A STUDY OF THE DANISH CRITICAL INFORMATION INFRASTRUCTURE PROTECTION SYSTEMS OF GOVERNANCE

A MULTI-SCALE SYSTEMS REPRESENTATION OF THE DANISH CRITICAL INFORMATION INFRASTRUCTURE

by

Mille Skovgaard Hansen

AALBORG UNIVERSITY
DENMARK

Master of Science in Technology in
Risk and Safety Management

Master Thesis

Dissertation submitted

December 20, 2019

Thesis submitted:	December 20, 2019
Master thesis supervisor:	Prof. Michael Havbro Faber Nielsen, University of Aalborg
Assistant supervisors:	PhD fellow. Linda Nielsen, University of Aalborg
	Post.doc Henning Brüske, University of Aalborg
Title:	A Study of the Danish Critical Information Infrastructure Protection Systems of Governance
Theme:	Master thesis dissertation Master of Science in Technology in Risk and Safety Management
Project period:	Autumn 2019
Page numbers:	99
Number of copies:	5

ACKNOWLEDGEMENTS

I would like to thank my supervisor Michael Havbro Faber and co-supervisors Linda Nielsen and Henning Brüske for enabling the existence of this master thesis research. Your different views gave me inspiration to expand my horizon of knowledge and provided me with the strength to seek beyond my immediate comfort zone. Thank you, for your guidance and firm belief in my abilities and research topic. I would like to thank Linda for not only being my co-supervisor for the master thesis, but also for being my academic mentor throughout my master programme. Your ability and persistence of working in the inevitable interdisciplinary field of engineering and social sciences, inspires me to continue to pursue an interdisciplinary risk management profile.

I would like to thank my dear friend PhD. in theology Trine Amalie Christiansen for her devotion in reading and commenting. I would like to thank my parents and parents-in-law for being there during times when the thesis required my full attention. Thank you for your constant curiosity and positive mindset. Thank you for spending time with my daughter when I was unable to. Finally, I would like to thank my wife for not only proofreading the majority of the research as well as for her patience when engaging in one out of many dialogues and for giving me the strength and motivation to keep pushing myself.

Thank you.

ABSTRACT

The identification of what constitute the Danish critical information infrastructure is currently vague and inconsistent strategically, tactically and operationally. This master study aims to fill a knowledge gap with a novel framework of CIIP governance by mapping the current systems of governance of the Danish critical information infrastructure protection by using a novel multi-scale system identification analysis. In addition, the study presents a bibliometric analysis that reviews current peer-reviewed and grey literature of alternative governance approaches and critical information infrastructure to examine the state-of-the-art practice. By evaluating the system from the perspective of the single-hazard, multi-hazard and all-hazard approaches the research discusses challenges of horizontal coordination and vertical integration with consideration of prioritisation and identification of criticality. Finally, the research suggests adopting an adaptive risk governance approach including a governmental organisation that prioritises critical information infrastructure protection at ministerial level as well as organising a horizontal coordination by identifying the criticality across existing sectors.

EXECUTIVE SUMMARY

In 2018, the Danish critical information infrastructure (CII) is identified by the Danish Ministry of Finance. Though, the responsibility of identifying the critical operators and assets is given to the sector authorities. There are discrepancies in what constitutes the critical information infrastructure and how resources should be allocated. Furthermore, there is generally very little transparency of the current systems of governance, from which it can be concluded that it is differentiated by sectoral authorities. The principle of sector responsibility is a cornerstone of Danish society that is still maintained. The control of the CII is therefore carried out in vertical top-down sectors, with no immediate organizational horizontal coordination.

To establish the context and support the arguments in the master thesis, a bibliometric analysis is introduced with the presentation of a network visualisation software using a datamining technique to illustrate keyword co-occurrence networks. In addition, the analysis showed a sparse number of publications contributing to a whole-of systems CII, which merely supports the novelty of the present master thesis.

The current research aims to identify two systems: (i) The physical critical information infrastructure system; and (ii) The governance systems of the critical information infrastructure system. The thesis includes a multi-scale system identification, where (i) Single-hazard represents the identification of the system from its subsystems; (ii) The multi-hazard approach represents the identification of the system from the dependencies of the subsystems; and (iii) the all-hazard approach represents identification of system dependencies without recognition of the subsystems.

The analysis within the perspective of the single-hazard approach resulted in a diverse system of governance of the critical information infrastructure protection (CIIP) with consideration of different political prioritised sectors and diverse sectoral network typologies. The multi-hazard approach is evaluated with consideration of vertical integration and horizontal coordination of systems of governance illuminating challenges such as tensions in public-private partnerships and risks posed by secondary dependencies. The system evaluation within the framework of an all-hazard approach resulted in illuminating the insignificance the sectoral boundaries provides.

The results led to a conclusion of modifying the current systems of governance toward an adaptive risk governance approach facilitated by an organisational structure prioritised at ministerial level yet crossing all current sectors enabling a coordination horizontally. Furthermore, the Norwegian approach of identifying critical assets, function and services horizontally instead of vertically forces a coordinative initiative among sectors that is appropriate with the recommended measures.

PREFACE

The master study is conducted solely by signatory as the final study to achieve the title of Master of Science in Technology in Risk and Safety Management from the University of Aalborg, placed under the Institute of Civil Engineering in the faculty of Engineering and Science.

With a bachelor's degree in Disaster and risk management, I have been able to use my practical knowledge of the Danish governance system and emergency procedures to identify authorities of the critical information infrastructure system. Based on experience from my current master programme especially from systems engineering and risk management in particular, I have been able to evaluate the characteristics of the system. My natural interest in organizational theories, risk governance and how this is applied has supported my methodological and altered structure in the study. The current literature on governance of critical information infrastructure protection is sparse, and especially in a Danish context it has not been possible to find much research on the topic. Therefore, the methodological approach of the thesis reflects my thoughts which hopefully can provide a multidisciplinary angle that can offer new findings.

The Danish critical information infrastructure system is currently administered and governed in the existing sectors, where each sector has authority to identify critical assets and functions, as well as operators and suppliers. This mapping has not yet occurred, which this study will elucidate further. This, of course, gives rise to a hugely heterogeneous system that is controlled top-down without an organizational cross-coordination. The Danish infrastructure (including critical information infrastructure) is highly interdependent, which means that the division of political authority is merely an artificial measure. The study presents a novel presentation of a multi-scale system identification of the Danish critical information infrastructure.

The information system, cyber and the internet are names for the same phenomenon that today solves everyday tasks, enables fast and efficient communication and automates social functions and services. It is also the same phenomenon that poses one of the greatest threats to society as a whole today. Anyone with access to the internet can acquire skills or pay for an attack on a given target, which means that everyone can become a suspect. Even the smallest and most insignificant items, which in themselves pose a small risk of damage, can cause major damage to other systems due to system dependencies. Attacks in cyberspace are no longer a phenomenon in the future, but something here and now that we must deal with. As a researcher, student, citizen, decision maker, authority or enterprise, we all have a responsibility to pose as little risk as possible to avoid the entire community experiencing a breakdown.

This study is important because it challenges the current social systems of governance and government organization, which are structured according to more traditional approaches that are appropriate at the time when the internet was a minor part of society. Now when the internet is embedded in the majority of the societal functions and services, it may require a radical change in the organisational structure and systems of governance of CIIP. The master thesis intends to push current practice towards a more resilient and adaptable systems of governance.

ABBREVIATIONS

Throughout this report a list of applied abbreviations is presented in each chapter to support the reader in the respective part of this study. The following list contains the acronyms in alphabetical order.

AD	Agency of Digitisation
APT	Advanced Persistent Threats
CERT	Computer Emergency Response Team
CFCS	Centre for Cyber Security
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
DBA	Danish Business Authority
DCIS	Decentralised Cyber Information Security
DEA	Danish Energy Authority
DeiC	Danish e-Infrastructure Cooperation
DEMA	Danish Emergency Management Agency
DESI	Digital Economy and Society Index
DGA	Danish Geodata Agency
DHA	Danish Health Authority
DMA	Danish Maritime Authority
DMI	Danish Meteorological Institute
ECI	European critical infrastructure
ENISA	European Network and Information Security Agency
EPCIP	European Programme for Critical Infrastructure Protection
ERTMS	European Railway Traffic Management System
EU	European Union
FAO	Food and Agriculture Organisation of the United Nations
FE	Danish Defence Intelligence Service
FMK	Common Medicine Card
FSA	Financial Supervisory Authority
FSOR	Financial Sector Forum for Operational Robustness
HDN	Health Data Network
HDPA	Health Data Protection Agency
ICT	Information Communication Technology
IOT	Internet of Things
IPCIS	Insurance-Pension CIS
ISAC	Information Sharing and Analysis Centre
KIH	Clinical Integrated Home Monitoring
MCEU	Ministry of Climate, Energy and Utilities
MCISF	Maritime Cyber and Information Security Forum
MD	Ministry of Defence
MF	Ministry of Finance
MH	Ministry of Health
MIBFA	Ministry of Industry, Business and Financial Affairs
MSDI	Marine Spatial Data Infrastructure
MTBH	Ministry of Transport, Building and Housing
NATO	North Atlantic Treaty Organization
NFCERT	Nordic Financial Computer Emergency Readiness Team
NOST	National Operational Staff

OECD	Organisation for Economic Co-operation and Development
OES	Operators of Essential Services
PET	Danish Security and Intelligence Service
PHA	Preliminary Hazard Analysis
RD	Road Directorate
SES	Single European Sky
SIFI	Systemically Important Financial Institutions
TCHA	Transport, Construction and Housing Agency
UN	United Nations
UNISDR	United Nation Office for Disaster Risk Reduction
UNOPS	United Nation Office for Project Services
WEF	World Economic Forum
WHO	World Health Organisation

LIST OF TABLES

LIST OF FIGURES

Glossary

Agency The agencies are under the jurisdiction of the respective ministry and is tasked with anchoring the ministry's strategic objectives to more operational measures. In this study, the term is referred to as the tactical political level.

Authority Authorities are public organisations that have political or administrative power and control, also including political institutions and state-owned companies.

Hazard A hazard is any phenomenon, substance, human activity or condition that threatens social, economic, health and livelihoods of a population, including environmental damage, adopted by the UNISDR (2017) [1]. Throughout this research this term is referred to as threats synonymously.

IT supplier IT suppliers are referred to as being the companies that provide an IT service or deliver an IT product for company or an authority.

Ministry A ministry is the regulative authority for the respective sector. In this study, the term is referred to as the strategic political level.

Operator The stakeholders that are identified as to be responsible for critical infrastructure assets, functions and services at operational level are referred to as operators.

TABLE OF CONTENTS

1 Introduction

Abbreviations

APT	Advanced persistent threats
CERT	Computer Emergency Response Team
CFCS	Centre for Cyber Security
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
DEMA	Danish Emergency Management Agency
ENISA	European Network and Information Security Agency
EPCIP	European Programme for Critical Infrastructure Protection
EU	European Union
FE	Military Defence Intelligence Service
ICT	Information Communication Technology
MD	Ministry of Defence
MF	Danish Ministry of Finance
NOST	National Operational Staff
OES	Operators of Essential Services
PET	Danish security and intelligence service
PHA	Preliminary Hazard Analysis
UNISDR	United Nation Office for Disaster Risk Reduction

The principle of sector responsibility is highly maintained in Denmark. This means that each societal sector e.g. transportation is responsible to mitigate, prepare, respond and recover from a given incident. The authority of each sector is a ministry, which has regulatory authority of the given sector. The principle of sector responsibility gives rise to a silo-based approach that is challenging in a complex environment of information security that naturally disregards vertical decision-making structures.

Denmark is in the top five most digitised countries in the EU based on connectivity, internet capacities, integration of digital technologies in the private and public sector according to the EU Digital Economy and Society Index (DESI) 2019 [2]. Critical information infrastructure (CII) systems are becoming more interconnected with the implementation of online services and information communication technology (ICT) systems in the vast majority of all public and private sectors.

With the increase of critical infrastructure interdependencies follows an increase in the threat of cascading failures and how noncritical systems pose a risk of disturbing most vital systems. If cascading effects are to happen, the failures would be difficult to manage when considering the decision makers representing multiple sectors. Further, the recovery time would be extended and challenging with consideration of the interdependencies. Another issue is the tension in public-private collaboration that might occur when preferences and objectives differ, due to a lack of common reference to what constitutes the Danish CII and how resources should be allocated.

Governance of CIIP is a cross-sectoral discipline that may be challenging if the hierarchy of decision-making is kept as demarcated silos. The master thesis is a desktop study aiming to identify the Danish CIIP and mapping issues concerning systems of governance regarding CII security policies and structures.

1.1 Danish Critical Information Infrastructure Protection

Critical infrastructure can be classified according to functions and services that the system provides to society. Rehak and Hromada (2018) address this by dividing infrastructure in technical and socioeconomic levels, where both include functions and services [3]. The technical level includes production and provision of specific commodities, whereas the socioeconomic level constitutes social or economic services e.g. healthcare, finance, emergency and public administration.

The criticality in a given system is usually perceived with a systemic view and characterised due to the strategic place in the system of infrastructure, and especially due to its interdependencies [4]. Metzger (2004) distinguishes between systemic and symbolic perception of the concept of criticality, where the symbolic view relates to the inherent role in society and the symbolic criticality is a national power symbol [5]. CII is a highly interlinked system of functions, services, assets, social systems etc. which are interdependent in a national context, yet also in an international context. The EU serves an important role to make sure that EU states follow a general denominator of an agreement. According to the NIS Directive (2016), all EU states must identify their national CII as well as CII operators [6].

1.1.1 Inconsistency at Political Level

Critical infrastructure differs from regular infrastructure as being the absolute vital systems and processes necessary for a society to function and provide citizens' welfare. In case of a disruption, the critical infrastructure would cause the society to be heavily disrupted [7]. EU defines CII as assets or systems that are crucial for maintaining vital societal functions, such as health, safety, security, economic and social well-being of the population [6]. The EU Commission launched in 2006 the European Programme for Critical Infrastructure Protection (EPCIP) to reduce the vulnerabilities among EU states, which included methods aimed to improve CIIP [8]. The strategy led to the development of the NIS Directive 2016/1148, requiring all EU states among else to define the national CII and conduct a national CII strategy [6].

The identification of the Danish CII appears to be inconsistent. The Danish Security and Intelligence Service (PET), Ministry of Finance (MF) and Danish Emergency Management Agency (DEMA) have distinctive proposals on what the CII consists of. The inconsistency at political level between the police, DEMA and FM may be an expression of different perspectives on how to allocate resources according to what is prioritised as critical. The information from PET and DEMA is still available on their websites despite the fact that MF has released the national cyber information strategy in 2018.

The EU Commission (2008) recommends the EU states to recognise specific cross-national CII sectors such as electricity, oil and gas, road transport, rail transport, air transport, inland waterways, ports, ocean and short-sea shipping [9]. It appears that Denmark only recognises a few of the recommended sectors (Table 1).

Table 1: Classification of critical infrastructure

PET identifies five sectors:	**DEMA identifies 12 sectors (2013):**	**EU identifies 11 sectors (2015):**
Energy	Energy	Energy
IT and telecommunications	ICT	ICT
Transportation	Transportation	Water
Food	Water	Food
Healthcare	Food	Health
	Finance	Financial
MF identifies six sectors (2018):	Rescue services	Public & Legal Order and Safety
Energy	Police duties	Civil Administration
Telecommunications	Defence assistance to civilian authorities	Transport
Transportation	Health and social care	Chemical and Nuclear Industry
Maritime	Defence, intelligence and security service	Space and Research
Finance	Exercise of authority at all levels	
Healthcare		

ENISA recommends the EU states to follow a certain methodological guide published by ENISA (2015) to support the process of identifying CII assets and services. ENISA identifies 11 sectors [10]. The critical sectors identified by DEMA (2013) share similarities with ENISA (2015); however, the National Cyber Strategy (2018), published by the Danish Government, identifies six critical sectors [11]. This definition is the only interpretation authored by a ministry and published by the government; hence this is considered the official Danish CII.

Norway has an alternative approach where the Norwegian Government identifies their CII by 14 sectors based on governance and sovereignty, population safety and societal functionality [12]. The Norwegian critical infrastructure does not follow the political vertical structures which forces all the ministries to coordinate across to govern the respective CIIP.

1.1.2 Danish Cyber Security Policy Development

In 2014 the Danish Government published its first cyber information strategy. It identified the main challenges and initiative strategies to form necessary institutions in military and police context to address cyber threats. In the same year the governmental computer emergency response team (GovCERT) (established in 2009) and the military CERT (MILCERT) (established in 2010) was merged into the Network Security Service, which allows CFCS (established in 2012) to monitor online activities for Danish CII operators. Denmark has a separate defence strategy apart from the cyber strategy, which is not necessarily common among EU states [13]. The Defence Agreement of 2004 was published by the Ministry of Defence and ever since, the lead governmental publisher has been the Danish Government. With the new Defence Agreement 2018-2023, the government raised the appropriation for cyber security with about 20% compared to the last settlement, corresponding to approximately DKK 800 million. There has been an increased focus on CIIP, resulting in an investment of DKK 1.4 billion to enhance CIIP [14].

As the first government in Europe in 2001, Denmark released an eGovernment strategy aiming to digitise the Danish society. In 2018, Denmark was named the world's best-digitized country by the UN [15]. There are more than 4000 different IT systems in the central government, and just as many IT systems in the local and regional governments, many of which do not operate according to the same standards and protocols. The Danish society is highly digitised and largely depends on IT systems and internet-based solutions. The current Digitization Strategy 2016-2020 encompasses that all IT systems must have a common programme language, management and standards for better implementation. The board responsible for this implementation is the Joint Public Digital

Architecture. The project uses standards developed by the European unit, the European Interoperability Framework, which is subject to the Interoperability Solution for public Administration businesses and citizens to ensure data sharing across sectors [16]. Data-sharing in the EU may be possible if common standards and protocols are implemented across EU states.

In 2004 ENISA was formed. Almost a decade later in 2013, the EU Commission published their first Cyber Strategy, of which ENISA was to ensure implementation. In the year of 2016 the European cyber strategy of 2013 was renewed and published, setting the direction of a unified and high-level security across EU states. In addition, two important regulations are published this year, namely the EU directive 2016/1148 - Security of Network and Information Systems (NIS directive) and the EU regulation 2016/679 - General Data Protection Regulation (GDPR).

In the wake of the EU NIS directive, the Danish Government published the Danish Cyber and Information Security Strategy in 2018 [11]. In the report, CFCS defines a coordinated strategy though lacking operational guidance or responsibility regarding the whole system. The strategy highlights collaboration as one of the key objectives, and still the operational support is divided into political silos in which the responsible authorities are prohibited to conduct their own cyber strategy.

1.1.3 National Risk Assessment Methodology

The methodology of the risk assessment used by Danish ministries, agencies and public operators is developed by the Danish Emergency Management Agency (2005) [17]. The method is based on a qualitative preliminary hazard analysis (PHA). According to DEMA, the applied method is characterised by an *all-hazard approach* accounting for all types of threats. By promoting a combination of a traditional risk management approach covering probabilities and consequences with an approach to strengthen resilience, DEMA relates resilience to the concept of continuity planning. According to the ISO Standard 31010 (2010), the PHA requires little specialised knowledge and can be applied in various contexts. However, there is a high level of uncertainty related to this method, and with no quantitative outputs. The method relies on the expertise, experience and knowledge within the team. PHA is characterised as a so-called look-up method, that does not provide detailed information about certain risks and preventive measures. ISO31010 states that a risk assessment should aim to provide evidence-based information in order to make informed decisions on how to handle the risk. The PHA is not on its own adequate to provide evidence-based information, hence institutions should use other risk methods as support. PHA is a risk identification and estimation method that results in a prioritisation of choice and countermeasures most often presented in a matrix [18].

1.2 Objectives of the Thesis

The increased political interest in information systems and critical infrastructure is to be seen in the light of the emerging technological developments that increase the threat of an accumulative breakdown of critical infrastructure, making this study highly relevant. The aim of the thesis is to provide decision makers with a mapping over the Danish critical information infrastructure protection (CIIP) systems of governance and relating challenges as to support risk-informed decisions.

There are no agreed definition nor designation on what constitutes critical information infrastructure (CII) in Denmark; though the Danish Government has published a strategy

constituting six sectors. Another issue discovered, is the non-transparent structure of responsibilities over which public and private entities have operational, tactical and regulative authority in relation to CIIP. This leads to the need for this study, in which I will:

- Identify all the operators at strategic, operational and tactical level
- Develop a system representation of the operators and their relations, mapping information flows and interdependencies
- Review current best practices in the governance frameworks, methodologies and regulatory mechanisms in the Danish context
- Compare alternative governance frameworks such as single-hazard, multi-hazard and all-hazard approaches and evaluate which approaches is best fitted for the Danish context.

Due to lack of mapping of the Danish CIIP, operators, decision makers and practitioners this study aims to fill a knowledge gap with a novel framework of CIIP governance. In addition, this research establishes a systematic, consistent and transparent basis for planning and preparedness for hazards related to CII.

1.3 Thesis Outline

The thesis outline intends to guide the reader along the creation of the master thesis. The thesis outline follows the structure illustrated in Figure 1.

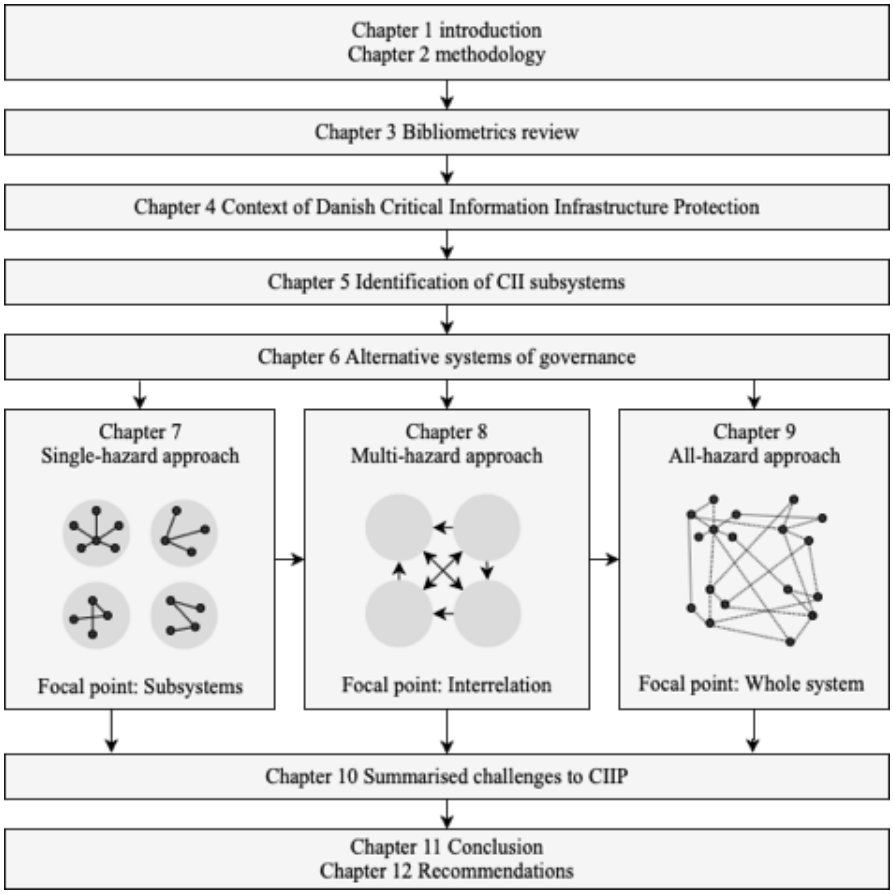

Figure 1: Illustration of the thesis outline

Chapter 1 is an introduction to the problem context that provides an overall framework of reference of how current practice of Danish CIIP is. It discusses some of the inconsistencies that appear to be within the current practice and how these in relation to the current CIIP policies may be challenging. Finally, the chapter presents the objectives of the thesis.

Chapter 2 introduces the methodological approach that is adopted throughout this research.

Chapter 3 provides a novel insight of current literature studies on the Danish CII system including the alternative systems of governance. A bibliometric review is performed on the two fundamental parts that define this study – the *physical system* (i) and the *system of governance* (ii): (i) a comparison of critical infrastructure with critical information infrastructure; and (ii) evaluation of the single-hazard, multi-hazard and all-hazard approaches. Furthermore, the review gives an indication of what focal point the current literature has which modestly indicate the preferred governance approach.

Chapter 4 analyses the current practice of CIIP with emphasising certain essential elements that constitute the Danish Government and Society. Whereas Chapter 5 identifies the CII subsystem' information flow, components, operators and authorities.

Chapter 6 discusses best practice of identifying and classifying CII hazards as well as examining three alternative governance approaches, that each constitutes the structure for the following three chapters.

In Chapter 7, 8 and 9 the system of CIIP is discussed within the context of respective governance approaches. The single-hazard approach is the framework for Chapter 7, where the system of CIIP

is characterised by non-related subsystems and a comparison of all. Chapter 8 represented the multi-hazard approach, by which the interrelation among the subsystems is evaluated horizontally and vertically. The all-hazard approach is considered in Chapter 9, where the subsystems are ignored, and interdependencies of the components are evaluated including a consideration of non-critical interdependencies. Each of the chapters illuminates and discusses the challenges relating to the respective systems of governance, by which Chapter 10 presents a summarised comparison of the three approaches.

Chapter 11 and 12 include the conclusion and recommendations.

2 Methodology

The current chapter presents an introduction and reflection of the methods used to examine the research problem.

Initial, the bibliometric review provides an insight in search trends and scientific research productivity of grey and peer-reviewed literature on critical information infrastructure and governance approaches. The bibliometric analysis is a statistical analysis with a focus on the quantitative analysis of citations and citation counts. Due to the novelty of the scope, the peer-reviewed literature is rather sparse and therefore it requires an insight in the grey literature that the citation database Scopus provides. In comparison with other databases such as Web of Science, where the majority of publications are peer-reviewed, Scopus covers publication from both peer-reviewed and grey literature. In order to identify patterns of keyword co-occurrence, the software VOSviewer is used as a network visualisation tool to construct term maps. The bibliometric analysis with emphasis patterns within keyword co-occurrence, is a way to review current practices and compare governance approaches, including the results as a support to develop a system representation of the critical information infrastructure protection (CIIP).

The identification of operators and authorities is done as a desktop study examining various peer-reviewed publications, grey literature and online articles. The system representation is conducted within the concept of single-hazard, multi-hazard and all-hazard approaches (Figure 2), where the results from the previous system characterisation is included, as well as used in the overall conclusion, illustrated in the figure.

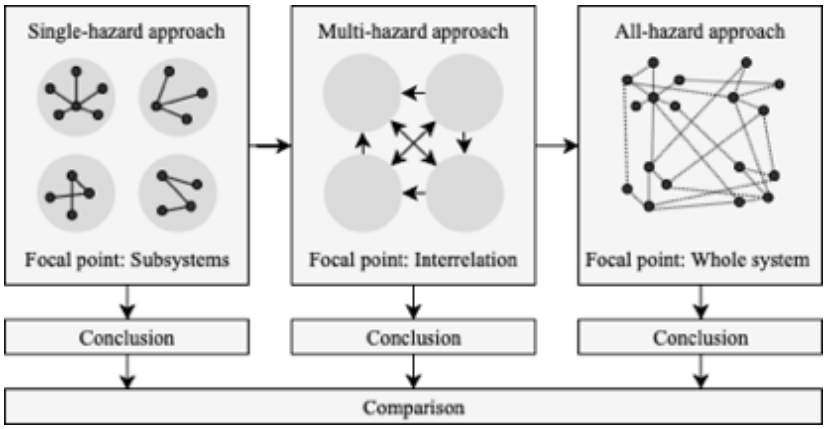

Figure 2: Methodology of the multiscale system representation

Within the concept of multi-scale governance, the system is characterised by following an inductive logical synthesis of examining the vertical integration relating to the dispersion of political authorities and the horizontal coordination relating to among else public-private-partnerships. Based on the three governance approaches, all strategic, tactical and operational operators are identified. In addition, the study develops a mapping of information flow and interdependencies within the framework of CIIP. Finally, the method allows for a comparison of the three governance approaches to evaluate the most suitable approach for the pragmatic application within the Danish context.

3 Bibliometric Literature Review

Abbreviations
CI Critical Infrastructure
CII Critical Information Infrastructure

A bibliometric technique is a numerical text mining procedure that facilitates an identification of certain research areas by evaluating certain patterns. In the current review, grey and peer-reviewed literature form the basis for a keyword co-occurrence network and bibliographic coupling, that is visualised and evaluated. The two research areas cover: (i) Critical information infrastructure (CII) system; and (ii) Alternative systems of governance.

Scopus only allows a view of and export up to 2000 records for which in the case of CII, the result covers more than 2000 records. Hence, the 2000 highest cited records are extracted to include in the network visualisation software VOSviewer.

The aim of the bibliometric review is to identify where the current study fits in the state-of-the-art literature up until this date and in which research disciplines CII is present. The first part of the bibliometric review presents how CII distinguish from critical infrastructure (CI). The second part presents three alternative types of governance approaches: (i) Single-hazard; (ii) Multi-hazards; and (iii) All-hazards, where similarities and variances differentiate the alternatives.

The cluster analysis includes visualised keyword co-occurrence networks referred to as term maps, representing the two domains. These networks provide a multi-disciplinary pattern of keyword co-occurrence illustrating clusters and link strengths. Surely, the interpretation of such visualisations is strongly subjective; however, the method is believed to provide an overview and a brief screening of most common keywords that are used in current literature for each domain.

The bibliometric review follows a step-by-step process based on various assumptions, in which the relating data report supports a verification of the review (Appendix).

3.1 Critical Information Infrastructure Review

The historical evolution of research in the domain of critical information infrastructure (CII) can be traced back to 1985. Critical infrastructure (CI) also emerged at that time (1984-2020) (Figure 3). Both domains show an upward trend until present time, although the number of records on CII (4000+ records) constitute roughly half of the number of records on CI (9000+ records).

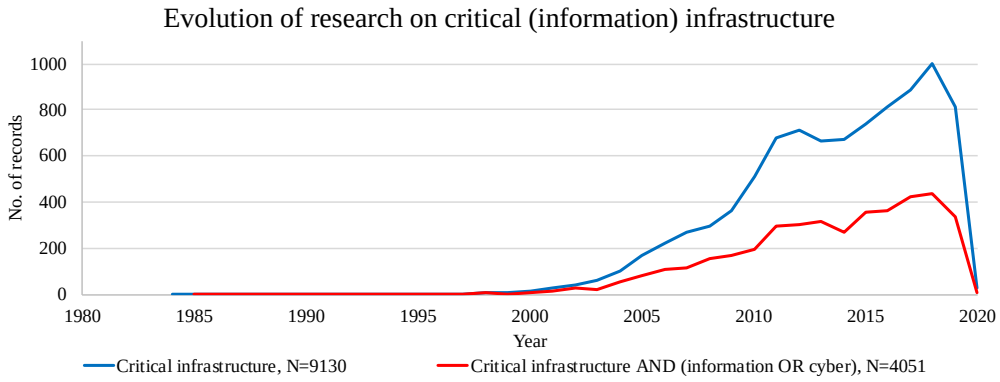

Figure 3: Historical evolution of annually record count on CI and CII.

There appears to be similarities within the top 10 keywords (Table 2), though sorted in different orders.

Table 2: Top 10 keywords and top 5 subject areas

Critical infrastructure, N=9130				**Critical information infrastructure, N=4051**			
TOP 10 keywords		**TOP 5 Subject area**		**TOP 10 keywords**		**TOP 5 Subject area**	
Critical Infrastructures	3647	Engineering	4462	Critical Infrastructures	1667	Computer science	2241
Public Works	2260	Computer Science	4306	Public Works	1091	Engineering	1819
Critical Infrastructure	1305	Mathematics	1407	Network Security	649	Mathematics	674
Network Security	962	Social Sciences	1264	Critical Infrastructure	564	Decision	539
Risk Assessment	887	Decision Sciences	772	Cyber Security	543	Social science	505
Critical Infrastructure Protection	641			Computer Crime	524		
Security Of Data	615			Security Of Data	496		
Computer Crime	591			Risk Assessment	371		
Cyber Security	549			Critical Infrastructure Protection	347		
Risk Management	492			Embedded Systems	335		

The top five subject areas (terminology adopted from Scopus) show the top five research disciplines for CI and CII (Table 2). Computer science and engineering have switched places, and the same applies for social sciences and decision sciences. The order of dominating research disciplines in CII indicates the attention towards information systems that CII logically has. For both CI and CII, the engineering and computer science are the most dominating disciplines.

3.1.1 Cluster Analysis

Figure 4 shows a visualisation of the domain of CI based on 123 terms occurring with a minimum of three terms per cluster, and with a minimum of 25 occurrences per term, showing three clusters.

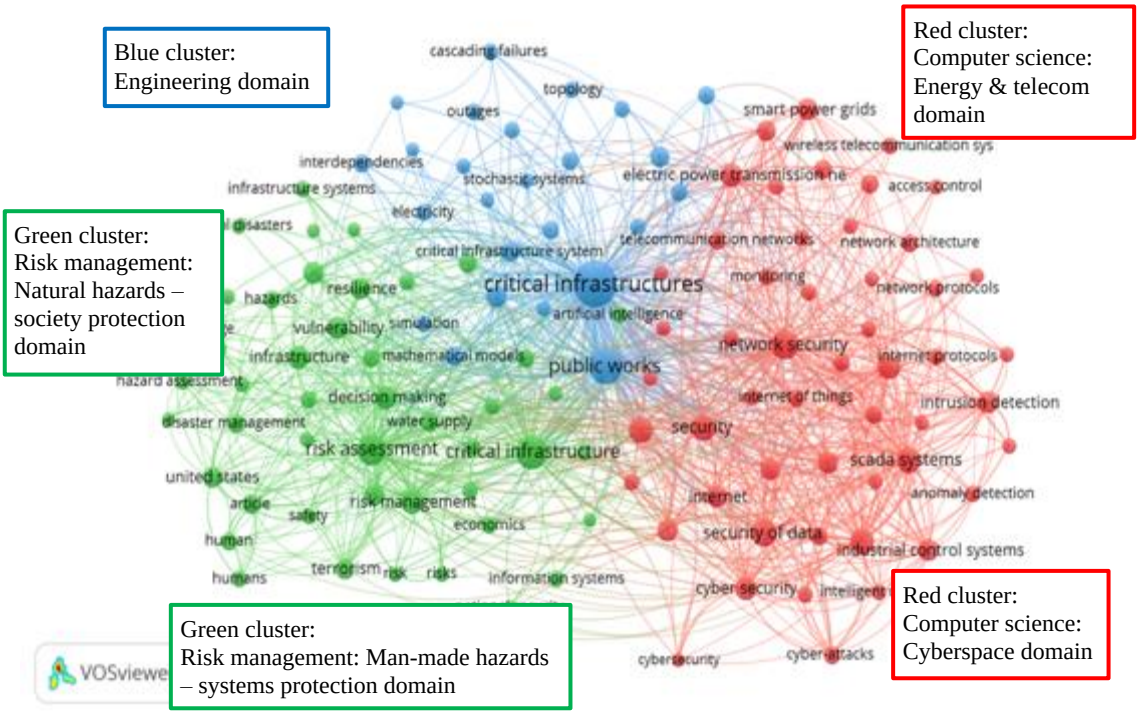

Figure 4: Network map on research on CI, N=2000 records

The largest cluster in CI network (Figure 4) is the red cluster identified in two parts: (i) The energy and telecom terms are dominating the top of the red cluster and connected with the blue cluster identified as the engineering domain; and (ii) The bottom of the red cluster is identified as the cyberspace domain and is represented by terms like *cyber-attacks*, *SCADA systems*, *intrusion detection*, *internet protocols* etc. The red cluster is assumed to belong to the discipline of computer science. The green cluster is identified as the risk management domain, where the upper part is more concerned with natural hazards and society protection, whereas the lower part is concerned with manmade hazards and systems protection. The blue cluster contains the two most occurrent keywords: *critical infrastructures* and *public works*, though the blue represents the smallest cluster in the network.

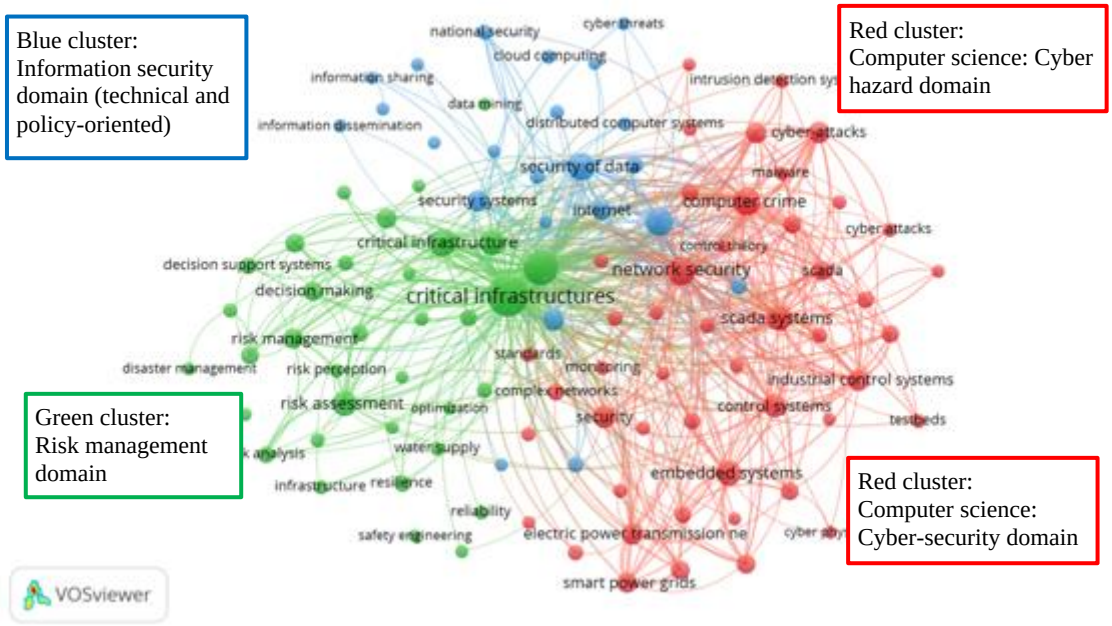

Figure 5: Network map on research on CII, N=2000 records

Keyword co-occurrence of the critical information infrastructure (CII) is visualised based on 106 keywords occurring with a minimum of four per cluster, and with a minimum of 30 occurrences per term, showing three clusters (Figure 5). The network map is created on the 2000 most highly cited records on CII extracted from Scopus.

