the equation (5.4.1), the Vensim policy payoff function is defined as weighted combinations of different model variables in which weights can be adjusted to emphasize different aspects of the payoff. The policy payoff is then integrated over the simulation by an efficient Powell hill-climbing algorithm that searches through selected parameters (Δt_D, n_D, and T_D in this case) looking for the largest cumulative payoff.

Accordingly, the optimization problem is to

$$
\begin{aligned}
\underset{\Delta t_D, n_D, T_D}{\text{maximize}} \quad & \int_{t_0}^{t_f} c(-\Phi_\alpha(t)) + (1-c)(\Phi_\beta(t))dt && (5.4.2)\\
\text{subject to} \quad & \Delta t_D \geq \Delta t_D^{min} > 0, && (5.4.3)\\
& 0 \leq n_D \leq n_D^{max}, && (5.4.4)\\
& 0 \leq T_D \leq T_D^{max}. && (5.4.5)
\end{aligned}
$$

The Vensim optimizer solves the optimization problem in 5.4.2 by looking for optimal combinations of Δt_D, n_D, and T_D subject to general constraints 5.4.3, 5.4.4, and 5.4.5, which represent limited capabilities of the defender due to the current state of IT and cybersecurity knowledge. Concrete assumptions upon which to define a feasible parameter space are described in the next section.

5.5 Proactive and Reactive Defense Analysis

The SD model is simulated over a 3-month time period with an hourly timescale, that is $[t_0, t_f] = [0, 2160]$ Hours (assuming months of 30 days each).

At the operational level, CI capabilities are $n_{OP} = 10000$ operations and the system is initially in its normal operational state, i.e. $OP_{run}(t_0) = n_{OP}$.

At the strategic level, of interest is the case in which the attacker is stronger than the defender (i.e. $T_A > T_D$, see Figure 5.2). In this scenario CI operational dynamics is triggered by successful attacks to vulnerabilities that the defender is not able to identify. In particular, high security risk scenario with $s_{loss} = 0.7$ is considered. The adaptive attacker launches very sophisticated attacks with threshold $T_A = 0.9$ and time to perform his moves $\Delta t_A = 24$ hours. Also, the attacker can move unlimitedly (i.e., no constraints on number of attacks).

Note that simulations assume that the time in which the attackers identifies the target CI and starts observing the system is equal to the initial time, $t_{target} = t_0 = 0$.

With this scenario setting, the goal is to find best defense policies under the following assumptions which limit defender capabilities (cf. constraints 5.4.3, 5.4.4, and 5.4.5):

$$\Delta t_D \geq \Delta 24 \text{ hours}, \tag{5.5.1}$$

$$0 \leq n_D \leq 15, \tag{5.5.2}$$

$$0 \leq T_D \leq 0.8. \tag{5.5.3}$$

In other words, the feasible parameter space to find optimal defense strategies is determined by assuming that

(i) the defender needs at least one day to check the entire IT system 5.5.1;

(ii) the highest frequency for periodic updates and system checking is every 6 days 5.5.2;

(iii) existing patches and available IT security tools can guarantee a level of system security up to 80% 5.5.3.

The latter implies that even investing in latest technologies, cyber activists can still successfully exploit system vulnerabilities up to 20%. In particular, the attacker considered in the simulation scenario is able to exploit 10% of vulnerabilities which are unknown to the defender. In fact, $T_D^{max} = 0.8 < T_A = 0.9$.

Under these assumptions, the optimization problem in 5.4.2 is discussed for scenarios of proactive ($c = 1$) and reactive ($c = 0$) defenses. Simulation analysis attempts to find out if improving time components (i.e. Δt_D and n_D) may lead to more effective defense strategies rather than investing in expensive technology (T_D).

Using Vensim optimization tools, the Powell hill-climbing optimization algorithm is able to find local optima. Nevertheless, preliminary simulation experiments have shown that the optimizer selects the optimum for Δt_D equal to its minimum feasible value at any initial point of search. Let Δt_D^* be the optimal time to defend. (Hereafter, optimal values are marked by an asterisk). In accordance with 5.5.1,

$$\Delta t_D^* = \Delta t_D^{min} = 24 \text{ hours}.$$

It is obvious that the faster the defender performs a move, the earlier he can take back control of the system. The practical recommendation to IT administrators is to minimize (whenever possible) the time needed for checking and updating the system.

On the basis of this finding, analysis of scenarios focus on the optimization of

- frequency of defenses n_D (i.e. ”when” to act for system checking),

- defender threshold T_D (i.e. ”how much” to invest in IT security tools).

Note that optimization is conducted for different initial points of search, which correspond to different periods of the periodic defense with a baseline threshold $T_D = 0.7$. Whitin the feasible parameter space $0 \leq n_D \leq 15$ (cf. 5.5.2), local optima are searched for $n_D = 3, 6, 9, 12$ (and $T_D = 0.7$). Optimal values n_D^* and T_D^* are global optima if the Vensim optimizer finds the same values for local optima at any initial point of search.

Proactive Defense

Proactive Periodic Strategy	Frequency n_D	Threshold T_D	Policy Payoff
30-days period	3	0.7	-56648.8
15-days period	6	0.7	-56993.7
10-days period	9	0.7	-56821.3
7-days period	12	0.7	-55134.6
Optimal Defense	$n_D^* = 15$	$T_D^* = 0.74$	-50734.1

Table 5.1: Proactive periodic defenses for different periods and optimal strategy

Table 5.1 shows non-optimized payoffs for different values of n_D, i.e., different periods of proactive defense with the baseline threshold $T_D = 0.7$. The last row reports optimal values n_D^* and T_D^* that maximize the payoff at any initial point of search. Optimal solutions correspond to the highest feasible frequency (cf. 5.5.2) ($n_D^* = n_D^{max} = 15$) and a threshold slightly bigger than the baseline value, i.e.

$$n_D^* = n_D^{max} = 15 \quad \text{and} \quad T_D^* = 0.74.$$

In reality, this means that the protection of CI operations from expensive damages is more effective if the IT administrator checks the system more often rather than investing in latest IT security tools. To compare effectiveness of proactive security policies in Table 5.1, the output graphs in Figure 5.6 illustrate defender benefit $G_D(t)$ (at the strategic level) and down operations $OP_{down}(t)$ (at the operational level) over time.

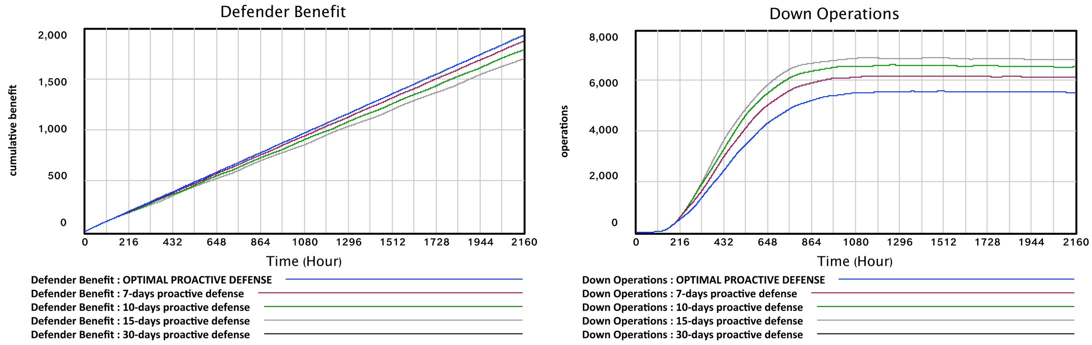


Figure 5.6: Effects of proactive defenses on down CI operations and defender benefit

Reactive Defense

Reactive Periodic Strategy	Frequency n_D	Threshold T_D	Policy Payoff
30-days period	3	0.7	49557.6
15-days period	6	0.7	50266.1
10-days period	9	0.7	50297.2
7-days period	12	0.7	49018.9
Optimal Defense	$n_D^* = 3$	$T_D^* = 0.8$	52642.3

Table 5.2: Reactive periodic defenses for different periods and optimal strategy

Similar to Table 5.1 , Table 5.2 shows numerical results of non-optimized payoffs for different values of n_D i.e., different periods of reactive defense with the baseline threshold $T_D = 0.7$. The last row shows optimal values n_D^* and T_D^* that maximize reactive policy payoff.

In contrast to proactive measures, optimal solutions for reactive strategies are found at relatively low frequency and highest defender threshold (cf. 5.5.2). That is

$$n_D^* = 3 \quad \text{and} \quad T_D^* = T_D^{max} = 0.8.$$

Once the CI operations are down due to cyber attacks, finding new patches and updates to restore CI services is more relevant than focusing on the frequency of periodic system checking. Therefore, it is recommended to invest in latest technologies for improving performances of mitigation response actions. Simulation graphs in Figure 5.7 compare defender benefits and CI operation recovery for periodic reactive strategies in Table 5.2.

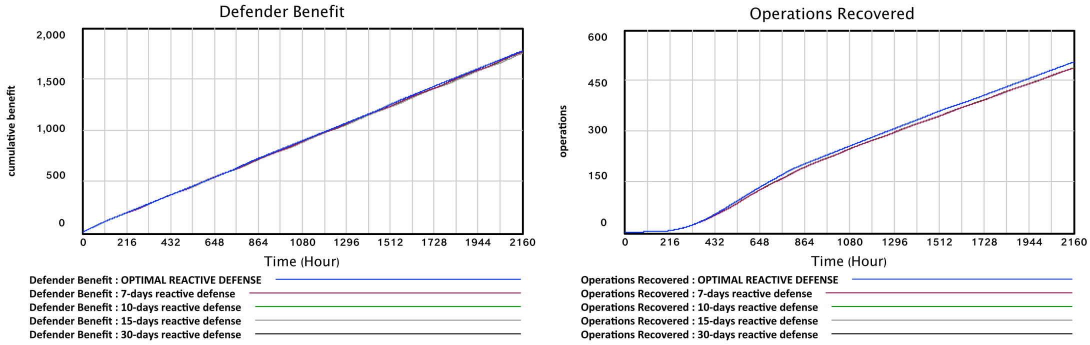


Figure 5.7: Effects of reactive defenses on recovered CI operations and defender benefit

Simulation comparisons show that optimizing preventive measures can decreases potential expensive damages up to 19%, while optimal mitigation responses can speed up operation recovery by about 4%. Therefore, effectiveness of periodic defenses strongly relies on the optimization of timing for system prevention rather than on IT investments in recovery plans. This finding is also demonstrated by optimization results in Tables 5.1 and 5.2.

5.6 Brief Summary

This chapter combines SD with a game-theoretic approach to better understand how strategic attacker and defender interactions impact operational dynamics of CIs. Different from many game theoretic approaches which focus on how much to invest in cybersecurity measures, the relevant aspect of timing is emphasized to demonstrate that effectiveness of strategic actions also depends on when to act.

In modeling, this contribution extends the block building modeling approach proposed in this thesis by introducing a new building block, named Block 1'. In fact, the dynamic attacker-defender model replaces the general disruptive event of Block 1 to generate strategic cybersecurity scenarios.

Inspired by the *FlipIt* game (Dijk et al., 2013), the dynamic attacker-defender model is presented as continuous game of timing to emphasize temporal dynamics of the players who compete to gain the control of CI operations through asynchronous decision making. Novelty resides in the fact that cyber game dynamics emerge from time players need to fully take over the CI and thresholds (i.e. player characteristics) upon which decisions are made over time.

The cyber game model considers scenarios with stealthy adaptive attackers and observable periodic defenders, which is the most common case in reality. Thus, simulations investigate scenarios of proactive and reactive periodic defenses against adaptive attackers using SD multi-objective optimization tools.

Analysis of results highlight that optimization of time components is key towards more effective cybersecurity policies within organizations. It follows the practical recommendation for IT administrators that should leverage timing rather than investing in latest technologies, especially when available security tools fail against evolving APTs. Simulation results demonstrate that proactive defenses are much more effective than reactive ones. Of interest is that such research outcomes are in line with the Codenomicon whitepaper (Juuso and Takanen, 2012), stating that “the only effective form of cybersecurity is proactive cybersecurity”.

Chapter 6

Cybersecurity across Organizations

The strategic use of information systems to coordinate response efforts across organizations is a major objective towards more resilient societies. This chapter presents an application of the dynamic interdependency model to the scenario of the project ECOSSIAN (European Control System Security Incident Analysis Network) as relevant contribution to the design of a cyber incident response and early warning system for CI operators in Europe.

Section 6.1 introduces early warning and incident response systems for CIP in the context of the ECOSSIAN. In particular, the interdependency model is extended by a perspective of CI operators in accordance with the work of the European Network Information Security Agency (ENISA) as discussed in Section 6.2. Section 6.3 describes analytical details of the interdependency model based on critical service and sectors. An example of scenario implementation using SD tools is given in Section 6.4. Section 6.5 emphasizes capabilities of the model to capture dynamic aspects of interdependencies due to environmental, human, economic and other impact factors. Section 6.6 presents a further extension of model features to the effects of structured demand patterns for CI services on disruption impacts.

Content of the chapter is based on the work done by the author of this thesis during two secondment periods at the Cyber Security Research Labs of Airbus Group Innovation, and published in (Canzani et al., 2016) and (Canzani et al., 2017).

6.1 Early Warning Systems for CI Operators

At present, developing effective Early Warning Systems (EWSs) for CIP is a difficult challenge for government agencies, private companies, and academic communities. An effective EWS should support prevention and mitigation actions in case of disruptive events by monitoring operations and sharing relevant incident information. The main goal is to identify impacts and cascading effects among CIs in time to permit an effective incident response that reduces or avoids potential breakdowns of CI networks. In this context, the crucial role of information sharing between CI operators is clear: comprehensive knowledge of the current threat state of the networked system of CIs facilitates both detection of large-scale attacks and coordination of response strategies among stakeholders. However, CIs usually adopt security measures that only make use of information collected from their own systems. For instance, a review of EWSs for the safeguard of public water supplies is (Hasan et al., 2004). Beyond securing one CI as independent system, insights for a network-based EWS that consider interdependent CIs are given (Bsufka et al., 2006).

This research specifically refers to the framework proposed by the ECOSSIAN project for the development of a real-time EWS and impact analysis to gain situational awareness in a European control system security network (Kaufmann et al., 2014). The ECOSSIAN ecosystem (Settanni et al., 2015) presents a layered security approach to support cybersecurity incident detection and management through Security Operations Centres (SOCs). Concerning incident reporting and information sharing, SOCs have specific focus and responsibilities at operator level (O-SOC), national level (N-SOC), and European level (E-SOC).

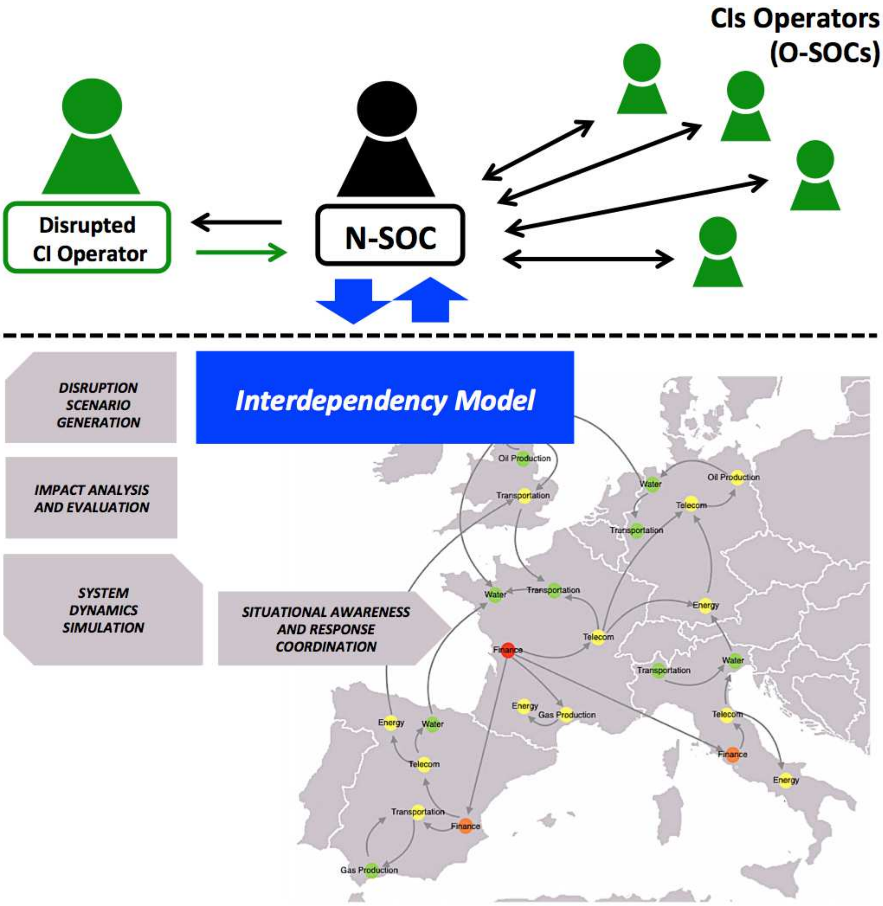


Figure 6.1: Use of the interdependency model in the ECOSSIAN scenario

Figure 6.1 shows how the interdependency model extends the ECOSSIAN framework for impact analysis and scenario evaluation purposes. Figure 6.1 describes the information sharing between the national entity (N-SOC), the disrupted CI operators and other O-SOCs.

The green arrow indicates that the disrupted operator must immediately inform the N-SOC about operational damages occurred in its own CI. The operator is asked to characterize the disruptive event as described later on (see Section 6.3.1). The N-SOC uses this data as input parameters of the interdependency model to generate the specific disruption scenario. Note that a list of general information about all CI operators is assumed to be available in advance in the ECOSSIAN scenarios, so that the N-SOC can identify and characterize the disrupted operator when a warning is reported. Once the model setting is completed, SD simulation can be run to calculate damage effects in the interdependent system of CIs. A simulation-based disruption impact analysis (cf. Section 4.6) is conducted by the N-SOC to gain situational awareness of national CIs and all CIs over Europe (through the E-SOC). Black arrows in Figure 6.1 indicates that the N-SOC starts response coordination strategy by informing O-SOCs about potential damages and cascade effects that will most-likely occur in their infrastructures due to the initial disruption. The final ECOSSIAN attempt is to timely coordinate mitigation actions and establish recovery priorities among CI operators through the use of a visualization map which shows the SD simulation results on a geographic map of Europe to facilitate the scenario evaluation.

Next sections explain how the dynamic interdependency model contributes to the design of such layered cybersecurity approach in the context of European CIs.

6.2 Identification of Critical Services and Sectors

Surveys conducted by the European Union Agency for Network and Information Security (ENISA) reveal that, in Europe, a significant number of member states present a low level of maturity and lack of a structured approach regarding identification of CIs and establishment of coordination plans. As a first step towards unifying CI protection programs among the European member states, the ENISA has recently issued guidelines to identify CI assets and services (ENISA, 2014).

This research work builds on the qualitative work of ENISA to move one step further by proposing an operator-driven approach to model and analyze CI dependencies and related critical services towards a unified framework for European member states. On the basis of ENISA definitions and reference lists (ENISA, 2014), this section gives an overview of the approach and concepts which are used in modeling.

In accordance with the ECOSSIAN objective to promote the use of information sharing to improve cybersecurity (cf. Section 6.1), the work of ENISA leverages on the role of communication networks to ensure the correct functioning of every CI. These IT assets, which generally refer to Critical Information Infrastructure (CII), are essential to operations of national and international CIs. A cyber attack affecting CII systems could lead to large-scale cascading effects in CI networks. See (Haemmerli and Renda, 2010) for more details on CIs and CIIs in Europe.

The ENISA proposes the following classification of approaches to identify CI/CII assets.

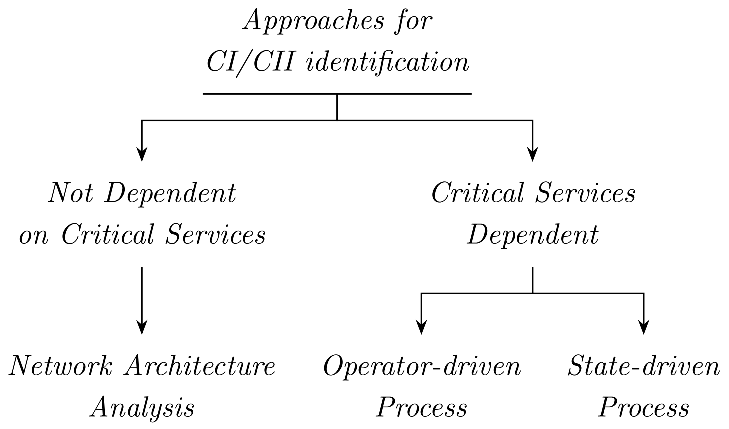

Approaches for CI/CII identification
Not Dependent on Critical Services
Critical Services Dependent
Network Architecture Analysis
Operator-driven Process
State-driven Process

Figure 6.2: Classification of approaches to identify CI/CIIs (ENISA, 2014)

According to Figure 6.2, data network analysis of national infrastructures is required for mapping and protecting network components in approaches that do not rely on critical services. However, the identification of all components that are critical to CI operations is costly and often prohibitive. Approaches dependent on critical services are based on consequences of impacts that a critical service disruption may have on the society. Also, critical service-dependent approaches can be classified depending on who has the leading role for the identification of critical services: government agencies (State-driven process) or CI operators (Operator-driven process).

The dynamic interdependency models (cf. Chapter 4) are extended by adopting an operator-driven approach based on critical services and sectors. This choice fits the ECOSSIAN mission to provide a layered security approach with specific focus on operators and critical services that they deliver for a correct CI functioning . In fact, specific responsibilities of CI operators for coordination purposes are considered in the design of such holistic EWS. (See Section 6.1). The model structure considers critical sectors, CIs (ENISA also refers to it as “subsectors”), and critical services in line with the reference list provided by (ENISA, 2014).

SECTOR	*CI*	*CRITICAL SERVICE*
Energy	Electricity	*Generation*
		Distribution
		Electricity Market
	Petroleum	*Extraction*
		Refinement
		Transport
		Storage
	Natural Gas	*Extraction*
		Transport
		Storage
Transport	Aviation	*Air Navigation Services*
		Airport Operations
	Road	*Road Network Maintenance*
		Bus / Tram Services
	Train	*Railway Transport Services*
		Public Railway Maintenance
	Maritime	*Shipping Traffic Management*
		Ice-Breaking Operations
Water	Drinking Water	*Water Storage*
		Water Distribution
		Water Quality Assurance
	Wastewater	*Wastewater Collection and Treatment*
Telecom	Information Technologies	*Web Services*
		Datacentre / Cloud Services
		Software (as a service)
	Communications	*Voice / Data Communication*
		Internet Connectivity
Financial		*Banking*
		Payment Transacitons
		Stock Exchange
Health		*Emergency Healthcare*
		Hospital Care
		Medical Supply
		Epidemic Control

Table 6.1: Reference list of critical sectors, CIs and related critical services (See (ENISA, 2014) for the complete list)

The reference list in Table 6.1 helps to understand the complex scenario of interdependenct CIs as system-of-systems. Each critical sector (e.g. the Energy) corresponds to a group of CIs (e.g. Electricity, Petroleum, Natural Gas), which in turn are able or not to provide respective final services and products depending on their internal operational state. The correct functioning of operations in a CI relies on critical services provided by other CI operators, which contribute to the complete chain value of the CI.

The ENISA classification in Table 6.1 is used as backbone structure of the dynamic interdependency model.

6.3 The Operator-driven Interdependency Model

In line with Table 6.1, the operator-driven interdependency model adopts a layered structure based on critical sectors, CIs, and critical services. Only if CI operators can adequately provide all critical services, the complete value chain of a CI is preserved. Accordingly, three types of dependency are identified as follows.

- **dependencies within a CI** (if critical services of a CI depend on the final product/service of the CI itself),
- **intra-sector interdependencies** (if two CIs belong to the same sector and a critical service of one of them depends on resources and final services of the other CI),
- **cross-sector interdependencies** (if two CIs belong to different sectors and a critical service of one of them depends on resources and final services of the other CI).

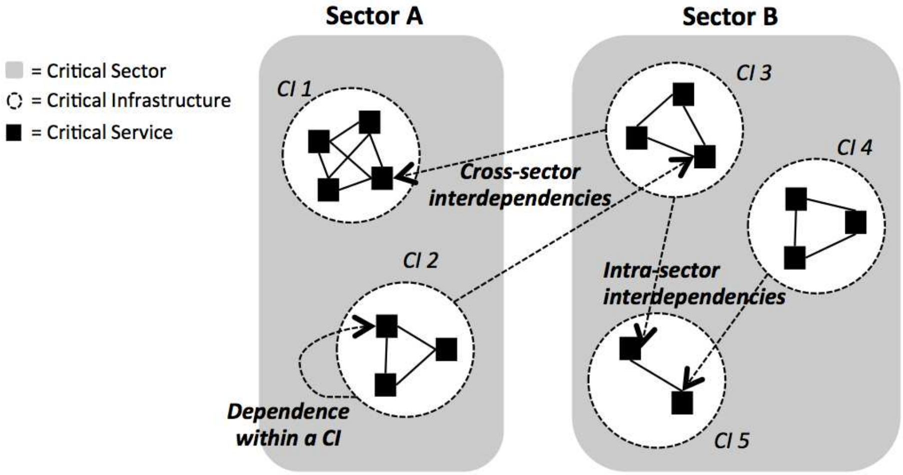


Figure 6.3: Structure of the operator-driven interdependency model

Figure 6.3 represents the model structure to clarify layered components (sectors, CIs, and critical services) as well as the three types of dependency. While in Chapter 4 the SD model assesses interdependencies between CIs on the basis of final services provided, the structure in Figure 6.3 allows considering different critical services that constitute the value chain of CIs.

Overall, the three building blocks of Chapter 4 are extended as follows.

(i) The disruptive event (cf. Block 1, Section 4.1) is characterized not only according to disruption time, duration and magnitude, but it also accounts for possible delays in recovery, importance of disrupted CI operators, and disruption impact factors.

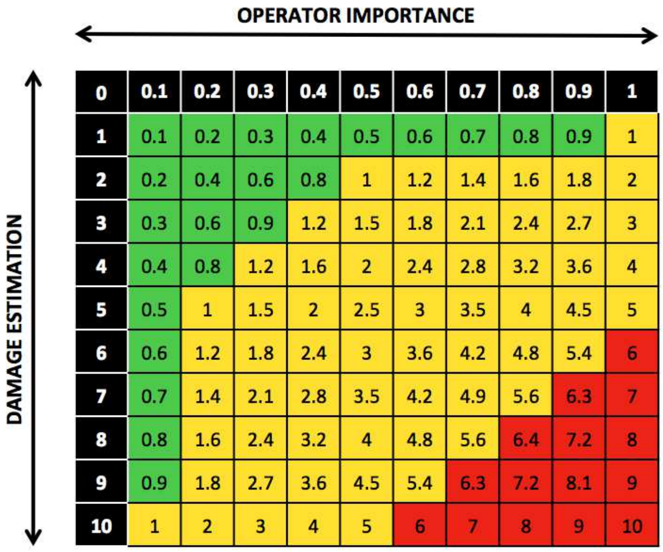
(ii) The operational dynamic of a single infrastructure (cf. Block 2, Section 4.2) is modeled with respect to the criticality of each critical service.

(iii) The interdependency matrix (cf. Block 3, Section 4.3) considers effects of final CI services on the operational state of each critical service according to the ENISA reference list in Table 6.1.

6.3.1 Block 1": Disruption Characterization

The ENISA (ENISA, 2014) identifies three main characteristics to describe a disruptive event: scope, magnitude, and time distribution. Similarly, Block 1 (cf. Section 4.1) represents the disruption as PULSE function of height given by a disruption magnitude factor, starting at the time in which the disruption occurs, and lasting a certain period (i.e. duration of the disruption). Note that the scope refers to intentions of the attacks as considered, e.g., in Block 1' for modeling cyber attack-defense dynamics.

In addition to these primary factors, Block 1" aims at characterizing disruptive events by a perspective of CI operators. More precisely, the magnitude of a disruption is assessed according to the following matrix.



OPERATOR IMPORTANCE

DAMAGE ESTIMATION

0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1
1	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1
2	0.2	0.4	0.6	0.8	1	1.2	1.4	1.6	1.8	2
3	0.3	0.6	0.9	1.2	1.5	1.8	2.1	2.4	2.7	3
4	0.4	0.8	1.2	1.6	2	2.4	2.8	3.2	3.6	4
5	0.5	1	1.5	2	2.5	3	3.5	4	4.5	5
6	0.6	1.2	1.8	2.4	3	3.6	4.2	4.8	5.4	6
7	0.7	1.4	2.1	2.8	3.5	4.2	4.9	5.6	6.3	7
8	0.8	1.6	2.4	3.2	4	4.8	5.6	6.4	7.2	8
9	0.9	1.8	2.7	3.6	4.5	5.4	6.3	7.2	8.1	9
10	1	2	3	4	5	6	7	8	9	10

Figure 6.4: Magnitude assessment matrix

The matrix in Figure 6.4 shows that *Disruption Magnitude* is a factor, varying from 0 to 10, obtained as a result of the product of two input parameters, i.e.

- *Damage Estimation* m_d^O, which is a parameter set by the O-SOC of a disrupted operator rating in a scale of 0 to 10 the magnitude of disruption effects in its own organization;

- *Operator Importance* O_{rank}, which serves to scale the disruption damage depending on how important is the disrupted operator for the supply of a specific critical service to national CIs. It ranges from 0 to 1 according to the piece of market segment the operator owns among critical service providers of a state.

Based on these values, the N-SOC assesses the *Disruption Magnitude* m_d with respect to the interdependent system of national CIs as follows.

$$m_d := m_d^O \times O_{rank}. \tag{6.3.1}$$

This is because, for example, even if a small telecommunication provider of importance $O_{rank} = 0.2$ is totally disrupted, i.e. $m_d^O = 10$, the country can still receive telecommunication services from major providers in the country. In this case, the magnitude of disruption is $m_d = 10 \times 0.2 = 2$

Note that to assess the importance of CI operators, publicly available data on market shares are considered. Metrics that can be used to rank operators are, e.g., total revenues and total number of subscribers. The pie chart in Figure 6.5 reports data of main mobile telecommunication providers in Germany (DSP, 2016).

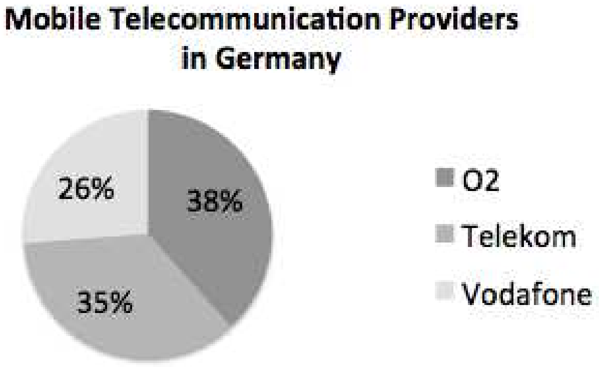


Figure 6.5: Market shares in the regular German mobile market 2015 (DSP, 2016)

In accordance with data in Figure 6.5, in the matrix in Figure 6.4 the importance of Vodafone, Telecom and O_2 operators would be 0.26, 0.35 and 0.38 respectively.