The red cluster represents the largest group, identified as the domain of computer science, though divided in two. The lower part being the cybersecurity domain is identified by terms like *embedded systems, testbeds, security, control systems, monitoring* etc. The top red cluster represents cyber hazards with terms like *cyber-attacks, computer crime, control theory, malware, intrusion detection systems* etc. The green cluster is dominated by risk management by terms like *decision making, risk analysis, resilience, disaster management safety engineering* etc. where it is most-likely dominated by quantitative methods. The blue cluster is identified as the information security domain with terms of a more technical tradition like *cyber security, security of data, internet, information dissemination* etc. The blue cluster also includes terms like *national security* and *information sharing* which may relate to the policy part of information security.

3.1.1.1 Conclusion

Based on the identified clusters in the network maps of CI and CII the following summaries the observations.

CI is focused on:

- Natural hazards and man-made hazards (green cluster)
- Engineering with emphasis on interdependencies and cascading failures (blue cluster)
- Computer science mainly on cyberspace and energy and telecom industries (red cluster)

CII is focused on

- Risk management with mainly quantitative assessments (green cluster)
- Information security represented by both technical and policy-related terms (blue cluster)

- Computer science divided in cyber security and cyber hazards (red cluster)

The *natural hazards* (green cluster, Figure 4) in CI are excluded in the network map of CII, which includes terms like *natural disaster, humans, terrorism, climate change, uncertainty, earthquake, flooding etc.* This also applies to the focus on interdependencies represented by the *engineering domain* (blue cluster, Figure 4), represented by terms like *information sharing, cloud computing* and *security of data*.

Instead, the *computer science* terminologies (red cluster, Figure 4) from CI is expanded into two groups in the network of CII represented by the blue and red cluster in Figure 5: *Cyber-related hazards* (red cluster, Figure 5); and *policy-oriented protection* (blue cluster, Figure 5). In addition to CII, there is a separate group of keywords present, relating to the application of cyber-related hazards, namely the risk management/policies (green cluster, Figure 5).

It appears there is less attention on interdependencies and cascading effects within the domain of CII, as these aspects are not present in the keywords co-occurrence analysis of CII. Additionally, the search on CII exclude all of non-cyber-related hazards. When splitting CI into CII, the majority of natural and manmade hazard non-related to cyber or information disappeared. The conclusion is that the overall focus within CII informational hazards originates from cyberspace and information and excludes hazards such as natural or manmade i.e. terrorism unless it is related to cyber. Apart from this, it is not prevalent in CII research to investigate possible relationships and dependencies in the information infrastructure as it appears to be in CI.

3.2 Alternative Systems of Governance Review

The historical evolution of the three governance approaches (Figure 6) shows that the all-hazard approach (951 records) is the first one published in 1957, whereas publications on single-hazard (159 records) and multi-hazards (1016 records) began in the 1980s. Research on the all-hazard approach experienced a few yet constant annual publications from roughly 1970 to 2000. In the early 2000, the number of publications on all-hazards drastically increased; however, the contribution is within the range of 50-70 records annually up until present. Both the single-hazard and multi-hazard approach are introduced in literature in the early 1980s.

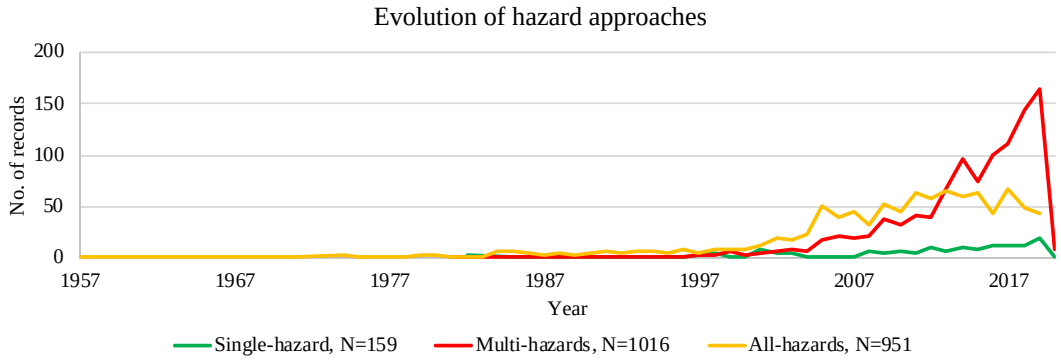

Figure 6: Historical evolution of annually publications on alternative hazard approaches

The keywords for the single-hazard and multi-hazard domains are relatively similar, with the exception of earthquakes, disasters, floods, article, multi-hazards and human(-s). This could indicate that a multi-hazard approach relates to the vast research mostly concerned with natural

hazards. Both research areas are dominated by the disciplines of engineering, earth and planetary science and environmental science (Table 4).

Table 3: Top 10 keywords for research on single-hazard, multi-hazards and all-hazards

	TOP 10 keywords					
Rank	**Single-hazard, N=159**		**Multi-hazards, N=1016**		**All-hazards, N=951**	
1	Risk Assessment	55	Hazards	459	Human	277
2	Hazards	53	Risk Assessment	290	Humans	229
3	Article	25	Earthquakes	198	Article	209
4	Human	24	Multi-hazards	157	Hazards	158
5	Hazard Assessment	23	Hazard Assessment	139	Risk Assessment	149
6	Natural Hazard	17	Disasters	121	Disaster Planning	146
7	Priority Journal	15	Floods	115	United States	131
8	Risk Management	15	Multi-hazard	102	All-hazards	98
9	Humans	13	Risk Management	94	Organization And Management	93
10	Vulnerability	13	Vulnerability	94	Disasters	79

Table 4: Top 5 subject areas for research on single-hazard, multi-hazards and all-hazards

	TOP 5 Subject area					
Rank	**Single-hazard, N=159**		**Multi-hazards, N=1016**		**All-hazards, N=951**	
1	Engineering	62	Engineering	560	Medicine	343
2	Earth and Planetary Sciences	39	Earth and Planetary Sciences	335	Engineering	323
3	Environmental Science	39	Environmental Science	221	Social Sciences	187
4	Social Sciences	27	Social Sciences	171	Environmental Science	139
5	Medicine	25	Computer Science	86	Earth and Planetary Sciences	79

The single-hazard and all-hazard approaches share similarities in top 10 keywords. The main difference is that the term *human(-s)* is ranked as the highest occurrent keyword in the all-hazard domain, which is obvious since medicine is the dominating research domain.

3.2.1 Cluster Analysis

The following network maps are created by importing the total number of records from Scopus in VOSviewer in which a visualisation of each search domain counting keyword occurrence and links generate clusters. Figure 7 shows a visualisation of the single-hazard approach based on 55 terms appearing with a minimum of five terms per cluster, and a minimum of five occurrences per term, visualising three clusters.

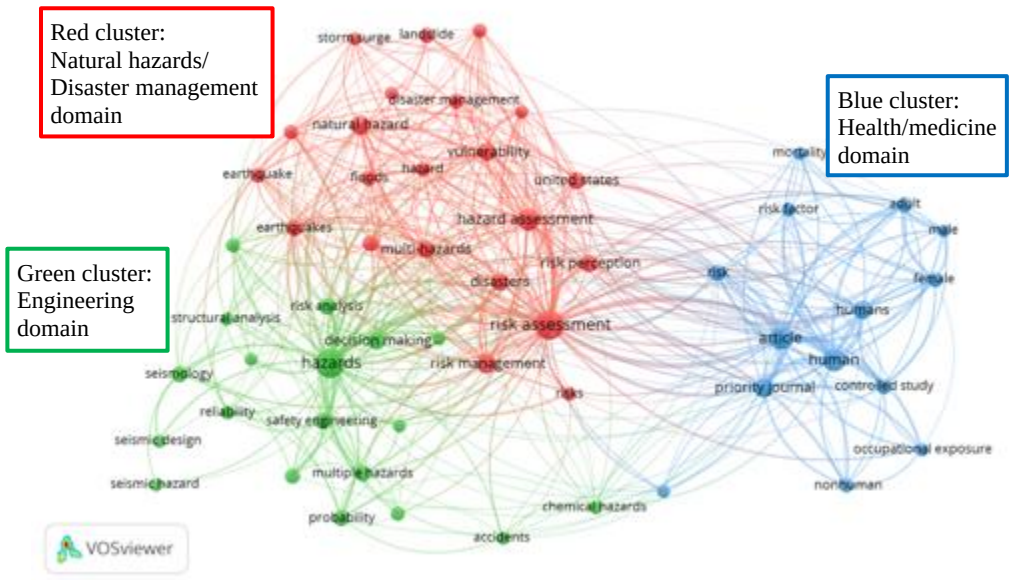

Figure 7: Network map of research on single-hazard extracted from Scopus, N=159

The red cluster is the largest with 22 linked terms such as *risk assessment, hazard assessment, risk perception, vulnerability, floods, earthquakes* etc. The cluster is interpreted to represent the natural hazard domain dominated by disaster management most-likely represented by mainly qualitative assessments with a high occurrence of isolated types of hazards. The green cluster is related to the red cluster and is defined as the engineering cluster with terms such as *decision making, probability, structural analysis, safety engineering* etc. The blue cluster is isolated from the two, and defined as the health domain with a concentration of individual healthcare terms within the discipline of medicine represented by terms such as *human, female, occupational exposure, risk factor* etc.

The visualisation of the multi-hazard domain (Figure 8) is based on 66 terms occurring with a minimum of six terms per cluster, and a minimum of 25 occurrences per term, visualising two clusters of equal size. The red cluster represents the domain of natural hazards and technological hazards (so-called natech) with terms such as *earthquakes, seismology, bridges, concretes, scour* etc. Whereas, the green cluster is defined as the natural hazard domain with an emphasis on disaster management represented by terms like storms, disaster prevention, hurricanes, disasters, climate change etc. The two clusters are connected by the centralised terms: *hazards, resilience, multiple hazards, probability* and *risk*, which is interpreted as the multi-hazard approach is unified around natural hazards assessed quantitatively, where one part of the domain (red) is focused on natech hazards and the other part (green) on natural hazards.

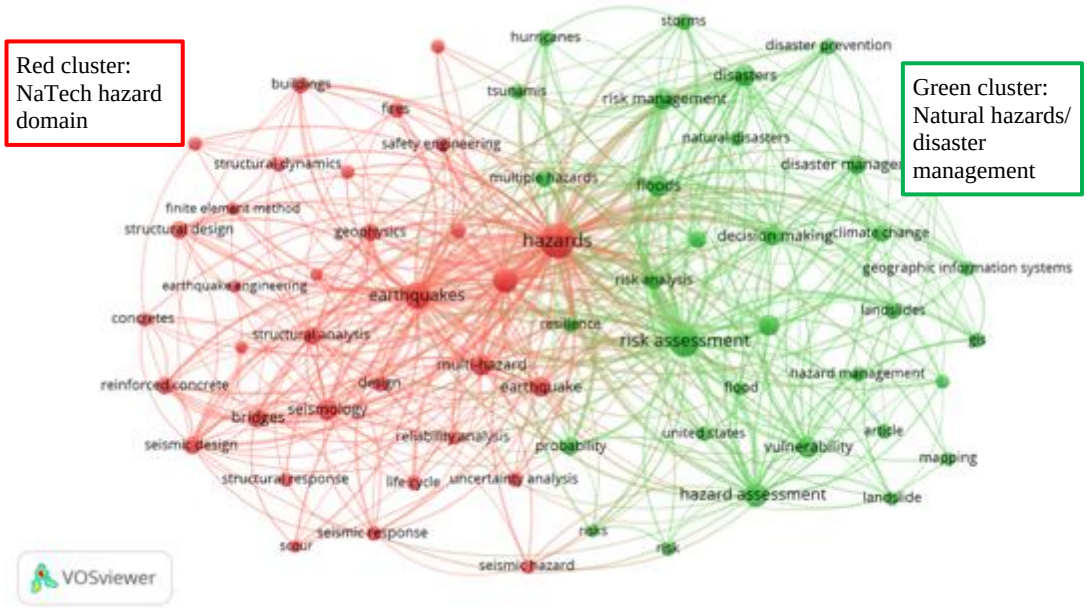

Figure 8: Network map of research on multi-hazards extracted from Scopus, N=1016

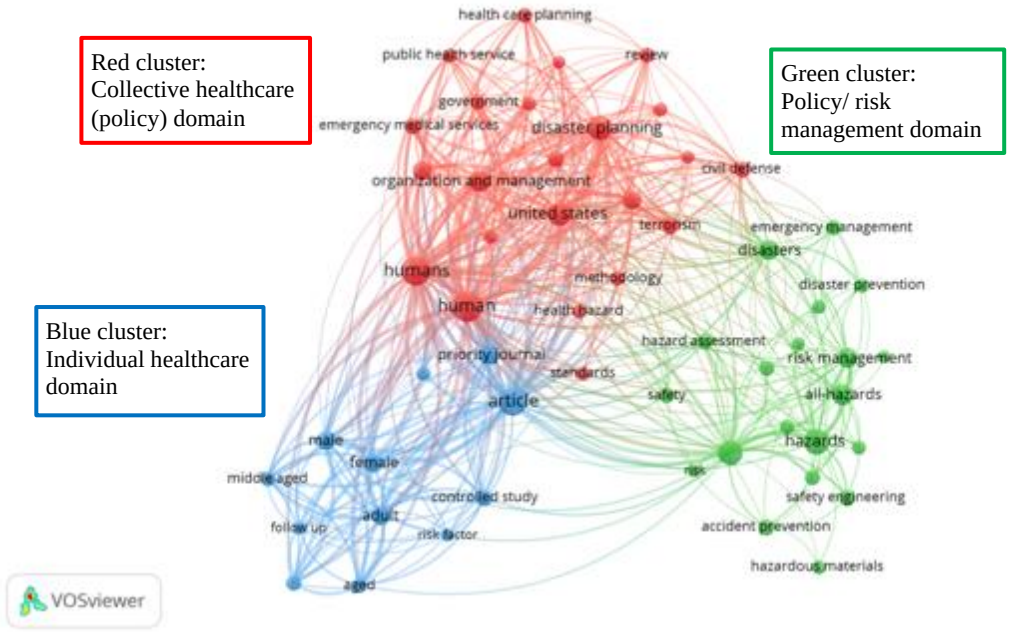

Figure 9: Network map of research on all-hazards extracted from Scopus, N=951

The research on the all-hazard approach is visualised in Figure 9 and based on 55 terms occurring with a minimum of six terms per cluster, and a minimum of 20 occurrences per term, visualising three clusters. The network is roughly divided in two dimensions: (i) Divided by domain topics; and (ii) Divided by keyword link strength. The domain division is visualised as the red and blue cluster both represent the healthcare domain, where the red cluster is more concerned with collective health, and the blue is more concerned with individual health.

The second type of division is made by the link strength, where it seems to be a closer connection between the red and the green cluster. The green cluster is defined as the policy/risk management domain, whereas the red is concerned with collective healthcare; however, the keywords in the red

cluster are government-oriented, which interrelate with the terms in the green domain. The all-hazard domain has a policy-oriented focus on hazards in general and a special focus on health-related hazards which is specified in collective and individual risks.

3.2.1.1 Conclusion

Based on the identified network maps of the governance alternatives, the following summaries the observations.

Single-hazard approach

- Natural hazard domain (red cluster)
- Engineering domain (green cluster)
- Health/medicine domain (blue cluster)

Multi-hazard approach

- Natech hazards domain (red cluster)
- Natural hazards domain (green cluster)

All-hazard approach

- Collective healthcare domain (red cluster)
- Individual healthcare domain (blue cluster)
- Policy risk management domain (blue cluster)

The *healthcare* group is strongly represented in the single-hazard and the all-hazard approaches, whereas it is excluded in the multi-hazard approach. While the single-hazard separates *natural hazards* (red cluster) and *engineering* (green cluster, Figure 7), the multi-hazards unite the two in one cluster defined as *Natech hazards* (red cluster) and further remains a *natural hazard* cluster (green cluster, Figure 8). In the all-hazard network, the *natural hazards* are merely a margin represented as a part of policy/risk management (blue cluster, Figure 9). Surprisingly, the single-hazard resembles all-hazards with similarities in keywords and clusters, where both are dominated by healthcare research.

The single-hazard approach is commonly recognised by organisations, individuals and nations as a traditional way to manage hazards. According to UNISDR (2017), the concept of single-hazard is used as an intuitive best practice [1]. The search result for *single-hazards* showed only a margin of publications compared to the two governance approaches. It may have to do with the choice of search terms, or it has to do with the fact that it did not become an interesting subject before the early 1980s, with the introduction of multi-hazard methods. There appears to be no general method of what constitutes the single-hazard approach in the current literature.

3.3 Summary of Reviews

The first part of the bibliometric review focused on the comparison of critical information infrastructure (CII) and critical infrastructure (CI). Literature on CI (1984-2020) resulted in 9000+ records, where the most dominating areas within the literature is interpreted as natural/manmade hazards, engineering with emphasis on dependencies and cascading effects, and computer science with a focus on cyber, energy and telecom. The review on CII (1985-2020) revealed a result on 4000+ records, where clustered areas are identified as quantitative risk management, technical and policy-oriented information security, and computer science.

In conclusion, the research on CII is mostly concerned with hazards originating from the information and cyber realm, whereas research on CI is also focused on natural and manmade hazards. In addition, the two research areas differ greatly in terms of relating to interdependencies, interrelations and cumulative effects are noticeable in the literature of CI, though it is not found in the review of CII. It appears that the CII research is dominated by quantitative methods, mostly concerned with the technical aspects of cyber security and only a marginal of the policy part. Furthermore, the hazards that are of interest in most of the literature originates from cyber systems without a particular focus on systems interdependencies.

With regards to the review on alternative governance approaches, the approach that has the longest history is all-hazards (1957-2020), whereas the concepts of single-hazard (1982-2019) and multi-hazards (1981-2020) had a later start in the early 1980s. This is surprising, as it would seem that the single-approach is a more traditional way to assess risks, which still may be the case. However, it might have to do with the fact that research on the topic has probably not been engaged until multi-hazards became popular. The overall conclusion of the review on governance approaches is that the literature on single-hazard is focused on natural and (individual) health hazards with a contribution of quantitative methods mainly from the discipline of engineering. Whereas the multi-hazard approach focuses on natural hazards and the natural hazards affecting industrial systems (so-called Natech hazards). Both governance alternatives appear to be mostly concerned with the types of hazards typically classified as natural hazards, where the main difference lies in the multi-approach embrace the interaction among hazards, where the single-hazard approach is focused on isolated hazards. The all-hazard approach resembles single-hazards in relation to their common attention toward (individual) healthcare hazards, where all-hazards also contributes with a focus on collective healthcare hazards. In addition, the all-hazard approach distinguish itself from the others by being the only approach comprising policy-related risk management, which may be related to a whole-of system practise at governmental level. None of the governance approaches appear to capture all possible societal hazards. In each governance approach there seems to be few dominating hazards such as the multi-hazards are mostly concerned with natech hazards, single and all-hazards are mostly concerned with health hazards. With consideration of the critical information infrastructure, the dominating hazards are cyber-related.

The information flow in the critical infrastructure system of (inter-)dependencies, and the fact that only a little or even any of the current publications are addressing this issue only emphasises the novelty of the scope of the master thesis. When searching for critical information infrastructure in relation to one of the three alternative systems of governance, no similar study has been found, which makes this research highly valuable but also methodological immature. Consequently, it is necessary to embrace all three governance approaches within this study and by this, illuminating the advantages and disadvantages of implementing one over the other in the protection of critical information infrastructure.

4 Context of Critical Information Infrastructure Protection

Abbreviations

APT	Advanced persistent threats
CERT	Computer Emergency Response Team
CFCS	Centre for Cyber Security
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
DEMA	Danish Emergency Management Agency
ENISA	European Network and Information Security Agency
EU	European Union
FE	Military Defence Intelligence Service
ICT	Information Communication Technology
MD	Ministry of Defence
NOST	National Operational Staff
OES	Operators of Essential Services
PET	Danish Security and Intelligence Service

The chapter introduces the context of Danish critical information infrastructure protection (CIIP), by examining the overall framework of governance, the procedural context of cyber incidents and the organisational structure for decision making. With an evaluation of the sectoral responsibility principle and the procedural framework of cyber emergency, it is possible to analyse the multilevel decision making that characterises the Danish systems of CIIP governance. The purpose of this chapter is to provide the reader with an understanding of the Danish societal context in which the governance of CIIP is integrated.

4.1 Sector Responsibility Principle

In the National cyber information strategy (2018), the Ministry of Finance defines the roles and responsibilities of cyber management across critical information infrastructure (CII) sectors for which general preparedness principles, including the sector responsibility principle, is underlined as the founding principle of the strategy. The principle comprehends the responsibility of the ministries if an emergency is to occur. If a cyber disruption affects a private or public company, the same company is responsible to manage the disruption. However, in the context of cyber incidents, it is up to the affected organisation to assess the severity of the event and decide when to contact authorities. Every company no matter their criticality to societal infrastructure decide for themselves how to manage an incident. Though, they are still obliged by the Act of Preparedness, Ch.5 §24, that defines the sector responsibility principle as: *"Each minister must plan within each area for the maintenance and continuation of the functions of society in the event of major accidents and disasters, including preparation of emergency plans."* [19]. Even though, the legislation defines only ministries, the principle is an overall rooted norm in the Danish society. In addition, the principle is embedded in Danish emergency and as well by the European traditions. Hence, the division of governance in vertical infrastructure sectors seems natural (see Chapter 1).

The sectoral classification is widespread among EU states, by which the European Network and Information Security Agency (ENISA) divides CII into individual sectors. As cyber incidents can impact multiple sectors due to various interdependencies. They can impact across borders and affect other nations as well. By creating a common methodological basis for the EU states, it creates a frame that supports an international collaboration among sectors. For example, the transportation sector is more or less equally perceived in all EU states consisting of railway, aviation, road networks and maritime ports. In some sectors e.g. aviation and railways, a European centralized information infrastructure has been established to make information sharing more convenient among nations. According to DEMA the sector responsibility is the guiding principle for the overall preparedness of the Danish society. The principle is embedded in the organisation of societal infrastructure, which might not be a sufficient approach nor an appropriate organisational structure when considering the interdependencies the CII systems is comprised of.

Jensen (2018) criticises the national cyber strategy (2018) of being too focused on the sectoral principle and therefore lacking a centralised strategy on state level [20]. Furthermore, Jensen suggests a more consistent characterisation of what constitutes the Danish CII at governmental level and in each sector as well as to identify a common approach of how to prioritise criticality and identification of CII operators and authorities [21]. The responsibility of managing cyber incidents in each sector is left within the sectors, of which Christensen & Petersen (2017) also criticise of being not enough proactive at state level in terms of preparedness and cross-sectoral coordination [22]. The US Government Accountability Office (2006) recommends that an agreement among authorities and involved operators is a key issue in CIIP [23]; however, such an agreement is missing in a Danish context. Without consensus on how CIIP should be managed before, during and after a cyber incident it is likely that the private CII operators make decisions that are directly cost-beneficial for themselves and not necessarily for the CII.

4.2 Procedural Framework for Danish Cyber Emergency

The Centre for Cyber Security (CFCS) is the national IT and cyber security authority, and in addition the responsible authority for the telecom sector. CFCS is capable of monitoring online activities of public and private CII operators and authorities, through the Network Security Service under the Act of Centre for Cyber Security [24]. The Network Security Service was formed in 2014 as a merger between the former GovCERT and MILCERT [25], with the purpose of monitoring, analysing and supporting the military, civilian and private sector. CFCS is a state-owned institution under the jurisdiction of the Military Defence Intelligence Service (FE), which is an agency under the Ministry of Defence (MD) [26].

CFCS is mostly concerned with cyber incidents involving advanced persistent threats (APT) that impact one or several CII sectors. If the incident is not an APT, the compromised organisation handles the incident by itself according to the sector responsibility principle. CFCS interferes only in case of; (i) If the organization is deemed insufficient to deal with the incident. (ii) If the incident concerns state security; and (iii) If the incident affects across sectors. In case of initiating the authorities, the typical approach is to form the national operational staff team (NOST) which consists of the National Police, PET, FE and CFCS including the ministers from the affected sector and other relevant authorities [27].

If an organisation experiences an IT breach, the official procedure is that the corporation is responsible to assess and possibly inform relevant stakeholders including the authorities *during* the

incident e.g. ministries, other corporations, suppliers and CFCS [27], if they judge the situation to be more comprehensive than what they can manage. However, the EU NIS Directive requires the CII operators and authorities to inform the national ICT authority *after* the incident has occurred [28]. It is conceivable that some companies may not necessarily find it beneficial to inform authorities on an early stage of the incident due to data sensitivity, financial and competitional reasons. CFCS has a forensic-objective and not necessarily an interest in minimising financial costs or maximising profit.

The EU Commission has issued cyber-incident reporting laws applicable to all EU states, in areas where cross-national disrupting events are expected to pose the greatest risk. Danish companies and authorities identified as operators of essential services (OES) by the EU, are required by the NIS Directive to notify CFCS as well as sectoral authorities when experiencing security incidents [28]. All Danish state authorities, municipalities and regions are required to notify CFCS of major IT security incidents [16]. In addition, according to the actor of telecommunication, all telecom providers must notify CFCS when negotiating contracts, experiencing IT breaches and when activating internal preparedness [29].

A cyber threat is a rather new phenomenon for which there is little tradition in Denmark on how to manage. It is only very recent Denmark has published their first strategy including cyber strategy and critical infrastructure (see Chapter 1.1.2). The current procedure is similar to a physical incident e.g. fire, burglary etc. [11]. Cyber-attacks are more than often related to sensitive information, either where data is held as a hostage for ransomware e.g. the WannaCry Ransomware attack in 2017 [30] or possible to disturb some kind of functionality or service like the case for the Iranian nuclear power plant in 2010 [31]. Whatever the purpose of the cyber-attack is, the attack affects companies' IT systems that control everything from financial transactions, contracts, employee and customer information to monitoring and controlling physical systems. Having authorities taken control over a cyber incident may not be appreciated by companies. The authority and company may have different preferences in terms of allocating resources, where decisions taken by the authority may not be preferable for the private operator and vice versa. Baezner & Cordey (2019) argue that private and public operators' financial perceptions might be very different, where the corporations have for-profit understanding and public authorities have a not-for-profit belief [13]. This may delay or even prevent the private operator to inform the authorities, which may have consequences for the CII system. It is a matter of a responsibility trade-off; on one hand the company is obligated to act in the interest of its shareholders and on the other hand the company is obligated to act in the interest of society. The decision of involving CFCS can have negative consequences for the shareholders in terms of experiencing financial losses due to longer recovery time or data loss. The decision of not involving CFCS or involving them too late can have an impact on society.

4.3 Multilevel Decision Making

Denmark has a constitutional parliamentary monarchy, where the legislative power belongs to the parliament, of which the majority regulatory decisions are transferred to the ministries. The parliament consists of 179 members elected for a four-year period. The executive power is performed by the Government with the Prime Minister as the lead authority. The political level is arranged at state, regional and local level. The state level constitutes the government and ministries, whereas the ministries have operationalised certain strategic tasks to the associated agencies. Currently, there are 19 ministries including the Prime Minister’s Office for which six are identified as CII responsible (Figure 10). The regional government consists of five geographical regions that

each is responsible for hospital and medical care including health insurance, social affairs, regional development and coordination with business, tourism, transport and environment. The local government consists of 98 municipalities, where each is responsible for handling services, assets and functions related to citizen welfare [32].

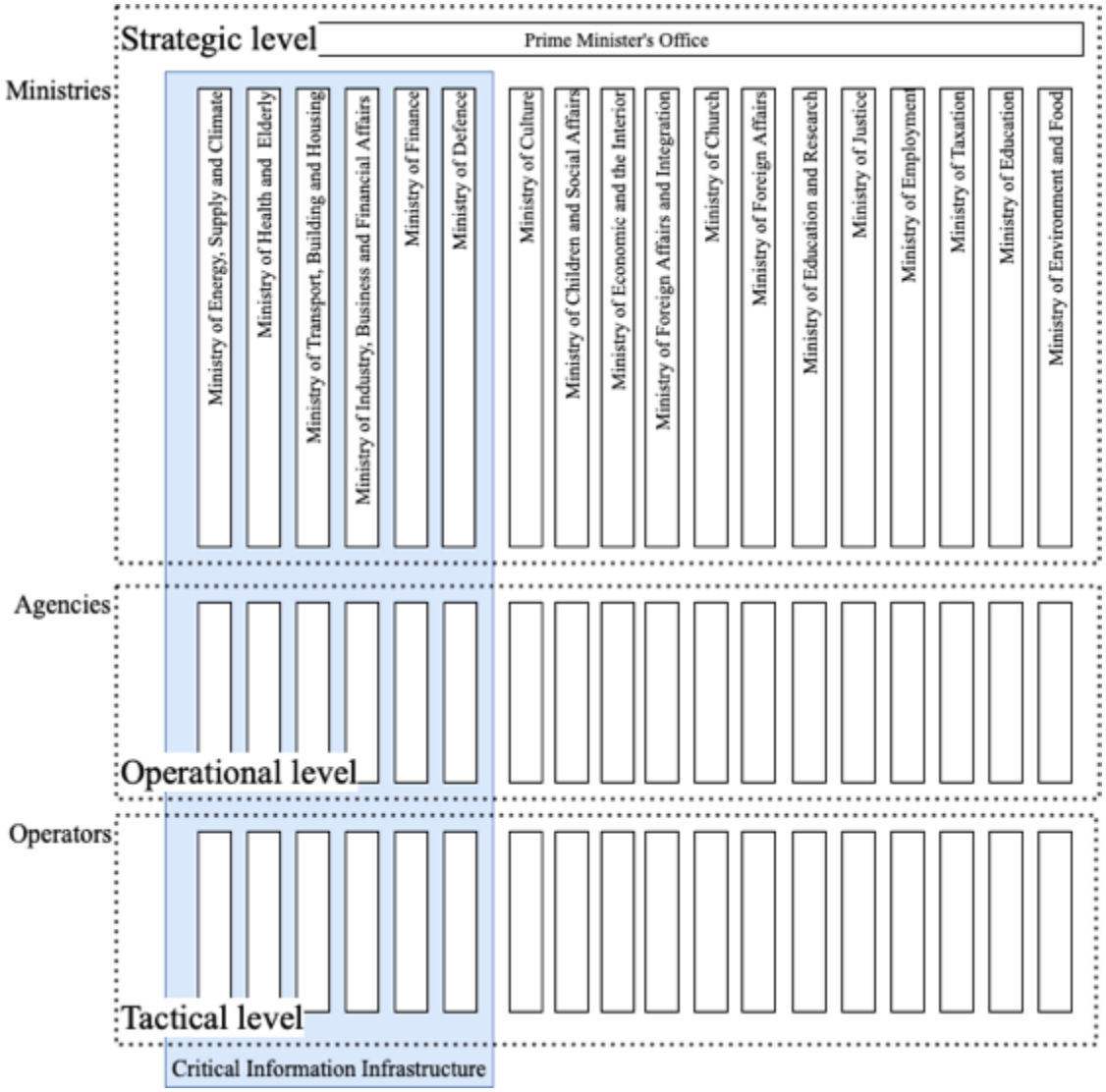

Figure 10: Danish political organisational diagram

The organisation structure of the Danish society is characterised by hierarchical vertical sectors composed of a strategic, tactical and operational level. For each sector, the respective ministry is political responsible to govern and regulate the sector (Figure 10). The majority of policies are made within the respective ministries, whereas the same applies for the sector cyber strategies. Each ministry is responsible of identifying and governing the sectoral CIIP

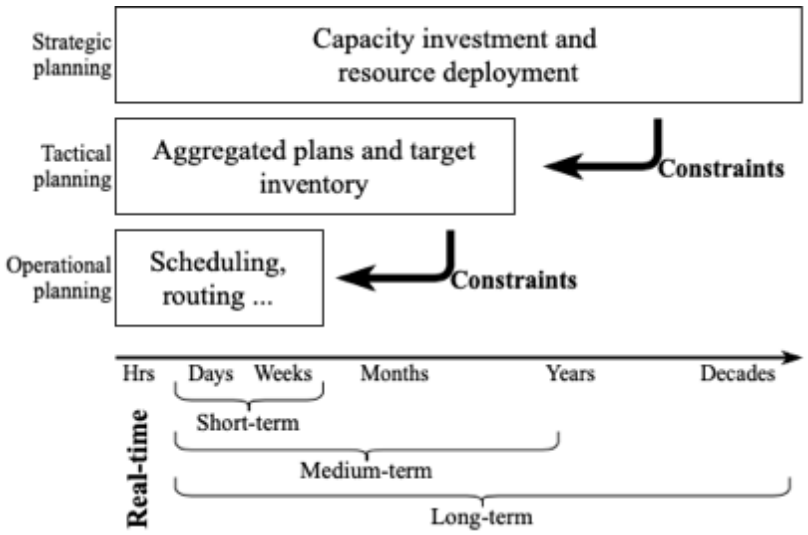

Figure 11: Strategic, tactical and operational decision levels, adopted from Jerbi et al. (2012) [33]

The objective for each decision-making level differs according to which level the decision aims towards. At different societal levels i.e. strategic, tactical and operational differs in objectives and preferences. As proposed by Jerbi et al. (2012), strategic decision making typically aims to have a long-term capacity investment and resource deployment, whereas tactical decisions are constrained by the strategic decisions and aims to decide on aggregated plans and target inventory (Figure 11). Operational planning is constraint by tactical decisions and has a short-term perspective aiming for efficiency, scheduling etc. [33]. The decisions made on the strategic level are anchored in the tactical level and tactical decisions are anchored at the operational level. Immediately, no strategic coordination process can be identified among the ministries. At the tactical level, coordination in relation to contingency planning occurs, where, among other things, the police, the Danish Emergency Management Agency (DEMA), the military and the Danish Health partly collaborate. At the operational level, more or less horizontal cooperation takes place between public and private operators. The vertical process of governance indicates an integration of regulations and policies at ministerial level to be anchored downwards to the lowest operational level in the sector.

5 Subsystems Identification

Abbreviations

AD	Agency of Digitisation
CFCS	Centre for Cyber Security
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
DBA	Danish Business Authority
DCIS	Decentralised Cyber Information Security
DEA	Danish Energy Authority
DeiC	Danish e-Infrastructure Cooperation
DGA	Danish Geodata Agency
DHA	Danish Health Authority
DMA	Danish Maritime Authority
DMI	Danish Meteorological Institute
ECI	European critical infrastructure
ERTMS	European Railway Traffic Management System
FE	Danish Defence Intelligence Service
FMK	Common Medicine Card
FSA	Financial Supervisory Authority
FSOR	Financial Sector Forum for Operational Robustness
HDN	Health Data Network
ICT	Information Communication Technology
IPCIS	Insurance-Pension CIS
KIH	Clinical Integrated Home Monitoring
MCEU	Ministry of Climate, Energy and Utilities
MCISF	Maritime Cyber and Information Security Forum
MD	Ministry of Defence
MF	Ministry of Finance
MH	Ministry of Health
MIBFA	Ministry of Industry, Business and Financial Affairs
MSDI	Marine Spatial Data Infrastructure
MTBH	Ministry of Transport, Building and Housing
NFCERT	Nordic Financial Computer Emergency Readiness Team
PET	Danish Security and Intelligence Service
RD	Road Directorate
SES	Single European Sky
SIFI	Systemically Important Financial Institutions
TCHA	Transport, Construction and Housing Agency

The current chapter introduces a system representation of the critical information infrastructure (CII) system by characterising the six subsystems that constitute the Danish CII [11]: (i) Energy sector; (ii) Maritime sector; (iii) Healthcare sector; (iv) Transportation sector; (v) Telecommunication sector; and (vi) Finance sector. The sections include a system representation of the sectoral operational, tactical and strategic operators and their relation, embracing the internal information flow and dependencies.

5.1 The Energy Sector

The Ministry of Climate, Energy and Utilities (MCEU) is responsible for the energy sector and has given the operational authority to the Danish Energy Authority (DEA), where DEA administers and monitors the energy distributors and producers (Figure 12) [34]. As required by the NIS Directive (2016) the decentralised cyber information security (DCIS) unit has been formed within the organisation of DEA as part of their existing emergency preparedness programme [34]. The Centre for Cyber Security (CFCS) supports the DCIS unit.

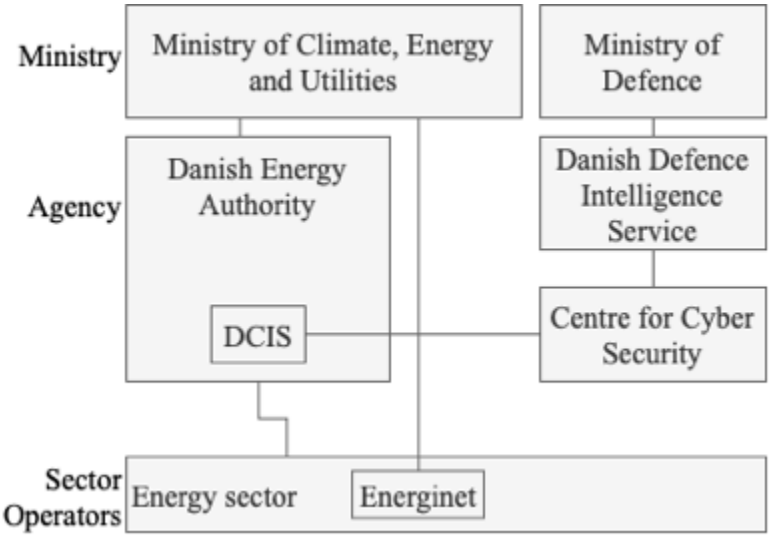

Figure 12: Representation of regulatory bodies within the energy sector

There are roughly 80 CII operators in the energy sector [35]. Energinet is a state-owned company, having a monopoly on electricity and gas transmission network, gas distribution, gas storage and the information database DataHub. All the activities from the manufacturer to the electricity suppliers and to the consumer requires a data and information exchange. To support and manage the information flow, Energinet implemented DataHub in 2013 to better secure and centralize all data sharing. DataHub is an IT system collecting all information about the consumers' electricity consumption and handles the communication processes in the electricity market between suppliers and distributors [36]. Table 5 shows a selection of the CII operators representing the energy sector including balance managers, power grid suppliers, gas suppliers, electricity suppliers, transmission network operator, gas distributor and gas storage facilitator [36].