Note that the reference list ranking CI operators based on their importance must be available to the N-SOC at the moment of the warning report in the ECOSSIAN scenario (see Section 6.1). Therefore, this research work refers to it also as "a priori" importance.

In addition to *Disruption Time* and *Disruption Duration*, O-SOCs have to provide information on

- *Expected Time to Recovery* ΔT_{rec}, and

- *Delay Recovery* δt_{rec}, i.e. delays (if any) with which the recovery started.

In the interdependency model, this is implemented with Vensim using a STEP function that considers time lags between *Disruption Time* t_d and *Start Recovery* t_{rec} that is the time in which response actions are carried out,

$$t_{rec} := t_d + \delta t_{rec}. \tag{6.3.2}$$

Operation recovery rate is then defined as follow.

$$\beta(t) := \begin{cases} \dfrac{OP_{rec}(t)}{\Delta T_{rec}}, & \text{if } \ t \geq t_{rec}, \\ 0, & \text{otherwise.} \end{cases} \tag{6.3.3}$$

Furthermore, the SD model allows to further characterize disruptive events according to impact factors that are discussed later on (Section 6.5).

6.3.2 Block 2": Single CI Dynamics based on Critical Services

Block 2" extends Block 2 (see Section 4.2) according to the purpose of ENISA to account for different critical services which are needed to provide the final CI service. The goal is to consider the "criticality" of such critical services. In fact, all critical services are needed to ensure the normal operational state of the CI, but some of them are more critical than others. For example, railway management and availability of train facilities are critical services of the Train Transport CI (see Table 6.1). If trains are out of services due to a cyber attack manipulating their control systems, operations to maintain the railway can be pursued anyway. If rail signal upgrades are hacked to cause crashes, trains cannot run safely. In both cases the final service of the Train Transport CI cannot be fully provided.

Given a general infrastructure i, operational dynamics are described by two compartments: the stocks of Running Operations $OP^i_{run}(t)$ and Down Operations $OP^i_{down}(t)$. The flow of operation breakdown $\alpha^i(t)$ (cf. Block 2 in Section 4.2) is split into different flows $\alpha^i_1(t), ..., \alpha^i_n(t)$ corresponding to breakdown rates of n critical services that must be provided by operators to guarantee the operational functioning of the complete CI value chain.

Thus, a criticality factor $c^i_k(t), k = 1, ..., n$ is assigned to each flow $\alpha^i_k(t), j = 1, ..., n$, to assess criticality of each critical service with respect to other critical services of the infrastructure i. Criticality factors $c^i_1, ..., c^i_n$ are constant parameters such that

$$c^i_1 + ... + c^i_n = 1. \tag{6.3.4}$$

Let $\gamma^i(t)$ be the recovery rate and n^i_{OP} the total number of CI operations (also denoted as maximum capability of the CI, see Block 3 in Section 4.3). The system of differential equations regulating the dynamics of CI operations based on critical service is as follows.

$$\begin{cases} \dfrac{\mathrm{d}}{\mathrm{d}t}\big(OP^i_{run}(t)\big) = -\sum_{k=1}^{n} c^i_k \alpha^i_k(t)\Big(\dfrac{OP^i_{run}(t)}{n^i_{OP}}\Big) + \gamma^i(t) OP^i_{down}(t) \\ \dfrac{\mathrm{d}}{\mathrm{d}t}\big(OP^i_{down}(t)\big) = \sum_{k=1}^{n} c^i_k \alpha^i_k(t)\Big(\dfrac{OP^i_{run}(t)}{n^i_{OP}}\Big) - \gamma^i(t) OP^i_{down}(t) \end{cases} \tag{6.3.5}$$

Likewise, the number of operations is constant over time. That is, at any time t,

$$OP^i_{run}(t) + OP^i_{down}(t) = n^i_{OP}. \tag{6.3.6}$$

As the dynamic behavior starts at the moment of time when the disruption occurs, the breakdown rate of operations of a critical service $\alpha^i_j(t)$ depends on disruptive events affecting a provider of that critical service as well as on the dependency of infrastructure i on final service of other CIs.

6.3.3 Block 3": Interdependency Assessment

In Chapter 4, Block 3 quantifies interdependencies between final CI services. Improving the modeling in this direction, Block 3" attempts to assess interdependencies between final CI services and specific critical services provided by operators to guarantee the complete CI value chain. On the basis of the ENISA reference list in Table 6.1, the connection matrix (or interdependency matrix) of Block 3 (cf. Section 4.3) is modified according to the three types of interdependencies defined in the model structure (cf. Figure 6.3).

			Energy			**Transport**				**...**	
SECTOR	*CI*	*CRITICAL SERVICE*	Electricity	Petroleum	Natural Gas	Aviation	Road	Train	Maritime	⋮	⋮
Energy	Electricity	*Generation*									
		Distribution									
		Electricity Market									
	Petroleum	*Extraction*									
		Refinement									
		Transport									
		Storage									
	Natural Gas	*Extraction*									
		Transport									
		Storage									
Transport	Aviation	*Air Navigation Services*									
		Airport Operations									
	Road	*Road Network Maintenance*									
		Bus / Tram Services									
	Train	*Railway Transport Services*									
		Public Railway Maintenance									
	Maritime	*Shipping Traffic Management*									
		Ice-Breaking Operations									
...	...	...									
	...	...									

Table 6.2: Interdependency matrix based on critical sectors, CIs, and critical services

In Table 6.2, the matrix identifies final CI services needed to guarantee the normal operational processes of each service which is critical for the functioning of a CI. It avoids to end up with a fully connected matrix of interdependencies between CIs by disaggregating the interdependencies at the critical service level. Next section gives an example of how the operator-driven interdependency model can be applied to identify specific links and relationships in the complex system of CIs.

Note that the connection matrix can be Boolean, indicating whether or not there is a dependence; or weighted to quantify magnitudes of effects on a CI if its critical services would be interrupted for a certain time period.

6.4 Implementation with Vensim

This section gives an idea of how the CIs interdependency model can be applied to ECOSSIAN scenarios using SD tools.

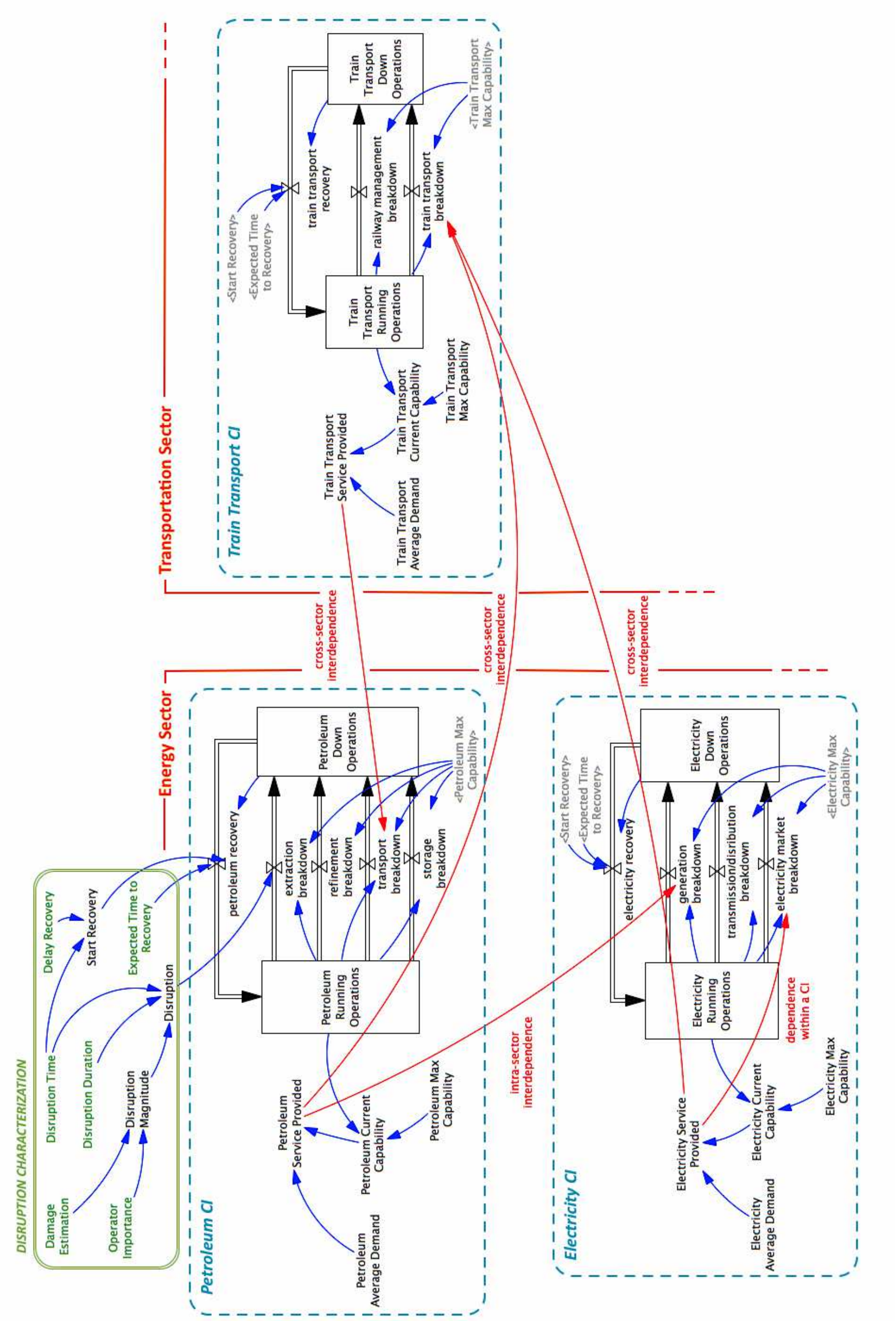

Transportation Sector
Train Transport CI
Train Transport Down Operations
<Train Transport Max Capability>
train transport recovery
railway management breakdown
train transport breakdown
<Start Recovery>
<Expected Time to Recovery>
Train Transport Running Operations
Train Transport Current Capability
Train Transport Max Capability
Train Transport Service Provided
Train Transport Average Demand
cross-sector interdependence
cross-sector interdependence
cross-sector interdependence
Energy Sector
DISRUPTION CHARACTERIZATION
Delay Recovery
Start Recovery
Expected Time to Recovery
Disruption
Disruption Time
Disruption Duration
Disruption Magnitude
Damage Estimation
Operator Importance
Petroleum CI
Petroleum Down Operations
<Petroleum Max Capability>
petroleum recovery
extraction breakdown
refinement breakdown
transport breakdown
storage breakdown
Petroleum Running Operations
Petroleum Service Provided
Petroleum Current Capability
Petroleum Max Capability
Petroleum Average Demand
intra-sector interdependence
Electricity CI
Electricity Down Operations
<Electricity Max Capability>
<Start Recovery>
<Expected Time to Recovery>
electricity recovery
generation breakdown
transmission/disribution breakdown
electricity market breakdown
Electricity Running Operations
dependence within a CI
Electricity Current Capability
Electricity Max Capability
Electricity Service Provided
Electricity Average Demand

Figure 6.6: Example of SD stock-and-flow diagram of the operator-driven interdependency model

Figure 6.6 illustrates how building blocks are integrated together in a scenario with three infrastructures:

- Petroleum CI (within the Energy Sector),
- Electricity CI (within the Energy Sector),
- Train Transport CI (within the Transportation Sector).

Critical services are identified and respective breakdown rates modeled for each block representing the CIs (dotted blue boxes). Red arrows in Figure 6.6 describe interdependencies of different types, e.g.:

- **Dependencies within a CI.** Price perturbations in the electricity market may occur if electricity cannot be provided; therefore a critical service of the Electricity CI depends on service breakdowns of the CI itself.
- **Intra-sector interdependencies.** Oil resources are crucial for power plants in order to generate electricity. Within the Energy Sector, the functioning of the Petroleum CI is vital for generation service providers in the Electricity CI.
- **Cross-sectors interdependencies.** Trains may need fuel or electric power to run and therefore final products and services of Petroleum and Electricity CIs are needed to train facilities, which is identified as a critical service of the Train Transport CI. Also, trains are needed to transport oil barrels.

As for initial purpose, the goal is to show how to apply the interdependency model to support early warning and coordination of response among CI operators in the ECOSSIAN scenario (see Section 6.1).

The double-line green box in Figure 6.6 shows the model input parameters, i.e. incident information that O-SOCs must provide to the N-SOC to characterize the disruptive event (cf. Section 6.3.1). The scenario describes a disruption of an operator providing petroleum extraction service which guarantees the correct functioning of the Petroleum CI. More precisely, the O-SOC of the disrupted operator must inform the national entity (N-SOC) about the moment of time when the disruption occurs, disruption duration, the expected time to recover and time delays (if any) with which the recovery started (i.e. green variables in Figure 6.6). The O-SOC should also estimate the damages occurred in its operational facilities.

Hence, the N-SOC uses incident information provided by the disrupted operator as input parameters of the SD model, which is indeed named ”operator-driven” interdepedency model. The N-SOC must assess magnitude of impacts on other CIs based on the a priori operator importance respect to the market shares of petroleum extraction providers. A simulation-based impact analysis supports then crisis management processes of coordination and response among CI operators in national and European scenarios.

Note that the SD model in Figure 6.6 is not exhaustive. Other interdependencies can be identified to characterize the network of CIs. This example mainly serves to clarify the model structure, existing types of interdependencies and analytical description of SD variables.

6.5 Impact Factors

Many of existing approaches to model interdependencies between CIs abstracts from the type of disruption when characterizing such interdependencies. However, magnitude of interdependencies strongly depends on the specific nature of a disruptive event. In turn, different cascading effects may arise when considering dynamic interdependencies varying according to diverse disruption consequences.

For example, power outages and explosions in a power plant may have different cascade effects on other infrastructures. In case of an explosion, emergency services and hospital care are crucial to injured people. Consequently, capabilities of the Health CI may be inadequate to satisfy the suddenly increasing demand for such services. This is not the case of a power outage, during which hospital generators may be able to supply electricity in the next hours. If crude oil spills into the ocean from a broken pipeline, the impact on environment could be catastrophic; in particular Food CI and Water CI services may be seriously compromised by cascading effects.

The ECOSSIAN ecosystem suggests accounting for potential human, environmental, economic and other consequences in assessing scenarios of disruption. Thus, it is crucial that O-SOCs inform the N-SOCs about potential consequences of cyber attacks. Accordingly, the following impact criteria are considered in modeling:

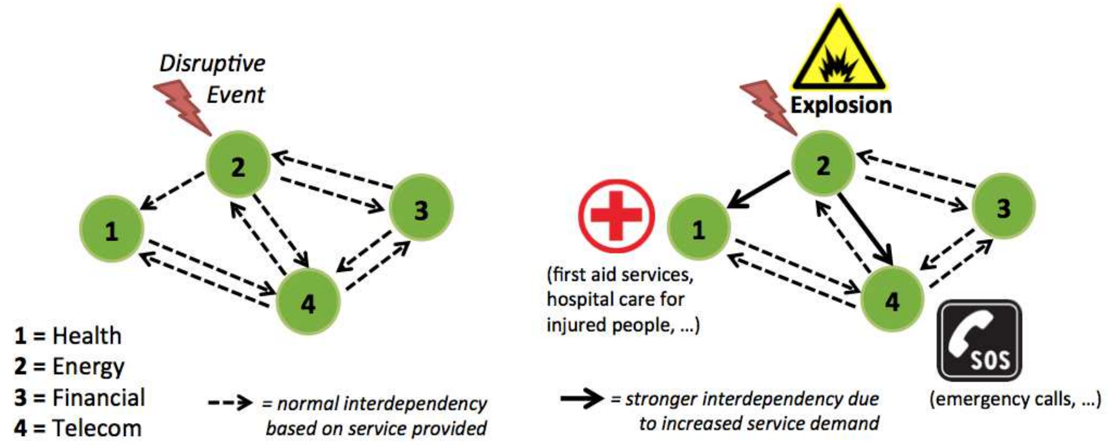
- *Human impact factor*, which estimates emergency and health care services needed both immediately and in the post-disruption phase based on the fraction of population affected.
- *Environmental impact factor*, which assesses pollution effects and other long-term damages to the environment.
- *Economic impact factor*, which attempts to evaluate whether the national economy may be compromised due to information disclosed by the cyber activist.

In the SD model, these factors are input parameters that vary on a scale of 0 to 10. Hence, disrupted O-SOCs are asked to provide such values to the N-SOC in the ECOSSIAN scenario (cf. Figure 6.1). Selected values are taken by the model to assess magnitude of demand perturbations and time duration of effects (e.g. short-term or long-term) for those specific infrastructures which provide crucial services to mitigate human, environment, economic consequences. Technically, analytic functions representing *CI service demand* and *breakdown rate* of critical service operations are changed on the basis of how human, environmental, and economic impacts affect a specific CI. Then, the SD model calculates different magnitudes of interdependencies over the time horizon in accordance with disruption characteristics. To clarify ideas, next section provides a detailed simulation example that considers human impacts.

Note that further potential consequences may be identified and considered in the model. For example, ENISA guidelines (ENISA, 2014) suggest considering public confidence and public order as impact criteria to assess dependencies.

Simulation Example

This example presents a simulation study that focuses on human impact analysis. As shown in Figure 6.7 (on left), a scenario with four CIs and a disruptive event in the Energy is considered.


Disruptive Event
1
2
3
4
1 = Health
2 = Energy
3 = Financial
4 = Telecom
= normal interdependency based on service provided
Explosion
(first aid services, hospital care for injured people, ...)
SOS
(emergency calls, ...)
= stronger interdependency due to increased service demand

(a) General disruption scenario

(b) Explosion scenario

Figure 6.7: Different scenarios of interdependencies based on human impacts

Figure 6.7 on the right shows a characterization of the same scenario on left in which the general disruption is a power plant explosion. Differently from power outages, explosions may have catastrophic impacts on people around the disrupted facilities. Bold black arrows highlight that this type of disruption provokes

- increased demand of telecommunication services for emergency calls during the first disruption phase (short-term effects);
- increased demand of health care services for injured people during the disruption, and also in the post-disruption phase in case of major explosions (long-term effects).

As consequence, cascading effects of a disruption with relevant impact on humans are increasing into Telecom and Health CIs.

Note that this simulation study consider the system of differential equations (6.3.5) to replicate operational dynamics of a single CI with $k = 1$, i.e. it is assumed each infrastructure i having only one critical service $\alpha_1^i(t)$ of criticality $c_{i1} = 1$. In this case, $\alpha_1^i(t)$ corresponds to $\alpha^i(t)$ of Block 2 (cf. Chapter 4).

Let d be the disruptive event occurring at time t_d, lasting ΔT_d hours, and having a *Human Impact Factor* h_d which can vary on a scale of 0 to 10. In particular, two cases are distinguished:

- if $h_d = 0$ there is no human impact factor characterization and therefore scenario simulation corresponds to the one in Figure 6.7 on left;
- if $h_d > 0$ the scenario characterization of Figure 6.7 on the right is mathematically implemented in the SD model as described below.

Hence, the objective is to model perturbations of service demand $D^i(t)$ and breakdown rate $s^i(t)$ in those infrastructures which provide critical services in case of an explosion, i.e. the Telecom CI and the Health CI (respectively $i = 4$ and $i = 1$ in Figure 6.7).

Perturbation of telecommunication service demand is replicated using a SMOOTH function that returns a first-order exponential smooth of a PULSE function of magnitude 10 h_d over the first disruption phase, which is assumed to be 1/3 of the disruption duration ΔT_d. In formula,

$$D^4(t) := \begin{cases} D_{Av} + f_{smooth}(10\ h_d, \frac{\Delta T_d}{3}), & \text{if } \ t_d \le t \le t_d + \frac{\Delta T_d}{3}, \\ \\ D_{Av}, & \text{otherwise.} \end{cases} \tag{6.5.1}$$

In this research work, CI service demand is defined as percentage of maximum operational capabilities, and the service level (in percent) is the ability to deliver an amount of service that meets the demand (cf. Chapter 4). In case the service demand exceeds maximum operational capabilities, the infrastructure will not be able to fully provide the final service requested. This is modeled by smoothing a PULSE function of magnitude $D^4(t)/100$ over the first disruption phase to replicate a breakdown of the critical service operations in case of exceeded demand. That, is, if $D^4(t) > 100\%$,

$$\alpha^4(t) := \begin{cases} \sum\limits_{j \in J_4} \dfrac{e_{4j}\big(1 - S^j(t)\big)}{|J_4|} + f_{smooth}(\frac{D^4(t)}{100}, \frac{\Delta T_d}{3}), & \text{if } \ t_d \le t \le t_d + \frac{\Delta T_d}{3}, \\ \sum\limits_{j \in J_4} \dfrac{e_{4j}\big(1 - S^j(t)\big)}{|J_4|}, & \text{otherwise.} \end{cases} \tag{6.5.2}$$

The same argument is used to replicate effects of human impacts on the Health CI. The only difference is that in this case the effects are longer as hospital capabilities must be adequate to host injured people also in the post-disruption phase. Accordingly, the pulse functions are smoothed over all the disruption duration time. In formula, the Health CI service demand is

$$D^1(t) := \begin{cases} D_{Av} + f_{smooth}(10\ h_d, \Delta T_d), & \text{if } \ t_d \leq t \leq t_d + \Delta T_d, \\ \\ D_{Av}, & \text{otherwise.} \end{cases} \tag{6.5.3}$$

Similarly, if $D^1(t) > 100\%$, the breakdown of health critical service operations is

$$\alpha^1(t) := \begin{cases} \sum\limits_{j \in J_1} \dfrac{e_{1j}\big(1 - S^j(t)\big)}{|J_1|} + f_{smooth}(\frac{D^1(t)}{100}, \Delta T_d), & \text{if } \ t_d \leq t \leq t_d + \Delta T_d, \\ \sum\limits_{j \in J_1} \dfrac{e_{1j}\big(1 - S^j(t)\big)}{|J_1|}, & \text{otherwise.} \end{cases} \tag{6.5.4}$$

After the mathematical description, disruption scenarios in Figure 6.7 are simulated to show how the SD model captures dynamics of interdependencies by changing magnitude of cascade effects according to the human impact factor h_d.

Model Parameter	**ECOSSIAN Responsibility**	**Input Value**
Disruption Time (t_d)	O-SOC → N-SOC	96 Hours
Disruption Duration (ΔT_d)	O-SOC → N-SOC	36 Hours
Expected Time to Recovery (ΔT_{rec})	O-SOC → N-SOC	30 Hours
Delay Recovery (δt_{rec})	O-SOC → N-SOC	0
Damage Estimation (m_d^O)	O-SOC → N-SOC	5
Operator Importance (O_{rank})	N-SOC	0.7

Table 6.3: Interdependency model setting through ECOSSIAN information sharing

Table 6.3 lists initial setting of model parameters and the roles of reporting such data in the ECOSSIAN early warning and incident response system. The O-SOC of the disrupted energy service provider must share information about the disruptive event with the N-SOC. The N-SOC is aware of the a priori importance of the provider and can assess the disruption magnitude as $0.7 \times 5 = 3.5$ (cf. the assessment matrix in Figure 6.4). Furthermore, the O-SOC has to characterize the disruption according to its impact on humans by assessing the factor $0 \leq h_d \leq 10$. Accordingly, a simulation-based human impact analysis is conducted for the following three scenarios:

- **Scenario 1:** no human impact ($h_d = 0$),

- **Scenario 2:** medium human impact ($h_d = 4$),
- **Scenario 3:** high human impact ($h_d = 10$).

Each scenario is simulated over 2 weeks time period with an hourly time scale. For convenience, every infrastructure has the maximum operational capability 100 operations. The average demand is then assumed being 90% of the maximum capability. Also, the system of CIs is in its normal operational state before the disruptive event triggers the nonlinear dynamics. See Chapter 4 for analytical details.

Simulation outputs in Figures 6.8, 6.9, and 6.10 show dynamics of running operations (in percent, graphs on left) and service provided (in percent, graphs on right) over time for Scenario 1, 2, and 3 respectively.

It follows the description and simulation analysis of the three disruption scenarios.

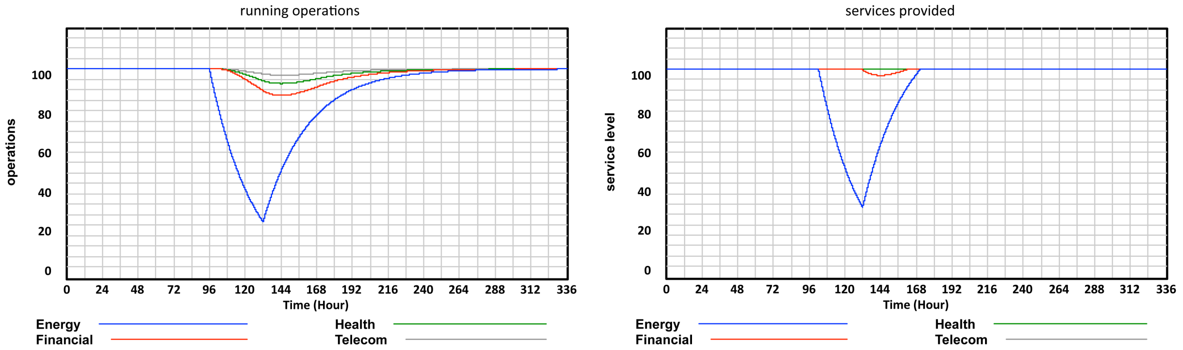


Figure 6.8: No human impact (Scenario 1)

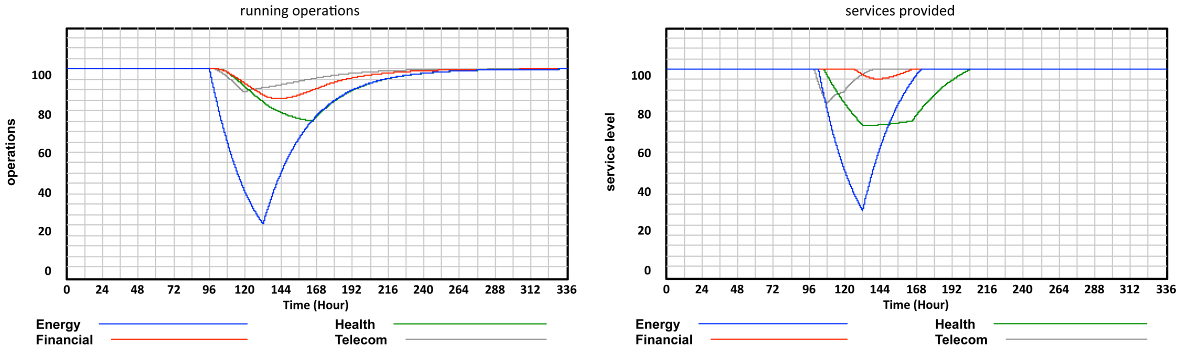


Figure 6.9: Medium human impact (Scenario 2)

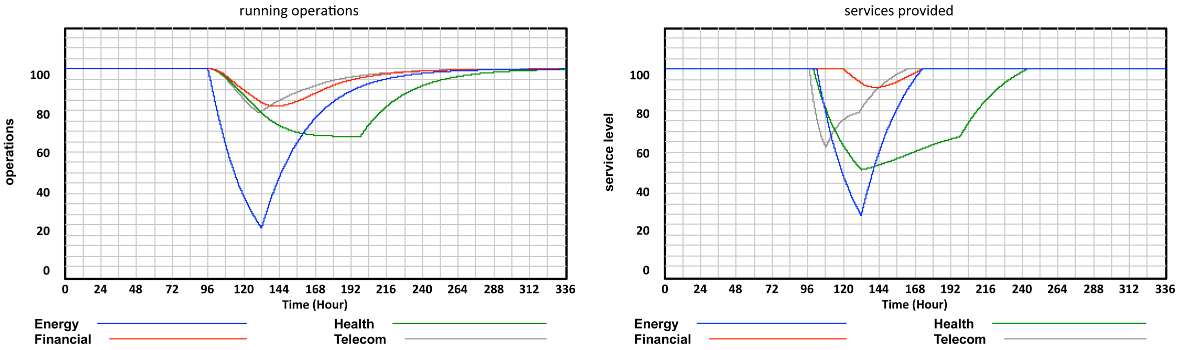


Figure 6.10: High human impact (Scenario 3)

Scenario 1

Scenario 1 describes dynamic effects of a disruption in the Energy CI without direct impacts on humans. For example, a target cyber attack to a power grid may succeed to exploits vulnerabilities of SCADA systems and cut off electricity supplies. The graph on left in Figure 6.8 shows how the power outage causes operational disruptions of the other CIs up to the 25 %. Observing the graph on the right, power generators of the Financial CI are able to supply an amount of electricity such that banking services can be fully provided for the first 24 hours of blackout.

However, financial service capabilities are reduced of about 5% one day after the disruption occurs. Nevertheless, the system of CIs is able to absorb the damage before disrupting services of the Telecom and Health providers, which have big power generators to prevent cascading effects of blackouts in their facilities.

Scenario 2

In Scenario 2, a small explosion is cause of dead and injured people in a power station. The impact on humans is medium, with people trying to call emergency services during to save their life and hospital cares needed also in the post-disruption phase. The graph on left in Figure 6.9 show increasing operational disruptions in all CIs with respect to Scenario 1. Observing the graph on the right in Figure 6.9, overloaded telecommunication networks lead to service interruptions in the Telecom CI with a peak of about 20% immediately after the explosion.

As the Financial CI relies both on power and telecommunication providers, simulations show a decreased level of financial services and for longer period than Scenario 1 (in which no telecom service disruptions occur). The Health CI is not fully operative due to the lack of electricity, while health service demand exceeds due to the number of injured people. More than 30% of medical cares cannot be provided by hospitals during and after the disruptive event, and health services are fully restored only 5 days after the explosion.

Scenario 3

A big explosion of power plant is simulated in Scenario 3. High is the number of people affected by the catastrophic event and dramatic are the consequences. With respect to Scenario 1 in which only financial services get disrupted, health and telecommunication service interruptions increase exponentially with peaks of service losses of about 50% and 40% respectively. The reason is that cascading effects are mainly affecting providers of those services which are crucial for mitigating human consequences of an explosion, while e.g. the Financial CI can still effort the lack of electric power.

After a sudden unavailability of telecommunication services in the initial disruption phase, the Telecom CI is able to restore its critical services along with one and a half days disruption of the Energy CI. Different impacts affect the Health CI, in which capabilities of emergency services and hospitals both during and after the explosion result inadequate due to the high number of injured people.

6.6 Structured Demand for CI Services

So far, simulations assume CIs having a constant average demand for critical services, that is $D(t) = D_{Av}$. The previous section discusses the effects of demand perturbations in case of specific disruption scenarios.

However, in reality CI operational facilities have to deal with service demand patterns which show

- **daily cycles** with, e.g., peak hours,
- **monthly or yearly variations**,
- dependence on **seasons**.

Such demand structures have high influence on dynamics of disruptive events. For example, energy blackouts during daylight or in the night may have different impacts on other CIs. Also, a disruption of transportation services would have significant impacts if occurring during the day times in which people go and leave from work.

The dynamic interdependency model can be implemented with demand structures by defining $D(t)$ over time t. As this research work studies disruption dynamics over relevant time periods of maximum 2 weeks, this section provides a simulation example which considers the daily demand structure for electricity.