Table 5: A selection of energy CII operators

Gas distribution (Energinet)
Evida

Gas storage facilities (Energinet)
Gas Storage Denmark
Lille Torup
Stenlille

Gas suppliers
OK a.m.b.a.
Aalborg Naturgas Salg A/S
SEF Energi A/S
EWII Energi A/S
Eniig Energi A/S
SE
DCC Energi A/S
Gasel
Energi Fyn Handel A/S
FRI Energy A/S
SK Forsyning
SEAS-NVE Strømmen A/S
Ørsted

Electricity transmission network
Energinet

Balance managers (cons., trade)
Entelios ApS
Los A/S
Modstrøm Danmark A/S
Statkraft Energi AS
Scanenergi A/S
Norsk Elkraft Danmark A/S

Electricity suppliers	
Vindstød	
Vindenergi	
Netpower	
Jysk Energi	

Power grid companies	
Radius	Evonet
Cerius	Trefor
Flow	Vores Elnet
Veksel	N1
RAH	Konstant
Thy-Morse	Nord Energi
NOE	Ravdex
Dinel	Læsø
Øst	

Balance managers (trade,cons.,prod)
Axpo Nordic AG
Centrica Energy Trading A/S
Danske Commodities A/S
Energi Danmark A/S
E.On Sverige AB
Kinect Energy Denmark A/S
Ewii Energi A/S
Markedskraft Danmark A/S
Modity Energy Trading AB
Uniper Global Commodities SE
Vattenfall A/S
Vestas Wind Systems A/S
Ørsted Salg & Service A/S

Balance managers (trade)
Alpiq AG
Edf Trading Limited
Ekologicke Zdroje Energie S.R.O
Electrade SPA
Enel Trade Spa.
Energya VM Gestión De Energía Slu
European Energy Exchange AG
Ewii Energi A/S
Global Energy Division
Axpo Trading AG
In Commodities A/S
Mercuria Energy Trading SA
Mft Energy A/S
Nord Pool Spot AS
Powermart ApS
Rwe Supply & Trading Gmbh
Shell Energy Europe Limited
Statkraft Markets Gmbh
Total Gas And Power Ltd.
Trailstone Gmbh
Vattenfall Energy Trading Gmbh
Vitol S.A.

Balance managers (prod., trade)
Hofor Energiproduktion
Stadtwerke Flensburg Gmbh
Østkraft Produktion
Ørsted Bioenergy & Thermal Power

The Executive order on IT preparedness in the electricity and natural gas sectors (2017) has guided the preparation of the sectoral strategy for these two subsectors [37]. The oil and water supply sectors are excluded from the CII system in the national cyber strategy (2018), as they are considered being insignificant dependent on information communication technology (ICT) [11]. The EU (2008) has identified European critical infrastructure (ECI) sectors including: electricity, gas and oil [9]. Despite the Danish legislation which sets emergency regulations for the oil sector [38] and the EU recommendations, the oil sector has been excluded as a critical asset. Energy CII is comprised of electricity, gas and heat, where heat constitutes merely a margin compared to the other two and is not elaborated any further [39].

The electricity system

There are roughly 100,000 electricity generating plants, of which electricity is sold from the production suppliers. The grid companies that operate the wiring grid from the transmission network (owned by Energinet) and to the end-user receive payment from the electricity suppliers to transport electricity to the end-users (Figure 13). The electricity suppliers are the end-users' primary contact with the electricity system. All suppliers that require access to customer data must have the approval of Energinet to request this from the end-user [40].

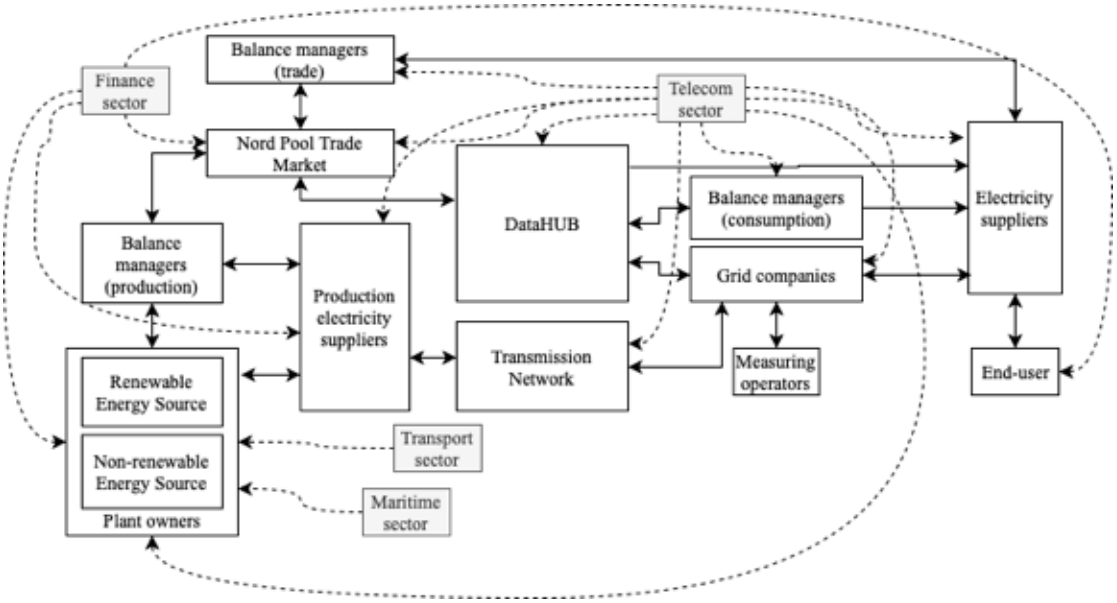

Figure 13: Conceptual illustration of the information flow in the electricity supply chain

Energinet administers the transmission network that is the centralised element in the supply chain of electricity. In addition, Energinet owns the ICT-system called DataHub, which stores data from all electricity operators to facilitate communication and data exchange [40]. The electricity subsector is characterised by being a supply chain, where each operator constitutes a significant part of the chain. The most centralised element in the chain is the transmission network and DataHub owned by the state-owned company Energinet.

The gas system

In the gas sector, the typical operators are suppliers, transportation operators, bio-natural gas sellers and storage operators. The gas is produced in fields in the North Sea or at biogas plants onshore, after which the gas is transported via pipelines to the two national gas storage facilities and to the end-users with support from gas suppliers [41].

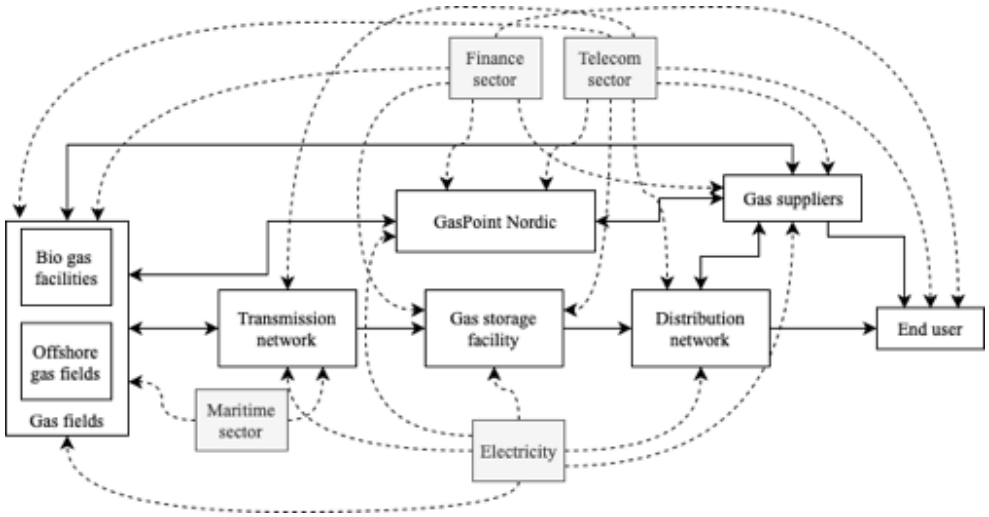

Figure 14: Conceptual illustration of information flow in the supply chain of gas

Energinet has a monopoly as a distribution, transmission and gas storage facility operator. In addition, Energinet is the authority responsible for maintaining the distribution and transmission network including processing the approval of new energy suppliers [41].

The energy sector is a centralized sector, with Energinet as the owner of the infrastructure. In the electricity sector, Energinet owns DataHub, where all electricity operators must submit and retrieve their data. In the gas sector it has not been possible to locate a similar central information system, however Energinet owns the entire gas infrastructure including transmission network, gas storage facilities and distribution network (Figure 14), which makes them the dominating operator.

5.2 The Maritime Sector

The ministry responsible for the maritime sector is the Ministry of Industry, Business and Financial Affairs (MIBFA), where the operational authority belongs to the Danish Maritime Authority (DMA) [42] (Figure 15). The Maritime Cyber and Information Security Forum (MCISF) has been formed to implement the cyber strategy (2019) [42] as the decentralised cyber information security (DCIS) unit. MCISF facilitates sharing of knowledge and general coordination within the maritime sector. MCISF is the maritime version of the DCIS unit, required by the NIS Directive (2016) [6]. MCISF consists of maritime IT-security authorities by which DMA is the coordinator with support from CFCS [42].

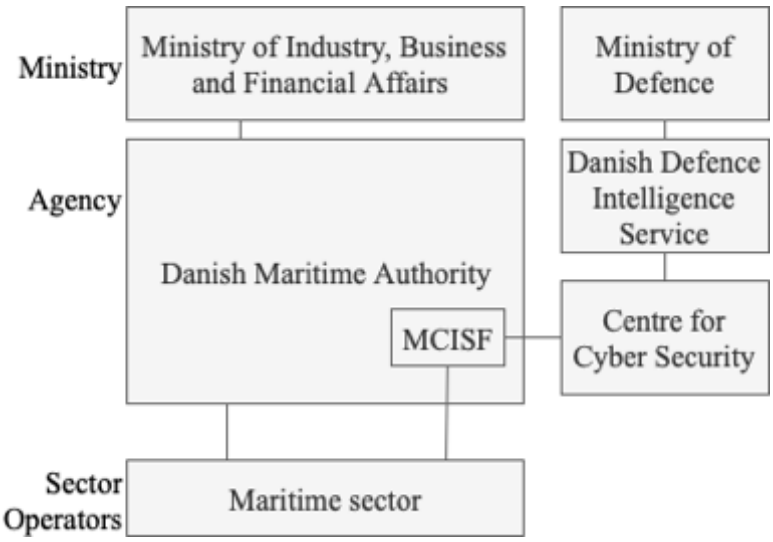

Figure 15: Representation of regulatory bodies within the maritime sector

The Blue Denmark is a synonym for the Danish maritime cluster of operators, all of which have activities related to the maritime sector. This includes offshore companies engaged in oil extraction; installation of wind turbines; shipping companies; Danish ports and freight terminals serving a regional catchment; freight forwarders and brokers; repair and new building yards; industrial companies that supply equipment and components to shipyards globally [43]. According to DAMVAD Analytics (2019), there are 800+ operators in the maritime sector (Table 6), where the majority is represented by technology suppliers with roughly 50%. The service providers, universities, educational institutions and port operators represent approximately 35%. Though, the shipping companies only represent 15%, they characterise a great part of the supply chain [44].

Table 6: Selection of maritime CII operators

Technology suppliers	**Shipping companies**	**Service providers, universities and educational institutions and port operators**
Represents 50% of maritime actors	*Represents 15% of maritime actors* e.g. Maersk and DHI	*Represents 35% of maritime actors*

At a strategic level the Ministry of Finance defines the CII maritime as being comprised of onshore and offshore activities, navigation, communication, cargo, security, environmental controls, sea traffic monitoring and shipping information [11]. At a tactical level DMA defines the sector as the safety of shipping in Danish waters and the safety in Danish ships, ship systems and software for ship operations, including propulsion and navigation, human resources and physical elements [42]. An interpretation of both definitions is illustrated in Figure 16.

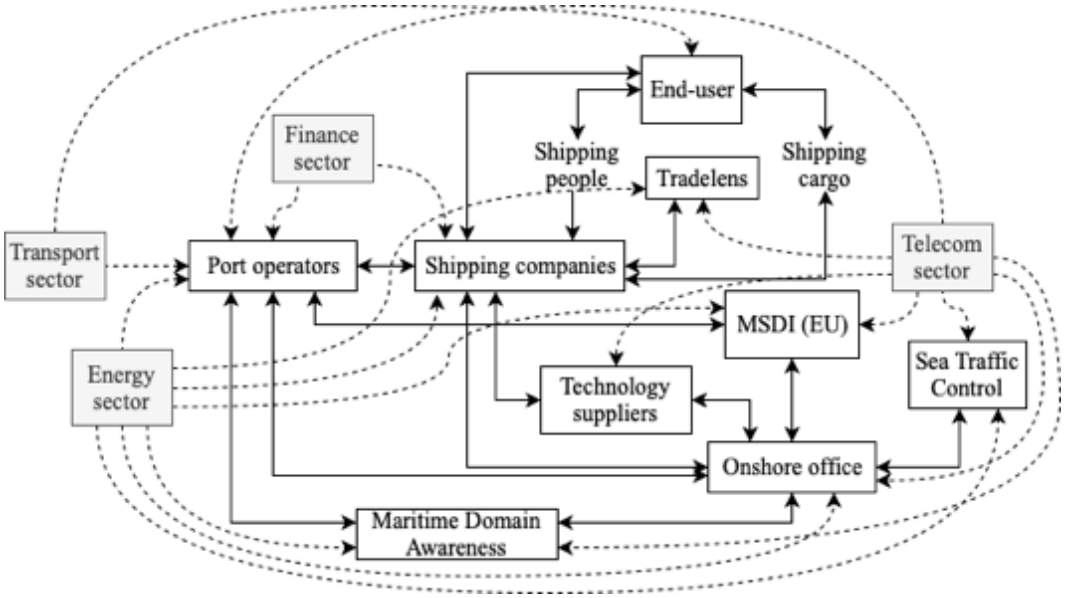

Figure 16: Conceptual illustration of the information flow in the maritime sector

The EU maritime database, Marine Spatial Data Infrastructure (MSDI) aims to monitor geographic and business information for all maritime authorities. It is a current project under way and if realised it becomes a centralised datahub [45]. The shipping companies, Maersk and IBM have developed an ICT system called Tradelens allowing shipping operators to monitor shipping activities in real-time through the whole supply chain. As well as MSDI is a datahub for authorities on an EU level; Tradelens is a datahub for private operators [45].

The maritime sector is characterized by a rather decentralised network of mostly service and technology companies supporting only a few larger shipping companies. The sector is structured in a supply chain, where the operators are self-governed, and the information flow is concentrated around the operation of shipping companies.

5.3 The Healthcare Sector

The Ministry of Health (MH) is the regulatory authority of the health sector where the tactical responsibility is presented by the Danish Health Authority (DHA) [46] (Figure 17). The sector is comprised of treatment sites, suppliers of medical equipment and technology, pharmacies, and research organisations and institutions [47]. The patient care is supported by an overall data system. There are several ICT systems that interconnect the operators such as the Health Data Network (HDN), sundhed.dk, KIH, FMK and Tele Medicines, allowing patient data to be transferred among operators [11].

A DCIS unit is formed within the Health Data Protection Authority and acts as the link between the sector and CFCS. DCIS facilitates coordination and knowledge sharing among health operators. In

an emergency, DCIS is in collaboration with DHA as the coordinating emergency authority with support from CFCS [46].

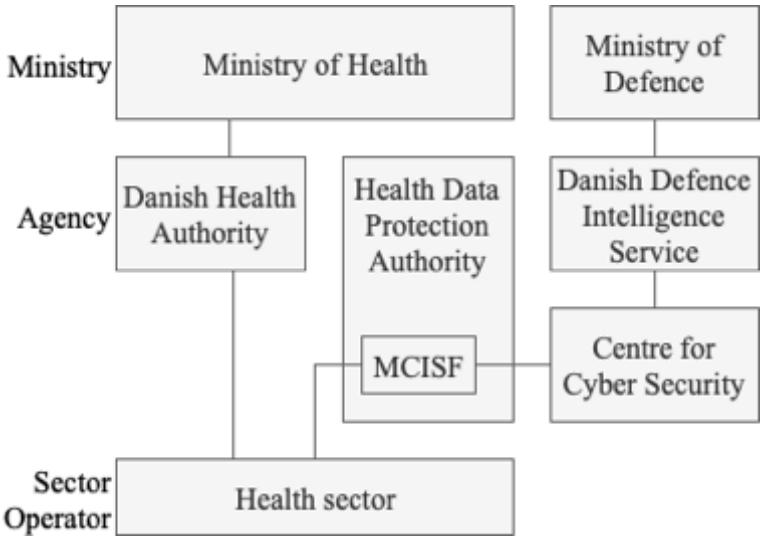

Figure 17: Representation of regulatory bodies within the health sector

The sector is divided in 96 municipalities and 5 regions, where each individual in the population is assigned to a general practitioner who operates within the boundaries of the local government (municipality) acting like gatekeepers to other specialists, hospitals and medical services (Table 7).

Table 7: Selection of health CII operators

Pharmacies	**Hospitals**	**Treatment facilities**
A-apoteket (200 pharm.)	69 public hospitals	Physiotherapists
Apotekeren A.m.b.a (100 pharm.)	19 private hospitals	Dentists
Pharma+ (20 pharm.)		Nursery homes
Apotekernes A.m.b.a (500 pharm.)	**General practitioners**	Specialised GP
	+3000 general practitioners	…

General Practitioners (GPs) store personal data regarding patients' drug use, medical history, family conditions and general health in various local, municipal and regional databases that are collected in a national database. This makes it possible to monitor and analyse the patient's development, as well as to extract statistics to evaluate the patient including the institutions' performance. Data is transferred from the GP to the regional health administration which then sends it to the DHA where the Health Data Network (HDN) collects all information [48]. The public has access to Sundhed.dk which is the national patient journal database, where each region has its own database (Figure 18).

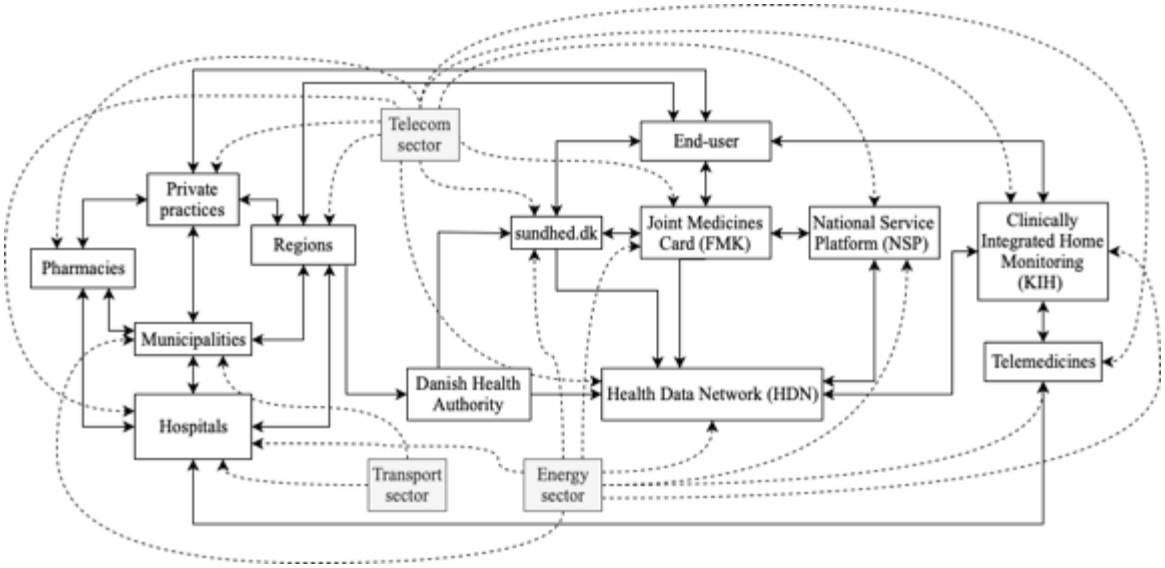

Figure 18: Conceptual illustration of information flow in the health sector

A relatively new approach is telemedicine, where the treatment takes place in the patient's home communicating through digital media, such as email, video, picture and audio via the internet. In this way, communication between the patient's computer and the treatment site's computer takes place [47]. This service poses a risk of malware on the patient's computer getting transferred to the operating system of telemedicine (KIH).

The sector is characterized by being highly integrated and centralised at a tactical level, where DHA owns the Health Data Network database in which all data from regional, municipal and GPs are transferred to.

5.4 The Transportation Sector

The subsystem of transportation is under the authority of the Ministry of Transport, Building and Housing (MTBH), where the tactical authority is given to the Danish Transport, Construction and Housing Agency (TCHA) as being responsible for the sector in general. The transport sector is comprised of railway, aviation, roads and maritime ports. There is an authority coordinating each subsector as: (i) Naviair is responsible of the aviation; (ii) Rail Net Denmark is responsible of the railway; (iii) Danish Road Directorate is responsible of the road network; and (iv) TCHA is sector responsible as well as responsible of the maritime ports [11] (Figure 19).

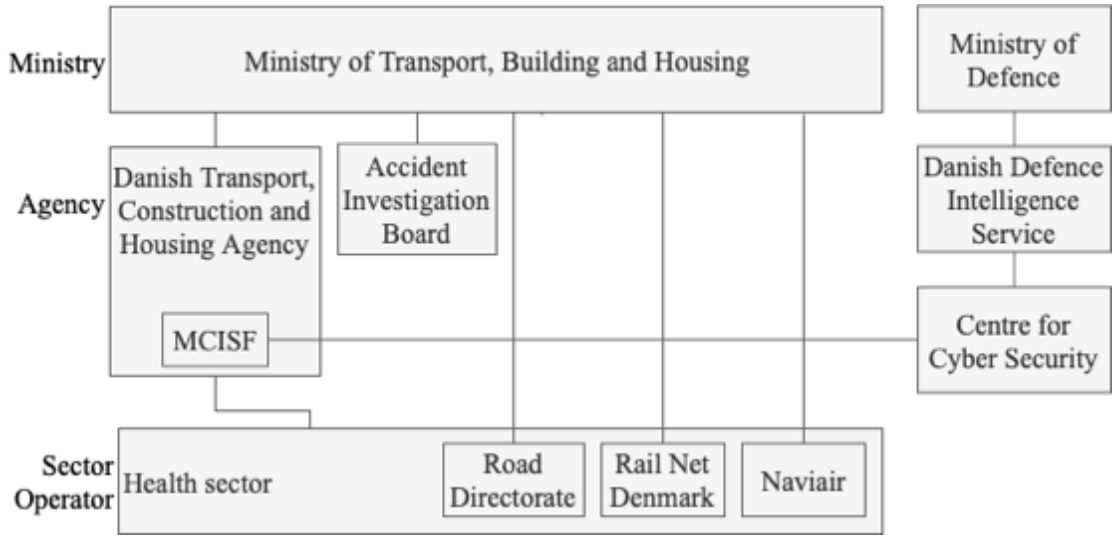

Figure 19: Representation of regulatory bodies within the transport sector

As required by the NIS Directive (2016) the MTBH formed a DCIS unit under the authority of TCHA, which regularly coordinates with Centre for Cyber Security (CFCS) and Danish Security and Intelligence Service (PET) [49].

The Railway system

The railway sub-sector is structured as the supreme political authority MTBH, of which TCHA acts as the tactical authority. It is further supported by the Accident Investigation Board and Rail Net Denmark. The Accident Investigation Board is an authority under MTBH, and Rail Net Denmark is a self-owned public company. Rail Net Denmark manages the railway infrastructure, where roughly 97% of traffic control is carried out by remote control [50]. The rail infrastructure consists of the state railway, regional railway, Copenhagen Metro, Aarhus Light Rail, S-train network and light rail in East of Denmark [51] (Table 8). Train operators use the infrastructure provided by infrastructure managers, of which the largest operator is DSB. DBS is a state-owned independent company that is under the jurisdiction of MTBH.

Table 8: Selection of railway CII operators within the transport sector

Railway operators	**Railway managers (infrastructure owners)**
Owned by MTBH:	Midtjyske
Sund & Bælt Holding A/S	Nordjyske
Udviklingsselskabet By & Havn I/S	Lokaltog
Hovedstadens Letbane I/S	Vestbanen
Fjordforbindelsen Frederikssund	A/S Øresund
Bornholmstrafikken Holding A/S	DB Netz
DSB	NEG Niebüll
Metroselskabet I/S	Rail Net Denmark
Private:	
DB Netz (freight operator)	
Arriva Tog	
CFL	
Cargo Denmark	

The European Railway Traffic Management System (ERTMS) centralizes and automates railway monitoring and control [11] and additionally centralises the information flow from infrastructure operators and railway managers as well as to connect Danish railway with other EU states rail systems (Figure 20).

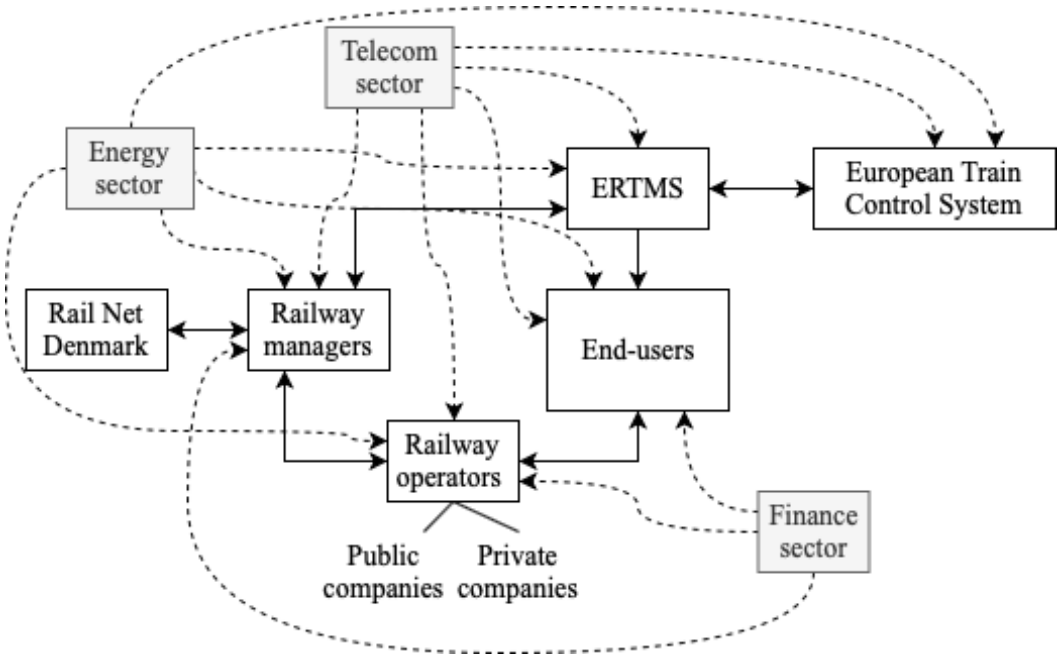

Figure 20: Conceptual illustration of information flow in the railway subsector

The railway sub-sector is characterised as being dominated by the public sector since the main infrastructure manager and railway company are publicly owned by respectively DSB and Rail Net Denmark. The information flow within the subsector is presumably centralised around the European traffic ICT system ERTMS and through this highly connected with EU states.

The aviation system

Naviair is responsible for managing and controlling aircrafts flying in Danish airspace and is the authority for the aviation subsector. The Accident Investigation Board and the Danish Meteorological Institute (DMI) are political institutions under MTBH, where DMI handles the meteorological service of civil aviation in Denmark. Naviair is a state-owned company owned by MTBH and operates from its own control towers in the Danish airports i.e. Copenhagen, Roskilde, Billund, Aarhus, Aalborg and Bornholm [52]. The aviation operators include airport owners, control towers, passengers, airlines, air traffic services and various suppliers [53] (Table 9).

Table 9: Selection of CII aviation operators within the transport sector

Airport companies	**Control tower operators**	**Other aviation actors**
Aarhus airport	Naviair	Military
Midtjyllands airport		Drone operators
Copenhagen airport	**Airline companies**	Passengers
Aalborg airport	67 operating airlines in Denmark	
Bornholm airport		
Sønderborg airport		
Billund airport		

Since 2001, the Single European Sky (SES) has been implemented in EU states to create unified airspace management across countries and by 2022, SES will be integrated in Danish aviation [54]. This will create an international information hub in the EU aviation sector.

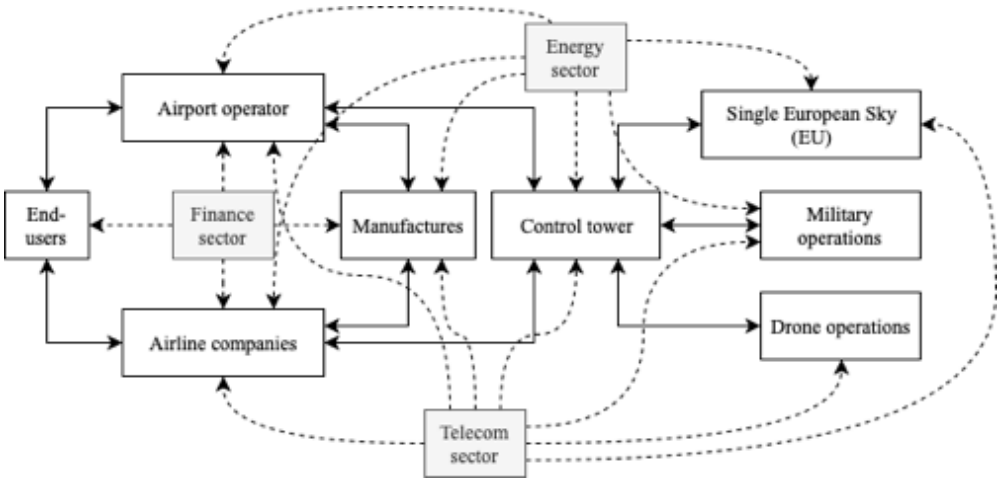

Figure 21: Conceptual representation of the information flow in the aviation subsector

The information flow is concentrated on the control tower operated by Naviair, which is the authority of the sub-sector (Figure 21). The majority of airports are municipal owned but operated at the same level as a company. The aviation sub-sector is characterised by the information flow that centralises the European ICT-system SES and consists of both public and private operators.

The road system

The critical information infrastructure road network consists of the state-owned road network operated and maintained by Road Directorate (RD), which is politically responsible [55]. In 2019, OTMAN is launched initiating a real-time ICT-system to centralise traffic information, radio, Twitter, navigation, winter services, GIS maps and external traffic information services [56] (Figure 22).

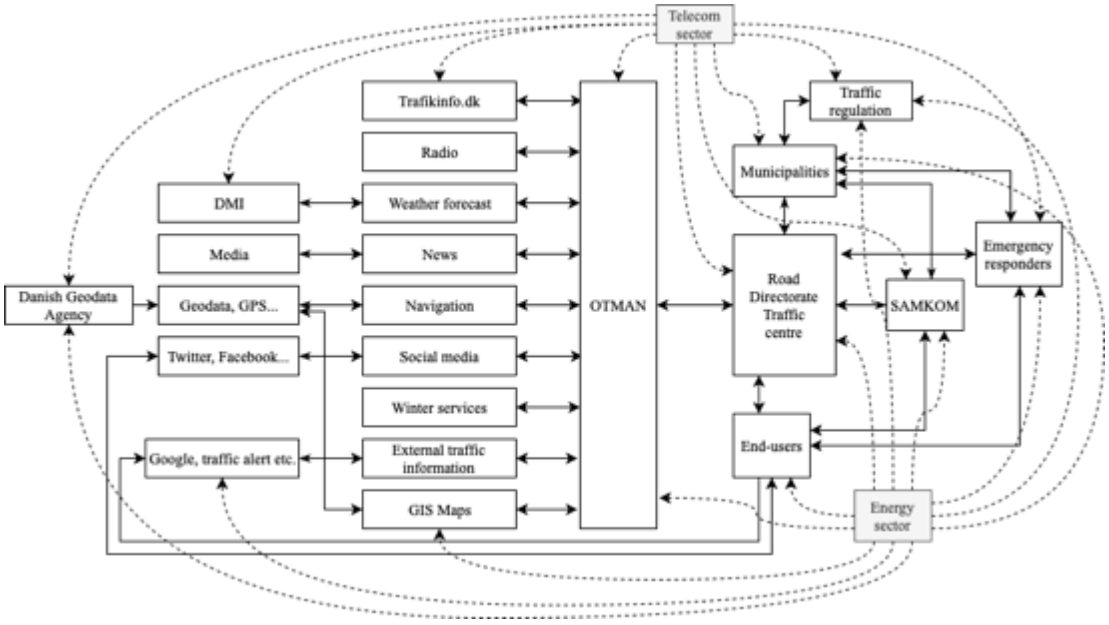

Figure 22: Conceptual illustration of the information flow in the road subsector

Another information hub besides OTMAN, which is more user-oriented is SAMKOM. SAMKOM was initiated by RD in collaboration with the Danish Geodata Agency (DGA) in 2017 to make the road network data more accessible through fewer accesses. DGA is under the political authority of MCEU and responsible for the geographical data and GPS services in Denmark. SAMKOM collects and processes road data to benchmark and develop road and traffic activities to make data access easier for municipalities and similar road stakeholders [57].

The flow of information in the road sector is centralised around RD connecting traffic information from OTMAN and SAMKOM and further communicates with municipalities and emergency responders as well as various road suppliers. The road network is characterised as a centralised public dominating subsector.

The port security sector

The port security sector is part of the transportation subsystem and is under the authority of TCHA under MTBH (Figure 23).

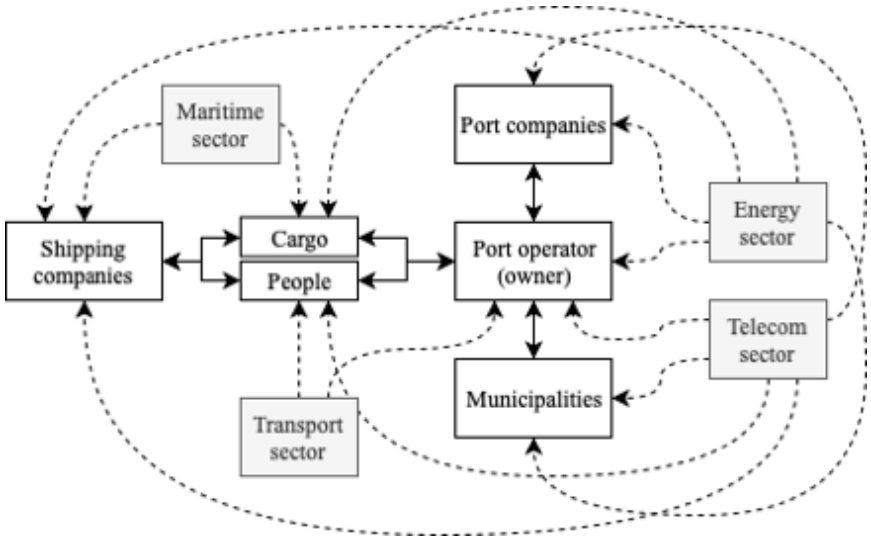

Figure 23: Conceptual illustration of the information flow in the port subsector

The ports are largely owned by the municipalities, whose tasks are to operate the ports. In many of the commercial ports, there are companies that have their operations in the port area. Many of which do their business primarily in the offshore industry. In that aspect the ports are physical connections between the transport sector and the energy sector that operates in offshore areas. Furthermore, the ports are the intersection between land and sea, which make them connected to the maritime sector as to the vessels communicating with the port before entering their area. When the cargo is unloaded it must be transported by either train or vehicle, hence the port sector is therefore coupled to the road network and the rail network.

5.5 The Telecommunication Sector

The telecommunication (referred to as telecom) sector is defined and governed by the sector itself meaning the cyber strategy for the telecom sector is conducted by the telecom operators in collaboration with CFCS. The most prominent industry associations Danish Industry, Danish Energy, Tele industry, IT-industry and Danish Business are responsible for implementing the strategy in collaboration with CFCS [58]. The sector consists of the internet, telephone network,

computer network, the radio broadcasting grid and ICT; however, the telecom sector is represented by its operators.

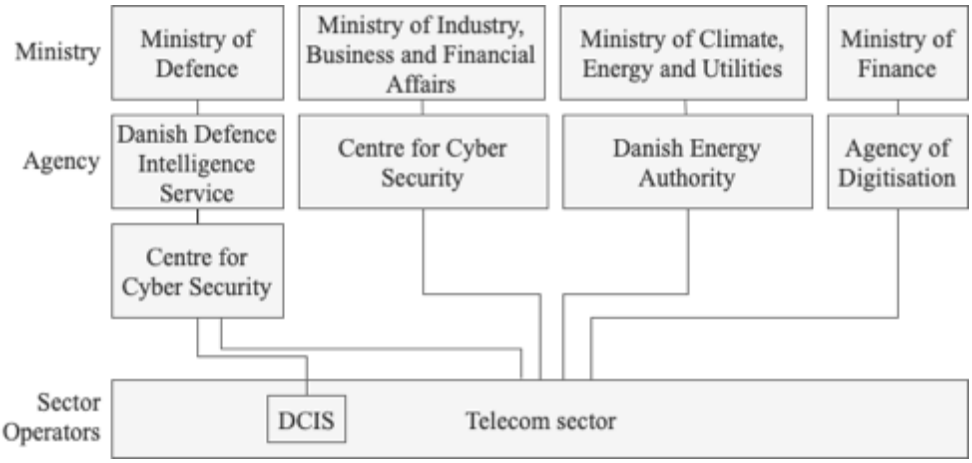

Figure 24: Representation of regulatory bodies within the telecommunication sector

The sectoral responsible authority is CFCS, which is an authority under the agency Danish Defence Intelligence Service (FE) under the Ministry of Defence (MD) [58] (Figure 24), where the MD is responsible for the strategic governance of information security in the telecom sector [11]. In addition, the Ministry of Climate, Energy and Utilities (MCEU) have a regulating responsibility of telecommunication technologies, where implementational responsibility is given to the Danish Energy Authority (DEA). MCEU is responsible for strategies within broadband, net neutrality, radio network and telecom infrastructure development, where the tactical responsibility is given to the DEA [59]. The Danish Business Authority (DBA) has the tactical responsibility of implementing regulations and strategies concerning competition published by the Ministry of Industry, Business and Financial Affairs (MIBFA). DBA administers industry compliance with the telecommunications regulations including enforcing sector-specific competition regulations [59]. The Ministry of Finance (MF) is not directly related to the sector but indirectly influences the range of information processes by regulating digitalisation through the Agency of Digitisation (AD) being responsible for the implementation of digitalisation [16].