Based on publicly available reports on energy (see (NREL, 2012) and (FEPC, 2015)), a LOOKUP function is manually built in Vensim to replicate typical variations of electricity demand in the 24 hours.

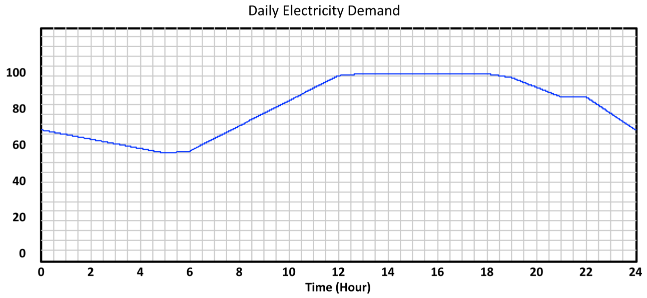


Figure 6.11: Example of electricity demand structure

Figure 6.11 describes a possible aggregate consumption (in percent, with respect to maximum operational capabilities) of commercial and residential areas. It assumes industrial facilities highly consume electricity for the functioning of machines with an extended peak between 7:00 in the morning and 20:00 in the evening (working time). Differently, the residential community has low consumption during the daylight and an extended peak in between 18:00 and midnight in which electricity is needed for lightening and domestic usages.

Considering the Electricity CI, a disruptive event of magnitude $m_d = 9$ and duration $\Delta T_d = 6$ hours is simulated by varying the time t_d in which such disruption occurs.

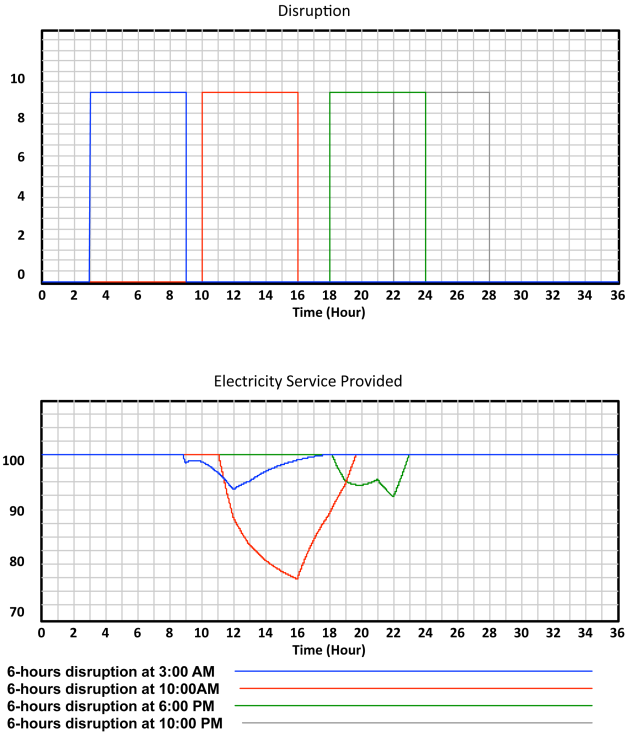


Figure 6.12: Effects of disruption time on service interruptions

The graph on top of Figure 6.12 represents disruptions of same magnitude and duration simulated at different time of the day (at 6 a.m., 10 a.m., 18 p.m., and 22 p.m.). Accordingly, the graph below of Figure 6.12 shows effects of such disruptions on electricity services.

Of interest is to notice different disruption effects on electricity service level according to the demand structure in Figure 6.11. In particular, a 6-hours disruption occurring at 3:00 (blue curves in Figure 6.12) would have impacts on service level only in the last phase, when the demand increases due to the beginning of the work day.

A disruption of 6 hours occurring at 10:00 (red curve in Figure 6.12) means that industrial activities have no enough electricity during all the working day, and therefore it highly reduces the CI ability to provide adequate electricity services. Service impacts are lower if a lack of electricity affects the community at 18:00 (green curves in Figure 6.12), time at which the business day is turning at the end. At 22:00, operations the Electricity CI would still able to fully provide a service that meets the low demand despite the disruption. (Note that the grey curve of electricity service provided in Figure 6.12 is constant at 100 % over the simulation time period).

6.7 Brief Summary

This chapter builds on findings of Chapters 4 and 5 to contribute to both crisis management and cyber security research. In fact, An operator-driven interdependency model is developed as key contribution to the design of cyber incident response and early warning systems for CI operators as well as to the development of other decision support tools for situational awareness purposes.

The three building blocks of Chapter 4 are iteratively extended and combined together to understand more complex aspects of the CI interdependency dynamics by a perspective of CI operators. With this purpose, ENISA guidelines (ENISA, 2014) are used to investigate disruptive dynamics at the level of critical sectors, CIs, and critical services.

In modeling, a special focus is given to the understanding of how different types of disruptive events may lead to sudden changes of magnitude of interdependencies. Hence, demand structures, disruption characteristics and impact factors are considered to analyze the dynamics of cascading effects. A criticality factor for each CI service is considered in the SD model to enable decision makers to prioritize recovery actions based on different criticality of critical service providers.

Building on the ENISA guidelines for the identification of critical services and assets, the operator-driven interdependency model improves of the current state of CI protection plans in Europe to be ready for future threats. Furthermore, the application to more realistic scenarios of the ECOSSIAN emphasizes the current need of achieving effective coordination of cybersecurity response actions among organizations.

Overall, extending model features by embedding more aspects of real-world dynamics add value to the use of the dynamic interdependency models in practice. Close collaborations with industrial partners and CI operators within the ECOSSIAN project particularly allow enriching the modeling in a way to provide key implications for practitioners through detailed SD simulation analysis.

Chapter 7

Conclusion

The relevance of recognizing interdependencies among CIs in planning for business operations is discussed in the introduction of this dissertation (see Chapter 1). CIs are described as complex cyber-physical systems that highly depend on critical services they have to provide to each other for the maintenance of the normal operational state.

The example of the 2003 blackout in US, which led to catastrophic cascading effects into all other CIs, shows the evidence of existing interdependencies between such infrastructure systems. Also, later investigations on the power outage pointed out that the US power outage was most likely triggered by a cyberattack. The fact that, beyond the well-known Stuxnet malware, other cyberattacks may have been responsible of CI disruptions motivates this research to address the field of cybersecurity of CIs.

The overall objective of this research is to improve the understanding of disruptive dynamics characterizing interdependent CI systems that are daily target by threats and cyber attacks via the strategic use of mathematical modeling techniques and combinations of them.

This chapter provides a summary of results and contributions of this research work in accordance with initial research objectives (cf. Chapter 1). In particular, Section 7.1 discusses research contributions to theory and practice in the field of cybersecurity of CIs. Section 7.2 highlights main characteristics of the set of modeling tools and methods presented in this dissertation. A relevant feature is the flexibility of the modeling approach, which allows a number of other applications. Thereby, Section 7.3 concludes with a brief discussion on further applications to inspire and support future research towards the understanding of complex dynamics underlying interdependent systems of different nature.

7.1 Contributions of the Thesis

At large, this research work contributes to the understanding of complex dynamics characterizing interdependent systems under disruptive events. Following principles of design science (cf. research design in Chapter 3), a set of new instruments and modeling tools are presented to cope with disruption spread and recovery phenomena into the nascent - and rapidly growing - field of cybersecurity of interdependent CIs.

As contribution to methodology, this dissertation presents a well-structured modeling process to understand relevant aspects of cybersecurity of CIs via the strategic use of mathematical modeling and simulation techniques. In particular, a block building modeling approach based on SD is proposed to capture nonlinear behaviors of networks of CIs under disruptive events. A key characteristic of this modeling approach is the possibility to implement model features which emphasize a particular aspects of the dynamics on the basis of specific applications.

Chapter 4 shows how building blocks of models can be used to support predictive analysis of cascading effects and evaluation of system resilience. Relevant to mention is that policies are easily implemented by changing model parameters to allow decision makers evaluating operational performance of interdependent CIs.

In details, three blocks of models are introduced to capture different aspects of both micro (single CI) and macro (across CIs) dynamics of operations in the complex system of interdependent CI systems. Building blocks are used for the generation of hypothetical disruption scenarios to conduct a simulation-based impact analysis by varying magnitude and duration of disruptive events. Also, the dynamic interdependency models are used to measure dynamic resilience with respect to both single CIs and the bigger system of CIs. For demonstration purpose, the SD model is applied to evaluate effectiveness of policy investments in CI capabilities for a specific scenario of disruption.

Of interest is that the overall modeling is primarily inspired by epidemic literature to understand how phenomena of spread and recovery dynamics can be explored using mathematical tools (cf. literature review in Chapter 2).

Dynamic interdependency models are iteratively extended and combined together during the modeling process to explore interdependent CIs through the lens of cybersecurity. In particular, Chapter 5 introduces a new building block to address cyber attack-defense dynamics by combining SD with a game-theoretic approach. This novel combination demonstrates that the dynamic interdependency models can be extended with new technologies and methodologies thanks to the block building modeling process.

In particular, combining SD with game-theoretic approaches allows investigating both operational and strategic dynamics of such complex cyber-physical systems. A dynamic cyber game model is developed to simulate strategic behaviors of attacker and defender to take over the CI control with a special emphasis on time components. Then, the SD model is applied to conduct a multi-objective optimization of proactive and reactive defenses and simulation analysis with the purpose of demonstrating how the model can support cybersecurity decisions within organizations. Beside interesting results on effectiveness of defense strategies, the analysis clearly shows that time-saving policy evaluation is another important feature of SD models.

Finally, Chapter 6 extends the building blocks of Chapter 4 to consider perturbations of CI service demand, market share of CI operators, and other impact factors which determine dynamics of cascade effects. Model extensions towards more realistic scenarios aim at providing insights for potential users of the SD model, such as CI operators that continuously attempt to forecast scenarios and assess risks of failures in interdependent CIs.

In practice, the dynamic interdependency models offer a valuable and flexible tool for predictive analysis to support risk managers in assessing scenario of crisis as well as CI operators towards more effective investment decisions and collective response actions. In fact, usability of the SD model includes the coordination of investment decisions to improve operational capabilities (cf. Chapter 4) and the optimization of cyber defense strategies to mitigate damage effects (cf. Chapter 5).

Further implications for practice are demonstrated through the application of the modeling approach to support crisis management processes in relevant cyber incident scenarios and use cases in the context of European CIs (cf. Chapter 6). More precisely, the dynamic interdependency model contributes to the design of the ECOSSIAN cyber incident response and early warning system. For such a purpose, the SD model is extended by a perspective of CI operators in accordance with the ENISA guidelines for the identification of critical services and sectors.

Note also that applicability of the modeling approach relies on the fact that dynamic simulations and graphical outputs provided by SD tools are particularly suitable for decision-makers who may not have mathematical background.

In sum, ranging from solid theoretical foundations to simulation models with practical relevance, research contributions accomplish the final scope of this design-oriented research to bridge theory and practice (cf. Chapter 3). On this note, relevant to mention are the collaborations with both industry and academia which highly strengthened the outcomes of this dissertation.

In the next section, final remarks include strengthens of the modeling approach and possible limitations due to the scarce availability of data in the field of cybersecurity of CIs.

7.2 Final Remarks

The overall scope of the dynamic interdependency models presented in this dissertation is to guide rational decisions in choosing building blocks of models for applications in - but not limited to - the field of cybersecurity of CIs.

A high level of abstraction is chosen for this research in order to preserve the applicability of the model to the field of CIs. As potential users of the interdependency model in the context of a pan-European early warning system (cf. Chapter 6), the CI operators partners of the ECOSSIAN project explicitly recommended not ask for sensitive data about CI components as input parameters of the model. The reason is that none of the operators would share information on what specific component is failed in its own infrastructure.

Relevant to mention is that choices on the abstraction level in the modeling and data required by the model are up to the user interest and application domain. This dissertation focuses on cybersecurity of CIs, but flexibility and potentials of the dynamic interdependency models allow to a number of other applications. For instance, the dynamics of each node may refer to a single process or component of an organization; and dynamic interdependencies among networked processes can be evaluated with the final goal of improving the organization's performance.

Overall the block building modeling approach based on SD allows to get a specific understanding of complex dynamics of systems in crisis situations without huge amounts of data required. Also, SD visualization tools facilitate the use of the dynamic interdependency models to experts and practitioners who may not have a mathematical background.

Limitations may concern unavailable real-world information to assess scenarios and model parameters. This research use data of the CI experts survey (Laugé et al., 2015) to quantify magnitudes of direct dependencies between CIs with the purpose of demonstrating usability and potential applicability of the modeling approach.

Motivated by the 2003 US power blackout, this dissertation analyzes interdependencies among Energy, Telecommunications, Transport and other CIs to facilitate research towards more complex CI disruption scenarios as well as the exploration of open issues such as internet of things and autonomous driving.

The next section briefly introduces further applications to inspire and support future research towards the understanding of complex dynamics underlying interdependent systems of different nature.

7.3 Further Applications

In line with the main purpose to contribute to the understanding of complex dynamics of interdependent systems under disruptive events, the set of mathematical instruments and modeling tools presented in this dissertation are suitable for further applications beyond the field of cybersecurity of CIs.

For instance, the idea of modeling operational capabilities and performance of a single CI may be shifted to the modeling of a specific device in an OT network. Operational Technology (OT) refers to the use of hardware and software dedicated to detecting or causing changes in physical processes through direct monitoring and/or control of physical devices (such as valves, pumps, etc.). Such technologies are process control domains (PCD), programmable logic controllers (PLC), distributed control systems (DCS), supervisory control and data acquisition (SCADA) systems, safety instrumented systems (SIS), and building management/automation systems (BAS), often collectively referred to as Industrial Control Systems (ICS). Interdependencies between these devices can be similarly modeled and cascade effects simulate on the basis of such dependencies. The OT network can be developed by integrating building blocks together. Further building blocks may model backup devices to test OT network capabilities to mitigate operational disruptions in presence of such devices which increase the redundancy of the system.

Moreover, the dynamic interdependency models can be applied to assess potential business interruptions in case of attacks to critical supply providers. Urban scenarios can be implemented to find the optimal allocation of priorities with respect to the provision of critical products and commodities to maintain the societal welfare. Therefore, complex operational challenges involve the logistic sector which must ensure an efficient and secure transport of critical supplies. Coupled dynamics will emerge from disruptive scenarios accounting for both transport and protection capabilities of suppliers. External impact factors which may temporary change supply priorities can be considered as well. Here, cybersecurity comes to play due to the increasing use of autonomous driving, drones and robots to improve manufacturing and supply capabilities.

Of interest of the author is to apply the findings of this research work towards a Comprehensive Approach (CA), defined as the strategic use of Operations Research and modeling and simulation tools for predictive analysis and multi-objective optimization of safety, security, health, political, economic, environmental, urban, and military aspects characterizing CIs of cities and nations.

In the context of military operations, the author of this dissertation has developed a CA demonstrator for military water supply in refugee camps under the supervision and guidance of the a.D. major-general of the German army force, Dr. Dieter Budde. The block building approach based on SD was used to develop the mathematical model which dynamically allocates available water resources accounting for prioritization of refugee needs, possible transport delays, and external factors such as heat waves. The dynamic model optimizes military water transport capabilities as well as the protection against terrorist attacks. Furthermore, a simulation interface was created to enable decision-makers to easily assess scenarios of crisis through an advanced visual analytics support. The CA demonstrator has been presented at the 2017 forum of the German society for defense technology (i.e. der Deutschen Gesellschaft für Wehrtechnik, DWT 2017) in Bonn as a valuable tool for military training purposes.

Bibliography

O. Akpa and B. Oyejola. Modeling the transmission dynamics of HIV/AIDS epidemics: an introduction and a review. *The Journal of Infection in Developing Countries*, 4(10): 497–608, 2010. (Cited on page 29.)

L. J. Allen and A. M. Burgin. Comparison of deterministic and stochastic SIS and SIR models in discrete time. *Mathematical Biosciences*, 163(1):1–33, 2000. (Cited on page 30.)

G. B. Anderson and M. L. Bell. Lights out: impact of the august 2003 power outage on mortality in new york. *Epidemiology (Cambridge, Mass.)*, 23(2):189, 2012. (Cited on page 10.)

R. M. Anderson. Discussion: the Kermack-McKendrick epidemic threshold theorem. *Bulletin of mathematical biology*, 53(1951):3–32, 1991. (Cited on pages 28, 30, and 31.)

G. Andersson, P. Donalek, R. Farmer, N. Hatziargyriou, I. Kamwa, P. Kundur, N. Martins, J. Paserba, P. Pourbeik, J. Sanchez-Gasca, et al. Causes of the 2003 major grid blackouts in north america and europe, and recommended means to improve system dynamic performance. *IEEE Transactions on Power Systems*, 20(4):1922–1928, 2005. (Cited on page 9.)

W. Arthur and E. Robert. Sensitivity Simulations. In *Proceedings of 14th International Conference of the System Dynamics Society*, 1996. (Cited on page 78.)

R. Ayoub and C. Richmond. Intelligence-Led Security. Technical report, IBM, 2016. (Cited on page 47.)

A. Azadeh, V. Salehi, M. Arvan, and M. Dolatkhah. Assessment of resilience engineering factors in high-risk environments by fuzzy cognitive maps: A petrochemical plant. *Safety Science*, 68:99–107, 2014. (Cited on page 83.)

S. Backhaus, R. Bent, J. Bono, R. Lee, B. Tracey, D. Wolpert, D. Xie, and Y. Yildiz. Cyber-physical security: A game theory model of humans interacting over control systems. *IEEE Transactions on Smart Grid*, 4:2320–2327, 2013. (Cited on page 92.)

R. Bagni, R. Berchi, and P. Cariello. A comparison of simulation models applied to epidemics. *Journal of Artificial Societies and Social Simulation*, 5(3), 2002. (Cited on page 37.)

V. A. Banuls and M. Turoff. Scenario construction via Delphi and cross-impact analysis. *Technological Forecasting and Social Change*, 78(9):1579–1602, 2011. (Cited on page 69.)

A.-L. Barabási and R. Albert. Emergence of scaling in random networks. *Science*, 286 (5439):509–512, 1999. (Cited on page 34.)

K. Barker, J. E. Ramirez-Marquez, and C. M. Rocco. Resilience-based network component importance measures. *Reliability Engineering & System Safety*, 117:89–97, 2013. (Cited on page 84.)

M. S. Bartlett. Some evolutionary stochastic processes. *Journal of the Royal Statistical Society. Series B (Methodological)*, 11(2):211–229, 1949. (Cited on page 30.)

R. Baskerville, J. Pries-Heje, and J. Venable. Soft design science methodology. In *proceedings of the 4th international conference on design science research in information systems and technology*, page 9. ACM, 2009. (Cited on pages 51 and 52.)

M. Beccuti, S. Chiaradonna, F. Di Giandomenico, S. Donatelli, G. Dondossola, and G. Franceschinis. Quantification of dependencies between electrical and information infrastructures. *International Journal of Critical Infrastructure Protection*, 5(1):14–27, 2012. (Cited on page 46.)

C. Beek, C. Castillo, C. Cochin, A. Hinchliffe, J. Jarvis, H. Li, Q. Liu, D. Mandal, M. Rosenquist, R. Samani, R. Sherstobitoff, R. Simon, B. Snell, D. Sommer, B. Sun, J. Walter, C. Xu, and S. Zhu. 2016 Threats Predictions McAfee. Technical report, Intel Security, 2016. (Cited on page 5.)

A. R. Berkeley and M. Wallace. A Framework for Establishing Critical Infrastructure Resilience Goals: Final Report and Recommendations. *Final Report and Recommendations by the Council*, pages 1–73, 2010. (Cited on page 82.)

D. Bernoulli. Essai d'une nouvelle analyse de la mortalité causée par la petite vérole et des avantages de l'inoculation pour la prévenir. *Histoire de l'Acad. Roy. Sci.(Paris) avec Mém. des Math. et Phys. and Mém*, pages 1–45, 1760. (Cited on page 25.)

A. Boin, M. Ekengren, and M. Rhinard. *The European Union as crisis manager: patterns and prospects*. Cambridge University Press, 2013. (Cited on page 10.)

A. Borshchev and A. Filippov. From System Dynamics and Discrete Event to Practical Agent Based Modeling: Reasons, Techniques, Tools. *The 22nd International Conference of the System Dynamics Society, July 25 - 29, 2004, Oxford, England*, 2004. (Cited on page 56.)

H. Bosetti, S. Khan, H. Aghaie, and P. Palensky. Survey, illustrations and limits of game theory for cyber-physical energy systems. *Automatisierungstechnik*, 62(5):375–384, 2014. (Cited on page 92.)

K. D. Bowers, M. Van Dijk, R. Griffin, A. Juels, A. Oprea, R. L. Rivest, and N. Triandopoulos. Defending Against the Unknown Enemy: Applying FLIPIT to System Security. In *Decision and Game Theory for Security*, pages 248–263. Springer Berlin Heidelberg, 2012. (Cited on page 93.)

S. Brandt. The changing landscape of cyber security, 2016. URL http://www.csooutlook.com/cioviewpoint/the-changing-landscape-of-cyber-security-nid-52.html. (Cited on page 47.)

F. Brauer and P. Van den Driessche. *Mathematical epidemiology*. Springer-Verlag, Berlin, 2008. (Cited on page 25.)

T. Britton. Stochastic epidemic models: a survey. *Mathematical biosciences*, 225(1): 24–35, 2010. (Cited on page 29.)

D. Brockmann, L. Hufnagel, and T. Geisel. The scaling laws of human travel. *Nature*, 439:462–465, 2006. (Cited on page 32.)

T. Brown. Multiple Modeling Approaches and Insights for Critical Infrastructure Protection. *Computational Models of Risks to Infrastructure*, pages 23–35, 2007. (Cited on page 45.)

T. Brown, W. Beyeler, and D. Barton. Assessing infrastructure interdependencies: the challenge of risk analysis for complex adaptive systems. *International Journal of Critical Infrastructures*, 1(1):108–117, 2004. (Cited on page 45.)

M. Bruneau and A. Reinhorn. Exploring the concept of seismic resilience for acute care facilities. *Earthquake Spectra*, 23(1):41–62, 2007. (Cited on page 84.)

M. Bruneau, S. E. Chang, R. T. Eguchi, G. C. Lee, T. D. O'Rourke, A. M. Reinhorn, M. Shinozuka, K. Tierney, W. a. Wallace, and D. Von Winterfeldt. A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. *Earthquake Spectra*, 19(4):733–752, 2003. (Cited on pages xvi, 84, and 85.)

BSI. Bsi-standards, 2017. URL https://www.bsi.bund.de/. (Cited on page 47.)

K. Bsufka, O. Kroll-Peters, and S. Albayrak. Intelligent network-based early warning systems. In J. Lopez, editor, *CRITIS 2006*, volume LNCS 4347, pages 103–111. Springer-Verlag Berlin Heidelberg, 2006. (Cited on page 108.)

S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin. Catastrophic cascade of failures in interdependent networks. *Nature*, 464(7291):1025–1028, 2010. (Cited on pages 5 and 40.)

E. Canzani. A review of epidemics modeling approaches to understand cyber crises. In R. Ortt, C. Bücker, and S. Klein, editors, *European Handbook on Networks in Innovation and Crisis management: Theory and Practice in a Dynamic and Disruptive Environment*, volume 2, pages 1–34. WWU Münster Academic Publications, 2016a. (Cited on pages 17 and 21.)

E. Canzani. Modeling Dynamics of Disruptive Events for Impact Analysis in Networked Critical Infrastructures. In *Proceedings of the 13th International Conference on Information Systems for Crisis Response and Management (ISCRAM 2016), Rio de Janeiro, Brazil.*, 2016b. (Cited on pages xv, 41, and 61.)

E. Canzani and U. Lechner. Toward Disruptions in the Boarding Process: A System Dynamics Approach. In *Proceedings of the Networking And Electronic Commerce Conference (NAEC 2014), Trieste, Italy.*, 2014. (Cited on page 16.)

E. Canzani and U. Lechner. Insights from Modeling Epidemics of Infectious Diseases - A Literature Review. In *Proceedings of the 12th International Conference on Information Systems for Crisis Response and Management (ISCRAM 2015), Kristiansand, Norway.*, 2015. (Cited on pages 17, 21, and 63.)

E. Canzani and S. Pickl. Cyber Epidemics: Modeling Attacker-Defender Dynamics in Critical Infrastructure Systems. In D. Nicholson, editor, *Series on Advances in Intelligent Systems and Computing (AISC): 7th International Conference on Applied Human Factors and Ergonomics (AHFE 2016), Orlando, Florida. Advances in Human Factors in Cybersecurity.*, volume 22, pages 377–389. Springer, 2016. (Cited on pages 17 and 91.)

E. Canzani, H.-C. Heldt, S. Meyer, and U. Lechner. Towards an Understanding of the IT Security Information Ecosystem. In H. Unger and W. Halang, editors, *Proceedings of the 7th GI Conference on Autonomous Systems 2014, Cala Minor, Maiorca.*, 2014a. (Cited on page 17.)

E. Canzani, S. Pickl, and R. De Leone. A System Dynamics Approach to the Airplane Boarding Process. In *Abstract Proceedings of the 20th Conference of the International Federation of Operational Research Societies (IFORS 2014), Barcelona, Spain.*, 2014b. (Cited on page 16.)

E. Canzani, H. Kaufmann, and U. Lechner. Characterizing Disruptive Events to Model Cascade Failures in Critical Infrastructures. In T. Brandstetter, H. Janicke, and K. Jones, editors, *Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research (ICS-CSR 2016), Belfast, Northern Ireland*, pages 95–101. BCS Learning & Development Ltd, 2016. (Cited on pages 18 and 107.)

E. Canzani, H. Kaufmann, and U. Lechner. An Operator-driven Approach for Modeling Interdependencies in Critical Infrastructures based on Critical Services and

Sectors. In G. Havarneanu, R. Setola, H. Nassopoulos, and S. Wolthusen, editors, *Critical Information Infrastructures Security: 11th International Conference (CRITIS 2016) Paris, France. Revised Selected Papers*, pages 308–320. Springer International Publishing, 2017. (Cited on pages 18 and 107.)

L. N. Carroll, A. P. Au, L. T. Detwiler, T. C. Fu, I. S. Painter, and N. F. Abernethy. Visualization and analytics tools for infectious disease epidemiology: A systematic review. *Journal of Biomedical Informatics*, 51:287–298, 2014. (Cited on page 35.)

E. Carvalho, L. Andrade, R. Chaim, and R. Pietrobon. A framework to streamline the process of systems modeling. *arXiv preprint arXiv:1112.5633*, 2011. (Cited on page 56.)

S. Chang, T. McDaniels, J. Mikawoz, and K. Peterson. Infrastructure failure interdependencies in extreme events: power outage consequences in the 1998 ice storm. *Nat. Hazards Earth Syst. Sci. Discuss.*, 41(2):337–358, 2007. (Cited on page 4.)

L. C. L. Chen and J. Leneutre. A Game Theoretical Framework on Intrusion Detection in Heterogeneous Networks. *IEEE Transactions on Information Forensics and Security*, 4(2):165–178, 2009. (Cited on page 93.)

K. K. R. Choo. The cyber threat landscape: Challenges and future research directions. *Computers and Security*, 30(8):719–731, 2011. (Cited on page 46.)

L. K. Comfort, Y. Sungu, D. Johnson, and M. Dunn. Complex Systems in Crisis: Anticipation and Resilience in Dynamic Environments. *Journal of Contingencies and Crisis Management*, 9(3):144–158, Sept. 2001. (Cited on page 2.)

W. Coombs. *Ongoing Crisis Communication: Planning, Managing, and Responding.* Thousand Oaks, CA: Sage, 2012. (Cited on page 2.)

L. Danon, A. P. Ford, T. House, C. P. Jewell, M. J. Keeling, G. O. Roberts, J. V. Ross, and M. C. Vernon. Networks and the epidemiology of infectious disease. *Interdisciplinary perspectives on infectious diseases*, 2011. (Cited on pages 31 and 32.)

G. Daryanani. Sensitivity Simulations: A Faster Alternative to Monte Carlo. *Journal of Financial Planning*, 9, 2002. (Cited on page 79.)

H. de Nijs. Concept Development and Experimentation Policy and Process: How Analysis Provides Rigour. *NATO Supreme Allied Command Transformation Norfolk VA*, 2010. (Cited on page 11.)

DHS. National Infrastructure Protection Plan 2009. Technical report, US Department of Homeland Security, Washington, DC, 2009. (Cited on page 43.)

DHS. NIPP 2013: Partnering for Critical Infrastructure Security and Resilience. Technical report, US Department of Homeland Security, 2013. (Cited on pages 3, 43, 86, and 88.)

A. Di Giorgio and F. Liberati. Interdependency modeling and analysis of critical infrastructures based on dynamic bayesian networks. In *Control & Automation (MED), 2011 19th Mediterranean Conference on*, pages 791–797. IEEE, 2011. (Cited on page 46.)

M. V. Dijk, A. Oprea, and R. L. Rivest. F L I P I T : The Game of "Stealthy Takeover". *Journal of Cryptology*, 4(26):655–713, 2013. (Cited on pages 91, 93, 94, and 106.)

DSP. Der deutsche Telekommunikationsmarkt im 2. Quartal 2016. Technical report, DSP Partners, Darmstadt, 2016. URL http://www.dsp-partners.com/2016/09/22/der-deutsche-telekommunikationsmarkt-im-2-quartal-2016/. (Cited on pages xvi and 114.)

D. D. Dudenhoeffer, M. R. Permann, and M. Manic. Cims: A framework for infrastructure interdependency modeling and analysis. In *Proceedings of the 38th Winter Simulation Conference*, pages 478–485, 2006. (Cited on page 45.)

L. Dueñas-Osorio, J. I. Craig, B. J. Goodno, and A. Bostrom. Interdependent response of networked systems. *Journal of Infrastructure Systems*, 13(3):185–194, 2007. (Cited on page 46.)

D. P. Duggan and J. T. Michalski. Threat Analysis Framework. Technical report, Sanida Reports, 2007. (Cited on page 47.)

C. Eckert. *IT-Sicherheit: Konzepte-Verfahren-Protokolle.* Walter de Gruyter, 2013. (Cited on page 47.)

ENISA. Methodologies for the identification of Critical Information Infrastructure assets and services. Technical report, European Network Information Security Agency, 2014. (Cited on pages xvi, xvii, 43, 109, 110, 111, 113, 121, and 128.)

ENISA. Definition of cybersecurity. Technical report, European Network Information Security Agency, 2015. (Cited on page 47.)

ENISA. The cost of incidents affecting CIIs. Technical report, European Network Information Security Agency, 2016a. (Cited on page 47.)

ENISA. Strategies for incident response and cyber crisis cooperation. Technical report, European Network Information Security Agency, 2016b. (Cited on page 47.)

ENISA. Threat Landscape 2015. Technical report, European Network Information Security Agency, 2016c. (Cited on page 47.)

P. Erdös and a. Rényi. On random graphs. *Publicationes Mathematicae*, 6:290–297, 1959. (Cited on pages 31 and 34.)

EU. Council of the European Union of 12 December 2008 on on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Official Journal of the European Union. L 345. Technical report, European Union, Brussels, Belgium, 2008. (Cited on page 3.)

EU. The EU Approach to Resilience: Learning from Food Security Crises. *Communication from the Commission to the European Parliament and the Council*, 2012. (Cited on page 82.)