The telecom DCIS unit consists of the same 11 telecom operators which also authored the cyber strategy (2018) with DKCERT as being the coordinator. DKCERT manages cyber emergency incidents at the research network Danish e-Infrastructure Cooperation (DeiC) which is under the jurisdiction of the Ministry of Higher Education and Science [60].

Table 10: Selection of CII telecom operators, some of which have multiple business areas

Network operators	**Tele infrastructure provider**	**IP and Broadcast providers**
Telenor, Telia (TT Network)	Telenor	Teracom
TDC (YouSee)	HI3G	
Hi3G (3)	STOFA	**Fibre Optics providers**
	Telia	Global Connect
Data centre operators	TDC	Fibia
Global Connect	Eniig	Waoo
	DK Emergency Communication	

In an operational level the sector consists of private operators that primarily includes network operators, infrastructure providers, data centre operators, IP and broadcast providers and fibre optics providers (Table 10) [11]. Additional operators include IoT manufactures, research and technology developers, telecom service providers e.g. Facebook, and television network companies. The

majority of the telecom operators are directly linked to consumers and therefore highly influenced by market controls and demands developing the sector rapidly.

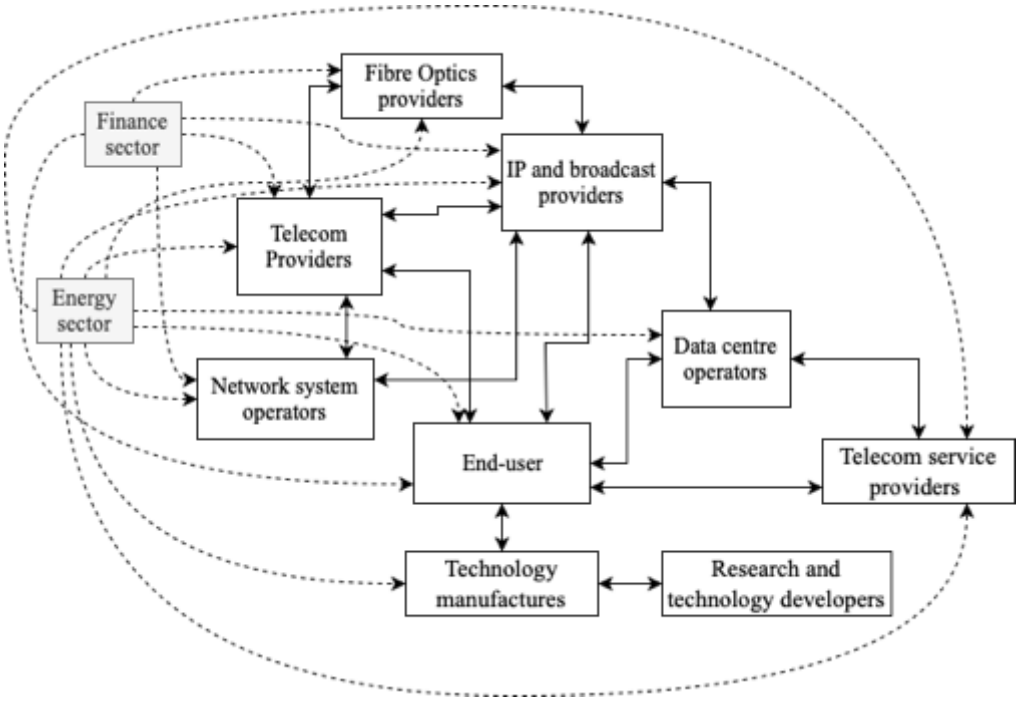

Figure 25: Conceptual illustration of the information flow in the telecom sector

The telecom sector is dominated by a few operators controlling most of the market. STOFA, Eniig, Fibia, Waoo and SE are all owned by the Danish telecom and energy supplier Norlys, which leaves eight main telecom operators consisting of TDC, Telenor, Telia, GlobalConnect, Teracom, Norlys, Hi3G and DK Emergency Communication of which all are owned by foreign companies. Except for a short list of independent telecom providers, the eight described telecom operators represent the CII operators in the sector, for which inter-active information flow is illustrated in Figure 25. The DCIS unit is represented by the telecom operators. The suppliers act as hubs for a number of smaller telecom providers. The telecom sector is characterised by self-governed private operators, with a few operators dominating the market. The sector is highly interlinked as the operators depend on each others services.

5.6 The Financial Sector

The Ministry of Industry, Business and Financial Affairs (MIBFA) has the regulatory responsibility at a strategic level to develop and maintain CIIP in the financial sector (Figure 26). The tactical authority is given to the Financial Supervisory Authority (FSA) controlling and monitoring all financial transactions [61].

The DCIS unit has been established under the authority of FSA and collaborates closely with the already existing Financial Sector Forum for Operational Robustness (FSOR) and Nordic Financial CERT (NFCERT) [62]. There are seemingly three cyber emergency units:

- FSOR is focused on the banking sector and governed by the Danish National Bank [63]
- Insurance-Pension CIS (IPCIS) is focused on the insurance and pension sector and governed by the Insurance & Pension Industry Association [64]

- DCIS is concerned with knowledge sharing in the financial sector and governed by FSA [62]

FSOR is part of DCIS. FSOR's members include, among others, banks, NETS, data centres, MIBFA, FSA, FinansDanmark, the industry association Insurance and Pension and CFCS.

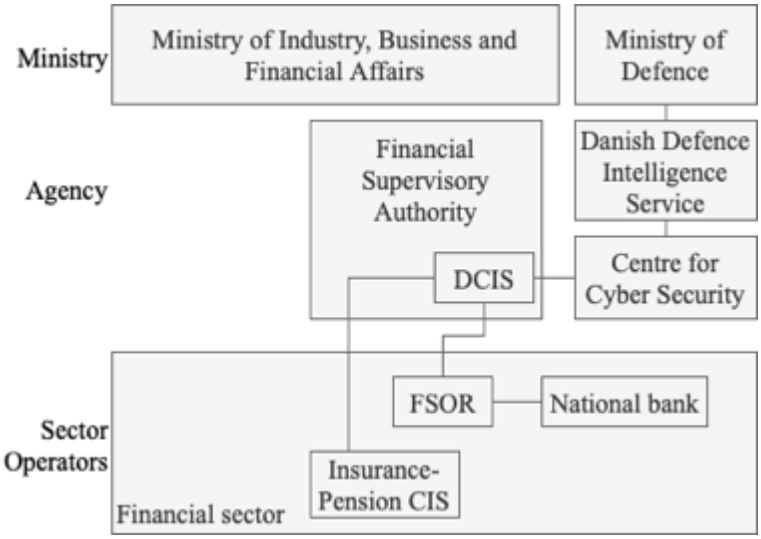

Figure 26: Representation of regulatory bodies within the financial sector

CFCS characterises the financial CII operators as companies that are subject to financial regulation [65] (Table 11). The Danish National Bank is a self-governing institution that acts as the intermediary of financial transfers among the Danish-located banks. FSA designates the most systemically important financial institutions (SIFI) in Denmark annually (Table 11), represented with a selection of financial CII operators [66] [67] [68].

Table 11: Selection of financial CII operators

SIFI actors (2019)	**Financial CII actors**
Danske Bank	96 Commercial and savings banks
Nykredit Realkredit	7 Mortgage-credit institutions
Nordea Kredit Realkreditaktieselskab	1 National Bank
Jyske Bank	42 Investment companies
Sydbank	3 (large) investment companies
DLR Kredit	10 small investment companies
Spar Nord Bank	65 Non-life insurance companies
	19 Life-insurance companies
Top 15 International banks	14 Lateral pension funds
Ikano Bank	17 Company pension funds
Handelsbanken	3 ATP, LD and AES
Handelsbanken kredit	24 Authorised alternative investment fund manager
Nordea Danmark	
SEB kort Bank	**Top 10 Danish banks (2019)**
Santander Consumer Bank	1 Danske Bank
DNB Bank ASA	2 Jyske Bank
FOREX Bank	3 Sydbank
Skandinaviska Enskilda Banken	4 Nykredit Bank
Swedbank	5 Spar Nord Bank
Nordnet Bank	6 Arbejdernes Landsbank
BIL Danmark	7 Ringkjøbing Landbobank
Carnegie Investment Bank	8 Saxo Bank
Resurs Bank	9 Vestjysk Bank
Citibank Europe plc	10 Sparekassen Kronjylland

There are several information systems that are used in the financial sector to facilitate easier communication among operators i.e. data transfers. To name a significant operator who facilitates information flow in the sector is NETS. NETS is a private Norwegian owned company and has more or less monopoly on facilitating financial transfers among banks, customers and companies.

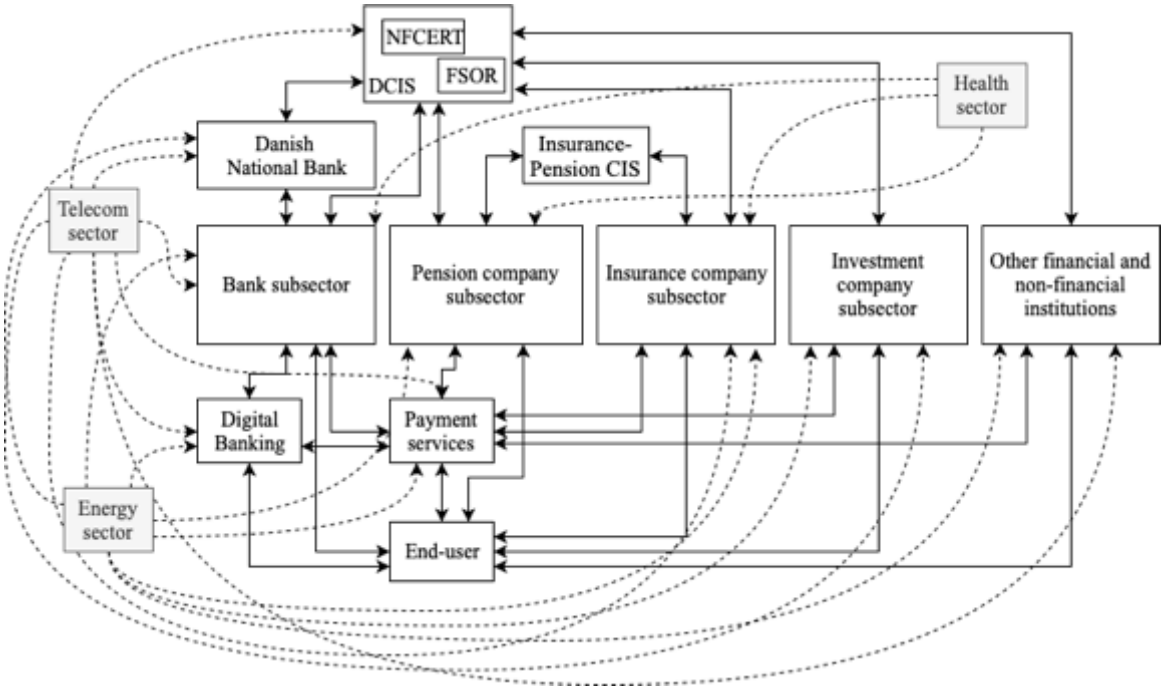

Figure 27: Conceptual illustration of the information flow in the financial sector

The sector of finance comprises citizens' wealth, and ensures, among other things, that citizens can pay for goods and services as well as receiving wages, tax regulation and benefits from the public sector. In order to map the main operators, the following five subsectors are suggested: (i) Bank; (ii) Pension company subsector; (iii) Insurance company; (iv) Investment company; and (v) Other financial and non-financial institutions. The information flow at operator level among the CII operators is conceptual represented in Figure 27.

The financial sector is characterised as a private decentralised sector with no direct coupling among subsectors besides the digital payment services where data is customer data and digital capital is transferred. The financial institutions presumably are interconnected through the end-users and payment services.

6 Alternative Systems of Governance

Abbreviations

AD	Agency of Digitisation
CFCS	Centre for Cyber Security
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
DBA	Danish Business Authority
DCIS	Decentralised Cyber Information Security
DEA	Danish Energy Authority
DeiC	Danish e-Infrastructure Cooperation
DGA	Danish Geodata Agency
DHA	Danish Health Authority
DMA	Danish Maritime Authority
DMI	Danish Meteorological Institute
ECI	European critical infrastructure
ERTMS	European Railway Traffic Management System
EU	European Union
FAO	Food and Agriculture Organisation of the United Nations
FE	Danish Defence Intelligence Service
FMK	Common Medicine Card
FSA	Financial Supervisory Authority
FSOR	Financial Sector Forum for Operational Robustness
HDN	Health Data Network
ICT	Information Communication Technology
IPCIS	Insurance-Pension CIS
KIH	Clinical Integrated Home Monitoring
MCEU	Ministry of Climate, Energy and Utilities
MCISF	Maritime Cyber and Information Security Forum
MD	Ministry of Defence
MF	Ministry of Finance
MH	Ministry of Health
MIBFA	Ministry of Industry, Business and Financial Affairs
MSDI	Marine Spatial Data Infrastructure
MTBH	Ministry of Transport, Building and Housing
NATO	North Atlantic Treaty Organization
NFCERT	Nordic Financial Computer Emergency Readiness Team
OECD	Organisation for Economic Co-operation and Development
PET	Danish Security and Intelligence Service
RD	Road Directorate
SES	Single European Sky
SIFI	Systemically Important Financial Institutions
TCHA	Transport, Construction and Housing Agency
UN	United Nations
WEF	World Economic Forum
WHO	World Health Organisation

The chapter presents an identification of main global hazards that are threatening the critical information infrastructure (CII) and evaluating the current practice of how hazards are classified as well as introducing three alternative methods of how hazards can be approached: (i) Single-hazard; (ii) Multi-hazards; and (iii) All-hazards.

6.1 Hazard Classifications

The current practice of hazard identification is classified by the source of origin. Nielsen & Faber (2019) argue, that the consequences of classifying hazards by their source of origin tend to become

the properties of specific academic disciplines. Instead, Nielsen & Faber suggest that hazards based on information type should be understood as classifying hazards according to their effects rather than causes. Nielsen & Faber (2019) suggest unifying hazards by crossing academic disciplines and keeping the source of origin insignificant, where they characterise four types (Table 12) [69].

Table 12: Hazard typologies based on the information flow adopted from Nielsen & Faber (2019) [69]

Type	Description	Examples
I	Rare large scale averaging with high consequence	Geo-hazards; and IT failures
II	Frequent with relatively small consequences (commonly ignored) but has cumulative effects that may trigger type III hazards	Exploitation of resources; inefficient regulations/ budgeting; human errors
III	Extremely rare and potentially disastrous events that may be triggered by type II hazards	Solar storms; super volcano eruptions; impact by asteroids; global climate change; major malevolent actions; out-of control technologies
IV	Events triggered by incorrect information (may resemble type I-III hazards) can play a role for all types of hazards and deserves special attention	Intentionally and unintentionally omitted or manipulated information (fake news); censored or erroneous observations

The classification of hazards and the way policy makers are dividing society into political subsystems are similar in the way that they both are methods of simplifying a complex system. In Denmark the political system is divided into several hierarchical sub-organisations where roughly each has a political regulatory authority. The national cyber information strategy (2018) emphasises the importance of interdisciplinary cooperation, yet the responsibility for each sectoral strategy belongs to the respective the sector authorities, resulting in a wide range of diverse strategies [11].

6.2 Identification of CII Hazards

The World Economic Forum (WEF) (2019) addresses technological hazards in relation to critical information infrastructure protection (CIIP) as being comprised of cyber dependencies which can lead to

- Data fraud and theft
- Cyber-attacks
- Critical information infrastructure Breakdown
- Adverse consequences of technological advances [70]

Technological threats may be categorised within the typologies suggested by Nielsen & Faber (2019). The above listed threats related to cyber interdependencies does not seem to fit in a single type of hazard category identified by Nielsen & Faber, but in several (Table 12). The overall threat identified by WEF (2019) relates to the Type II hazards due to its frequent and rather minor impacts, moreover it also relates to Type III due to its cumulative behaviour, and finally it relates to Type IV due to how it may change the information flow and the perception of information. The way

cyber threats do not fit into any of the suggested typologies only emphasises the complexity and the trans-boundary nature of the hazard.

Besides, the obvious cyber-related hazards, the majority of all hazards are directly or indirectly related to CIIP. With consideration of the various interdependencies the system of CII consists of, a wide range of hazards that are not cyber-related can influence the CII system. WEF (2019) addresses various slow-arising and sudden hazards including a range of economic, geopolitical, societal, political, environmental and technological hazards [70]. This leaves a need to strengthen the system making it more resilient to minor and greater disturbances.

6.2.1 Hybrid Threats

One of the current issues that has high political attention is hybrid threats. Hybrid threats are comprised of isolated non-related threats with no immediate connection but are deliberately applied to disrupt a system in a given direction. It is a form of coordinated and synchronized military strategy that utilizes a wide range of means such as political warfare, conventional warfare, and irregular physical and cyberspace warfare including other influential methods to exploit vulnerabilities in an infrastructure system. The activities aim to influence decision-makers at various political levels in favour of a given strategic objective. Fake news, diplomacy, legislation and foreign electoral intervention are methods to influence a given system [71]. In 2016, 22 actions are identified at European level to combat hybrid threats and strengthen cooperation across EU States to increase overall resilience [72]. One action is to form a collaboration between the EU and NATO to counter hybrid threats through research and knowledge sharing [71]. Another action is to strengthen cyber security in each of the EU States which among other the NIS directive (2016) is meant to initiate [6].

The combination of typologies that cyber interdependencies and hybrid threats represents, only emphasise the complexity of these hazards, and therefore the current practice of dealing with hazards in isolated systems is indeed inadequate. There is a need for a comprehensive approach to govern these systems and hazards, which allows inter-sectoral processes that encompass all potential hazards. The single-hazard approach relates to the current best practice, whereas a more comprehensive method is multi-hazard or all-hazard approach. The next paragraph introduces the three types of governance approaches.

6.3 Alternative Approaches of Governance

In the international perspective, the strategies for managing hazards are developed by a variety of governmental bodies located at the office of the prime minister such as the case for France, Ireland and the United Kingdom, or within so-called portfolio ministries responsible for national security e.g. Canada and the United States, or within the military e.g. Israel and Slovenia [73]. In the case of Denmark, the body responsible for the national security is the PET and for the ICT security the Centre for Cyber Security is responsible [11].

6.3.1 Single-Hazard Approach

A single-hazard approach refers to assessing and treating a hazard as isolated and independent [74]. The governance approach that relates to best and current practice as well as the classifying hazards by their source of origins, is called “single-hazard”. EU defines a single-risk assessment as a risk

of one particular type of hazard [75]. This approach relates very well with the Type I hazard suggested by Nielsen & Faber (2019), as these hazards are contained and averaging over time, meaning the hazards are levelled out as time goes by [69]. The sectoral responsibility principle indicates the silo-structured governance approach. The approach is imposed by the EU, where the division of critical sectors is a general applied method in the majority of EU states according to Baezner & Cordey (2019) [13].

The single-hazard approach is logically linked with identifying the system based solely on its subsystems similar to the method used in the Danish cyber security strategy (2018). For each sectoral strategy, the Centre for Cyber Security (CFCS) has conducted a threat assessment specified for each sector. In all threat assessment reports, the cyber threats are identified as cyber espionage; cybercrime; cyber activism; cyber terror; and foreign state attacks on CII. All of which are directly related to cyber security and none of them are related to other sources of hazards such as ecological, technical or biological and political hazards. These reports only emphasise the hazard classification and approach from Danish authorities are domain specific and very source-oriented instead of building the assessment on the assumption of derived consequences or informational patterns as proposed by Nielsen & Faber (2019) [69]. According to OECD (2019), a single-hazard approach is insufficient to build infrastructure resilience due to its nature of interdependencies and range of potential disruptions [73].

In Chapter 7 the subsystems that encompasses the Danish CII are evaluated within the framework of the single-hazard approach, where the system is understood on behalf of its subsystems disregarding any interdependencies.

6.3.2 Multi-Hazard Approach

The approach of considering multiple hazards and their interrelation is called “multi-hazards”. Kappes et al. (2012) argue that multi-hazard method refers to the interrelation between more than one type of hazard. EU defines a multi-hazard approach as assessing several hazards occurring at roughly the same time due to their cumulative dependencies or as they are caused by the same event; or threatening the same vulnerable exposed elements [75]. Multi-hazard assessments are widely used within natural hazards impacting industrial activities, so-called Natech hazards, where Western & Greiving (2017) attempts to model multiple types of hazards and cascading events, though preserves the linearity among the various hazards [76]. Where another study performed by Girgin et al. (2019) as representatives of the European Joint Research Centre examines the methodology of assessing Natech risks within the context of national risk assessments. Girgin et al. assess multiple hazards as being dependable however treated based on the type of hazards classified by their source of origin, making the interrelationship causal [77].

Gill & Malamud (2016) identify multi-hazard approach as an integration of all aspects of hazard interactions with consideration of vulnerability and exposure. However, Gill and Malamud (2016) suggests differentiating between a multi-layer single-hazard and multi-hazard approach, where a multi-layer single-hazard approach is characterised as dependent multiple different hazards; and the multi-hazard relates to an all-hazard approach, where one seeks to assess all possible relevant hazards and non-independent hazards. In their study they exemplify hazard interrelations in which they classify hazards by source of origin and even though they discuss the dilemma of causality as belonging to retrospective, they still determine cause-related hazard interrelationships. The multi-layer single-hazard approach is similar to the approach used by e.g. Western & Greiving (2017) and Girgin et al. (2019). The multi-hazard approach provided by Gill and Malamud (2016) is similar to

the all-hazard approach defined by OECD (2019), elaborated in the following section. Another interpretation of the concept of multi-hazards is found in the study performed by Clark-Ginsberg et al. (2018) that define a multi-hazard approach as a process of recognising and prioritising risks found within the same context or circumstance [78]. Although Clark-Ginsberg et al. propose a network analysis technique that offers multiple points of analysis and is in no way simplified, this approach still has the same risk focus and uses the same linear method as the approaches used in the aforementioned studies.

The methodology of multi-hazard assessment is widespread defined in grey and peer-reviewed literature; however the various methods appear to have a few common characteristics that is adopted in the current research: (i) Causality in the dependencies and interdependencies; (ii) A risk-focus (instead of a focus on resilience); and (iii) The hazards are determined by their source of origins. It has not been possible to identify country specific national risk assessment methodologies; nevertheless, it is assumed that most countries operate within the span of single-hazard and multi-hazard approach. In the context of Denmark, the Danish emergency authorities participate yearly in national and international exercises across sectors, and coordinating unit established in the wake of the sectoral cyber security strategies) the decentralised cyber information security units (DCIS) aims to facilitate knowledge sharing across sectors. In the view of the society's sector-divided structure and how strongly the sector principle is embedded as part of applied governance, it is assumed that Denmark uses a single-hazard approach.

Multi-hazards are still assessed within the mindset of classifying hazards by source of origins, even though the interrelation is considered. The approach is logically related to the systems identification of the subsystem’s interdependencies. Chapter 8 represents the multi-hazard approach where the subsystems are identified based on their interrelations. The interrelations are defined horizontally in which coordination is a focal point and vertically for which interdependencies are identified.

6.3.3 All-Hazard Approach

According to the US Department of Homeland Security (DHS) (2011) all-hazards are defined as the environmental and manmade conditions that poses potential hazards to life safety, equipment loss, breakdown of infrastructure services, property damage or degradation of social, economic, or environmental functions [79]. OECD (2019) refers to the all-hazard approach as a method to address resources towards significant (known) risks and also to strengthen a country to deal with the known unknown risks by which OECD argues that mapping systems interdependencies are an initial way to do so [80]. OECD (2019) recommends an all-hazard approach to better prepare for the unexpected, which is assumed to be related to resilience. The method suggested by OECD consists of (i) Identification of most critical infrastructure based on dependency modelling and criticality assessment; (ii) Interdependency mapping; (iii) Addressing transboundary dimensions of critical infrastructure; (iv) Lifecycle approach; (v) Integration of the full emergency management cycle; and (vi) Risk-based and layered approach [73]. The approach relates to a somewhat whole-of system methodology that is strongly related to building a resilient system that is able to adapt to and comprehend disruptions. In this way the all-hazard method enables the country to develop a wide-ranging protection regardless of the threat. Canada has structured their governmental organisation with a centralised body at ministry level ensuring coordination across all federal departments and agencies responsible for national safety, so-called Public Safety Canada established in 2003**Invalid source specified.**.

The all-hazard approach appears to distinguish itself from multi-hazards and single-hazards as being a whole-of-system method focusing less on the subsystems and more on the protection of the whole system itself. However, the identified hazards are still classified by source of origins, even though the approach considers known and unknown threats. The method still promotes a causal relationship between source and derived consequences; though, the all-hazard approach is less focused on sectoral boundaries. In chapter 9, the all-hazard approach is logically associated with a systems identification concerned only with informational patterns within the Danish critical information infrastructure.

7 Single-Hazard Approach

Abbreviations

CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
DHA	Danish Health Authority
FSOR	Financial Sector Forum for Operational Robustness
HDPA	Health Data Protection Agency
MCEU	Ministry of Climate, Energy and Utilities
MD	Ministry of Defence
MF	Ministry of Finance
MH	Ministry of Health
MIBFA	Ministry of Industry, Business and Financial Affairs
TCHA	Transport, Construction and Housing Authority

Within the approach of single-hazard-single sector, the current chapter presents an identification of the individual subsystems. In the previous chapter the system is characterised by the individual subsystems. In the current chapter these subsystems are compared and evaluated in which policies and network structures are assessed.

The critical sectors are compiled in Figure 28, illustrating regulatory bodies, overall sectoral components and the general flow of information. It is assumed that information flow is (though not always) bidirectional, whereas for visualization purposes the arrows are replaced by lines.

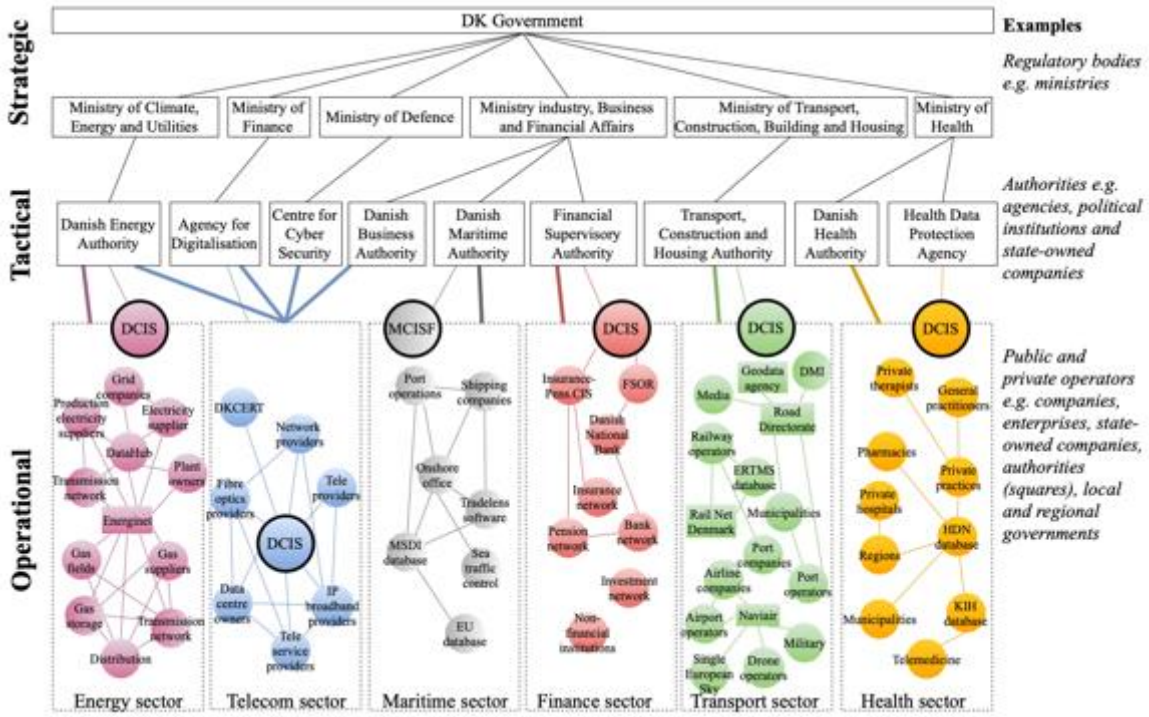

Figure 28: Conceptual illustration of information flow for the CII subsystems, where circles represent operators and rectangles represent authorities.

The sectoral structures are very similar presenting the government and ministries on a strategic level, the agencies on a tactical level and finally the operators on the operational level. In the operational level there are a few governmental bodies represented (illustrated as squares) and the

decentral cyber information security (DCIS) unit for the telecom sector is also placed at operational level compared to the rest of the DCIS-units, which are placed between tactical and operational level.

7.1 Comparison of Sectoral Cyber Strategies

The CII subsystems differs greatly in the overall perspective, though there are few similarities across, as the following sections covers (Table 13). The sectoral strategies are published in 2018-2019 framing a strategy over two to three years. The political level of publications indicate how cybersecurity is prioritised. The energy strategy is authored and published by the same regulatory ministry, whereas the health sector is prioritised at state, regional and local level. In the transport and financial sectors, the strategies are published by agencies, whereas the strategies for maritime and telecom are published and authored by the sectoral DCIS units.

Table 13: Comparison of the nature of core sectoral cyber strategies

	Telecom	**Maritime**	**Transport**	**Financial**	**Energy**	**Health**
Year of current	2018	2019	2019	2019	2019	2019
Author	Telecom actors	Decentralised Cyber Information Security unit	Transportation, Construction and Housing Authority	Financial Supervisory Authority	Ministry of Climate, Energy and Utilities	Ministry of Health, Local Government Denmark and Danish Regions
Publisher	Telecom business associations	Decentralised Cyber Information Security unit	Ministry of Transportation, Building and Housing	Ministry of Industry, Business and Financial Affairs	Ministry of Climate, Energy and Utilities	Ministry of Health, Local Government Denmark and Danish Regions
Length of report	14	11	43	20	24	55
Time horizon	2018-2021	2019-2022	2019-2021	2019-2021	2018-2021	2019-2022
Lead agency/body	Danish Energy Authority Danish Business Authority Agency of Digitisation Centre for Cyber Security	Danish Maritime Authority	Transportation, Construction and Housing Authority	Financial Supervisory Authority	Danish Energy Authority	Danish Health Authority
Regulative authority	Ministry of Climate, Energy and Utilities Ministry of Industry, Business and Financial Affairs Ministry of Finance Ministry of Defence	Ministry of Industry, Business and Financial Affairs	Ministry of Transportation, Building and Housing	Ministry of Industry, Business and Financial Affairs	Ministry of Climate, Energy and Utilities	Ministry of Health
Decentralised Cyber Information Security unit **members**	Telecom (private) actors	-	-	-	-	-
Decentralised Cyber Information Security unit **coordinator**	DKCERT (a part of DeiC)	Danish Maritime Authority	Transportation, Construction and Housing Authority	Financial Supervisory Authority	Danish Energy Authority	Health Data Protection Agency
Cooperation with private sector as primary actors	Yes	Yes	Partially	Yes	Partially	No
Cooperation with private sector as secondary actors	Yes	Yes	Yes	Yes	Yes	Yes

The coordinating unit for each sector is the DCIS unit. DCIS aims to facilitate knowledge sharing within each sector and cross-sectoral. The sectoral DCIS units for the financial, maritime, health, energy and transportation sectors are placed within an authority at strategic/tactical level, however telecom DCIS is placed at the operational level represented by private telecom operators. There appears to be an imbalance of horizontal coordination as well as telecom being the only private DCIS unit meant to collaborate with the public DCIS units represented by authorities. There may be an inequality in the public-private relationship, where the result may be to isolate the privately represented entity.

Based on the comparison of the critical information infrastructure protection (CIIP) policies (Table 13), the sectors differ in relation to how extensive the sectoral strategies are and how they are governed. The following points illuminate the main differences evaluated:

- Report lengths vary within the range of 11-55 pages
- Authors and publishers originate are at different governmental levels
    - Telecom is written by the private industry and published by the telecom associations (operational)
    - Transportation and financial are authored by agencies (tactical)
    - Energy is authored and published by the Ministry of Climate, Energy and Utilities (strategic)
    - Maritime is authored and published by the maritime DCIS (tactical)
    - Health is authored and published by the Ministry of Health, Local Government Denmark and Danish Regions (state, regional and local government) (strategic)
- The timespan for each strategy differs from two to three years
- Health sector differs from the rest as having the DCIS unit placed in the authority of Health Data Protection Agency (HDPA) except that the sectoral authority is identified as Danish Health Authority (DHA)
- Telecom sector differs from the rest as having the DCIS unit placed within the CII operators
- Telecom, finance and maritime are dominated by the private industry
- Health, energy and transportation are partly or not dominated by private industry

Table 13 highlights the main differences of the sectoral strategies, which indicates the political priority given to each sector. In addition, sectoral policies specify how each sector is governed. The telecom sector is highly self-governed, whereas the energy sector is governed from top political level (having the ministry publishing and authoring the strategy, as well as being the sectoral responsible). The maritime sector is governed by the DCIS unit, as the unit has authored and published the strategy as well as being placed within the Danish Maritime Authority as the leading body. Health is governed by and highly represented in state, regional and local governments.

Another finding made within the process of mapping the Danish CII system, is that it appears that the Ministry of Industry, Business and Financial Affairs (MIBFA) is responsible for both the financial, maritime and telecom sectors. Where MIBFA shares the responsibility of the telecom sector with the Ministry of Climate, Energy and Utilities (MCEU), Ministry of Finance (MF) and Ministry of Defence (MD) (Figure 29).

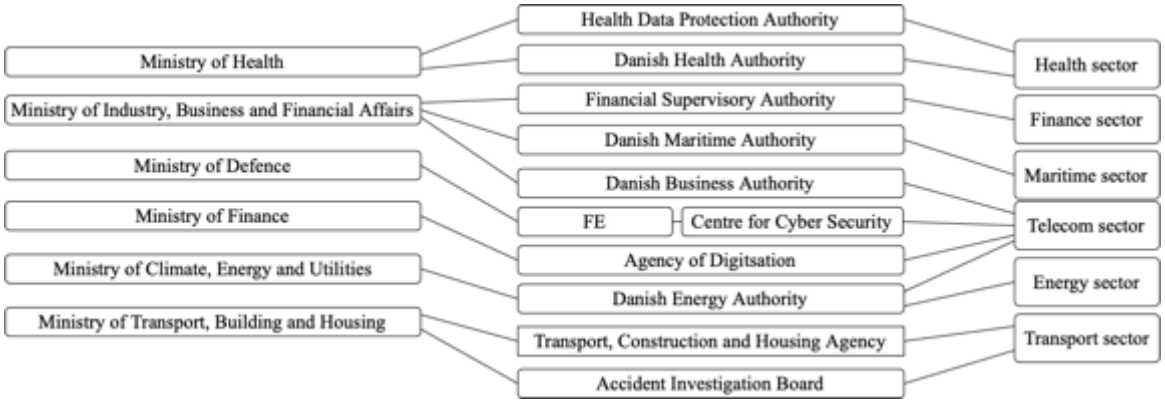

Figure 29: Visualisation of responsible authorities of the CII subsystems

Having multiple political bodies as responsible authorities for CII sectors may lead to a need of prioritising resource allocation. If more than one sector is impacted and require resources, the ministry needs to decide which sector that needs priority. On the other hand, adopting regulations in finance and maritime may be done with lack of collaborating with other ministries. In the telecom sector policies are made based on the collaboration of four ministries.

7.2 Network Intradependencies

Intradependencies refer to the internal dependencies of a subsystem. The network of information flow is categorised according to the components couplings within the sectors and the number of contact points to end-user. Intra-dependencies refer to the interrelation within a given subsystem. Contact points to end-user indicate the number of contacts an end-user i.e. citizen, company, CII subsystems etc. In a supply chain there may be few interfaces with customers as the operators are reliant to accommodate the customer with a certain product or service. In the case where there are multiple interfaces the network operators are less dependent on each other to provide the given service. In this context the number of interfaces relates to how interdependent the sectoral operators are named: dependent or independent.

Based on the typologies suggested by Truong et al. (2016) [81] i.e. centralised, decentralised and distributed networks, it is possible to determine the types of networks for the CII subsystems. As the name implies, a centralised network collects all information within a central operator, leaving the surrounding operators highly dependent on the centre. In a decentralised network there are more than one operator the majority depend on, and the dependencies may be visualised in a chain. In a distributed network the information flow is independently exchange among operators without having a centralized entity. The CII subsystems are classified based on their network typologies and end-user interfaces (Figure 30).