I. Eusgeld, W. Kröger, G. Sansavini, M. Schläpfer, and E. Zio. The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures. *Reliability Engineering & System Safety*, 94:954–963, 2009. (Cited on pages 10 and 41.)

I. Eusgeld, C. Nan, and S. Dietz. System-of-systems approach for interdependent critical infrastructures. *Reliability Engineering and System Safety*, 96(6):679–686, 2011. (Cited on pages 41, 46, and 62.)

J. M. Fair, R. J. LeClaire, M. L. Wilson, A. L. Turk, S. M. DeLand, D. R. Powell, P. C. Klare, M. Ewers, L. Dauelsberg, and D. Izraelevitz. An integrated simulation of pandemic influenza evolution, mitigation and infrastructure response. In *Technologies for Homeland Security, 2007 IEEE Conference on*, pages 240–245. IEEE, 2007. (Cited on page 45.)

R. Faturechi, E. Levenberg, and E. Miller-Hooks. Evaluating and optimizing resilience of airport pavement networks. *Computers and Operations Research*, 43:335–348, 2014. (Cited on page 83.)

B. Faulkner. Towards a framework for tourism disaster management. *Tourism management*, 22(2):135–147, 2001. (Cited on page 3.)

FEPC. Graphical Flip-chart of Nuclear & Energy Related Topics 2014 (The Federation of Electric power Companies of Japan). Technical report, The Federation of Electric power Companies of Japan, 2015. (Cited on page 126.)

S. Forrest, S. Hofmeyr, and A. Somayaji. Computer Immunology. *Communications of the ACM*, 40(10):88–96, 1997. (Cited on page 39.)

J. W. Forrester. *Industrial Dynamics*. MIT Press, 1961. (Cited on page 53.)

J. W. Forrester. *World Dynamics*. Wright-Allen Press, 1971. (Cited on page 53.)

J. W. Forrester. Some basic concepts in system dynamics. *Sloan School of Management, Massachusetts Institute of Technology, Cambridge*, 2009. (Cited on pages 9 and 54.)

R. Francis and B. Bekera. A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliability Engineering & System Safety*, 121:90–103, 2014. (Cited on pages 82 and 84.)

X. Fu, M. Small, D. M. Walker, and H. Zhang. Epidemic dynamics on scale-free networks with piecewise linear infectivity and immunization. *Physical Review E - Statistical, Nonlinear, and Soft Matter Physics*, 77:1–8, 2008. (Cited on page 40.)

S. Funk, M. Salathé, and V. a. a. Jansen. Modelling the influence of human behaviour on the spread of infectious diseases: a review. *Journal of the Royal Society, Interface / the Royal Society*, 7(50):1247–56, 2010. (Cited on page 36.)

S. Galea, M. Riddle, and G. a. Kaplan. Causal thinking and complex system approaches in epidemiology. *International journal of epidemiology*, 39(1):97–106, 2010. (Cited on page 36.)

J. Gao, D. Li, and S. Havlin. From a single network to a network of networks. *National Science Review*, 1:346–356, 2014. (Cited on page 41.)

K. W. Goodman and E. M. Meslin. Ethics, Information Technology, and Public Health: Duties and Challenges in Computational Epidemiology. In *Public Health Informatics and Information Systems*, pages 191–209. Springer London, 2014. (Cited on page 36.)

P. E. Greenwood and L. F. Gordillo. Stochastic epidemic modeling. In *Mathematical and Statistical Estimation Approaches in Epidemiology*, pages 31–52. Springer, 2009. (Cited on page 29.)

T. Gross, C. J. D. D'Lima, and B. Blasius. Epidemic dynamics on an adaptive network. *Physical Review Letters*, 96(20), 2006. (Cited on page 35.)

B. Haemmerli and A. Renda. Protecting Critical Infrastrcuture in the EU. Technical report, CEPS Center for European Policy Studies, Brussels, Belgium, 2010. (Cited on page 110.)

Y. Haimes and P. Jiang. Leontief-Based Model of Risk in Complex Interconnetted Infrastructures. *Journal of Infrastructure Systems*, 7(1):1–12, 2001. (Cited on page 45.)

Y. Y. Haimes. *Risk modeling, assessment, and management*. John Wiley & Sons, 2015. (Cited on pages 10 and 79.)

Y. Y. Haimes, B. M. Horowitz, J. H. Lambert, J. Santos, K. Crowther, and C. Lian. Inoperability Input-Output Model for Interdependent Infrastructure Sectors. I: Theory and methodology. *Journal of Infrastructure Systems*, 11:67–79, 2005. (Cited on page 45.)

M. E. Halloran, I. M. L. Jr, A. Nizam, and Y. Yang. Containing Bioterrorist Smallpox. *Science*, 298(5597):1428–1432, 2002. (Cited on page 32.)

J. Hasan, S. States, and R. Deininger. Safeguarding The Security Of Public Water Supplies Using Early Warning Systems: A Brief Review. *Journal of Contemporary Water Research & Education*, 129:27–33, 2004. (Cited on page 108.)

F. He, J. Zhuang, and N. S. V. Rao. Game-Theoretic Analysis of Attack and Defense in Cyber-Physical Network Infrastructures. *Proceedings of the Industrial and Systems Engineering Research Conference*, 2012. (Cited on page 92.)

P. Hernández, M. Muñoz Herrera, and A. Sánchez. Heterogeneous network games: Conflicting preferences. *Games and Economic Behavior*, 79:56–66, 2013. (Cited on page 93.)

J. Hernantes, E. Rich, A. Laugé, L. Labaka, and J. M. Sarriegi. Learning before the storm: Modeling multiple stakeholder activities in support of crisis management, a practical case. *Technological Forecasting and Social Change*, 80(9):1742–1755, 2013. (Cited on page 10.)

H. Hethcote. Three basic epidemiological models. In L. Gross, T. G. Hallam, and S. A. Levin, editors, *Applied mathematical ecology*, pages 119–144. Springer-Verlag, Berlin, 1989. (Cited on pages 25 and 28.)

H. Hethcote. A thousand and one epidemic models. *Frontiers in mathematical biology*, 1994. (Cited on page 25.)

H. Hethcote. The mathematics of infectious diseases. *SIAM review*, 42(4):599–653, 2000. (Cited on page 26.)

H. W. Hethcote and J. a. Yorke. Gonorrhea; transmission dynamics and control. *Lecture notes in biomathematics*, 56:1–105, 1984. (Cited on page 29.)

A. Hevner and S. Chatterjee. *Design science research in information systems*. Springer, 2010. (Cited on page 51.)

A. R. Hevner. A three cycle view of design science research. *Scandinavian journal of information systems*, 19(2):4, 2007. (Cited on page 52.)

J. Hines et al. Molecules of structure: Building blocks for system dynamics models. *Unpublished Manuscript, MIT Sloan School of Management, Cambridge, MA*, 2139: E53–305, 1996. (Cited on page 57.)

R. Holden, D. V. Val, R. Burkhard, and S. Nodwell. A network flow model for interdependent infrastructures at the local scale. *Safety Science*, 53:51–60, 2013. (Cited on page 45.)

J. Holmstr, M. Ketokivi, and A.-P. Hameri. Bridging Practice and Theory : A Design Science Approach. *Decision Science*, 40(1):65–87, 2009. (Cited on pages 51 and 52.)

J. B. Homer and G. B. Hirsch. System dynamics modeling for public health: background and opportunities. *American journal of public health*, 96(3):452–8, 2006. (Cited on page 36.)

S. Hosseini, K. Barker, and J. E. Ramirez-Marquez. A review of definitions and measures of system resilience. *Reliability Engineering & System Safety*, 145:47–61, 2016. (Cited on pages xvi, 82, and 83.)

J. Huang. Eradicating Computer Viruses on Networks. *arXiv:1207.3388*, pages 1–8, 2012. (Cited on page 40.)

L. Hufnagel, D. Brockmann, and T. Geisel. Forecast and control of epidemics in a globalized world. *Proceedings of the National Academy of Sciences of the United States of America*, 101(42):15124–15129, 2004. (Cited on page 32.)

Intel Security. Critical Infrastructure Readiness Report: Holding the Line Against Cyberthreats. Technical report, The Aspen Institute, 2015. (Cited on page 47.)

V. Isham. Stochastic Models for Epidemics with Special Reference to AIDS. In *The Annals of Applied Probability*, volume 3, pages 1–27. Institute of Mathematical Statistics, 2008. (Cited on pages 29 and 30.)

ISO. Final Report: On the August 14, 2003 Blackout. Technical report, ISO New York Independent System Operator, 2005. (Cited on pages 8 and 9.)

J. Johansson and H. Hassel. An approach for modelling interdependent infrastructures in the context of vulnerability analysis. *Reliability Engineering & System Safety*, 95 (12):1335–1344, 2010. (Cited on page 46.)

A.-M. Juuso and A. Takanen. Proactive Cyber Security: Stay Ahead of Advanced Persistent Threats (APTs). Technical report, Codenomicon WP, 2012. (Cited on pages 48 and 106.)

J. H. Kahan, A. C. Allen, and J. K. George. An Operational Framework for Resilience. *Journal of Homeland Security and Emergency Management*, 6(1):1–48, 2009. (Cited on page 83.)

F. Karaca, P. G. Raven, J. Machell, and F. Camci. A comparative analysis framework for assessing the sustainability of a combined water and energy infrastructure. *Technological Forecasting and Social Change*, 90:456 – 468, 2015. (Cited on page 45.)

Kaspersky. Cyberthreat real-time map, 2017. URL https://cybermap.kaspersky.com. (Cited on page 48.)

H. Kaufmann, R. Hutter, F. Skopik, and M. Mantere. A structural design for a pan-European early warning system for critical infrastructures. In *Elektrotechnik und Informationstechnik*. Springer Verlag Wien, 2014. (Cited on page 108.)

E. K. Keating. Everything You Ever Wanted to Know about How to Develop A System Dynamics Model, But Were Afraid to Ask. In *16th International Conference of the System Dynamics Society*, 1998. (Cited on page 57.)

M. J. Keeling and K. T. D. Eames. Networks and epidemic models. *Journal of the Royal Society*, 2(4):295–307, 2005. (Cited on pages 31 and 33.)

J. Kephart, S. White, and D. Chess. Computers and epidemiology. *Spectrum, IEEE*, 1993. (Cited on page 38.)

J. O. Kephart. A biologically inspired immune system for computers. In *Artificial Life IV: proceedings of the fourth international workshop on the synthesis and simulation of living systems*, 1994. (Cited on page 39.)

M. Kermack and A. G. McKendrick. Contributions to the mathematical theory of epidemics. Part I. *In Proc. Roy. Soc. London Ser A*, 115(5):700–721, 1927. (Cited on pages 27, 29, and 39.)

W. O. Kermack and A. G. McKendrick. Contributions to the Mathematical Theory of Epidemics II . The Problem of Endemicity. *Proceedings of the Royal society of London. Series A*, 138(834):55–83, 1932. (Cited on page 28.)

A. S. Klovdahl. Social networks and the spread of infectious diseases: the AIDS example. *Social science & medicine*, 21(11):1203–1216, 1985. (Cited on page 31.)

R. D. Knabb, J. R. Rhome, and D. P. Brown. Tropical cyclone report: Hurricane katrina, august 23-30, 2005. *Fire Engineering*, 159(5):32–40, 2006. (Cited on page 4.)

E. D. Knapp and J. T. Langill. *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems.* Syngress, 2014. (Cited on page 10.)

W. Kröger. Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools. *Reliability Engineering and System Safety*, 93:1781–1787, 2008. (Cited on pages 10 and 42.)

B. Krogh, E. Lee, I. Lee, A. Mok, R. Rajkumar, L. Sha, A. Vincentelli, K. Shin, J. Stankovic, and J. Sztipanovits. Cyber-Physical Systems, Executive Summary. Technical report, CPS Steering Gruop, Washington DC, 2008. (Cited on page 5.)

M. N. Kuperman. Invited review: Epidemics on social networks. *Papers in Physics*, 5: 17, 2013. (Cited on pages 31, 34, and 35.)

L. Labaka, J. Hernantes, A. Laugé, and J. M. Sarriegi. Enhancing resilience: implementing resilience building policies against major industrial accidents. *International Journal of Critical Infrastructures*, 9(October 2015):130, 2013. (Cited on page 83.)

J. Ladyman, J. Lambert, and K. Wiesner. What is a complex system? *European Journal for Philosophy of Science*, 3(1):33–67, 2013. (Cited on page 2.)

F. Landriscina. *Simulation and Learning: A Model-Centered Approach.* Springer, 2013. (Cited on page 54.)

R. Langner. To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve. *Langner Group, Arlington, VA*, 2013. (Cited on page 5.)

A. Laszka, M. Felegyhazi, and L. Buttyan. A Survey of Interdependent Information Security Games. *ACM Computing Surveys*, 47:1–38, 2014. (Cited on page 93.)

J. Laudan, V. Roezer, T. Sieg, K. Vogel, and A. Thueken. Brief communication: On-site data collection of damage caused by flash floods: Experiences from Braunsbach, Germany, in May/June 2016. *Manuscript under review for Journal Natural Hazards and Earth System Sciences Discussions*, 2016. (Cited on page 4.)

A. Laugé, J. Hernantes, and J. M. Sarriegi. Critical infrastructure dependencies: A holistic, dynamic and quantitative approach. *International Journal of Critical Infrastructure Protection*, 8:16–23, 2015. (Cited on pages xvii, 43, 59, 65, 66, 67, 69, 80, and 134.)

A. B. Lawson. *Statistical methods in spatial epidemiology.* John Wiley & Sons, 2013. (Cited on page 35.)

J. Leskovec, K. J. Lang, A. Dasgupta, and M. W. Mahoney. Community Structure in Large Networks: Natural Cluster Sizes and the Absence of Large Well-Defined Clusters. *Internet Mathematics*, 6(1):29–123, 2009. (Cited on page 33.)

B. Liscouski and W. Elliot. Final report on the august 14, 2003 blackout in the united states and canada: Causes and recommendations. *A report to US Department of Energy*, 40(4), 2004. (Cited on pages 8 and 9.)

E. Luiijf, A. Nieuwenhuijs, M. Klaver, M. van Eeten, and E. Cruz. Empirical findings on critical infrastructure dependencies in europe. In *International Workshop on Critical Information Infrastructures Security*, pages 302–310. Springer, 2008. (Cited on pages 43 and 80.)

D. A. Luke and K. A. Stamatakis. System science methods in public health: dynamics, networks and agents. *Annual review of public health*, 33:357–376, 2012. (Cited on page 36.)

N. Madar, T. Kalisky, R. Cohen, D. Ben-Avraham, and S. Havlin. Immunization and epidemic dynamics in complex networks. *European Physical Journal B*, 38:269–276, 2004. (Cited on page 39.)

S. Magazine. The changing cybersecurity landscape in 2016, 2016. URL http://www.securitymagazine.com/articles/86915-the-changing-cybersecurity-landscape-in-2016. (Cited on page 47.)

M. H. Manshaei, Q. Zhu, T. Alpcan, T. Bacşar, and J.-P. Hubaux. Game theory meets network security and privacy. *ACM Computing Surveys*, 45(3):1–39, 2013. (Cited on page 92.)

M. V. Marathe and N. Ramakrishnan. Recent Advances in Computational Epidemiology. *IEEE Computer Society*, 13:96–101, 2013. (Cited on page 37.)

R. May and R. Anderson. Transmission dynamics of HIV infection. *Nature*, 326(6109): 137–142, 1987. (Cited on pages 29 and 31.)

T. McDaniels, S. Chang, K. Peterson, J. Mikawoz, and D. Reed. Empirical framework for characterizing infrastructure failure interdependencies. *Journal of Infrastructure Systems*, 13(3):175–184, 2007. (Cited on page 43.)