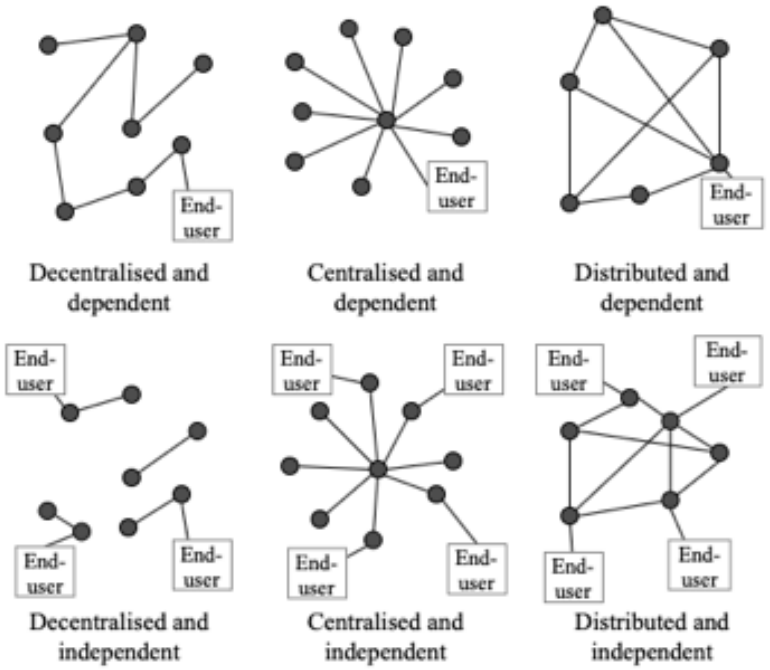

Figure 30: Different network typologies of information flow depending on intra-dependencies and contact to end-user

- **Telecom - Independent and distributed**
  - With a group of heterogeneous telecom operators many of which have contact to end-users, the subsystem is considered to be independent. The operators are distributed though they provide services to each other
- **Energy - Dependent and centralised**
  - The majority of operators rely on a centralised operator (i.e. Energinet) with only a few interfaces of end-users
- **Finance - Independent and decentralised**
  - The majority of operators have contact to end-users and share limited interrelation, though they follow similar procedures
- **Maritime - Dependent and distributed**
  - The operators are distributed as the majority depend on each other's services, though with only a few end-user interfaces
- **Transportation - Independent and centralised**
  - The assorted subsystems of transportation are individually centralised i.e. aviation is centralised by Naviair, railway by Railway Denmark and the road network by Road Directorate. All subsystems are characterised by having multiple end-user contacts and therefore operates independently
- **Healthcare - Independent and decentralised**
  - The health operators have multiple end-user contacts and furthermore related according to their data sharing collected by the Danish Health Network (DHN). Though, there is no connection in terms of decision-making

According to Truong et al. (2016), different network typologies pose different risks [81]. A centralised network requires less maintenance but is rather unstable since it depends on one central entity; therefore, a single disturbance can cause the system to break down. On the other hand, it is assumed that development and management of such a network is relatively easy, as the number of

links between the central operator and the rest of the network are limited. In the case of the Danish CII system, the energy and transportation sectors relate to this typology.

The decentralised network is moderately maintained and managed, as the system consists of autonomous units where there is no single point of failure (as the case with a centralised network); though, the units operate under the same framework [81]. This typology creates a heterogeneous system where each unit operates within the local context and not necessarily consistent with the rest of the system. The decentralised network poses a risk of failure from multiple points, which also results in a rather stable network as the intra-dependencies are limited. If a unit within the financial or health subsystem is disrupted the cascading effect would be limited to a few couplings in the individual subsystems, yet the incident can accumulate impacting other CII subsystems that the affected units are coupled to.

The telecom and maritime subsystems are classified as distributed networks, as they consist of inter-related operators similar to a chain of supply, however each operator provides a variety of services that are used for several operators within the mesh. The typical property behaviour is that the points of failure are considered limitless with the result of the system being very stable to disturbances. The mesh is characterised as a highly diverse network, where maintenance and management can be rather difficult. In the case of the maritime and telecom subsystems, the inter-relation among CII operators is somewhat dependent, which differs from the typical distribution network. Even though, the subsystems may be characterised as decentralised systems as well as distributed, in this context they are assumed to be the latter.

7.3 Summary

In the context of the single-hazard approach, the CII is characterised by its subsystems by which a comparison is made with an emphasis on the policies and network structures in each subsystem. The subsystems appear very different in terms of governmental organisation, governance approach and in operation.

Energy subsystem

The energy subsystem appears to be highly prioritised and closely governed, as the sector strategy is authored and published at ministerial level, as well as the operational subsystem is organised as a centralised network around a public operator that are closely connected to regulatory decisions. The Energy DCIS unit is placed within the sector authority in which the centralised energy operator is a member.

Telecom subsystem

The responsibility of the telecom subsystem is shared among four ministries. Some have responsibility in other CII subsystems. The subsystem is structured as a distributed network and is highly self-governed as the telecom operators themselves published and authored the sector policy. The DCIS unit is placed at operational level and consist of telecom operators.

Maritime subsystem

The maritime subsystem is identified as a distributed network of private operator with a few interfaces of end-user contacts. The sector policy is authored and published by the DCIS unit, which is placed at tactical level; however, with consideration of the short length of the report and the choice of author and publisher the subsystem appears to be less prioritised than e.g. energy.

Finance subsystem

The financial subsystem is a decentralised network of private operators with several interfaces with end-users. The DCIS unit is placed within the sector authority, though it operates closely with the operational and CII operator represented unit, Financial Sector Forum for Operational (FSOR). Finance, maritime and telecom share the same ministry as regulatory authority.

Health subsystem

The health subsystem is a decentralised network consisting of mostly public operators that has several end-user interfaces. The subsystem is prioritised at local, regional and state level as the author and publisher of the health policy is a collaboration of the three. The policy is the longest version of all sector strategies. Furthermore, the DCIS unit is placed within a data-specialized authority (DPHA), which is not the sector authority. This does not occur in the other subsystems.

Transportation subsystem

The transport subsystem is comprised of three centralised networks i.e. aviation, railway and roads. Due to lack of intra-dependencies the transport subsystem is characterised as a centralised network with multiple end-user interfaces. The sector is prioritised at a ministry level and consists of public authorities representing the central components within the sub-centralised network similar to the energy subsystem.

There are differences among the policies, the governance of the sectors and the sector responsibility, which show that the individual subsystems are to a certain extent self-governed at ministry level. Although, with a politically prioritized distribution initiated by state. In this view, the principle of sector responsibility becomes clear as the subsystems are not only political divided but also share a minimum of similarities.

8 Multi-Hazard Approach

Abbreviations

CFCS	Centre for Cyber Security
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
DCIS	Decentralised Cyber Information Security
DEMA	Danish Emergency Management Agency
DHA	Danish Health Authority
ENISA	European Network and Information Security Agency
FSOR	Financial Sector Forum for Operational
HDPA	Health Data Protection Agency
ICT	Information Communication Technology
IOT	Internet of Things
ISAC	Information Sharing and Analysis Centre
MCEU	Ministry of Climate, Energy and Utilities
MD	Ministry of Defence
MF	Ministry of Finance
MH	Ministry of Health
MIBFA	Ministry of Industry, Business and Financial Affairs
MTBH	Ministry of Transport, Building and Housing
PET	Danish Security and Intelligence Service

The current chapter evaluates the Danish Critical Information Infrastructure (CII) within the framework of a multi-hazard methodology.

The multi-hazard approach includes an assessment of multiple hazards and their inter-relation in order to prioritise certain hazards for the protection of a given system. As discussed in Chapter 6, the multi-hazard approach is characterised as being system-orientated and focused on the linear-connectivity among these systems. In the context of evaluating the governance of the Danish CII system the method of multi-hazards is logically interpreted as being comprised of a way to divide the system into subsystems and assess the interrelation among subsystems. The dependencies in the current chapter are assessed horizontally where the focus is on coordination, and vertically where the focus is on integration.

8.1 Horizontal Coordination

Horizontal coordination relates to the cohesiveness of sectoral operators and institutionalization of collaboration among authorities including public-private partnerships. For each subsystem, there is a decentralised cyber information security (DCIS) unit designated to facilitate preventive cyber activities and to coordinate among the involved parties, if a significant part of the sector is disrupted (Figure 31).

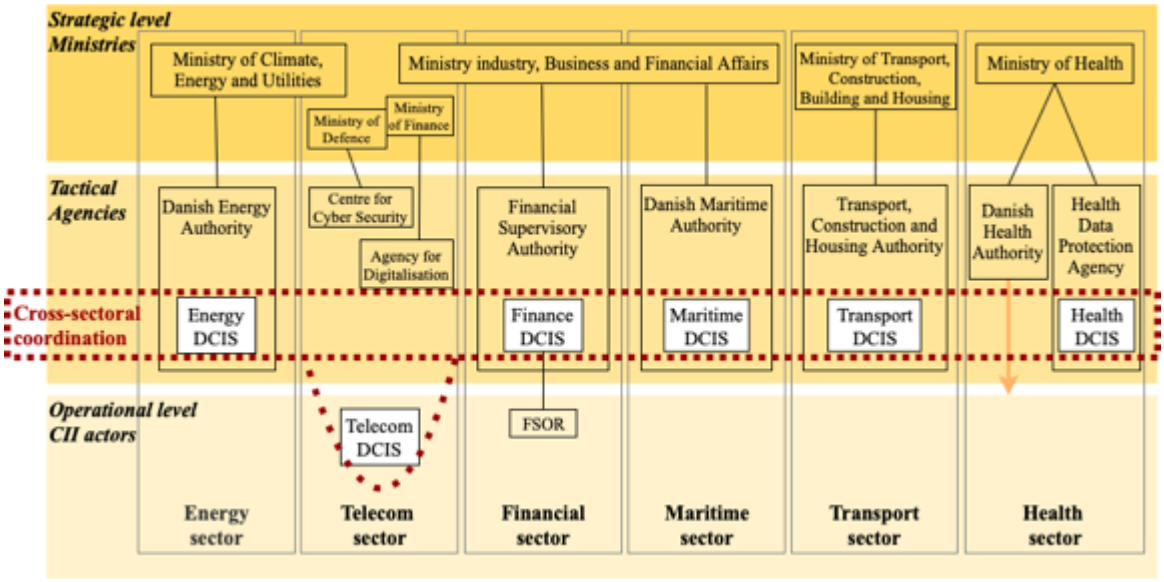

Figure 31: Illustration of governmental levels by which sector DCIS-units are illuminated.

The DCIS units are placed as the link between tactical and operational levels in order to allocate information among authorities and CII operators. However, the purpose of the DCIS units are to accommodate cross-sectoral coordination and knowledge sharing, by which may be challenging as the different DCIS units are not placed at similar levels (Figure 31). The telecom DCIS is placed at an operational level comprised of operational CII telecom operators, which differentiates from the rest of the sectoral specific DCIS units, that are placed at a more tactical level and represented by authorities. The financial DCIS unit is in close cooperation with the existing financial sector forum for operational Robustness (FSOR) unit which is occupied by financial private operators under the coordination of the Danish National bank, but the financial DCIS is still formally represented by an authority. Another issue relating to DCIS coordination is that the health DCIS unit is placed within the Health Data Protection Agency (HDPA), which in itself does not raise any particular concern. However, the fact that the DCIS unit is not located in the sectoral authority, as is the case for the remaining CII disregarding the telecom sector, may make interdisciplinary and internal sectoral coordination difficult. If the sector responsibility is assigned to the Danish Health Authority (DHA) but the coordinating unit is managed by DPHA, there can be a challenge in the division of who is in charge.

8.1.1 Public and Private Collaboration

The collaboration between the public and private sector is distinctly present in the Danish CII, whether it is among sector DCIS units, DCIS and the operational level or among operational CII operators. This particular relationship poses a few possible tensions: (i) Differences in economic preferences; and (ii) Distorted power relations. Duhamel et al. (2018) argue that the private and public sectors have different objectives and preferences on which to base their decisions [82]. According to Baezner & Cordey (2019), the economic perception differs between private and public operators. The public-private-partnership is about harmonizing operational logic of private for-profit understanding and public not-for-profit belief. Baezner & Cordey argue that an overall top-down management of this diverse relationship is difficult due to conflicting interests and the development of new technological knowledge and capacities [13]. A way to address this is adopted from the study done by Dunn-Cavelty & Suter (2009), where the placement of the DCIS units close-to-operation under the circumstances where the sector is highly privatised, has potential to be more

self-governed, which is applicable in the telecom and finance sectors. By having a government facilitating coordination, leaves the operators being more or less self-governed due to the high level of expertise which is found in the private industry. Despite the fact that Dunn-Cavelty & Suter recommend this self-governing approach, they also state that outsourcing vital functions to self-regulating private networks may compromise the security of CII and in that case should be avoided [83].

Another challenge related to public-private collaborations is how the political power is fragmented, having private operators being responsible for public activities and interests. Donahue & Zeckhauser (2006) use the concept of collaborative governance, describing the collaboration of public-private sector in the context of critical information infrastructure protection (CIIP). Their idea is based on shared discretion among partners, who are separated from contractual arrangements [84]. In a self-regulating CII, the state can give private operators authority. In the Danish context, this can be compared with Rail Net Denmark in the transport sector and Energinet in the energy sector, both of which are publicly owned companies though they operate as private. To some extent this transfer of authority is seen in the financial sector, where the private banks, pension companies and insurance companies have somewhat a responsibility similar to a public authority but still the regulatory responsibility belongs to the ministries. In the general literature on public-private partnerships there are common issues; unclear division of responsibilities and to what extent should the state control private operators. According to Dunn-Cavelty & Suter (2009) the population' expectations are not necessarily in line with the established policies, which may create a distorted relationship of trust between the population and CIIP operators [83].

8.1.1.1 Trust

Rajaonah (2017) argues that trust is the fundamental element in any system where sharing of information occurs [85]. OECD (2019) supports the importance of trust in public-private partnerships [73]. The European Union Agency for Network and Information Security (ENISA) provides a list of initiatives to build trust in public-private partnerships e.g. face-to-face meetings, joint exercises, thematic conferences etc. Though, ENISA does not clarify what trust is comprised of or how it may be measured [86].

There are examples on how different organisational structures may facilitate information sharing within the framework of CIIP. Australia formed a so-called Trusted Information Sharing Network for Critical Infrastructure Resilience in 2003, seeking to facilitate a trust-based relationship among all public and private operators with shared responsibility for critical infrastructure [87]. A similar approach is done by the Government of Canada, where the Critical Infrastructure Information Gateway functions in a similar way [88]. An alternative approach is done by the United States, establishing sector specific Information Sharing and Analysis Centres (ISACs) to facilitate information sharing within each sector [89]. At transnational level, the European Union's Critical Infrastructure Warning Information Network foster a trust-based connection among EU states and serves as an alert system as well [90]. In 2017, ENISA published a report concerning the European ISACs in which Denmark is mentioned to have none [91]. The Danish sectoral DCIS units are formed in 2019, which may be a Danish alternative to ISAC. The DCIS units share similarities with ISACs by facilitating information sharing, though the DCIS units do not constitute a database, as the ISACs does [89].

8.2 Vertical Integration

Within the concept of multi-scale governance, vertical integration relates to the dispersion of political authority at multiple levels with an emphasis on hierarchical decision-making processes between strategic and operational level. The following sections illuminate *primary* dependencies among the subsystems' operational levels. In addition, the *secondary* dependencies are studied based on the relation to suppliers and manufacturers of internet-of-things. The chapter is then finalised by evaluating the primary dependencies by three examples of cascading events. The links between sectors are established based on the definite sectoral purpose comprising both structural and informational dependencies e.g. the purpose of the financial sector is to facilitate financial transactions, insurance, pensions, loans and investments.

8.2.1 Subsystems Dependencies

Creating an insight into approximate dependencies is assumed to highlight the complexity of the CII and at the same time support a scenario and hazard identification. This insight can better assess the behaviour of the system in the event of a system disruption. To determine sector dependencies, a normative scale describes the level of dependency existing among subsystem levels as:

(0) None
(1) Low
(2) Medium
(3) High

In order to have a metric that applies for the in- and output of all sectors, a time-based scale shows the level of dependency there is among the sectors intuitively. The matrix of dependencies is developed on a qualitative basis, where the assumptions of such dependencies are highly subjective; however, it is believed to serve a purpose of illustrating the imbalance among sector dependencies.

Time	Months-years	Days-months	Hours-days	Minutes-hours
Dependency	None	Low	Medium	High
Value	0	1	2	3

Figure 32: Scale of dependency constructed as a time-based metric

The time-based metric is understood as the time it takes a system to be affected by another, which illustrates the dependency level i.e. high, medium or low. For example, if system A is reliant on the input from system B on a minute to hourly basis the dependency is considered *high*, which is given the value 3 (Figure 32). On the other hand, if system B is reliant on the input from system A on a daily to monthly basis the dependency is assumed to be *medium*, which is given a value of two. In such case, there is an imbalance in the interdependency between the two systems, where system A is more reliant on system B than vice versa. The same applies for the *low*-dependency which is assigned a value of one. In addition, the *none*-dependency is assigned to systems that rely on input on a monthly to yearly basis, which is assigned a value of zero.

Figure 33 is developed as a matrix, where the horizontal axis represents inputs and the vertical axis represents outputs. In each cell, a brief argument is included to support the classification of the subsystem dependency e.g. the input from transport is important for the maritime subsystem, as the maritime services rely on fully functioning roads, railways and ports to be able to perform shipping. It is assumed that the maritime subsystem is still functioning if the services from the transportation subsystem are disrupted in hours or days, yet after some hours or days the maritime subsystem would also be affected. Hence, the dependency is assumed to be medium. Another example is the

relationship between telecom and healthcare, while healthcare relies on the services of telecom in the timescale of minutes-hours (high dependency), telecom do not rely on the services provided by health, by which the dependency is *none*.

Sector dependencies	Input Finance	Input Transport	Input Energy	Input Telecom	Input Maritime	Input Health	Output
Output Finance	Low (1) Financial transfers occur but on a monthly basis	None (0) The finance sector depends insignificant on the transport sector	High (3) Digital transfers, facilities and customer contact require electricity	High (3) Transfers and facilities need telecom services	None (0) Finance is not reliant on maritime	Low (1) Finance require personale data and health information on a regular basis	8
Output Transport	High (3) Transport is reliant on sales and financial transfer B2B and B2C	Medium (2) Each subsector is intra-dependent with a few dependencies between	High (3) Means of transport and ICT-dependent vehicles require electricity	High (3) Means of transport need internet, radio and GPS	Low (1) Cargo transport is connected to maritime on a daily basis	None (0) Transport is not reliant on health services	12
Output Energy	Medium (2) Energy relies on financial services as energy is a commodity	None (0) Energy supply does not rely on transport services	High (3) Chain of energy supply is self-dependent	High (3) The chain of energy services and supplies depend on ICT systems	None (0) Energy supply does not rely on maritime services	None (0) Energy supply does not rely on health services	8
Output Telecom	Medium (2) Financial services are needed for B2C and B2B	None (0) Tele services does not rely directly on transport	High (3) Tele actors depend on a constant energy supply actors e.g. data centre	High (3) Tele actors depend on tele actors	None (0) Tele services does not rely on maritime services	None (0) Tele services does not rely on health services	8
Output Maritime	Medium (2) Financial services are needed for B2C and B2B	Medium (2) Cargo & people rely on ports, roads and rails when being shipped	High (3) Shipping, ICT-systems and GPS require constant energy supply	High (3) Shipping, ICT-systems and GPS require telecom services	High (3) Supply chain of maritime is intra-dependent	None (0) Maritime does not rely on health services	13
Output Health	Low (1) Financial transfers occur but on a monthly-yearly basis	Medium (2) Patient transport and ambulances need ICT-systems	High (3) Healthcare depends on energy for light, surgeries, water etc.	High (3) Health IOT-devices and ICT-systems are dominating the sector	None (0) Healthcare does not require healthcare services	Low (1) Healthcare is intra-datadependent yet can function over a long period without	10
Input	11	6	18	18	4	2	

Figure 33: Matrix of in- and output of sectoral dependencies including numerical values and the sum of in- and output for each subsystem

The matrix of in- and output dependencies shows that energy and telecom are vertically the highest dependent subsystem in CII. On the horizontal axis the transportation subsystem is not only highly reliant on telecom and energy, but also on the supply from finance. Besides telecom and energy, maritime is the only subsystem that shows a high dependency within its own sector. The subsystems that the rest rely a minimum on are the health and maritime services; however, it appears that they rely relatively on the services from the other subsystems.

Table 14 illustrates the imbalance between in- and output that apply for all critical sectors. The sectors that rely more on others than the others rely on them (low input and high output) are health, maritime and transport, whereas sectors that rely less on others than the others rely on them (high input and low output) are telecom, finance and energy. In general, all sectors show dependencies within the overall system of CII, but there is a difference in the level of in- and output dependencies. While energy and telecom have an input sum of 18, compared to health having a sum of two shows that energy and telecom are the most reliant sectors and health is the least reliant sector in CII (Table 14). The sectors that rely mostly on others, are the maritime and transport sector, where maritime scores 13 and transport scores 12 in output dependency.

Table 14: Inputs, outputs and percentage differences

		Input						
		Finance	**Transport**	**Energy**	**Telecom**	**Maritime**	**Health**	Total
Output	**Finance**	1	0	3	3	0	1	*8*
	Transport	3	2	3	3	1	0	*12*
	Energy	2	0	3	3	0	0	*8*
	Telecom	2	0	3	3	0	0	*8*
	Maritime	2	2	3	3	3	0	*13*
	Health	1	2	3	3	0	1	*10*
	Total	*11*	*6*	*18*	*18*	*4*	*2*	

	Finance	**Transport**	**Energy**	**Telecom**	**Maritime**	**Health**
Output	8	12	8	8	13	10
Input	11	6	18	18	4	2
Difference	3	6	10	10	9	8
%difference	27%	50%	56%	56%	69%	80%

The score for energy and telecom and to some extend finance, indicates that any disruption in one of these subsystems may affect the entire CII system. The lowest score of input belongs to health. In the event of a disrupted health sector, the remaining sectors would probably not be greatly affected. Instead, the health system is most-likely affected if any other sector is disrupted, scoring an output sum of 10. Based on the results, health and the maritime are isolated sectors with an input score of two and four. When identifying the system based on the direct dependencies, it appears that a disruption of health and maritime and partly transportation will most-likely not disrupt the entire system. On the other hand, a disruption of finance, energy or telecom may disrupt the full system. The directional interdependencies show in- and outputs (Figure 34), where the left image includes all dependencies as clarified in Figure 33, whereas the right image disregards the none-relations (green arrows) and includes in- and outputs for each subsystem.

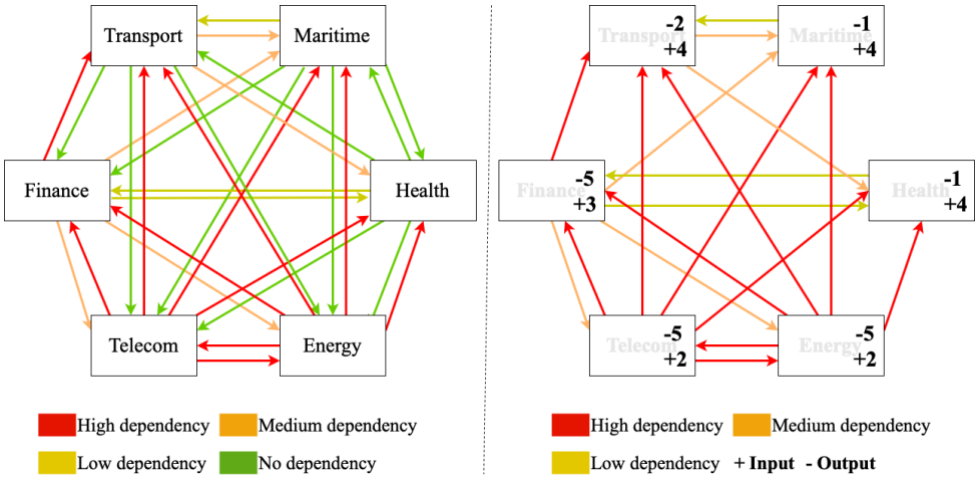

Figure 34: Illustration of subsystems dependencies, where in- and outputs are illuminated (colours correlates to the legend used in Figure 32)

The dependencies are assessed with a rather conceptual approach in order to illustrate the imbalance when characterising the system based on the allocated critical operators. This illustration elucidates how some subsystems pose a greater risk for a full CII breakdown than others. This is no surprise, as the bibliometric review in Chapter 3 discusses how energy and telecom are dominating in one part of the network visualisation of critical infrastructure (CI).

8.2.2 Dependencies and Cascading Effects

Within the approach of multi-hazards, the current section introduces a system identification based on how certain points of disruption accumulate among the subsystems.

In order to illustrate the dependencies in the CII system it is necessary to use a method applicable to all of the subsystems. The method applied to illustrate the dependencies in the diagrams is exemplified in Figure 35. Based on the assumptions made in Chapter 7 and the dependencies determined in Chapter 8, the dependencies are illustrated by multiple in- and output arrows:

- High dependency is illustrated by three arrows
- Medium dependency is illustrated by two arrows
- Low dependency is illustrated by one arrow

The input from the energy to the financial subsystem is defined as high and therefore there are three arrows going from the energy to the financial sector (marked with purple numbers: 1, 2 and 3 in Figure 35). All the arrows derive from the central energy operator, as this is the only component having end-user contact.

The input from the financial to the energy subsystem is defined as medium which are shown by two arrows (marked with red number: 1 and 2). As the financial system is comprised by several end-user contacts the input from the financial component may derive from multiple operators.

All of the subsystems' components can receive inputs from other operators (Figure 35).

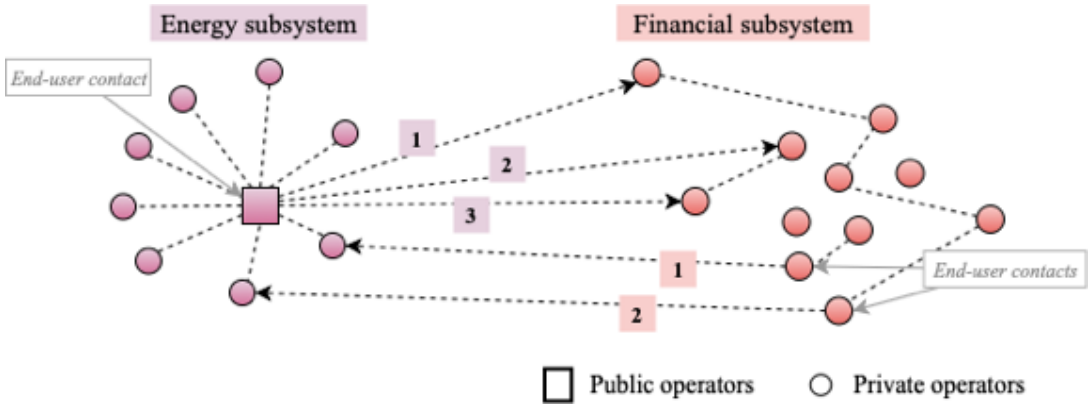

Figure 35: Illustration of the dependencies exemplified, where input from energy derives from the central unit and input from financial subsystem derives from decentralised units

In order to illustrate the cascading effects, the three most dependent subsystems are isolated and used as examples. The three subsystems: energy, telecom and finance are illustrated based on their characterisation and network typologies recognised in Chapter 7.2:

- Telecom sector: Independent and distributed network
- Energy sector: Dependent and centralised network
- Finance sector: Independent and decentralised network

The network is constructed as having the "end-user"-point of contact replaced with dependencies to the other subsystems. This means that the energy subsystem is a distributed dependent network and has one end-user contact, which is considered as the input (of energy) to finance and telecom. The financial and telecom subsystems are independent and have multiple points of output contacts. Figure 36 is illustrated by the dependency value being equal to the number of arrows, that is: (i)

High dependency has three arrows; (ii) *Medium* dependency has two arrows; and (iii) *Low* dependency has one arrow.

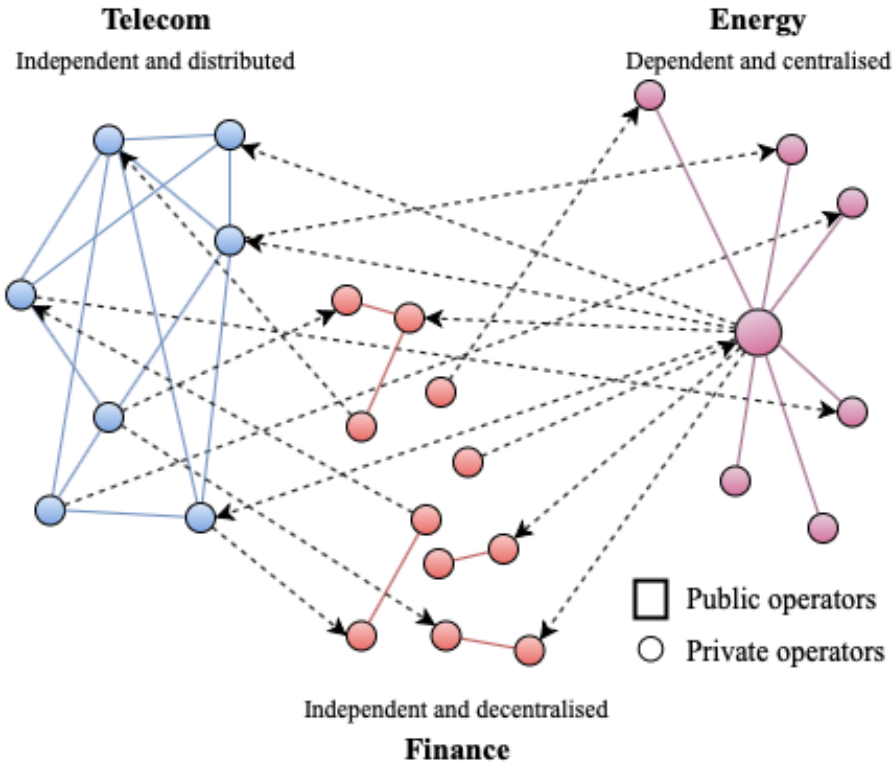

Figure 36: Subsystems dependencies represent: (i) telecom (distributed network with multiple end-user contacts); (ii) finance (decentralised network with multiple end-user contacts); and (iii) energy (centralised network with one end-user contact). Lines with no arrows illustrate bidirectional intra-dependencies, whereas the dotted arrows show the dependencies among the subsystems.

In case of a disruption, the distributed network represented by the telecom subsystem is rather stable due to its many operators but has various end-user contacts which can direct the disruption toward other subsystems. The financial subsystem is a decentralised system with limited internal interactions that poses a minimum of risk of enhancing the cascading disruption internally. However, in the centralised energy subsystem a disruption that affects the central operator may disturb the whole energy subsystem. Figure 36 is used as a basic to present three different conceptual cascading events, where the trigger is respectively initiated at each subsystem (Figure 37, Figure 38 and Figure 39).

Information flow can be directed from one decision maker to another and it can be bidirected called interdependent. Rinaldi et al. (2001) define dependencies as linkages among systems, where the condition of one system influences the other. When the relationship is bidirectional the condition of each system influences each other [7]. The weight of dependency among the systems are not necessarily equal as evaluated in Chapter 8.2.1.

It is conceivable that if the CII system is disrupted the causal effect (1st order, 2nd order, 3rd order etc.) occurs in multiple layers e.g. physical, cyber, geographically etc. In the context of the information infrastructure the actual type of impact is considered irrelevant. The aspect that is of importance is the information flow. The cause can occur in all layers and the effect will probably not be singular but is expected to disrupt the system in different directions. System failures can occur as either cascading events, escalating events and as common cause, where several systems

are disrupted by the same trigger [7]. In the subsequent cases, the systems dependencies of cascading effects are conceptualised illustrated to underpin the complexity of the system disregarding dependencies suppliers and sub-suppliers create.

The reaction upon systems interdependencies can create loops of reciprocal effect, where the state of component A can disrupt component B, which can cause component A to fail [92]. However, the cascading effect can cause new cascading reactions, which are especially challenging in the restoration phase.

A disruption in the energy subsystem (1st order), may lead to a full system disruption. By using a causal relation impacting the system by 4th order effects, Figure 37 shows how a nearly full system disruption may occur disregarding where the disruption initiated in the energy subsystem. The 2nd order impact disrupts the centralised unit in the energy subsystem, which leads to the 3rd order impact affecting all the energy operators. By the 3rd impact the finance and telecom subsystems are also affected. The 4th impact disrupts most of the telecom subsystem, and some in the financial subsystem. The 4th order creates loops of reciprocal effect within the energy subsystem.

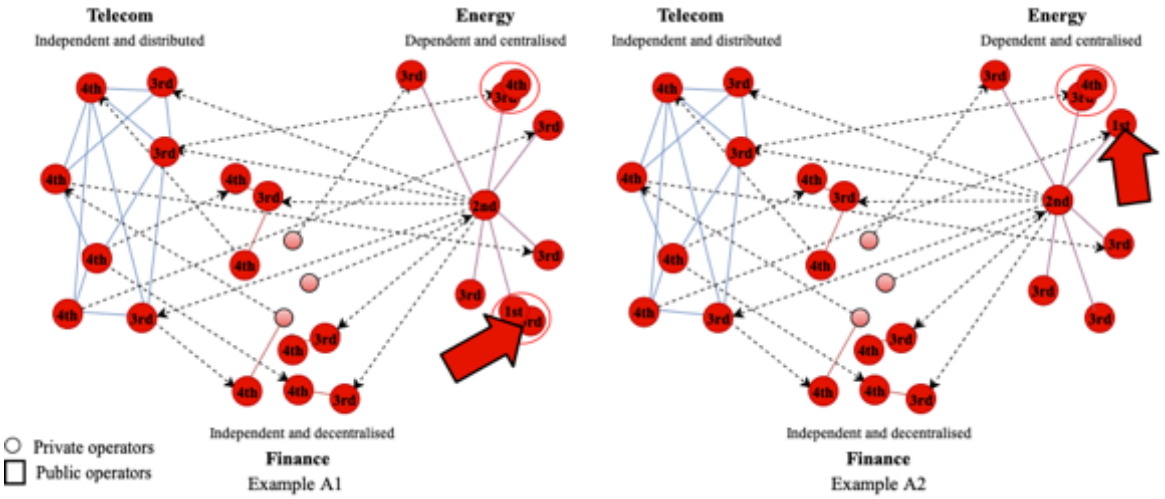

Figure 37: Two examples of a disrupted energy sector causing accumulated effects up until 4th order impact

The two examples in Figure 38 are highly similar. The 2nd impact disturbs the central energy component. Telecom and energy are highly intraconnected subsystems for which they are affected by the cascading effects, whereas the financial subsystem has limited intra-couplings and therefore is slightly less affected. Example B1 in Figure 38 shows almost a full disruption including multiple loops of reciprocal effects initiated in the telecom subsystem. Example B2 shows a partial system disruption of finance and energy with less loops of impact.

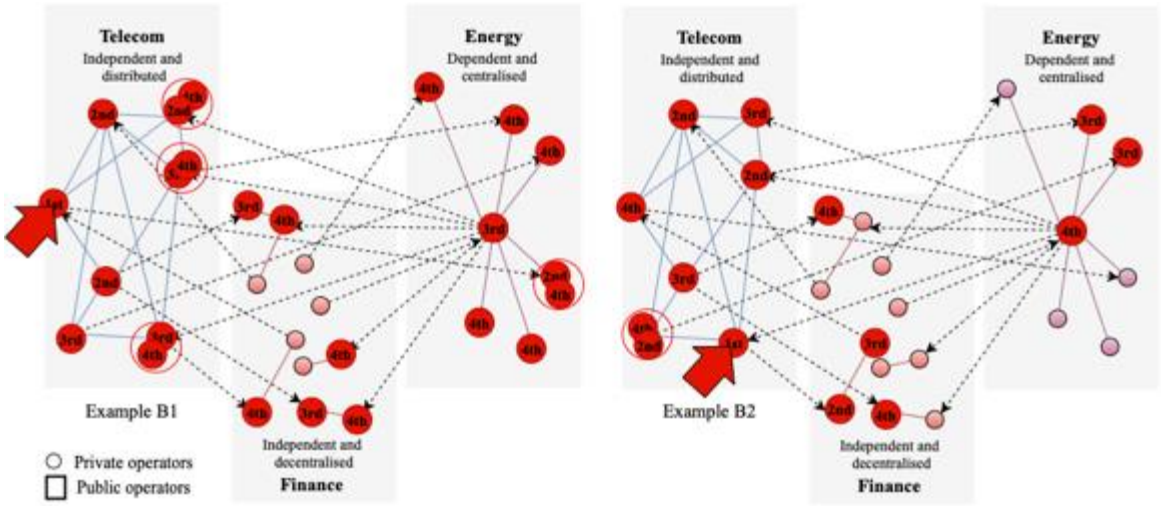

Figure 38: Two examples of a disrupted telecom subsystem causing accumulated effects up until 4th order impact

Example C1 shows a limited disruption initiating in finance (Figure 39); however, in example C2 the 1st order impact is at a component by which services are important of the central energy component. Compared to example C1, example C2 is close to a full system breakdown, as the central energy component is disturbed in the second impact. This results in the entire energy subsystem being disrupted by the 3rd impact including large parts of telecom and finance. By the 4th order impact the system is near to a full breakdown.

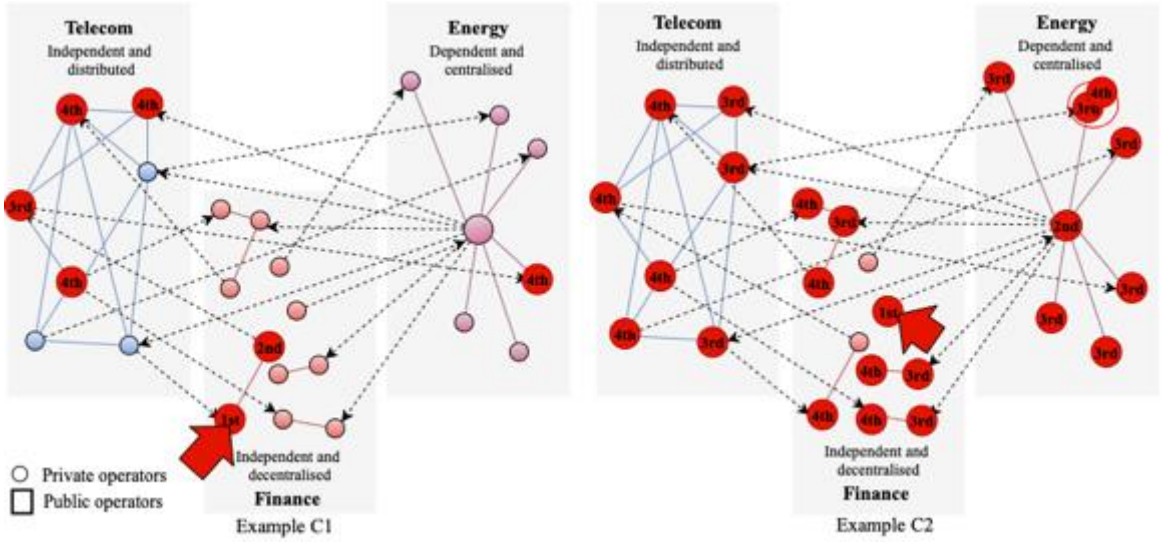

Figure 39: Two examples of a disrupted financial subsystem causing accumulated effects up until 4th order impact

Based on the six examples of causal cascading impacts the concept of the systems interdependencies are shown, with the result of a quite fast accumulating event occurring with a minimum of couplings. The cases intend to appear with a minimum of linkages among subsystems and therefore disregard couplings to the non-critical infrastructure and society. Surely, the cascading events may occur in different time scales and the severity may change, where the contextual environment, security measures and specific responses surely affect the chain of events. In addition, there may also be barriers to prevent certain outcomes and informational transfers. However, the six rather simple presented conceptual cases illuminate the complexity of CIIP management and governance.