D. H. Meadows and D. Wright. *Thinking in systems: A primer*. Chelsea Green Publishing, 2008. (Cited on page 54.)

M. Meisel, V. Pappas, and L. Zhang. A taxonomy of biologically inspired research in computer networking. *Computer Networks*, 54(6):901–916, 2010. (Cited on pages xv, 37, 38, and 39.)

D. Mendonca and A. William. Impacts of the 2001 World Trade Center attack on New York City critical infrastructures. *Journal of Infrastructure Systems*, 12(4):260—-270, 2006. (Cited on page 4.)

S. Milgram. The small world problem. *Psychology today*, 2(1):61–66, 1967. (Cited on page 33.)

R. Milo, S. Shen-Orr, S. Itzkovitz, N. Kashtan, D. Chklovskii, and U. Alon. Network motifs: simple building blocks of complex networks. *Science*, 298(5594):824–827, 2002. (Cited on page 57.)

B. K. Mishra and N. Jha. SEIQRS model for the transmission of malicious objects in computer network. *Applied Mathematical Modelling*, 34(3):710–715, 2010. (Cited on page 39.)

M. Mitchell. Complex systems: Network thinking. *Artificial Intelligence*, 170(18):1194–1212, 2006. (Cited on page 2.)

J. P. Monat and T. F. Gannon. What is systems thinking? a review of selected literature plus recommendations. *American Journal of Systems Science*, 4(1):11–26, 2015. (Cited on page 54.)

M. Morris. Epidemiology and Social Networks: Modeling Structured Diffusion. *Sociological Methods & Research*, 22(1):99–126, 1993. (Cited on pages 31 and 37.)

J. Mossong, N. Hens, M. Jit, P. Beutels, K. Auranen, R. Mikolajczyk, and W. J. Edmunds. Social contacts and mixing patterns relevant to the spread of infectious diseases. *PLoS medicine*, 5(3), 2008. (Cited on page 32.)

J. Moteff, P. Parfomak, and I. Ave. Critical Infrastructure and Key Assets: Definition and Identification. Technical report, CRS Report for Congress, 2004. (Cited on page 4.)

W. Murray. The application of epidemiology to computer viruses. *Computers & Security*, 7(1988):139–145, 1988. (Cited on page 38.)

R. B. Myerson. *Game theory*. Harvard University Press, 2013. (Cited on page 92.)

National Research Council and others. Complex and interdependent systems. In *Making the nation safer: The role of science and technology in countering terrorism*. National Academies Press, 2002. (Cited on page 2.)

NERC. Technical Analysis of the August 14, 2003, Blackout: What Happened, Why, and What Did We Learn? Technical report, NERC Steering Group, 2015. (Cited on page 6.)

M. E. J. Newman. The spread of epidemic disease on networks. *Physical Review E*, 66 (1), Apr. 2002. (Cited on pages 31, 33, and 34.)

M. E. J. Newman. The structure and function of complex networks. *SIAM review*, 45 (2):167–256, 2003. (Cited on pages 32 and 33.)

A. Nieuwenhuijs, E. Luiijf, and M. Klaver. Modeling dependencies in critical infrastructures. In *International Conference on Critical Infrastructure Protection*, pages 205–213. Springer, 2008. (Cited on page 41.)

M. S. Nistor, S. W. Pickl, M. Raap, and M. Zsifkovits. Network efficiency and vulnerability analysis using the flow–weighted efficiency measure. *International Transactions in Operational Research*, (0):1–12, 2017. ISSN 1475-3995. (Cited on page 45.)

NITIM. Nitim international graduate school, 2017. URL https://www.nitim.org/. (Cited on page 16.)

A. Nochenson, J. Grossklags, et al. A behavioral investigation of the flipit game. In *Proceedings of the 12th Workshop on the Economics of Information Security (WEIS)*, 2013. (Cited on page 93.)

NREL. Renewable Electricity Futures Study: End-use Electricity Demand. Technical report, National Renewable Energy Laboratory), 2012. (Cited on page 126.)

E. H. Oh, A. Deshmukh, and M. Hastak. Disaster impact analysis based on interrelationship of critical infrastructure and associated industries: A winter flood disaster event. *International Journal of Disaster Resilience in the Built Environment*, 1(1): 25–49, 2010. (Cited on page 46.)

G. P. O'Reilly, A. Jrad, A. Kelic, and R. Leclaire. Telecom critical infrastructure simulations: Discrete event simulation vs. dynamic simulation how do they compare? *GLOBECOM - IEEE Global Telecommunications Conference*, pages 2597–2601, 2007. doi: 10.1109/GLOCOM.2007.493. (Cited on pages 10 and 41.)

R. S. Ostfeld, G. E. Glass, and F. Keesing. Spatial epidemiology: an emerging (or reemerging) discipline. *Trends in ecology & evolution*, 20(6):328–36, 2005. (Cited on page 35.)

M. Ouyang. Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering and System Safety*, 121:43–60, 2014. (Cited on pages xvii, 4, 10, 41, 42, 43, 44, 46, 49, and 56.)

T. D. O'Rourke. Critical Infrastructure, Interdependencies, and Resilience. *Bridge-Washington-National Academy of Engineering-*, 37(1):22–29, 2007. (Cited on page 4.)

R. Pant, K. Barker, and C. W. Zobel. Static and dynamic metrics of economic resilience for interdependent infrastructure and industry sectors. *Reliability Engineering & System Safety*, 125:92–102, 2014. (Cited on page 84.)

R. Pastor-Satorras and A. Vespignani. Epidemic spreading in scale-free networks. *Physical review letters*, 86(14), Oct. 2001. (Cited on pages 34 and 39.)

P. Patlolla, V. Gunupudi, A. R. Mikler, and R. T. Jacob. Agent-based simulation tools in computational Epidemiology. In *Innovative Internet Community Systems*, pages 212–223. Springer Berlin Heidelberg, 2006. (Cited on page 37.)

P. Pederson, D. Dudenhoeffer, S. Hartley, and M. Permann. Critical infrastructure interdependency modeling: a survey of US and international research. *Idaho National Laboratory*, pages 1–20, 2006. (Cited on page 46.)

J. R. C. Piqueira and V. O. Araujo. A modified epidemiological model for computer viruses. *Applied Mathematics and Computation*, 213(2):355–360, 2009. (Cited on page 39.)

Ponemon Institute. 2015 cost of cyber crime study: Global. Technical report, PPonemon Institute, 2015. (Cited on page 11.)

C.-A. Popescu and C. P. Simion. A method for defining critical infrastructures. *Energy*, 42:32–34, 2012. (Cited on pages 41 and 42.)

S. D. Porcellinis, R. Setola, S. Panzieri, and G. Ulivi. Simulation of heterogeneous and interdependent critical infrastructures. *International Journal of Critical Infrastructures*, 4:110–128, 2008. (Cited on page 41.)

PSEPC. Ontario–U.S. Power Outage — Impacts on Critical Infrastructure. Technical report, Public Safety and Emergency Preparedness in Canada, 2006. (Cited on pages 6, 8, and 9.)

T. Radzik. Results and Problems in Games of Timing. *Lecture Notes-Monograph Series in Statistics, Probability and Game Theory*, 30:269–292, 1996. (Cited on page 93.)

J. J. Randolph. A Guide to Writing the Dissertation Literature Review. *Practical Assessment, Research & Evaluation*, 14(13), 2009. (Cited on pages xvii, 22, 23, and 25.)

M. Rezaeian, G. Dunn, S. St Leger, and L. Appleby. Geographical epidemiology, spatial analysis and geographical information systems: a multidisciplinary glossary. *Journal of epidemiology and community health*, 61(2):98–102, 2007. (Cited on page 35.)

S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21:11–25, 2001. (Cited on pages 4, 40, 41, 42, and 70.)

S. Risau-Gusman and D. H. Zanette. Contact switching as a control strategy for epidemic outbreaks. *Journal of Theoretical Biology*, 257(1):52–60, 2009. (Cited on page 35.)

S. E. Robinson, M. G. Everett, and R. M. Christley. Recent network evolution increases the potential for large epidemics in the British cattle population. *Journal of the Royal Society Interface*, 4(15):669–674, 2007. (Cited on page 32.)

A. Rose. Economic resilience to disaster. Technical report, Community and Regional Resilience Institute (CARRI), 2009. (Cited on page 84.)

A. Rose and S.-Y. Liao. Modeling regional economic resilience to disasters: A computable general equilibrium analysis of water service disruptions. *Journal of Regional Science*, 45(1):75–112, 2005. (Cited on page 45.)

R. Ross. *The Prevention of Malaria*. Murray, 2nd edition, 1911. (Cited on page 25.)

S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu. A Survey of Game Theory as Applied to Network Security. In *43rd Hawaii International Conference on System Sciences*, pages 1–10, 2010. (Cited on pages xvi and 92.)

SANS. An Overview of Threat and Risk Assessment. Technical report, SANS Institute, 2002. (Cited on page 47.)

P. Senge. *The Fifth Discipline: The Art and Practice of the Learning Organization*. Doubleday/Currency, 1990. (Cited on page 53.)

G. Settanni, F. Skopik, Y. Shovgenya, R. Fiedler, H. Kaufmann, T. Gebhardt, and C. Ponchel. A Blueprint for a Pan-European Cyber Incident Analysis System. In *3rd International Symposium for ICS & SCADA Cyber Security Research 2015*, pages 84–88, 2015. (Cited on page 108.)

Shodan. Computer search engine, 2017. URL https://maps.shodan.io. (Cited on page 48.)

A. Shostack. *Threat Modeling: designing for security*. Wiley, 2014. (Cited on page 48.)

S. P. Simonovic. *Systems Approach to Management of Disasters: Methods and Applications*. John Wiley & Sons, Inc., Feb. 2011. (Cited on page 3.)

Spiegel Online. Anti-Virus Pioneer Evegeny Kaspersky: 'I fear the net will become soon a war zone', 2011. URL http://www.spiegel.de/international/world/anti-virus-pioneer-evgeny-kaspersky-i-fear-the-net-will-soon-become-a-war-zone-a-770191.html. (Cited on pages 5, 9, and 10.)

T. Spyridopoulos, G. Oikonomou, T. Tryfonas, and M. Ge. Game Theoretic Approach for Cost-Benefit Analysis of Malware Proliferation Prevention. *Security and Privacy Protection in Information Processing Systems*, pages 28–41, 2013. (Cited on page 92.)

J. P. Sterbenz, E. K. Cetinkaya, M. A. Hameed, A. Jabbar, S. Qian, and J. P. Rohrer. Evaluation of Network Resilience, Survivability, and Disruption Tolerance: Analysis, Topology Generation, Simulation, and Experimentation. *Telecommunication Systems*, 52(2):705–736, 2013. (Cited on pages 64, 83, and 85.)

J. P. G. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller, and P. Smith. Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks*, 54(8):1245–1265, 2010. (Cited on page 83.)

J. D. Sterman. *Business Dynamics: Systems Thinking and Modeling for a Complex World*. Irwin/McGraw-Hill, 2000. (Cited on pages 56 and 79.)

J. D. Sterman. System Dynamics Modeling: Tools for Learning in a Complex World. *California Management Review*, 4(43), 2001. (Cited on page 56.)

J. D. Sterman. All models are wrong: reflections on becoming a systems scientist. *System Dynamics Review*, 18(4):501–531, 2002. (Cited on page 56.)

D. Strauss and O. Frank. Markov Graphs. *Journal of the American Statistical association*, 81(395):832–842, 1986. (Cited on page 34.)

N. K. Svendsen and S. D. Wolthusen. Connectivity models of interdependency in mixed-type critical infrastructure networks. *Information Security Technical Report*, 12(1): 44–55, 2007. (Cited on pages 10 and 46.)

S. Swarup, S. Eubank, and M. Marathe. Computational epidemiology as a challenge domain for multiagent systems. *Proceedings of the 2014 International Conference on Autonomous Agents and Multi-agent Systems*, pages 1173–1176, 2014. (Cited on page 36.)

C.-W. Ten and G. Manimaran. Cybersecurity for Critical Infrastructures: Attack and Defense Modeling. *IEEE Transactions on Systems, Man, and Cybernetics*, 40(4):853–865, 2010. (Cited on page 92.)

A. Vahdat and D. Becker. Epidemic routing for partially connected ad hoc networks. *Technical report number CS-200006, Duke University*, pages 1–14, 2000. (Cited on page 38.)

Vensim. Ventana systems, inc., 2015. URL https://vensim.com. (Cited on pages 11 and 58.)

L. Von Bertalanffy. An outline of general system theory. *The British Journal for the Philosophy of science*, 1(2):134, 1950. (Cited on pages 53 and 54.)

E. D. Vugrin and R. C. Camphouse. Infrastructure resilience assessment through control design. *International Journal of Critical Infrastructures*, 7(3):243, 2011. (Cited on page 45.)

T. Wai. *Stochastic Modeling of AIDS Epidemiology and HIV Pathogenesis.* World Scientific Publishing, 2000. (Cited on page 30.)

C. W. C. Wang, J. Knight, and M. Elder. On computer viral infection and the effect of immunization. *Proceedings 16th Annual Computer Security Applications Conference (ACSAC'00)*, 2000. (Cited on page 40.)

M. Wang and T. Suda. The Bio-Networking Architecture: a biologically inspired approach to the design of scalable, adaptive, and survivable/available network applications. *Proceedings 2001 Symposium on Applications and the Internet*, pages 1–25, 2001. (Cited on page 38.)

Y. Wang and D. Chakrabarti. Epidemic spreading in real networks: An eigenvalue viewpoint. *Reliable Distributed Systems, 2003. Proceedings. 22nd International Symposium on. IEEE*, pages 25–34, 2003. (Cited on page 39.)

R. A. Watson, G. S. Hornby, and J. B. Pollack. Modeling building-block interdependency. In *International Conference on Parallel Problem Solving from Nature*, pages 97–106. Springer, 1998. (Cited on page 56.)

D. J. Watts and S. H. Strogatz. Collective dynamics of 'small-world' networks. *Nature*, 393(6684):440–442, 1998. (Cited on page 34.)

J. Webster and R. Watson. Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MISQ*, 26(2):13–23, 2002. (Cited on page 22.)

G. Weng, U. S. Bhalla, and R. Iyengar. Complexity in biological signaling systems. *Science*, 284(5411):92–96, 1999. (Cited on page 2.)

S. R. White. Open Problems in Computer Virus Research. *Virus Bulletin Conference*, pages 1–11, 1998. (Cited on pages 40 and 49.)

X. Yang and L.-X. Yang. Towards the Epidemiological Modeling of Computer Viruses. *Discrete Dynamics in Nature and Society*, 2012:1–11, 2012. (Cited on page 39.)

J. M. Yusta, G. J. Correa, and R. Lacal-Arántegui. Methodologies and applications for critical infrastructure protection: State-of-the-art. *Energy Policy*, 39(10):6100–6119, Oct. 2011. (Cited on page 46.)

K. Zetter. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.* Crown Publishers, 2014. (Cited on page 47.)

M. Zhang, Z. Zheng, and N. B. Shroff. Stealthy Attacks and Observable Defenses : A Game Theoretic Model Under Strict Resource Constraints. *Signal and Information Processing (GlobalSIP), 2014 IEEE Global Conference on. IEEE*, pages 813–817, 2014. (Cited on pages 93 and 94.)

J. Zhuang and M. E. Nikoofal. Robust Allocation of a Defensive Budget Considering an Attacker's Private Information. *Risk Analysis*, 32:930–943, 2012. (Cited on page 92.)

R. Zimmerman and C. E. Restrepo. The next step: quantifying infrastructure interdependencies to improve security. *International Journal of Critical Infrastructures*, 2:215–230, 2006. (Cited on page 41.)

C. C. Zou, W. Gong, and D. Towsley. Code red worm propagation modeling and analysis. *Proceedings of the 9th ACM conference on Computer and communications security - CCS '02*, page 138, 2002. (Cited on page 39.)