In addition, there is not necessarily a linearity in the cascading incidents. The response may enhance or decrease the severity and even directing the disruption in an unpredicted direction.

Ouyang (2014) argues that studies on CI mainly focus on parts instead of the whole system. Academia has drawn special attention to the subsystems of energy, water, gas and communication, whereas financial, commercial and governmental subsystems receives less attention [93]. According to Kammouh and Cimellaro (2019) the energy sector is considered as one of the most critical infrastructures because it is interdependent with all the other sectors [94]. It may make sense to pay attention to the subsystems that pose the greatest risk of creating cascading disruptions; though the subsequent section illuminates a few arguments why a whole-of systems approach is appropriate with consideration of secondary dependencies.

8.2.3 Secondary Dependencies

The characterization of criticality levels as evaluated in the previous section, is seen in the early stages of deciding what constitutes the critical infrastructure system. Most global, transatlantic and regional international organisations have developed policies to accommodate cyber-attacks against critical information infrastructure e.g. EU, NATO, UN and OECD, where they recommend (and some require) that nations define their most critical infrastructure by which strategies and actions should be taken to secure these systems. As an example, the OECD (2019) recommends that a general definition in all countries benefits a transnational cooperation and strengthen the security of the transnational network [73]. The NIS Directive (2016) require all EU States to clarify their critical infrastructure through certain strategies and actions [6].

By deciding what constitutes critical infrastructure implies that it has priority over something that is secondary. The Ministry of Finance (2018) defined six subsystems as constituting the primary critical infrastructure, for which six specific strategies are developed. As previously mentioned, the water supply system is not defined as critical due to its limited use of information communication technology (ICT) [11]. The same applies for food supply, safety, governmental services, environment and climate etc. (see Chapter 1). In addition, the Centre for Cyber Security (CFCS) has assigned telecommunications as being the most critical infrastructure in Denmark [11].

The obvious benefit of prioritising levels of criticality is, to allocate resources to secure and protect the absolute vital services and assets. By doing so there is a possibility that the down-prioritised infrastructure systems are neglected. When setting the system boundaries at national level instead, the CII becomes a subsystem of the system of society, which results in other subsystems appearing. The approach of securing the most critical asset makes sense if the asset is isolated and not dependent on services from other parts of the system. The single- and multi-hazard approaches are therefore inappropriate when dealing with a complex system as the case with the Danish CII.

Although there has been discrepancies with the current definition of critical infrastructure (Chapter 1), Denmark prioritizes six critical subsystems, of which telecom is the most critical [11]. To choose a certain subsystem as being critical is a political priority that indicates what is considered primary and secondary infrastructure that most-likely has an impact on what best practice and academic research prioritize. CII is usually addressed by evaluating one or a few (most critical) parts of the CII and assess boundaries and dependencies with the rest of CII, with a more or less causal method of choice; as argued by Ouyang (2014) energy and telecom are mostly addressed [93]. Dunn & Wigert (2004) argue that it is uncommon by most nations to identify the CII as a subsystem within

an overall system [95], though the interdependencies between the critical and non-critical systems seems appropriate to do so. Figure 40 illustrates the CII as a subsystem within a system.

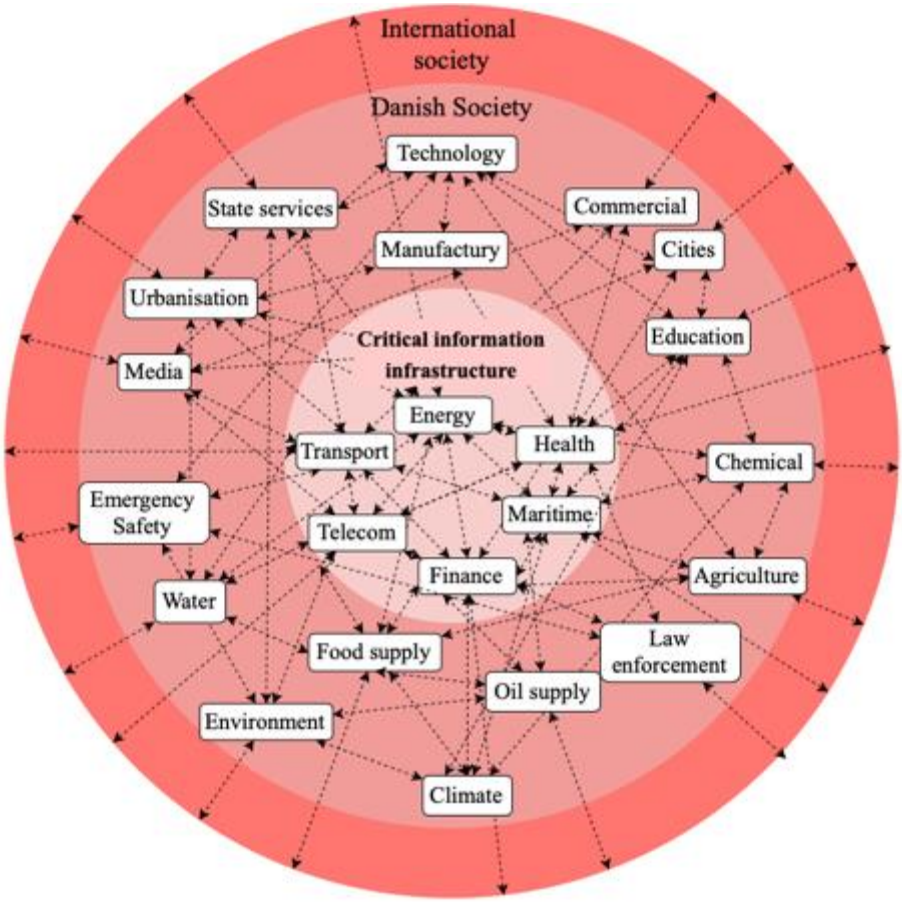

Figure 40: Illustration of the critical information infrastructure as a subsystem of the societal system as a part of the international system

The CII is a system highly integrated with society at a national and international context. When isolating the CII system (Figure 40) it merely serves an artificial purpose assumingly with a financial and political interest. The information flow ignores societal boundaries and governmental structures and if the focus is only on protection the CII system, the "rest" will most-likely be so undermined that the CII may terminate due to the systems interdependencies.

8.2.3.1 IT Outsourcing

According to Statistics Denmark (2016), more than half of the private sector outsource their IT services to other companies (referred to as suppliers) [96]. The practice is quite common in the public sector as well according to the Digitalisation Agency [32]. It is also possible for suppliers to further outsource their IT services to other IT hosting companies (referred to as sub-suppliers). This may leave a chain of IT contractors responsible for the security of the clients' IT systems, by which other clients are dependent on and connected to (Figure 41)

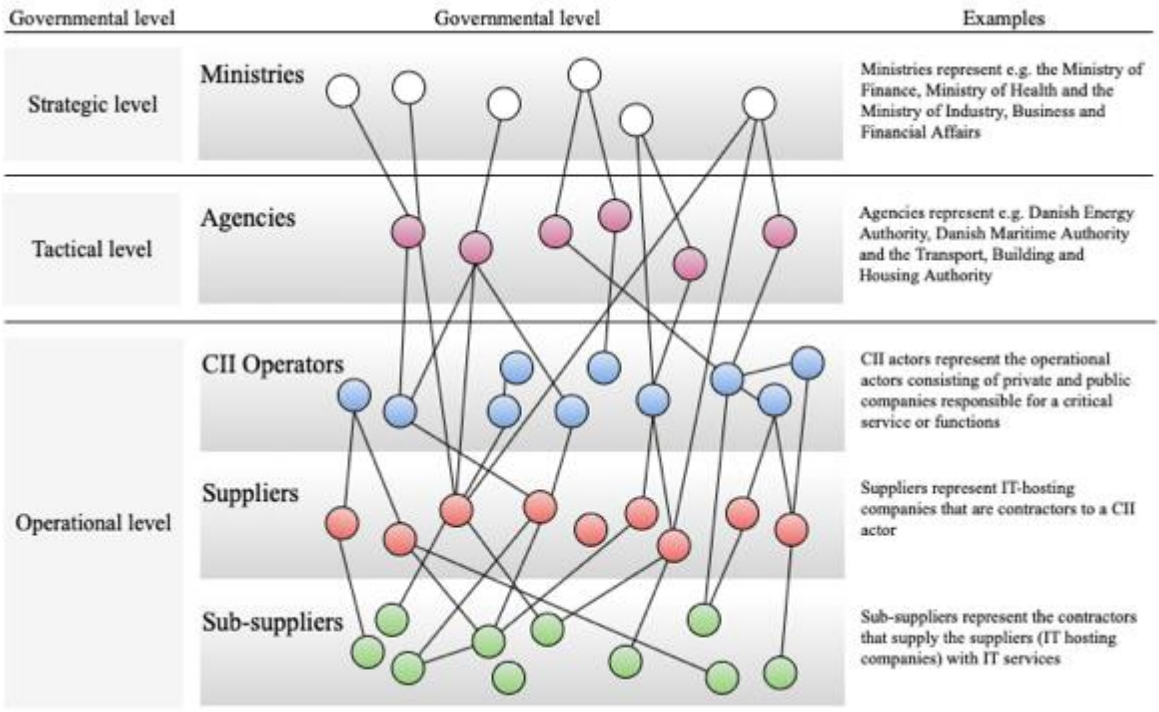

Figure 41: Illustration of the systems dependencies on IT-systems suppliers

There is a responsibility issue in relation to the chain of IT suppliers, by which the Danish Executive Order on Outsourcing states that the responsibility of the outsourced task rests on the client, in this case the CII operator [97]. This may appear peculiar; however, the partnerships are formalised in contracts and the legislation merely highlights the importance of integrating certain matters. Based on this regulation the contractual relation is important and also highlighted by CFCS [98] that emphasizes the importance of formalised communication and collaboration among business partners.

In relation to cyber and information systems comes the risk of transferring viruses or malware, where the transfer can occur along the chain of IT suppliers and finally disturb the CII system. There are several companies that specialize in IT solutions and they have multiple clients. This ends up with the IT suppliers being informational hubs that, if compromised, can be detrimental to the CII system. There have been cases where breaches of the suppliers' IT systems have compromised the client's [98], which only underline the hazard IT suppliers pose.

8.2.3.2 Internet of Things

Another secondary dependency rises on behalf of the manufacturers from the technologies that are connected to the internet, the so-called internet of things (IoT). In the coming years, the society may be affected by the growing popularity of IoT devices. According to CFCS (2019), IoT manufacturers prioritize functionality and not necessarily security. Therefore, the items can pose a risk of different cyber-attacks e.g. IoT devices can be integrated into bot-networks and used for DDoS attacks (Distributed Denial of Service-attacks) [99].

The European NIS directive (2016) requires a national recognition of CII operators; though, there is no such demand on identifying IT suppliers nor IT sup-suppliers. Instead, the Directive phrases that suppliers have a duty to notify the national cyber authority i.e. CFCS in the event of a significant security breach [6]. However, this requirement comes with a challenge, when the landscape of suppliers and sub-suppliers is enormous and dynamic. There may be suppliers and sub-suppliers

including IoT-manufacturers unaware of their potential critical role and unaware of their responsibility of informing the CFCS in case of an IT breach.

8.2.4 Inconsistency in the Distribution of Responsibility

There are three discrepancies found in the system identification, namely: Selection of CII subsystems, Maritime responsibility authority and the division of responsibilities between PET and CFCS.

First, the following Danish emergency authorities: (i) Danish Security and Intelligence Service (PET); (ii) Danish Emergency Management Agency (DEMA); and (iii) Centre for Cyber Security (CFCS) each identify the critical infrastructure sectors differently (Chapter 1). Inconsistency on top political level may lead to disorder in responsibility division on the tactical and operational levels and who are considered CII operators. The responsibility of identifying the CII operators as per requirement of NIS Directive (2016) is imposed to the sector authorities according to the national cyber strategy (2018) [11]. When the critical subsystems are defined with inconsistency it may influence the governance of such responsibility vertically in the system, resulting in uncertainty among CII operators' role. This study acknowledges that the Danish CII consists of six subsystems identified by the Ministry of Finance (2018). Though, the inconsistency the three authorities i.e. DEMA, PET and MF presents leaves a strategic framework that is unclear to the tactical and operational actors. The national cyber information strategy (2018) gave the responsibility of defining critical assets and operators to the individual ministries for the six CII sectors. Still, such a list is nowhere to be found. There is very little transparency in the governance planning of the Danish CIIP. This leaves the actors at operational level with very little guidance when navigating in what their role is and how to allocate specific resources to follow the national strategy.

Second, in the Danish version of the National Cyber Information strategy (2018), the assigned coordinator for the maritime subsystem is the Ministry of Finance, whereas in the English version the authority assigned is the Ministry of Industry, Business and Business Affairs (MIBFA). The English version is coherent with the maritime sector strategy, where the authority is given to the Financial Supervisory Agency, which is an agency under MIBFA [61]. It is most-likely a minor mistake, though the error supports an even less transparent structure of responsibilities.

Third, there are discrepancies in what is formalized responsibility and how it is operationalized between PET and CFCS. PET is the security authority prescribed to consult and assist private and public operators with information security issues with a focus on the human factor and physical security. CFCS is the authority on information and communication technology (ICT) security and is responsible for preventive and mitigating tasks including advisory services. The differences are phrased as CFCS is tasked with providing support, monitoring and guidance on technical challenges, of which PET is responsible for advising on CII management. However, this division is unclear to see when CFCS is the main CII support and authority as CFCS is assisting the leading authority in national and sectoral cyber security strategies and threat assessments. In addition, CFCS has published guides, threat assessments and investigative reports that are of a lesser technical nature and more concerned with CII management even though it is prescribed to be the responsibility of PET. The reports published by PET involve terrorism and radicalization and less about CII and information security [11]. Each authority shows a different concern through their publications. While PET shows a focus on non-related informational terrorism and radicalisation, CFCS is more concerned with information security. This implies that PET has a much smaller responsibility than prescribed in the national strategy, whereas CFCS has a much more central role.

Disagreements at political level may be rooted at tactical and operational level, leaving CII operators and authorities self-governing without a common understanding and direction. This may have consequences for the identification of CII operators including suppliers and sub-suppliers, which results in high level of uncertainty on responsibility and *who-does-what* in case of an emergency. Understanding and recognizing the complexity and interdependence that exists in the CII system and one's own role in this system is essential to being able to mitigate, prevent, prepare and respond to any systems disruption.

8.3 Summary

The current chapter has illuminated some issues relating to horizontal and vertical dependencies in the Danish CII system. First, the horizontal coordination is analysed with consideration of, the DCIS unit and the private-public partnerships that are dominating the CII system. The majority of the sector DCIS units are formed within an authority, usually in the authority that is responsible for the given sector. This does not apply for the telecom and health sector, where telecom DCIS is represented at operational level as well as it consists of private CII operators. The health DCIS unit is represented at authority level although not by the authority responsible for the health sector. In the analysis of the horizontal coordination, public-private partnerships are discussed, as the Danish CII system is largely characterized by the private industry. It is seen that in addition to the contractual formalities, trust is an essential factor that is facilitated in other countries such as the United States, Canada and Australia through a coordinating unit that enables information sharing within the applicable sector. The purpose of DCIS is to coordinate among sectors and internally in the current sector. Although the DCIS groups have similarities among the ISACs, there is no indication that DCIS aims to build trust or facilitate information sharing. It seems that the DCIS groups aim to disseminate regulations and policies from authorities to operators, in such a way where they represent a kind of ambassadors for the sector strategy. In this way, they support a vertical information flow to facilitate governance.

The vertical integration has been analysed by evaluating subsystems dependencies. Based on a qualitatively weighed matrix of in- and output dependencies, the result is that subsystems are not equally dependent on each other. While the CII system relies most on the services provided by energy and telecom, health and maritime services are the least important. It appears that there is an inequivalent relation between input and output for the CII subsystems. The subsystems that depend less on the services from the overall CII is energy, telecom and finance, whereas health, transport and maritime services depend highly on the services provided by the first three. It can therefore be concluded that there is a tendency that the subsystems that are most reliant on the CII system, also are the subsystems on which the CII system is least dependent on. The CII system is sort of divided into two parts: the most critical and the least critical subsystems.

The CII subsystems interdependencies of energy, telecom and finance are assessed based on a conceptual study of accumulated events of four impacts. By using the network typologies classified in Chapter 7 and the subsystems dependencies determined in Chapter 8.2.1 it is possible to illustrate a causal disruption in all of the three subsystems. Based on the results, the energy subsystem appear vulnerable to disturbance due to its network structure, where the central energy component poses a risk of transferring the undesirable incident to the connecting energy operators. The telecom subsystem is more stable, though in most of the examples the entire system ends up being disrupted. Finance is structured as a decentralised network with limited intra-dependencies, which is shown

to be less disrupted in all examples. Having the two most reliant subsystems being the most vulnerable due to the way they are structured indicate the entire CII system being similar vulnerable.

The energy and telecom are classified as the primary CII subsystems and leaves a few challenges. By prioritizing a subsystem over others based on their immediate direct dependencies may pose a risk of neglecting the secondary dependencies. Based on the evaluation of some secondary threats to CII breakdown the chapter introduces:

- IT suppliers can pose a threat to disrupt multiple CII subsystems as they are identified as potential informational hubs
- Internet-of-things (IoT) are embedded in the critical and non-critical infrastructure, and due to a tendency in neglecting security in the production process, IoT poses a threat to be compromised and used individually or collectively to damage a CII operator
- Non-defined critical infrastructure is highly interdependent with the defined critical infrastructure and therefore poses a threat

In relation to governing the CII system there appears to be inconsistencies at highest political level in what the Danish CII is comprised of and who the authorities are. Different definitions can create different workflows and inconsistencies in what must be prioritized in the decision-making process before, during and after an incident. In accordance with the principle of sector responsibility, several top decision makers are seen at the same level of authority making decisions that affect each other. Different perceptions of what is constituted as *critical* have a major impact on what the decision maker prioritizes, and this can have an impact on the vertical integration of CIIP governance.

9 All-Hazard Approach

Abbreviations

CFCS	Centre for Cyber Security
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
DESI	Digital Economy and Society Index
EU	European Union
OECD	Organisation for Economic Co-operation and Development
UNOPS	United Nations Office for Project Services

The present chapter evaluates the systems of governance planning of the Danish critical information infrastructure (CII) within the framework of an all-hazard approach. The attention is drawn to the whole system and less focus on the subsystems. In the context of the CII, the approach is interpreted as a way to view all of the dependencies in and outside the system as a way to identify informational patterns. The purpose of the chapter is to examine the system of governance and the sharing of responsibility when the focus is on the interdependencies and the political subsystems are ignored.

Chapter 9 is a continuation of Chapters 7 and 8, where results and assumptions are anchored. This mainly include the identified network typologies and the subsystems interdependencies.

9.1 Systems Dependencies

In this section, the all-hazard approach is interpreted as representing the whole system disregarding demarcated subsystems. To illustrate the subsystems and the limitations the prioritisation provides the dependencies of the six subsystems are presented in Figure 42.

The dotted lines with no arrows represent the intra-dependencies that constitutes the subsystems network typologies, in which the bidirectional relations are implied. The dotted arrows show the directional dependencies among the subsystems. The input from system A to system B depends on the number of end-user contacts in system A which is equal to the method applied in Chapter 8.2.2.

The number of arrows depends on the level of dependency, where a high dependency is illustrated with three arrows and a low dependency is shown with one arrow, which is equal to the method applied in Chapter 8.2.2.

The colours represent the respective subsystems. The circles represent private operators and the squares represent authorities.

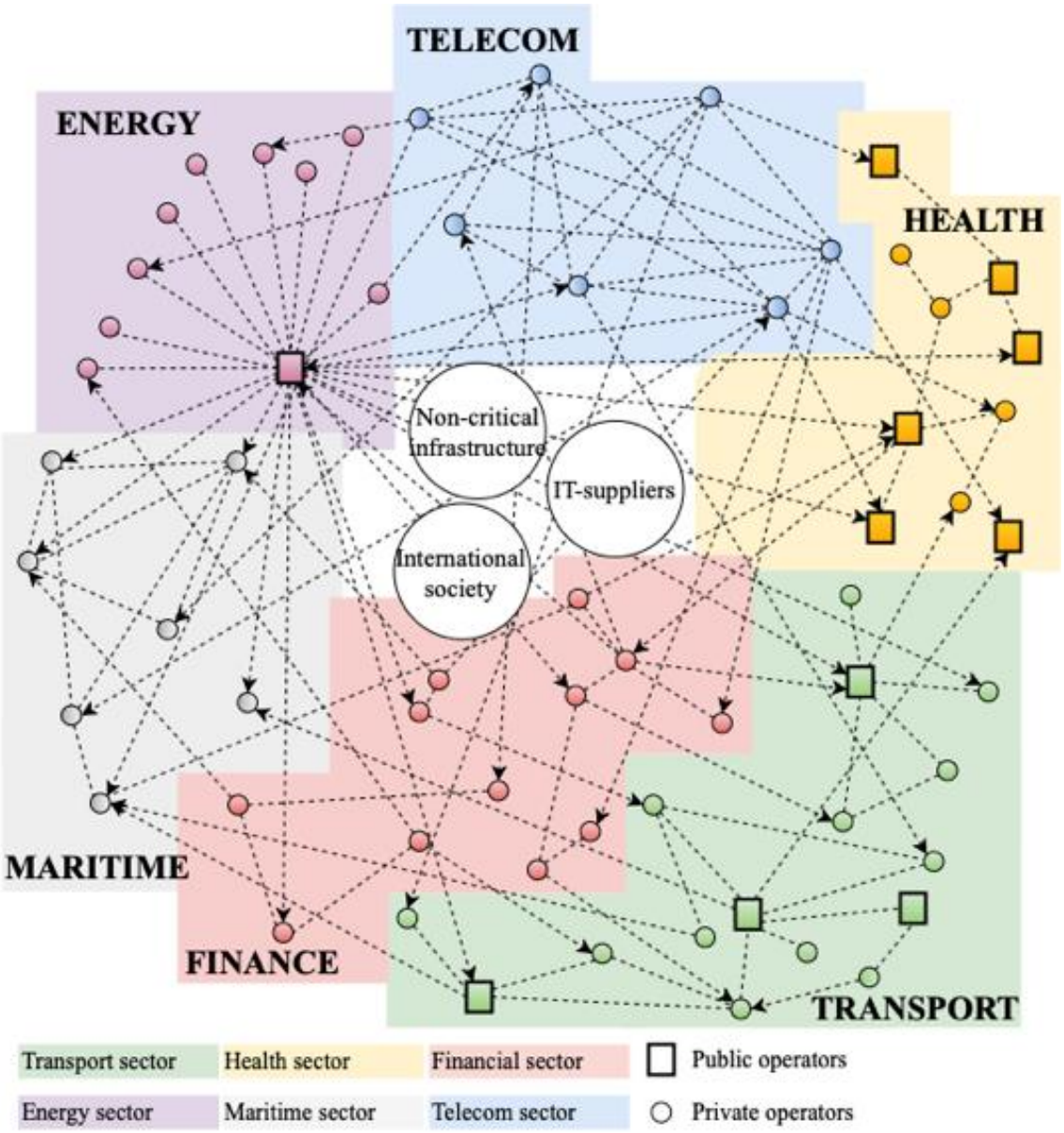

Figure 42: Conceptual illustration of the CII system highlighting the subsystems primary and secondary dependencies

By maintaining the subsystems components and dependencies and disregarding the individual subsystems colouring and titles, as well as illustrating the non-critical infrastructure and international society as representing the overall system, the CII systems dependencies are presented in Figure 43. Although Figure 42 shows a clear division among subsystems, Figure 43 shows a system that does not immediately allow a division into subsystems.

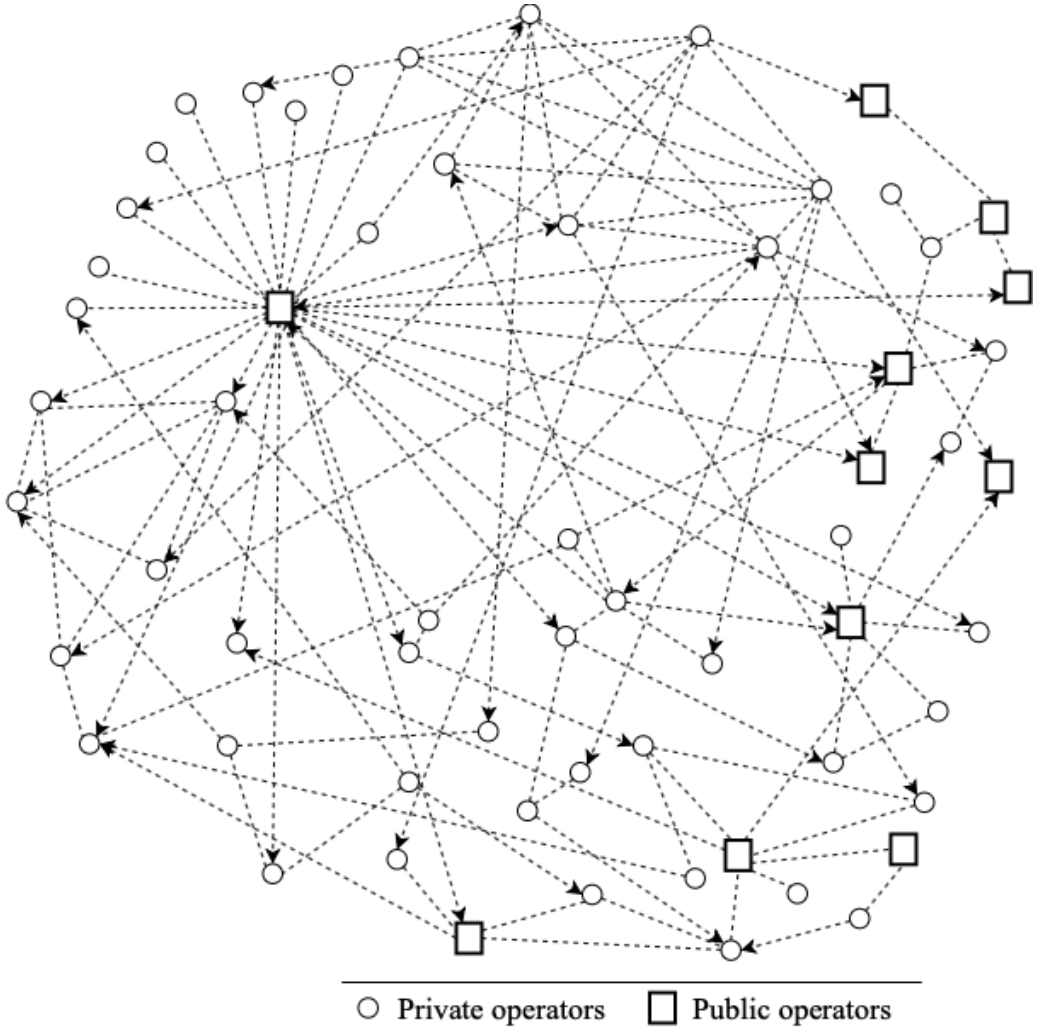

Figure 43: A conceptual illustration of the Danish CII disregarding the sectoral boundaries

In Figure 43, the system of CII is illustrated as a whole system by its interdependencies. There is no apparent natural division of the system. This can in this study only be speculated as it requires a quantitative analysis to be further evaluated. However, from the illustration the CII system appears to be one system and therefore any division or isolation of specific subsystems will be a simplification.

9.2 Accumulating Effects

As the all-hazard approach accommodates a whole-system it is necessary to evaluate an interruption accumulating though the systems interdependencies. The approach is similar to the method used in Chapter 8.2.2; though, in these three examples of impacts, all of the CII subsystems are accounted for. To ease the visualisation, the non-affected components are removed from the illustrations.

The cascading effects accounting two impacts are shown in Figure 44. The red incident initiates in the centralised unit within the energy sector, impacting all of the energy including parts of all other sectors by the 2nd effect. The blue incident initiates in the financial sector and by the 2nd impact it affects two other sectors. The green incident initiates in the telecom sector and affects the majority of the telecom operators as well as two others.

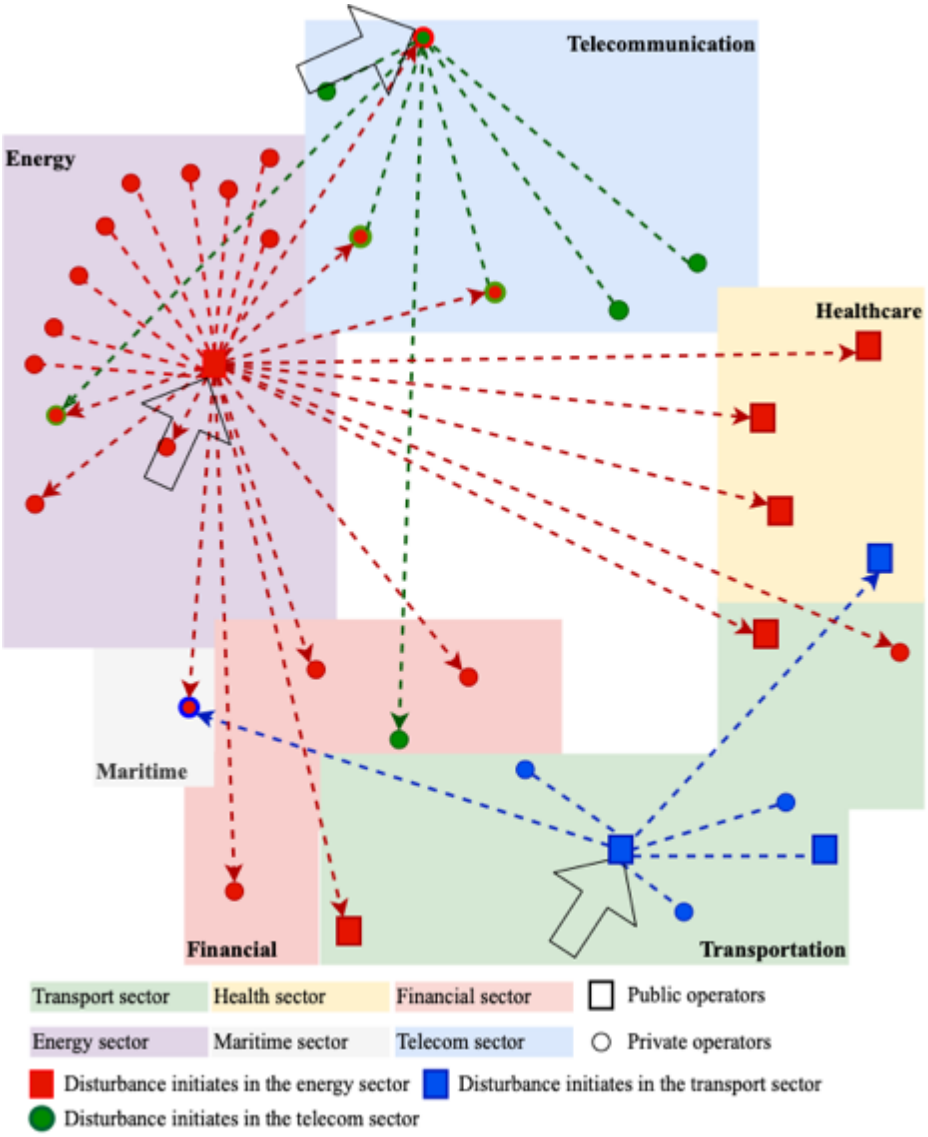

Figure 44: Illustration of three examples of cascading events of 2nd order impacts disregarding non-affected components

Based on the exemplified disturbances in Figure 41, the incidents would activate the relevant authorities. For example, the red incident would activate decision makers from respectively all of the sectors. In addition, the four ministries that share responsibility for the telecom sector would have to coordinate decisions. Moreover, the Ministry of Industry, Business and Financial Affairs would have to prioritise resources to accommodate different decisions necessary in the financial, maritime and telecom sector.

In order to illuminate the complexity created by the interdependencies, the exemplified incidents are expanded to include three impacts (Figure 41). The red incident shows an accumulated event that affects all of the energy system, the majority of the maritime sector and large parts of the transport, financial and health sectors. The blue incident impacts the transportation and minor parts of the maritime and health sectors. The green incident disturbs all of the telecom sector and moderately parts of all other sectors.

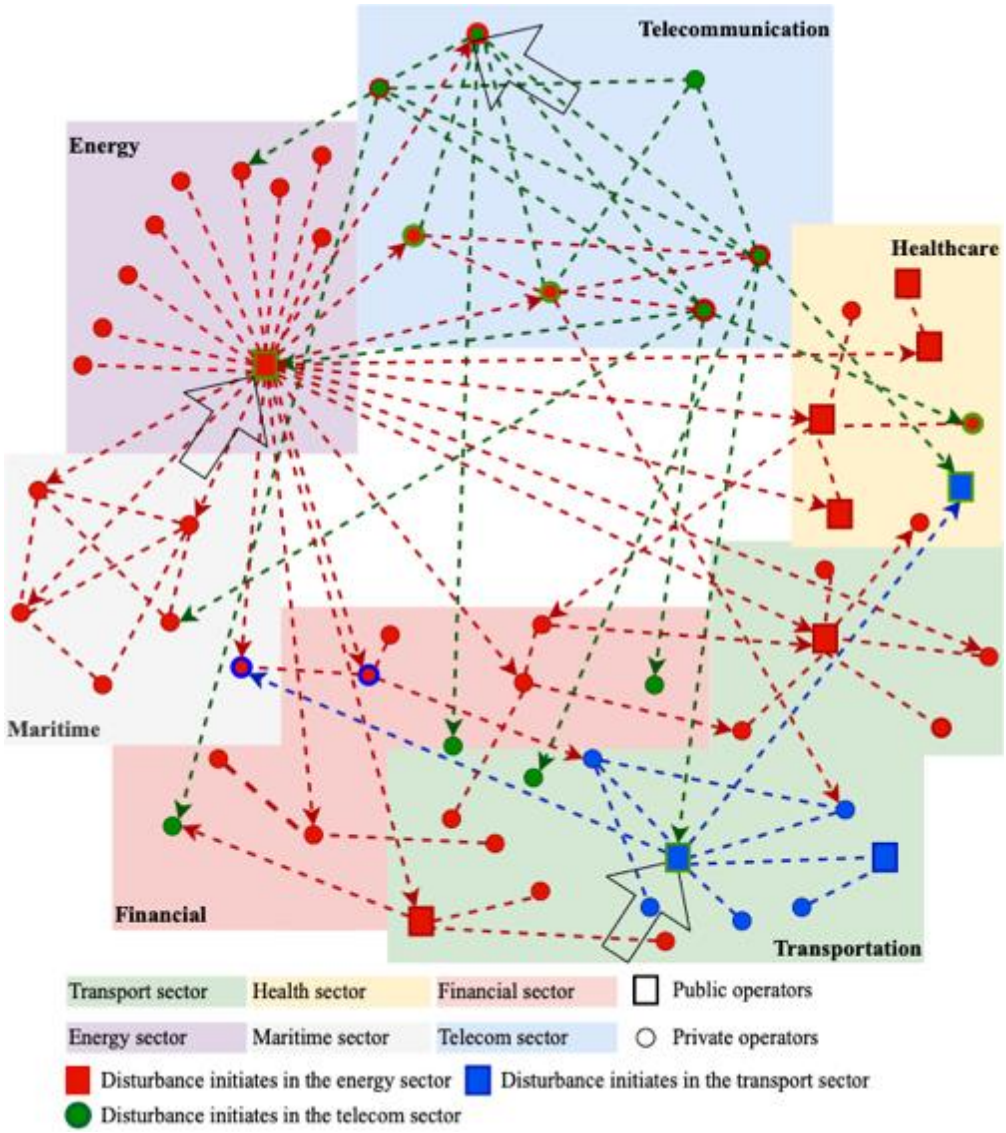

Figure 45: Illustration of three examples of cascading events of 3rd order impacts

The decision makers that would be activated as a result of the exemplified incidents in Figure 45 would be extensive. The red incident requires similar decision makers as with two accumulated disturbances (Figure 45), though the number of components has increased. The blue incident is roughly similar with 2nd impact. The green incident, that initiated in the telecom sector has developed to involve all sectors by the 3rd impact.

The three accumulated incidents affecting 2nd and 3rd impacts, shows a system where the sectoral boundaries are easily ignored by the hazard behaviour. Especially, the energy sector initiates an accumulated impact affecting most of the sectors, whereas disturbance in the transportation sector does not. The examples show how network typologies have an impact on how incidents behave in the system. It shows that a centralised network that has only a few end-user interfaces, as the energy sector, pose a vulnerability to interrupt the rest of the CII system. On the other hand, a decentralised network with several end-user contacts, as the financial sector, is less ideal to facilitate an entire system disruption.

The demonstration is obviously highly subjective and based on simplified assumptions, though the accumulated effects in Figure 41 and Figure 42 shows the interconnectivity of the Danish CII

system, where the political boundaries of the subsystems play an insignificant role. With consideration of governing such an interlinked system, the principle of sector responsibility appears contrary and challenging to operationalise.

9.3 Time Dependencies

The CII systems is dynamic, which means that the system is constantly evolving, and the system has predictable and unpredictable behavioural patterns due to a change in authorities, CII operators, technologies, regulations, trends etc. Faber (2019) argue that the temporal performance of the interlinked system must account for time-dependencies. The temporal performance is illustrated in Figure 46, showing hazards, trends and regulations influencing the critical, non-critical and international infrastructure system. In addition, the figure illustrates the system being dependent on previous historical system performances [100].

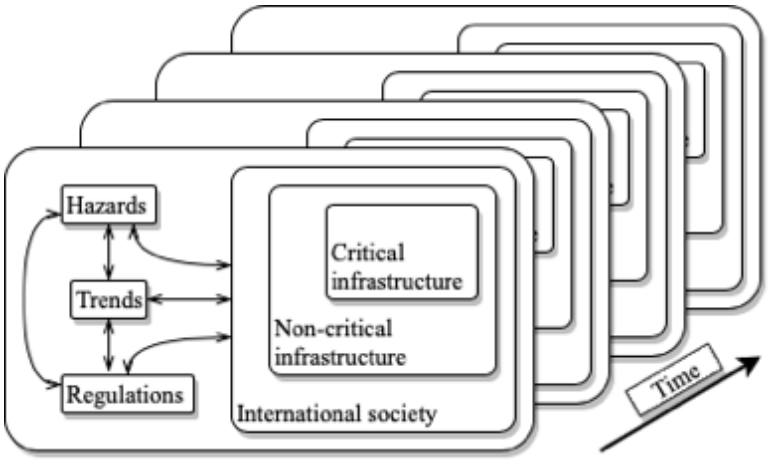

Figure 46: A modified illustration of the principal interlinked system adopted from Faber (2019) [100]

The life cycle of the CII system is relevant to include, though it may be difficult to define i.e. defining the boundaries of its creation to its dissolution.

Another dynamic dimension relates to the decisions made based on various preferences and objectives according to the decision makers' political preferences i.e. strategic, tactical or operational preferences (see Chapter 4). The lifespan of the decisions shows relevance in the dynamic dependencies. While strategic decisions are focused on capacity investment and resource utilisation and have a long-term lifespan, tactical decisions are attentive on aggregated procedures with a shorter lifespan, and operational decisions are mainly concerned with effectivity within a short-term period [33]. Decisions may vary in terms of short- and long-term achievement of objectives, that can affect the quantity and quality of the derived consequences. This can be seen in the light of the emergency management phases including mitigation response, recovery or preparedness. With consideration of community planning there are different time frames e.g. decades or generations, and different objectives e.g. fast recovery or use of renewable resources [101]. The time slicing dynamics, the life-cycle perspective and the variation of preferences merely increase the complexity of the CII system. However, in the view of an all-hazard approach such considerations should be accounted when planning governance of CIIP.

9.4 Summary

According to UNOPS (2018), a robust and resilient national critical infrastructure is necessary to maintain and develop with a long-term and resilient approach. UNOPS is currently researching and developing a systems-of systems approach to critical infrastructure based on the belief that a sustainable, robust and resilient infrastructure can be achieved by working with the entire lifespan of the infrastructure interdependencies [102].

A typical all-hazard approach is to assess in a more general matter, counting for most threats. Zhuang and Bier (2007) criticise the approach for being too broad and failing to simultaneously mitigate natural hazards with the protection of specific assets [103]. The approach is meant to comprehend all potential known and unknown hazards, it may join a variety of incidents that does not resemble the generalness e.g. highly unpredictable and possibly unknown threats requiring unusual authorities or resources that is unavailable under normal conditions. However, the OECD (2019) recommends nations to adopt the all-hazard approach as a way to strengthen the nation to manage unpredictable risks [80].

The chapter presents descriptive examples on accumulating incidents showing a disruption of the entire CII system. Simplified examples of 2nd and 3rd order cascading effects illustrates how the interdependencies facilitate a close to entire system breakdown. However, the examples show a difference in where the incident initiates from. A disruption starting in the energy sector showed a significant larger impact on the entire CII system than an impact in the transport sector initiated. All exemplified cascading events showed that the CII system quickly disrupt several subsystems – meaning several respective authorities would be involved.

The chapter presents the CII system by visualising the insignificance the subsystems boundaries provide to the systems´ interdependencies. When removing the political subsystems and remaining the interdependencies, the CII system appear as one system where no subsystems emerge. The current practice of a sub-divided hierarchical top-down governance approach is inappropriate when the system is interdependent. In addition, UNOPS (2018) recommends that this somewhat traditional government approach should be changed toward a more holistic long-term systems-of-systems approach in order for the CII to respond, adapt and recover from any disruptions [102].

10 Summarised Challenges to CIIP

Abbreviations

CFCS	Centre for Cyber Security
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
OECD	Organisation for Economic Co-operation and Development
R&D	Research and Development

The results from the single-hazard approach show heterogenous subsystems based on the political priority, the political level of sector authority and network typologies. The dependency analysis within the framework of multi-hazard approach shows an imbalance where some critical information infrastructure (CII) subsystems pose a risk of disrupting the entire system due to its relation of in and output dependencies, whereas other subsystems appear to pose a minor risk. The all-hazard approach exemplifies that the sectoral division places a great amount of responsibility on several sector-specific decision-makers and on their internal cooperation and communication. The current chapter illuminates four overall challenges that are summarised of the discussions from Chapter 7, 8 and 9: (i) Classification of CII; (ii) Adaptive risk governance; (iii) Governmental organisation; (iv) Short-term and long-term achievement of objectives.

10.1 Classification of Critical Information Infrastructure

The identification of what is considered critical infrastructure varies among nations. International organisations induce an identification on what constitutes national CII with the aim of strengthening the transnational CIIP due to cross-national interdependencies. The study of 25 OECD countries (Denmark is not included) shows that there are large differences in national classifications of CII, for which OECD recommends a shared definition for all countries, in order to strengthen the transnational network. The task of identifying a number of subsystems as being more critical than others, underline the down prioritisation of other subsystems. Surely, it is a way to prioritise resources; however, the assumption of isolating a subsystem that is in nature largely interconnected with the whole system is contradictory. The interdependencies between primary and secondary subsystems are embedded in the systems of critical information infrastructure protection (CIIP). Securing one part without strengthen the other pose a threat of the unsecured part disrupting the secured, as they are interdependent (Figure 47).

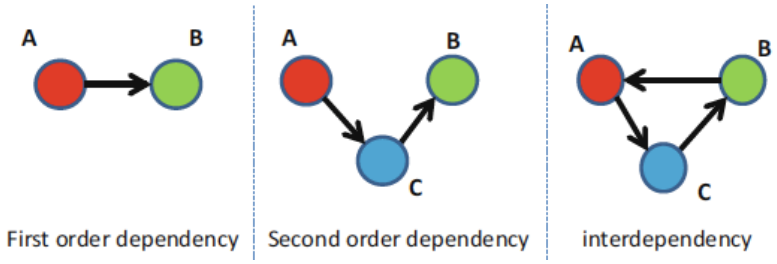

Figure 47: Principle illustration of dependencies and interdependencies adopted from Setola & Theoharidou (2016)

The ideology of prioritising one system over another, applies for CII operators as well, where the designated CII operators are made aware of their critical role and therefore have the opportunity to act accordingly. Those operators who are not aware of their critical role cannot be expected to behave in the same way as the prioritised CII operators. The EU Commission has, through the NIS Directive, made a claim for the identification of all CII operators in all EU states. A list of Danish critical operators has not been possible, although several sectoral strategies have promised that such will be developed in the near future. Either way, the list prioritizes some operators over others, which may give the impression that the non-critical operators are not important to the CII system. As already discussed in previous chapters, the non-critical operators and systems including IT suppliers are interdependent with CII operators and systems, thus these need to be protected in order to protect the CII. A whole-of system approach is needed to secure a part of the Danish society. Consequently, the all-hazard approach may be appropriate to apply, where the focus is to strengthen the whole system rather than focusing on specific parts. Though, the all-hazard approach embraces the whole of critical and non-critical systems, the method is still based on a belief in causal hazards classified by their source of origin. As elaborated in Chapter 6, this classification supports a tendency of certain hazards being the properties of specific academic disciplines. This is discussed in the bibliometric analysis in Chapter 3, where the majority of publications on all-hazards are focused on hazards specifically related to healthcare and to some extend toward risk management policies.

10.2 Adaptive Risk Governance

Folke et al. (2005) [104] and Berkes (2009) [105] introduce adaptive governance as an approach to comprehend collaboration on multiple governmental levels. With a policy-centric process, the approach aims to balance centralized and decentralized controls with consideration of the integration of local knowledge and formal scientific knowledge. In addition, Folke et al. (2005) introduce the concept of *bridging organizations*, to enhance the strength of social capital and the capacity for effective multilevel governance. The bridging organisations shares similarities with the coordinating DCIS units [104]. The concept of adaptive governance is treated by Nielsen & Faber (2018) in their review on sustainability, resilience and risk governance, where they conclude that adaptive governance is an essential part of an overall strategic framework aiming to enhance resilience. The adaptive governance approach focuses on capacity building by the inclusion of societal public and private operators, whereby issues like social cohesion, trust, social capital, legitimacy and transparency of decisions are integrated into the overall risk governance framework. Diversity of knowledge that the framework of public-private collaboration postulates is a key element that stimulates the adaptability of a system' capacity to ensure dynamic goals, strategies and knowledge [106].

Dunn-Cavelty & Suter (2009) propose that the government should be coordinating instead of directing the network of operators as well as identifying instruments supporting the operators to meet the task of protection. In addition, the CIIP policies should be based on more or less self-regulating and self-organising networks [83]. With the desire to enlarge infrastructure resilience, Nielsen & Faber (2019) argue that adaptive governance is a strategic direction for achieving this goal. Adaptive risk governance does not necessarily classify hazards according to their information pattern, though the concept appears to fit better in the context of CIIP, due to the concept focusing on decision alternatives rather than the best decision. Bjerga & Aven (2015) argue that operational adaptive risk governance follows a set of dynamic alternatives to gain knowledge on the effects of

information flows [107]. It is assumed that a system of CIIP interdependencies (including non-critical systems and dynamic time-dependencies) require a flexible governance approach to strengthen the overall system. It is believed that this can be achieved by an adaptive risk governance approach.

10.3 Government Organisation

The political vertical sectors that constitutes the Danish society are significantly maintained in Denmark. This may not be equivalent with hazardous effects as previously discussed. The informational pattern of hazards may cross sector boundaries and occur in a non-linear accumulative way, where the severity may be dynamic and influenced by the pattern of decisions.

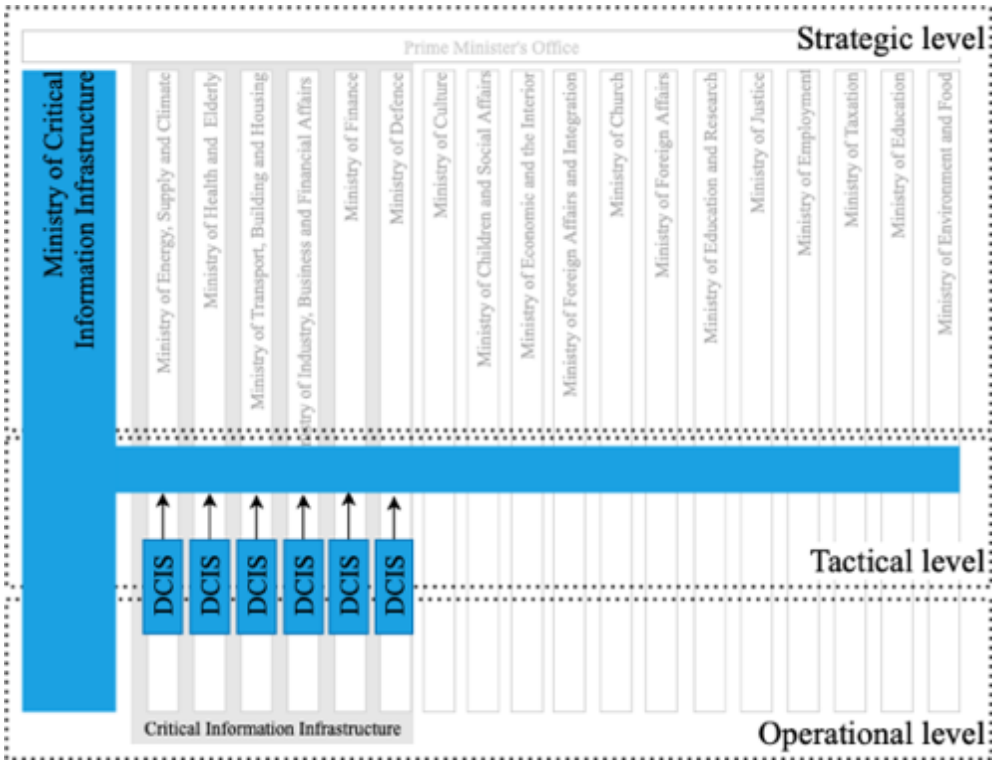

Figure 48: An example of how the proposed ministry of critical information infrastructure may be organised

The Danish governmental structure is dominated by vertical structures and less on horizontal coordination. As the hazard behave vertically and horizontally, the current organisational structure appears to be inadequate to coordinate among sectors as the sector responsibility principle describes otherwise. By having a ministry that works across the sectors and coordinates among the already established DCIS units (Figure 48) may ensure the current vertical sectors and at the same time manage cyber incidents.

11 Conclusion

Abbreviations

CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
PET	Danish Security and Intelligence Service
DEMA	Danish Emergency Management Agency
DCIS	Decentralised Cyber Information Security
ISAC	Information Sharing and Analysis Centres

It is a challenge that Denmark lacks a common institutional understanding and anchoring of what constitutes critical information infrastructure (CII) and how criticality is operationalised. The sector responsibility principle is an overshadowing cultural context that constitutes the Danish governance approach, where each sectoral authority manages vertically with a minimum of any organizational coordination horizontally. The current chapter presents the conclusion for the master thesis in which the aim is intended fulfilled. The thesis aims to provide a mapping over critical information infrastructure protection (CIIP) systems of governance and related issues, where the CIIP systems of governance are mapped in Chapter 7, 8 and 9, and Chapter 5 provides a characterisation of the CII subsystems. The current chapter presents the key challenges discovered throughout this research.

Heterogenous Critical Information Infrastructure

The system identification revealed that the Danish CII is highly differentiated in terms of organizational governance and structure, which only supports the vertical silo-structured protection of the CII. The analysis of the subsystem dependencies within the framework of multi-hazards revealed that some CII subsystems immediately pose a greater risk of causing total system breakdown than others. In addition, the bibliometric analysis also showed prioritised subsystems within current publications. The single-hazard analysis showed that the energy sector is prioritised at political level. In general, there appears to be a difference in which subsystems are being prioritised, how the subsystems are structured and how they are governed.

Secondary dependencies

In continuation of prioritised systems, Denmark faces another challenge, namely the non-prioritised systems dependencies. When analysing the system dependencies and resolving the subsystem boundaries, a simple demonstration shows that the political boundaries does not appear when evaluating the interdependencies among components (Chapter 9). With consideration of the discussion in Chapter 6 regarding classification of hazards, it is assumed that hazards do not behave within the boundaries of political systems. Hence, there is a need for a governance approach that goes beyond the subsystem boundaries. The critical infrastructure is interdependent with various secondary systems; hence, any hazard roughly affects both systems. Instead of protecting only one part, it is necessary to protect the whole system including critical and non-critical subsystems. A whole system protection approach is covered by enhancing the resilience of the system, which the all-hazard approach attempts to do.

Discrepancy at the strategic level risks propagating at tactical and operational level

The Danish CII is defined by the Ministry of Finance (2018) constituting six sectors. Additional documents are also defined by the Danish Emergency Management Agency (DEMA) and Danish Security and Intelligence Service (PET) respectively, describing alternative infrastructure systems. This may create confusion at strategic, tactical and operational levels of what constitutes the critical infrastructure and to what extent it should be assessed. Due to the lack of horizontal coordination each sector may be compelled to define their own criticality and decision preferences. The majority of the Danish CII is represented by private operators. What virtually all sectors have in common is the pronounced tendency to outsource IT systems to private operators, giving the private industry even more space in CII. There is a need for a common understanding of what the critical infrastructure is, what and who it consists of and based on what strategic objectives decisions are expected to be made from.

Clear rules for government interference

A challenge immediately arises when the procedure for managing cyber events is as little regulated as it is. In addition to the EU requiring every IT security breach to be reported after an incident, the Danish procedures are based on a much more voluntary basis related to the incident. In the event that a CII operator or authority experiences breaches of IT systems, it is up to the person concerned to assess whether and when the Centre for Cyber Security should be informed. This study shows that the identification of CII operators is imposed on each sector authority and in the vast majority of cases they have not identified who this includes. Furthermore, the European organization ENISA did not require identification of the operators' IT suppliers, which could pose a great risk of IT attacks being transferred. So, immediately there are some issues regarding this cyber-attack procedure, where the vast majority of operators are not aware of their critical responsibilities, nor are their suppliers. Another issue is that the procedure for informing CFCS is based on a voluntary basis and this will probably discourage more people from informing well in advance if at all informing CFCS. It is proposed that specific, possibly risk-based, rules be established for when the relevant authority should be intervened. In addition, this authority should have not only IT competencies but equally business competencies to be able to handle the operator's financial situation and to balance this with cyber information risks. This may create greater trust between private operators and authorities, so that private operators can inform responsible authority in a timely manner.

Adaptive risk governance

This study shows that Danish CIIP governance is characterized by a high degree of heterogeneous approaches that are differentiated into silo-based structures, which is characterized by top-down government control, despite the fact that the vast majority of the critical (and not critical) infrastructure is undertaken by private individuals. On the basis of the discussion on whether such a governance approach is appropriate, I suggest that the Danish emergency preparedness operators e.g. ministries, DEMA, police, military and health, identifies what constitutes the Danish CII and gets inspired by the Norwegian model. The Norwegian Government defines their CII based on governance and sovereignty, population safety and societal functionality. The organizational sectors are forced to coordinate horizontally though they still maintain their sectoral authority. Therefore, the report concludes to change the approach of governance toward an adaptive risk governance. The approach focuses on capacity building through the inclusion of societal public and private actors, where especially transparency of decisions are integrated into the overall risk governance framework.

Critical information infrastructure as a top priority

With regard to a proposal for organizational change that can create a closer vertical integration among strategy, tactics and operations, priority is given to critical information infrastructure protection in a ministry that works vertically and horizontally, i.e. across existing sectors. Information systems are unique as they are just integrated throughout the community and by placing this responsibility at ministerial level a political priority is shown and by having the working cross, the political influence can be integrated in coordination with the other ministries.

Information sharing

As discussed, trust is a fundamental part of coordination across sectors and between public and private operators. The information sharing and analysis centres (ISACs) is a organisational approach to facilitate information sharing among CII public and private operators. It is assumed that the Danish decentralised cyber information security (DCIS) units is the Danish variety of the concept. Though, the idea of having sector specific units only emphasise the already vertical divided silo structure, then ISACs also have the advantage of being able to build trust between public and private and this can probably be better achieved if it happens among equals within the same industry. Of course, this requires that the private operators must be able to find the value in offering information by also obtaining information. ISACs are different from DCIS in that ISAC stores and analyzes information and then gives operators back information. When establishing a possible ministry, an associated political institution can be set up that has the task of coordinating all DCIS units, which is bound by a great deal of intelligence and therefore not very transparent. Therefore, it is proposed that a ministry be set up and an associated board coordinate the existing DCIS units. Furthermore, these DCIS entities should be anchored and presented to the sector concerned to a much greater extent, where representatives of private and public operators should appear and be involved in the decision-making process. In addition, the DCIS unit should not only facilitate knowledge sharing, but information sharing, where data and events should be processed and disseminated to sector operators and the applicable responsible ministry.

IT suppliers pose a risk of CII breakdown

This study revealed a tendency for private and public operators to outsource their IT systems and services, and there is a further tendency for IT vendors to outsource to sub-suppliers. As discussed in this research, this could pose a risk that they will become the focal point for several CII players operating in different sectors, and if a supplier or sub-supplier is compromised, it could initiate accumulated effects in large parts of the CII system. Here it is suggested that the French model is used as inspiration. The French model includes an annually updated list of approved IT suppliers conducted by the French authorities or an expert company, where the state has beforehand approved a list of IT-suppliers for which their CII operators can choose from. Surely this require the Danish State and sector authorities to identify exactly what constitutes the Danish CII and who the CII operators are. In addition, these suppliers as they pose a great risk of damaging large parts of the CII should be identified and specifically prioritised, monitored and regulated.

12 Recommendations

The following recommendations are based on the discussion and results of the current study. None of the results have been validated by any authorities or experts with deep knowledge on the subject, and neither has the suggestions been tested. However, the following recommendations summarises the conclusion of the report:

- **Prioritise governance planning for CIIP at highest political level**
  - A ministry responsible for the Danish CIIP on a strategic, tactical and operational level as well as being the coordinating authority for all sector DCIS units

- **Identify the Danish CII functions and services across the vertical sectors**
  - Based on inspiration from the Norwegian approach horizontal-identified CII functions and services initiates a cross-sectoral coordination

- **IT suppliers should be approved by the State to manage IT-services for CII operators**
  - Based on inspiration from the French method of beforehand identifying IT suppliers ensures a certain level of security when outsourcing IT services

- **Risk-based directives raise awareness of governance of CIIP for CII operators**
  - Based on inspiration from European and Danish legislation regarding unmanned aircraft systems (i.e. drones), a risk-based directive requires public and private CII operators to plan IT emergency operations and share with respective authorities

- **Centre for Cyber Security requires financial and business-related training**
  - The Danish CIIP authority (currently CFCS) may advance in financial and business-related competencies reflecting the industry's objectives to better serve the interests of private CII operators

- **Adaptive risk governance accommodates public and private interests**
  - Implementing an adaptive risk governance is a way to build capacity by including trust, social cohesion, social capacity, legitimacy and transparency between public and private operators

This report is a most relevant contribution to support governance planning for the Danish CIIP. In addition, research on public-private partnerships is needed to be elaborated further as it appears to be an overall challenge in the governance of CIIP. As the CII consists of heterogeneous subsystems there may be a need for further study on standards and regulations that can comprehend the diversity – possibly risk-based policies that can include both public and private operators as well as IT suppliers.

13 Appendix

13.1 Bibliometric Analysis Data Report

The data report is performed for verification purposes in which the following steps are followed:

I. Collection of data
II. Construction of the bibliometric network

Step I

As the current research aims to identify two systems: (i) The physical critical information infrastructure system; and (ii) The governance systems of the critical information infrastructure system, it is essential to establish the current literature for both systems. Based on the identified search terms it is possible to extract a number of records from Scopus with the exclusion of non-English records due to the errors they may create when imported in the text mining software VOSviewer. Since, the topic of interest is a rather novel approach within academia, all record sources are required to achieve a high enough number of records that provides a general overview of the topic.

Step II

To create an overview of the significant topics related to critical infrastructure and alternative systems of governance, maps of keyword co-occurrence is created using VOSviewer discounting noun terms by implementing data from the bibliographic database, Scopus. The type of analysis chosen is “co-occurrence” of “all keywords”, based on the counting method “full counting”.

Please notice that Scopus does not allow access to or export of more than 2000 records, so the bibliometric literature review is done by exporting 2000 of the highest cited records. This applies for the domains of critical infrastructure (9000+ records) and critical information infrastructure (4000+ records).

VOSviewer uses a datamining technique on terms extracted from the titles and abstracts of the records downloaded from Scopus. The software excludes 40% of the terms with a low relevance score, for which a further exclusion is available. No terms have been excluded in the current analysis. The relevance score is calculated by the software Apache OpenNLP toolkit, which excludes noun phrases, whereas the relevance score indicates how random terms co-occur. A low relevance score indicates that a term co-occurs with other terms following a more or less random pattern whereas a high relevance score is attributed to noun phrases that co-occur mainly with a limited set of other noun phrases [108].

The network visualisations are composed by terms and interconnections, where the size of the terms indicates the number of records wherein the term is included in the title or abstract. The terms are connected by links, that each has a strength depending on how many records they both occur together in, illustrated in the thickness of the line. Furthermore, the terms located close together co-occur regularly, whereas the opposite is illustrated as the terms are located furthest apart. In this way the clusters appear in coloured lines and terms. Table 15 lists the choices made for each search keywords in chronological order.

Table 15: Co-occurrence network analysis of terms

Search terms	"Critical infrastructure*"	"Critical infrastructure*" AND ("information" OR "cyber")	"single-hazard*" OR "singlehazard*"	"Multi-hazard*" OR "multihazard*"	"All-hazards*" OR "Allhazard*"
Total number of records	9130	4051	159	1016	951
Language	English	English	English	English	English
Records imported into VOSviewer	2000	2000	159	1016	951
Title and abstract	Yes	Yes	Yes	Yes	Yes
Binary Count	Yes	Yes	Yes	Yes	Yes
Min. no. of occurrences of a term	25	30	5	25	20
Final number of terms selected	123	106	55	66	55
Number of clusters	3	4	3	2	3
Min. of cluster size	20	21	5	6	6
Number of links	4606	3997	623	1714	1078
Total link strength	19578	25335	1476	11270	10296

Critical information infrastructure

The historical evolution of research in the domain of critical information infrastructure (CII) can be traced back to 1985 (4000+ records), whereas critical infrastructure (CI) had its birth in 1984 (9000+ records) (Figure 49). Both domains show an upward trend but publications on CII are relatively marginal, constituting roughly half of the total amount of CI.

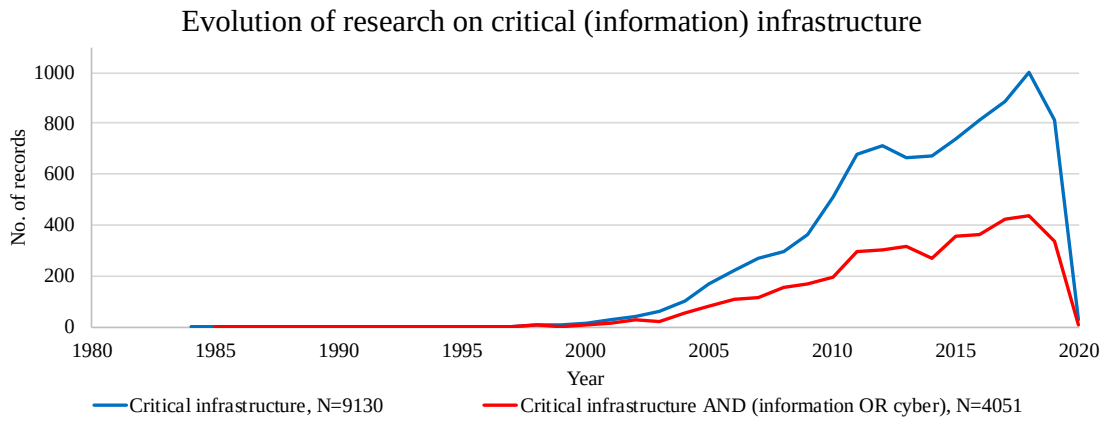

Figure 49: Historical evolution of number of records on CI and CII

When evaluating the top 10 keywords occurring in the total number of hits (CI: 9000+ records; CII: 4000+ records) there are many similarities (Table 15). Besides the frequency of keywords being ranked differently in each domain, the main difference is within CI having the term "risk management" included frequently, whereas in CI is the term "embedded systems". For both domains the keyword "public works" apply as second most frequent. Public works relates to a community-based approach.

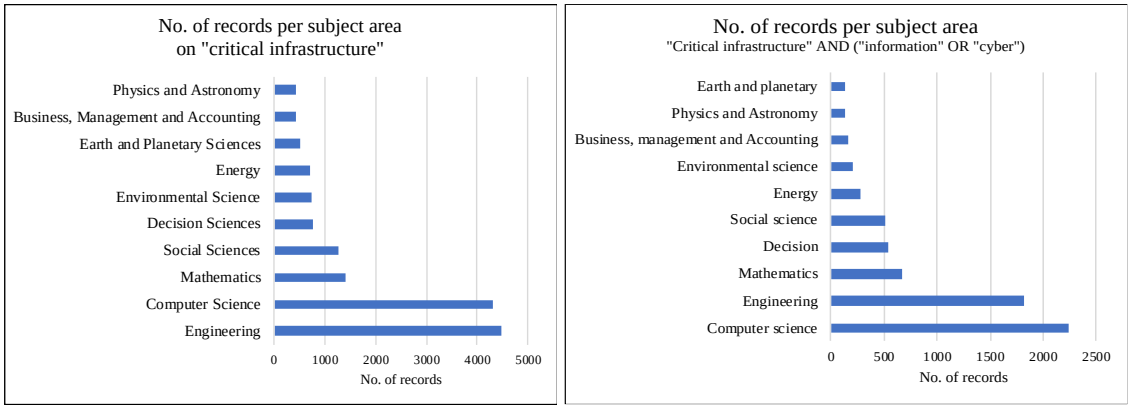

Figure 50: Top 10 subject areas on records concerning CI (left) and CII (right)

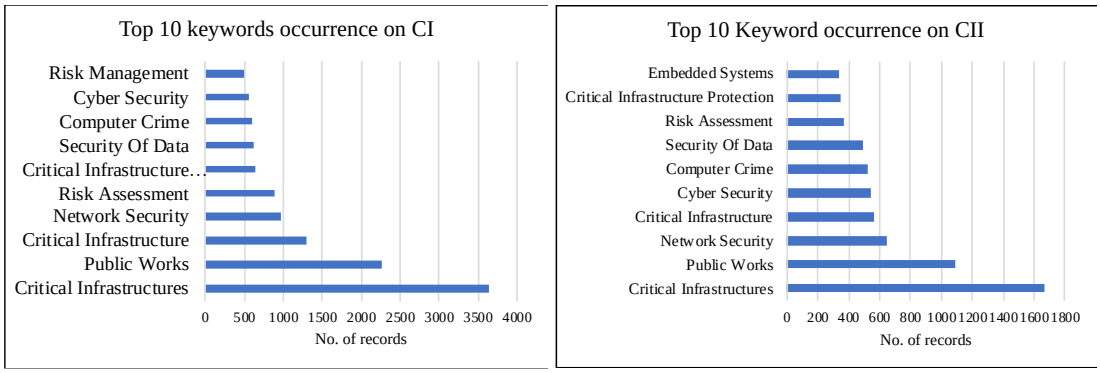

Figure 51: Top 20 most occurrent keywords in records on CI (left) and CII (right)

The following figures and tables include the cluster analysis consisting with step III, illustrating visualised network maps of keyword co-occurrence and the related keywords listed in tables according to their cluster belonging ranged according to the link strength.

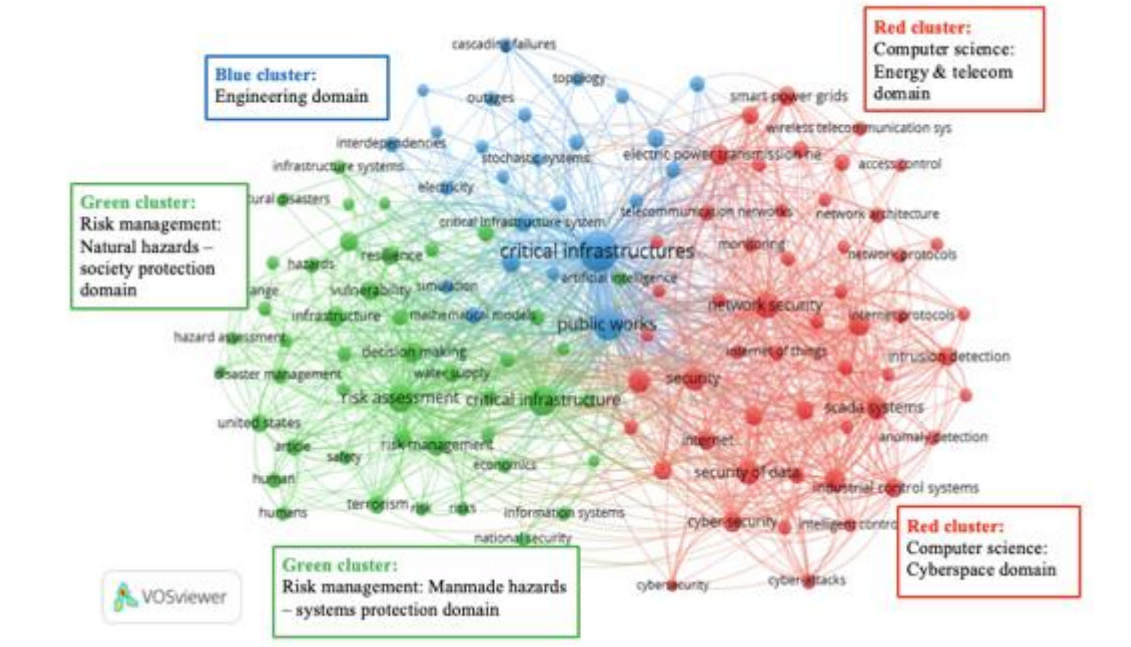

Figure 52: Network map of CI

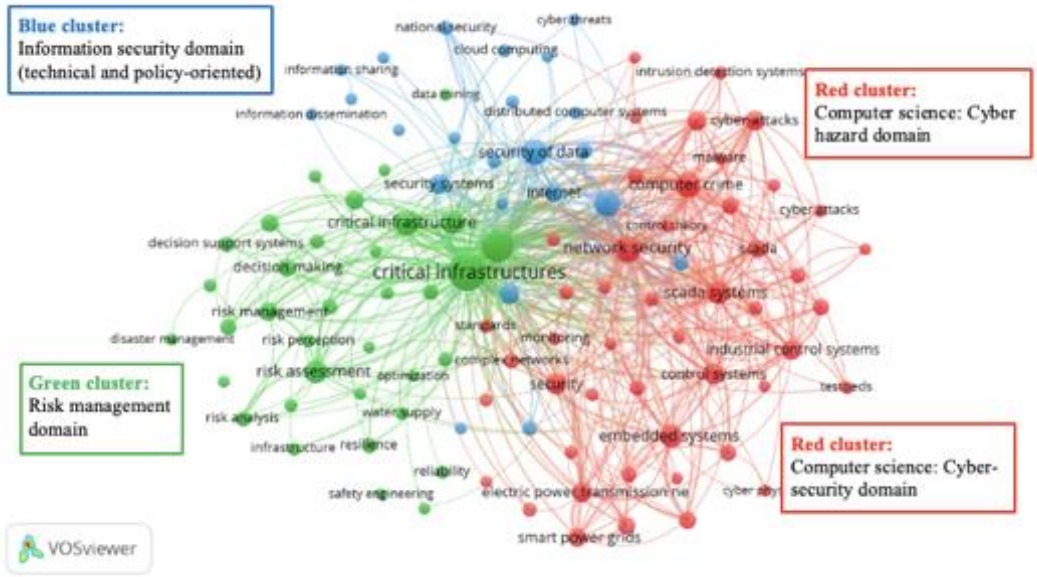

Figure 53: Network map of CII

The following tables (Table 16 and Table 17)provide a list of the terms in each cluster as illustrated in Figure 52 and Figure 53. The tables are ranked from highest to lowest according to the link strength.

Table 16: Keyword clusters illustrated with occurrence and link strength in each cluster colour on the search on "critical infrastructure".

Cluster 1 (n=52)			Cluster 2 (n=46)			Cluster 3 (n=25)		
Term	**Occurrence**	**Link strength**	**Term**	**Occurrence**	**Link strength**	**Term**	**Occurrence**	**Link strength**
network security	202	1091	critical infrastructure	295	1226	critical infrastructures	758	3146
scada systems	137	843	risk assessment	217	1168	public works	380	2038
computer crime	132	801	risk management	98	575	computer simulation	85	389
security of data	152	717	decision making	97	489	complex networks	65	311
embedded systems	118	651	risk analysis	81	480	critical infrastructure systems	62	310
critical infrastructure protection	138	634	vulnerability	85	423	mathematical models	60	268
security	127	612	infrastructure	98	408	electric power distribution	43	245
cyber security	98	605	disasters	80	390	electric power systems	45	237
electric power transmission network	91	504	resilience	83	369	reliability	51	224
control systems	82	474	terrorism	66	328	graph theory	34	210
industrial control systems	77	472	united states	75	321	interdependencies	44	210
smart power grids	83	457	article	59	303	power grids	43	208
intrusion detection	84	436	water supply	56	279	vulnerability analysis	34	208
security systems	90	433	optimization	56	248	outages	38	199
smart grid	75	427	hazards	45	240	simulation	37	190
internet	81	384	risk perception	42	235	reliabiilty analysis	32	183
scada	52	370	disaster management	50	230	cascading failures	36	181
information technology	73	353	transportation	47	226	electricity	35	177
cyber-attacks	46	310	human	44	224	topology	35	177
cyber physical systems	48	290	risk	29	206	stochastic systems	33	173
data acquisition	46	279	risks	29	202	vulnerability assessment	26	157
crime	35	257	algorithms	44	201	systems engineering	30	145
cyber-physical systems	36	246	decision support systems	36	189	models	34	144
wireless sensor networks	59	236	disaster prevention	34	188	large scale systems	31	143
network architecture	46	232	infrastructure systems	37	184	interdependent infrastructures	25	122
intelligent control	33	230	investments	39	184			
internet of things	43	228	economics	36	182			
telecommunication network	48	211	humans	39	179			
cyber physical system	32	208	safety	33	179			
information management	37	207	artificial intelligence	36	170			
internet protocols	41	198	climate change	49	169			
supervisory control and data acquisition	28	198	hazards assessment	31	162			
cybersecurity	26	197	infrastructure planning	37	161			
intrusion detection systems	32	196	information systems	37	159			
network protocols	39	195	water supply systems	26	157			
sensors	54	193	national security	33	155			
supervisory control and data acquisition system	29	188	floods	31	148			
anomaly detection	35	176	probability	31	144			
surveys	30	167	safety engineering	31	139			
cloud computing	41	166	flooding	25	133			
distributed computer systems	36	165	natural disasters	28	129			
monitoring	36	163	uncertainty analysis	26	127			
game theory	32	162	research	29	119			
automation	34	153	costs	27	108			
cryptography	27	147	sustainable development	31	104			
wireless communication	34	146	earthquakes	25	86			
communication	35	145						
quality of service	35	144						
sensor networks	30	138						
real time systems	29	126						
Access control	27	114						
design	33	114						

Table 17: Keyword clusters illustrated with occurrence and link strength in each cluster colour on the search on "critical infrastructure" AND ("information" OR "cyber")

Cluster 1 (n=48)			Cluster 2 (n=35)			Cluster 3 (n=23)		
Term	**Occurrence**	**Link strength**	**Term**	**Occurrence**	**Link strength**	**Term**	**Occurrence**	**Link strength**
network security	323	1962	critical infrastructures	859	4101	cyber security	256	1589
computer crime	276	1905	public works	553	3080	security of data	284	1457
scada systems	207	1410	critical infrastructure	280	1352	information technology	142	678
embedded systems	198	1136	critical infrastructure protection	197	1018	security systems	122	637
industrial control systems	142	1010	risk assessment	199	974	internet	101	522
control systems	157	1007	risk management	111	624	cybersecurity	69	420
cyber-attacks	135	949	information management	103	525	internet of things	60	336
security	154	822	decision making	99	491	national security	56	308
electric power transmission networks	123	796	information systems	96	429	information and communication technologies	51	283
intrusion detection	110	687	critical infrastructure systems	60	369	distributed computer systems	42	228
smart power grids	110	685	risk analysis	65	348	situational awareness	41	222
crime	84	669	disasters	77	338	information security	46	205
scada	91	656	resilience	68	332	game theory	34	193
smart grid	89	550	decision support systems	58	301	cyber threats	30	186
intelligent control	71	547	telecommunication networks	55	265	cloud computing	39	185
cyber physical systems (cpss)	88	513	artificial intelligence	50	256	information sharing	32	181
cyber physical system	76	512	water supply	44	235	big data	31	175
cyber physical systems	65	441	risk perception	39	210	investments	32	156
data acquisition	61	435	vulnerability	44	209	information analysis	30	153
complex networks	64	392	information infrastructures	44	205	information dissemination	30	152
supervisory control and data acquisition	46	376	terrorism	39	205	computer software	33	137
network architecture	63	360	infrastructure	45	194	information services	31	119
intrusion detection systems	45	330	computer simulation	61	189	societies and institutions	30	114
automation	57	326	diaster prevention	36	182			
anomaly detection	53	299	surveys	34	182			
process control	44	292	reliatbility	42	178			
cyber attacks	39	291	accident prevention	31	174			
testbeds	36	286	safety engineering	31	146			
electric power distribution control	33	272	mathematical models	34	145			
electric power systems	49	264	transportation	33	143			
malware	37	244	data mining	31	137			
power grids	43	242	optimization	31	125			
personal computing	35	241	disaster management	32	124			
supervisory control and data acquisition systems	32	238	information science	31	124			
Denial of Service Attack	31	236	geographic information systems	35	120			
internet protocols	40	234						
cryptography	37	229						
access control	42	226						
standards	36	221						
wireless sensor networks	53	221						
electric power distribution	34	210						
monitoring	36	202						
control theory	30	201						
cyber-physicals	34	201						
network protocols	38	197						
sensors	40	179						
communication	38	175						
real time systems	30	167						

Alternative systems of governance

The historical evolution of the three governance approaches (Figure 54) shows that the all-hazard approach (951 records) is the first one published in 1957, whereas publications on single-hazard (159 records) and multi-hazards (1016 records) began in the 1980s. Research on the all-hazard approach experienced a few yet constant annual publications from roughly 1970 to 2000. In the early 2000, the number of publications on all-hazards increased drastically; however, the contribution is within the range of 50-70 records annually up until present. Both the single-hazard and multi-hazard approach are first introduced in literature in the early 1980s and have since been modestly studied. The single-hazard constitutes a minor part compared to multi-hazards and all-hazards.

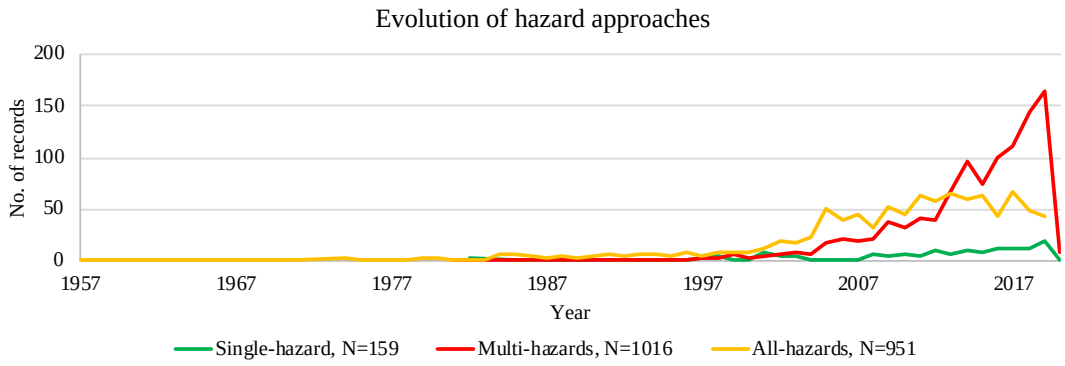

Figure 54: Historical evolution of annually publications on alternative hazard approaches

The keywords for the single-hazard and multi-hazard domains are relatively similar, with the exception of earthquakes, disasters, floods, article, multi-hazards and human(-s). This could indicate that multi-hazard approach relates to research concerned with natural hazards. Both research areas are dominated by Engineering, Earth and Planetary Science and environmental science (Figure 56).

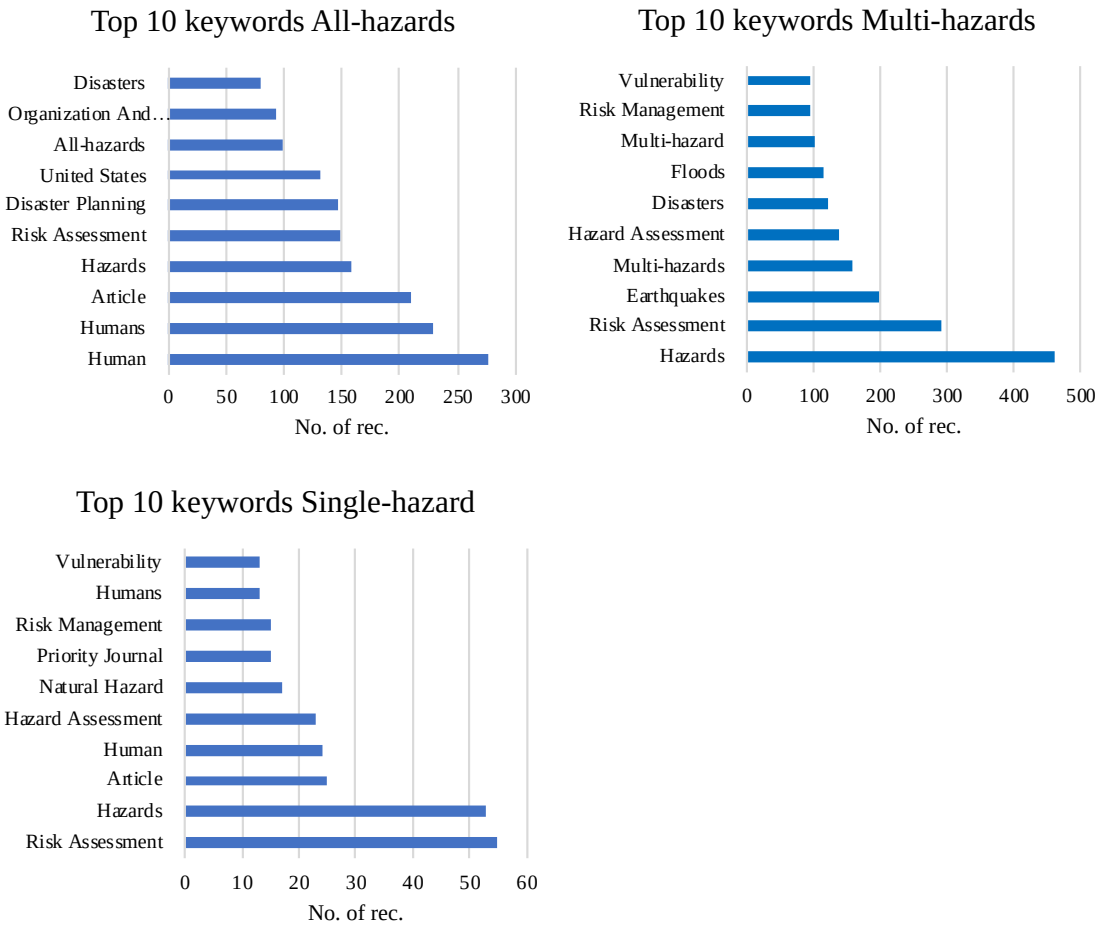

Figure 55: Top 10 keywords in three domains of the three alternative governance approaches

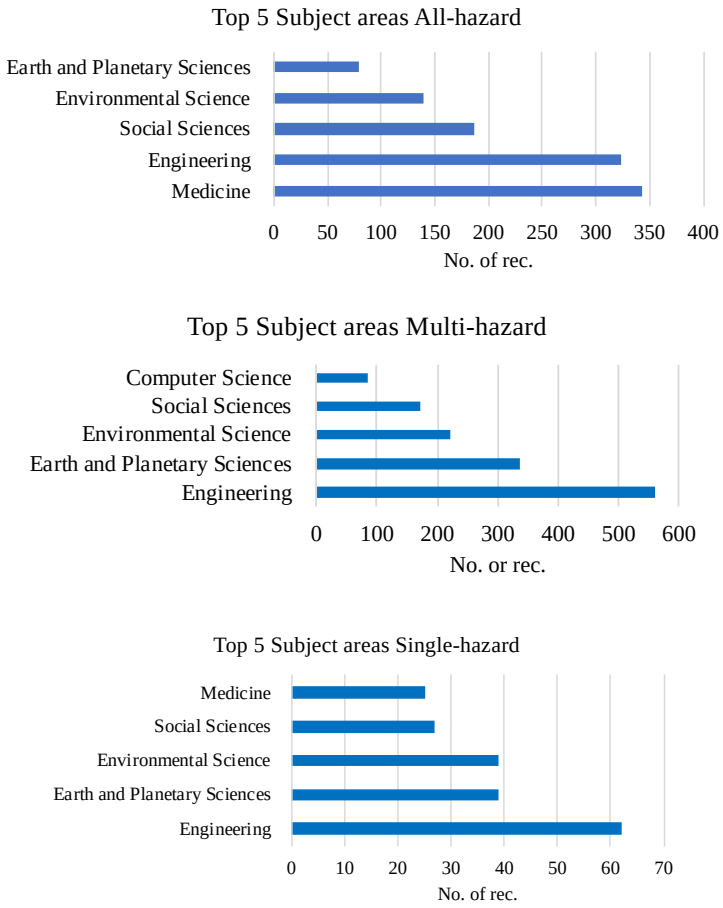

Figure 56: Top 5 subject areas for the three alternative governance approaches

The following figures include network maps of keyword co-occurrence for each alternative system of governance including the cluster keywords associated with each cluster listed in individual tables.

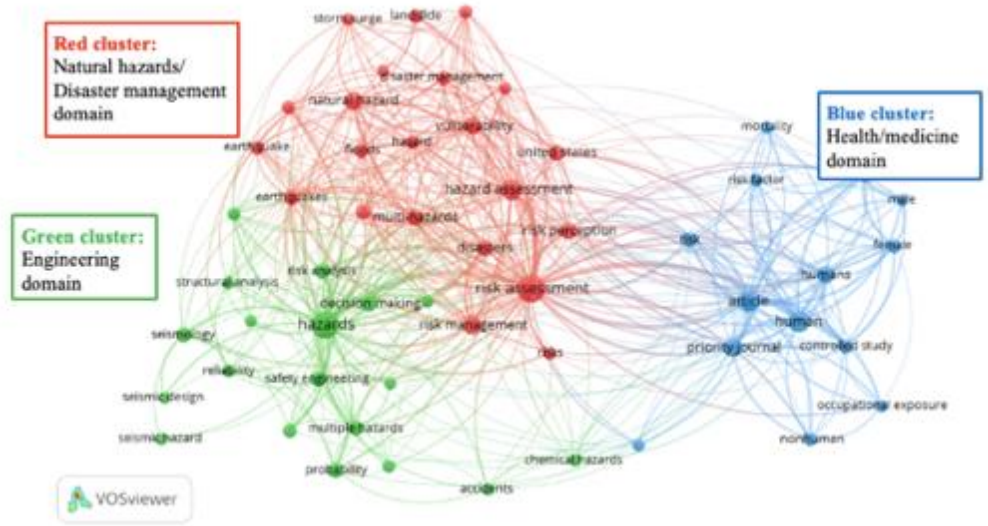

Figure 57: Network map of research on single-hazard extracted from Scopus, N=159

Table 18: Keyword clusters on single-hazard illustrated with occurrence and link strength

Cluster 1 (22 terms)			Cluster 2 (19 terms)			Cluster 3 (14 terms)		
Term	**Occurrence**	**Link strength**	**Term**	**Occurrence**	**Link strength**	**Term**	**Occurrence**	**Link strength**
risk assessment	55	275	hazards	53	206	article	25	144
hazard assessment	23	116	risk analysis	10	50	human	24	126
natural hazard	17	83	decision making	11	49	priority journal	15	88
risk perception	12	83	probability	10	38	humans	13	79
vulnerability	13	82	safety engineering	9	38	risk	9	60
risk management	15	77	seismology	9	38	female	8	58
multi-hazards	11	63	hurricanes	6	35	adult	7	52
eartquakes	10	62	multiple hazards	10	34	controlled study	7	49
disasters	12	60	life cycle	8	31	male	5	41
united states	11	54	structural analysis	5	31	nonhuman	6	35
multi-hazard	10	51	resilience	5	29	risk factor	6	35
floods	8	44	reliability	6	24	mortality	5	30
disaster management	8	40	structural design	5	24	occupational exposure	5	26
hazard	6	40	chemical hazards	5	22	quantitiative analysis	5	24
hurricane	6	40	geographic information systems	5	22			
eartquake	8	38	accidents	5	17			
storm surge	5	36	seismic design	5	17			
Climate change	5	33	accident prevntion	6	12			
hazard management	6	32	seismic hazard	5	8			
risks	6	27						
landslide	7	22						
landslides	5	22						

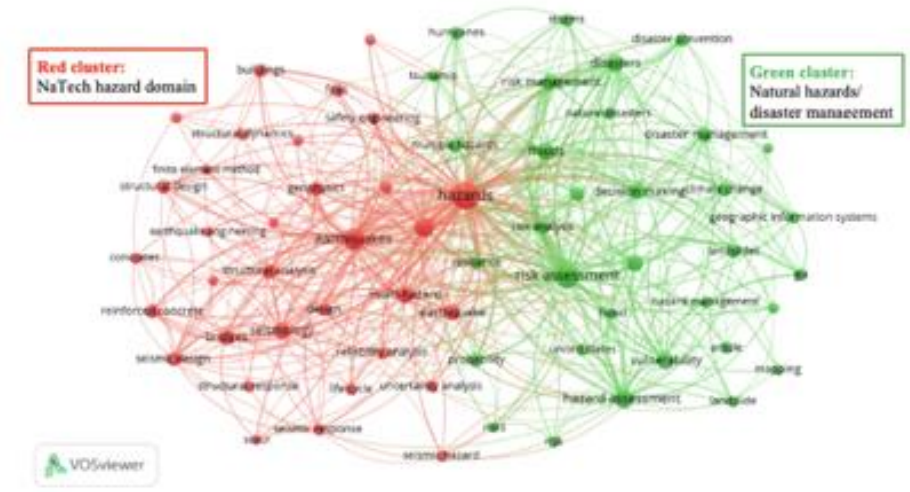

Figure 58: Network map of research on multi-hazards extracted from Scopus, N=1016

Table 19: Keyword clusters on multi-hazards illustrated with occurrence and link strength

Cluster 1 (33 terms)			Cluster 2 (33 terms)		
Term	**Occurrence**	**Link strength**	**Term**	**Occurrence**	**Link strength**
hazards	461	2249	risk assessment	290	1429
earthquakes	199	1191	floods	115	688
multi-hazards	158	819	hazard assessment	139	688
multi-hazard	104	516	disasters	122	614
seismology	92	498	decision making	83	464
earthquake	83	492	risk management	94	452
geophysics	61	424	natural hazard	93	428
structural analysis	58	372	vulnerability	94	428
Bridgets	65	348	risk perception	55	361
seismic design	61	345	probability	60	350
design	47	279	risk analysis	57	329
reinforced concrete	54	274	multiple hazards	53	298
structural design	54	272	disaster management	71	289
seismic response	38	251	geographic information systems	34	277
safety engineering	39	237	disaster prevention	48	271
damage detection	35	215	landslides	47	267
uncertainty analysis	37	214	climate change	54	262
buildings	43	211	storms	47	253
fires	44	197	gis	41	224
seismic hazard	31	189	natural disasters	37	218
reliability analysis	31	187	tsunamis	40	212
life cycle	35	186	flooding	32	197
monte carlo methods	26	176	united states	39	191
scour	25	174	landslide	30	189
multi hazard approach	29	167	risks	26	189
structural response	28	167	flood	32	185
structural dynamics	31	158	hazard management	41	174
earthquake engineering	25	157	resilience	35	158
concretes	28	145	remote sensing	26	156
finite element method	25	145	risk	27	148
multihazard	30	143	article	34	141
multihazard deseign	26	137	mapping	27	141
progressive collapse	28	127	hurricanes	50	126

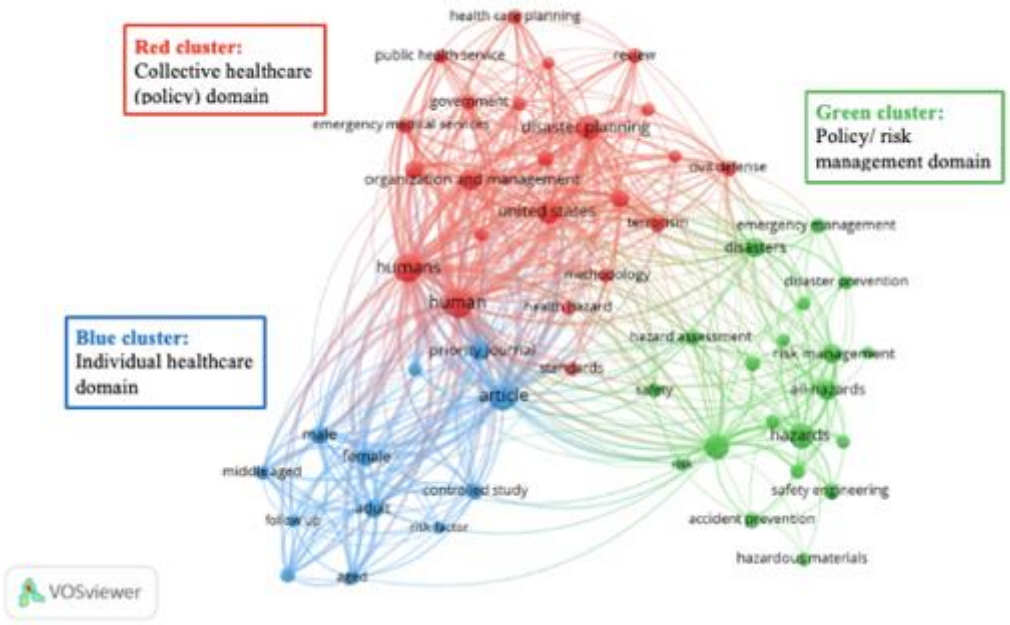

Figure 59: Network map of research on all-hazards extracted from Scopus, N=951

Table 20: Keyword clusters on all-hazards illustrated with occurrence and link strength

Cluster 1 (23 terms)			Cluster 2 (20 terms)			Cluster 3 (12 terms)		
Term	**Occurrence**	**Link strength**	**Term**	**Occurrence**	**Link strength**	**Term**	**Occurrence**	**Link strength**
human	277	1883	risk assessment	149	613	article	209	1462
humans	230	1670	disasters	79	422	priority journal	79	634
disaster planning	146	1086	hazards	158	419	female	63	561
united states	131	925	risk management	80	303	male	62	556
organisation and management	93	680	all-hazards	99	277	adult	60	495
emergency health service	67	559	hazard assessment	38	209	controlled study	43	362
disaster	61	450	safety	32	183	aged	39	357
terrorism	54	343	decision making	32	150	major clinical study	37	329
public health	47	337	risk analysis	37	133	middle aged	34	322
emergency medical service	40	334	emergency management	32	125	follow up	23	207
civil defence	47	327	accident prevention	48	119	procedures	28	194
government	35	293	disaster prevention	26	109	risk factors	21	173
public health service	31	288	safety engineering	43	108			
health care planning	32	262	risk perception	27	103			
health care personnel	28	248	disaster management	25	101			
review	36	230	probability	25	95			
methodology	33	229	earthquakes	21	89			
education	25	216	risk	20	84			
emergency care	20	186	resilience	24	57			
health hazard	27	182	hazardous materials	30	27			
mergency	27	173						
emergency preparedness	23	171						
standards	26	142						

14 Bibliography

[1] UNISDR, "National Disaster Risk Assessment - Governance System, Methodologies, and Use of Results," UNISDR, 2017.

[2] EU Commission, "Digital Economy and Society Index (DESI) 2019 Country Report - Denmark," EU Commission, 2019.

[3] D. Rehak and M. Hromada, "Failures in a Critical Infrastructure System," in *System of System Failures*, 2018, pp. 75-93.

[4] E. M. Brunner and M. Suter, "International CIIP Handbook 2008/2009," ETH - Center for Security Studies, Zurich, 2008.

[5] J. Metzger, "The Concept of Critical Infrastructure Protection (CIP)," *Business and Security: Public-Private Sector Relationships in a New Security Environment*, p. 197–209, 2004.

[6] EU Commission, "EUR-Rex NIS Directive 2016/1148," EU Commission, Brussels, 2016.

[7] S. Rinaldi, J. Peerenboom and T. Kelly, "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," IEEE Control Systems, 2002.

[8] EU Commission, "European Programme for Critical Infrastructure Protection," EU Commission, Brussels, 2006.

[9] EU Commission, "Council Directive 2008/114/EC - 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*, vol. L 345, pp. 75-82, 2008.

[10] ENISA, "Methodologies for the identification of Critical Information Infrastructure assets and services," European Union Agency for Network and Information Security, 2015.

[11] Ministry of Finance, "Danish Cyber and Information Security Strategy," Danish Government, Copenhagen, 2018.

[12] Direktoratet for samfunnssikkerhet og beredskap, "Samfunnets kritiske funksjoner," 2016.

[13] M. Baezner and S. Cordey, "National Cybersecurity Strategies in Comparison," Center for Security Studies (CSS), ETH Zurich, 2019.

[14] Danish Government, "Aftale på Forsvarsområdet 2018-2023," Danish Government, 2018.

[15] United Nations - Economic and Social Affairs, "United Nations eGovernment Survey 2018," United Nations, 2018.

[16] Danish Government, "A stronger and more secure digital Denmark 2016-2020," Danish Government, 2016.

[17] Danish Emergency Management Agency, “DEMA’s Approach to Risk and Vulnerability Analysis for Civil Contingency Planning,” Danish Emergency Management Agency, Birkerød, 2005.

[18] R. Lahidji and M. Undseth, “OECD Studies in Risk Management Denmark,” OECD, Paris, 2006.

[19] Danish Ministry of Defence, “Act of Preparedness,” 2008.

[20] M. S. Jensen, “Sector Responsibility or Sector Task? New Cyber Strategy Occasion for Rethinking the Danish Sector Responsibility Principle,” *Scandinavian Journal of Military Studies,* vol. 1, no. 1, pp. 1-18, 2018.

[21] M. S. Jensen, “Cyberresiliens, sektorprincip og ansvarsplacering – nordiske erfaringer,” *Internasjonal Politikk - Skandinavisk Tidsskrift for Internasjonale Studier,* vol. 77, no. 3, pp. 266-277, 2018.

[22] K. K. Christensen and K. L. Petersen, “The Cyber Threat,” University of Copenhagen, Copenhagen, 2017.

[23] US Government Accountability Office, “Internet Infrastructure DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan,” GAO, 2006.

[24] Ministry of Defence, “Bekendtgørelse af lov om Center for Cybersikkerhed,” Danish Government, 2018.

[25] Ministry of Defence, “Bekendtgørelse af lov om Center for Cybersikkerhed,” Danish Government, 2014.

[26] Centre for Cyber Security, “Cyber and Information Security Strategy for the Tele Sector,” Agency for Digitisation, 2018.

[27] Danish Government, “Danish Cyber and Information Security Strategy,” Ministry of Finance, Copenhagen, 2018.

[28] EU Commission, “Regulation No 910/2014,” *Official Journal of the European Union,* vol. 257, pp. 73-114, 2014.

[29] Danish Ministry of Defence, “Bekendtgørelse om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed,” Danish Government, 2016.

[30] V. Vassilakis and I. D. Moscholios, “Static and Dynamic Analysis of WannaCry Ransomware,” 2018.

[31] M. Baezner and P. Robin, “Stuxnet,” Center for Security Studies (CSS), ETH Zürich, 2015.

[32] Agency for Digitisation, “Det offentlige Danmark 2019,” Ministry of Finance, 2019.

[33] W. Jerbi, J. Gaudreault, M. N. S. L. Sophie D’Amours, P. Marier and M. Bouchard, “Optimization/simulation-based Framework for the Evaluation of Supply Chain Management Policies in the Forest Product Industry,” in *FORAC Research Consortium, Université Laval*, Québec, Canada, 2012.

[34] Ministry of Climate, Energy and Utilities, “Cyber- og informationssikkerhedsstrategi for energisektorerne,” Ministry of Climate, Energy and Utilities, 2019.

[35] C. f. C. Security, “Cybertruslen mod energisektoren,” Centre for Cyber Security, 2018.

[36] Energinet, “Roller på elmarkedet,” 2019. [Online]. Available: https://energinet.dk/El/Elmarkedet/Roller-paa-elmarkedet. [Accessed 2019].

[37] Danish Ministry of Climate, Energy and Utilities, “Bekendtgørelse om it-beredskab for el- og naturgassektorerne,” Danish Government, 2019.

[38] Danish Ministry of Climate, Energy and Utilities, “Bekendtgørelse om beredskab for oliesektoren,” Danish Government, 2018.

[39] Danish Ministry of Climate, Energy and Utilities, “Cyber and information security strategy for the energy sectors,” 2018.

[40] Energinet, “Introduktion til elmarkedet,” Energinet.dk, 2016.

[41] Energinet, “Energinet,” 2019. [Online]. Available: https://energinet.dk. [Accessed 2019].

[42] Danish Maritime Authority, “Strategy for the maritime sector's cyber and information security,” 2019.

[43] Danish Maritime Authority, “The Blue Denmark,” 2019. [Online]. Available: https://www.soefartsstyrelsen.dk/Presse/temaer/DetBlaaDanmark. [Accessed 2019].

[44] DAMVAD Analytics, “Danish Maritime Research 2008-2017,” DAMVAD Analytics, 2019.

[45] Open Geospatial Consortium and International Hydrographic Organisation, “Development of Spatial Data Infrastructures for Marine Data Management,” 2019.

[46] Danish Ministry of Health, KL and Danish Regions, “En styrket, fælles indsats for cyber- og informationssikkerhed,” 2019.

[47] Centre for Cyber Security, “The cyber threat to the Health sector,” CFCS, 2018.

[48] V. Venkatraman, P. Mani and A. Ussing, “Mapping the Healthcare Data Landscape in Denmark,” Leapcraft, 2015.

[49] Transport, Construction and Housing Authority, “Strategi for cyber-og informationssikkerhed i transportsektoren, 2019-2021,” Ministry of Transport, Building and Housing, 2019.

[50] Rail Denmark, “Network Statement 2019,” 2019.

[51] Transport, Construction and Housing Authority, “Plan for the Traffic, Building and Housing Authority's Safety Supervision 2019 - Railway,” 2019.

[52] Naviair, “Web page,” 2019. [Online]. Available: http://www.naviair.dk. [Accessed 2019].

[53] Ministry of Transport and Housing, “Danish Aviation: Summary of the report from the committee of Danish aviation,” Ministry of Transport and Housing, 2012.

[54] SESAR Joint Undertaking, “Accelerating the pace of change in air traffic management,” 2019. [Online]. Available: https://www.sesarju.eu/node/3366. [Accessed 2019].

[55] Danish Road Directorate, “Future of the roads,” 2019. [Online]. Available: https://www.vejdirektoratet.dk/side/fremtidens-veje. [Accessed 2019].

[56] Road Directorate, “OTMAN - Common traffic information,” 2019.

[57] Road Directorate, “Catalog of sector development forums in the Road Directorate,” 2017.

[58] Teracom, Telenor, G. HI3G, STOFA, TDC, Eniig, Fibia, Waoo, Telia and D. Beredskabskommunikation, “Telesektoren,” DI, Digital, DE, Teleindudstrien, IT-branchen and Dansk Erhverv, 2018.

[59] Danish Energy Agency, “Competition regulation in the telecommunications field,” 2019. [Online]. Available: https://ens.dk/ansvarsomraader/telepolitik/konkurrenceregulering-paa-teleomraadet. [Accessed 2019].

[60] DeiC, “TELEDCIS,” 2019. [Online]. Available: https://www.teledcis.dk. [Accessed 2019].

[61] Danish Financial Supervisory Authority, “Financial Sector Strategy - Cyber and Information Security (2019 - 2021),” 2019.

[62] Financial Supervisory Authority , “Strategy for the financial sector - Cyber and information security 2019 - 2021,” 2019.

[63] Danish Financial Supervisory Authority, “Decentral enhed for cyber- og informationssikkerhed for finanssektoren (DCIS),” 2019. [Online]. Available: https://www.finanstilsynet.dk/Om-os/DCIS. [Accessed 2019].

[64] Danish Financial Supervisory Authority, “Strategi for cyber- og informationssikkerhed i finanssektoren,” 2019.

[65] Centre for Cyber Security, “Cyber Threat against the Financial Sector,” 2018.

[66] Financial Supervisory Agency, “Systemisk vigtige finansielle institutter (SIFI),” 2019. [Online]. Available: https://www.finanstilsynet.dk/~/media/Nyhedscenter/2019/SIFI-udpegning-2019-Danmark-samlet-oversigt-pdf.pdf?la=da. [Accessed 2019].

[67] Financial Supervisory Authority, “Key figures for financial undertakings under supervision in the period 2013-2017,” 2017.

[68] FindBank, “Banker i Danmark,” 2019. [Online]. Available: https://www.findbank.dk/banker-i-danmark/. [Accessed 2019].

[69] L. Nielsen and M. H. Faber, “Toward an information theoretic ontology of risk, resilience and sustainability and a blueprint for education,” *Journal of Sustainable and Resilient Infrastructure.*

[70] World Economic Forum, “The Global Risks Report 2019 14th Edition,” World Economic Forum, Geneva, 2019.

[71] Hybrid CoE, “Hybrid CoE,” 2019. [Online]. Available: https://www.hybridcoe.fi. [Accessed 2019].

[72] EU Commission, “Joint Framework on countering hybrid threats a European Union response,” EU Commission, 2016.

[73] OECD, “Governance challenges for critical infrastructure resilience - Good Governance for Critical Infrastructure Resilience,” OECD Publishing, Paris, 2019.

[74] J. C. Gill and B. D. Malamud, “Hazard interactions and interaction networks (cascades) within multi-hazard methodologies,” *Earth Syst. Dynamics,* vol. 7, p. 659–679, 2016.

[75] M. Theocharidou and G. Giannopoulos, “Risk assessment methodologies for critical infrastructure protection. Part II: A new approach,” EU Commission: Joint Research Centre Institute for Protection and Security of the Citizen, Luxembourg, 2015.

[76] C. J. V. Westen and S. Greiving, “Multi-hazard risk assessment and decision making,” in *Environmental Hazards Methodologies for Risk Assessment and Management,* IWA Publishing, 2017, pp. 31-94.

[77] S. Girgin, A. Necci and E. Krausmann, “Dealing with cascading multi-hazard risks in national risk assessment: The case of Natech accidents,” *International Journal of Disaster Risk Reduction,* vol. 35, 2019.

[78] A. Clark-Ginsberg, L. Abolhassanic and E. A. Rahmatic, “Comparing networked and linear risk assessments: From theory to evidence,” *International Journal of Disaster Risk Reduction,* vol. 30, pp. 216-224, 2018.

[79] US Homeland Security, “Buildings and Infrastructure Protection Series Integrated Rapid Visual Screening of Buildings,” US Homeland Security Science and Technology, 2011.

[80] OECD, “All hazards and transboundary risk governance,” in *Assessing Global Progress in the Governance of Critical Risks,* 2019, pp. 21-41.

[81] N. B. Truong, U. Jayasinghe, T.-W. Um and G. M. Lee, “A Survey on Trust Computation in the Internet of Things,” *The journal of Korean Institute of Communication and Information Sciences,* pp. 10-27, 2016.

[82] F. B. Duhamel, G.-M. Isis, S. Picazo-Vela and L. Luna-Reyes, “Determinants of collaborative interfaces in public-private IT outsourcing relationships,” *Transforming Government: People, Process and Policy,* vol. 12, no. 1, pp. 61-83, 2018.

[83] M. Dunn-Cavelty and M. Suter, “Public-Private Partnerships are no silver bullet: an expanded governance model for critical infrastructure protection,” *International Journal of Critical Infrastructure Protection,* vol. 2, no. 4, pp. 179-187, 2009.

[84] J. D. Donahue and R. f. Zeckhauser, “Sharing the watch: Public-private collaboration in infrastructure security,” in *Seeds ofDisaster, Roots ofResponse: How Private Action Can Reduce Public Vulnerability*, New York, Cambridge University Press, 2006, pp. 429-456.

[85] B. Rajaonah, *A view of trust and information system security under the perspective of critical infrastructure protection*, 2017.

[86] E. U. A. f. N. a. I. Security, “Public Private Partnerships (PPP) Cooperative models,” EU Commssion, 2017.

[87] TISN, “Trusted Information Sharing Network,” 2019. [Online]. Available: https://www.tisn.gov.au/Pages/Cyber_security.aspx. [Accessed 2019].

[88] Government of Canada, “Canadian Critical Infrastructure Information Gateway,” 2019. [Online]. Available: https://cigateway.ps.gc.ca. [Accessed 2019].

[89] Homeland Security, “Information Sharing and Analysis Organizations (ISAOs),” 2019. [Online]. Available: https://www.dhs.gov/cisa/information-sharing-and-analysis-organizations-isaos. [Accessed 2019].

[90] EU Migration and Home Affairs, “Critical Infrastructure Warning Information Network (CIWIN),” 2019. [Online]. Available: https://ec.europa.eu/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network_en. [Accessed 2019].

[91] European Union Agency For Network and Information Security, “Information Sharing and Analysis Centres (ISACs) Cooperative models,” EU Commission, 2017.

[92] R. Setola and M. Theocharidou, “Modelling Dependencies Between Critical Infrastructures,” in *Managing the Complexity of Critical Infrastructures*, Springer, 2017, pp. 19-41.

[93] M. Ouyang, “Review on modeling and simulation of interdependent critical infrastructure systems,” *Reliability Engineering and Systems Safety*, vol. 121, pp. 43-60, 2014.

[94] O. Kammouh and G. P. Cimellaro, “Cyber threat on critical infrastructure,” in *Routledge Handbook of Sustainable and Resilient Infrastructure* , Routledge, 2019, pp. 359-373.

[95] M. Dunn and I. Wigert, “International CIIP Handbook 2004 - An Inventory and Analysis of Protection Policies in Fourteen Countries,” ETH Zurich, Zurich, 2004.

[96] Denmark Statistik, “It-anvendelse i virksomheder,” 2017.

[97] Ministry of Industry, Business and Financial Affairs, “Bekendtgørelse om outsourcing af væsentlige aktivitetsområder,” Danish Government, 2010.

[98] Centre for Cyber Security, “Outsourcing - who is in charge?,” CFCS, 2017.

[99] Centre for Cyber Security, “Trusselsvurdering: Cybertruslen mod telesektoren,” CFCS, Copenhagen, 2019.

[100] M. H. Faber, "On sustainability and resilience of engineered systems," in *Routledge Handbook of Sustainable and Resilient Infrastructure*, Taylor & Francis Ltd, 2019, pp. 28-48.

[101] T. P. McAllister and S. Moddemeyer, "Aligning community resilience and sustainability," in *Handbook of Sustainable and Resilient Infrastructure*, Routledge Taylor & Francis, Oxon, 2019, pp. 15-27.

[102] S. Thacker, D. Adshead, G. Morgan, S. Crosskey, A. Bajpai, P. Ceppi, J. W. Hall and N. O'Regan, "Infrastructure - Underpinning Sustainable Development," UNOPS, Copenhagen, 2018.

[103] J. Zhuang and V. Bier, "Balancing Terrorism and Natural Disasters: Defensive Strategy with Endogenous Attacker Effort," *Operations Research,* vol. 55, no. 5, pp. 976-991, 2007.

[104] C. Folke, T. Hahn, P. Olsson and J. Norberg, "Adaptive governance of social-ecological systems," *Annual Review of Environment and Resources,* vol. 15, no. 30, pp. 441-473, 2005.

[105] F. Berkes, "Evolution of co-management: Role of knowledge generation, bridging organizations and social learning," *Journal of Environmental Management,* vol. 90, p. 1692–1702, 2009.

[106] L. Nielsen and M. H. Faber, "Impacts of Sustainability and Resilience Research on Risk Governance," *Sustainable and Resilient Infrastructure,* 2018.

[107] T. Bjerga and T. Aven, "Adaptive risk management using new risk perspectives - An example from the oil and gas industry," *Reliability Engineering & System Safety*, vol. 134, pp. 75-82, 2015.

[108] N. J. van Eck and L. Waltman, "Manual for VOSviewer version 1.6.6," Scopus, 2017.

[109] Federal Republic of Germany, "National Strategy for Critical Infrastructure Protection (CIP Strategy)," Berlin, 2009.