Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Jakob Vagle

Investigating Business Alignment Issues Rooted in the Norwegian Specialist Health Services' Cybersecurity Culture, Through a Systems Thinking Approach

Master's thesis in Information Security
Supervisor: Mazaher Kianpour
June 2020

NTNU
Kunnskap for en bedre verden

Jakob Vagle

Investigating Business Alignment Issues Rooted in the Norwegian Specialist Health Services' Cybersecurity Culture, Through a Systems Thinking Approach

Master's thesis in Information Security
Supervisor: Mazaher Kianpour
June 2020

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

Abstract

The Norwegian Healthcare System (NHS) is composed of heterogeneous, interacting stakeholders with different roles at different societal levels (i.e. national, national professional, regional, and operational). This complex system is digitalizing at a rapid pace through a plethora of technological inventions and social structures. As a consequence of the system becoming the target of an increasing number of cyber attacks, cybersecurity has become one of its primary concerns. This paper adopts the socio-technical paradigm and employs concepts such as systems thinking, system dynamics, and various behavioral theories in order to understand the system's nonlinear behavior. This understanding will help us frame and discuss problems rooted in the cybersecurity culture of relevant stakeholders, as these issues lead to misalignment and the provision of inadequate cybersecurity. Through considering relevant documents and related work, this thesis investigates the system to identify the stakeholders, their responsibilities, and their relationships. Causal loop diagrams are used to visualize how different variables in the system are interrelated. Further, these diagrams are transformed into stock and flow diagrams in order to study the system quantitatively. Finally, we simulated the model of the system being studied and analyzed the results.

Modeling the system helps us understand the unique characteristics of the NHS, determine meaningful relations among its stakeholders, and identify the factors affecting its cybersecurity posture. Further, system dynamics simulation enables the observation and prediction of the system's state while considering the dynamics, complexities, and uncertainties that arise from incomplete and imperfect information in the system. Finally, it provides a base case of the NHS, which can be further improved upon if given more information. The simulation model can be used to aid decision makers in the system in order to find solutions for cybersecurity cultural problems, as well as align stakeholders to enhance cybersecurity resilience in the system. The results show that national level interventions that target the root issue of decentralized management, strategic direction, and legal frameworks could increase the influence of both national professional and regional level stakeholders. This increased influence would, in turn, increase the opportunity and willingness of operational stakeholders to increase capability development. Ultimately, the NHS' cybersecurity posture would enhance through developing solutions that target the culturally-rooted issues which lead to business misalignment.

Abbreviations

Table 1: Abbreviations

Abbreviation	Meaning
HT	Health Trusts
HOD	Ministry of Health and Care Services/Helse- og omsorgs-departementet
ISMS	Information security management system
IKT-Providers	Information technology provider
NHS	National health service
NSHS	Norwegian Specialist Health Care Service
PH	Primary Healthcare
RHA	Regional healthcare authorities
RQ	Research Question
ST	System Thinking
STS	Socio-technical System
DSR	Design science research methodology

Contents

Figures

Tables

Chapter 1

Introduction

1.1 Topics covered

This thesis covers two main topics and several subtopics. The first of which regards understanding complex systems through an approach largely based on systems thinking (ST), system dynamic modelling (SD), and socio-technical systems (STS). Together, these theories create a holistic framework for analyzing and modeling systems [1][2]. The second primary focus of this thesis surrounds cybersecurity and cybersecurity culture, based on the ST/STS paradigm of understanding system concepts -— culture included —- and interaction between systemic constructs. Cybersecurity culture is also examined from the perspective of social sciences and behavioral theories. These theories, models, and modelling techniques will together aid in the investigation of cybersecurity issues in the Norwegian Health Sector (NHS) rooted in cybersecurity culture.

Keywords

1. Business alignment
2. Cybersecurity
3. Culture
4. Cybersecurity behavior
5. Information security
6. Healthcare
7. System Thinking
8. System Dynamics
9. System dynamic modelling

1.2 Cybersecurity in the health sector

As societies become increasingly digitalized, their dependency on technology increases. As a consequence, cybersecurity is an important aspect of any contemporary business or organization interested in protecting the confidentiality, integrity,

and availability of their information and systems. In the last few decades, the protection of information assets in healthcare such as personally identifiable information (PII) and protected health information (PHI) has failed. Poor cybersecurity practices can lead to sensitive information being exposed, and may even cause healthcare services to become temporarily unavailable. In 2018, a Norwegian regional healthcare authority (RHA) fell victim to a cyber attack (Helse Sør-Øst [3]). The attacker(s) were professional and tried to access the RHA's networks, potentially exposing three million sensitive patient records. "Politiets Sikkerhets Tjeneste" (PST) never found the culprit [4]. In 2013, the Oslo University Hospital was the target of a successful virus attack, which rendered their systems unavailable [34]. Further, a ransomware cryptoworm, WannaCry, impacted around 200,000 computers across 150 different countries in 2017. One of the sectors hit hardest was healthcare, especially in the United Kingdom. It is estimated to have cost UK healthcare £20 million as a consequence of the 19,000 appointments canceled between the 12th and 19th of May. When accounting for the cleanup and upgrade process, the total cost to UK healthcare services rises to a total £92 million [5]. As these cases demonstrate, cyber attacks and increased risk exposure due to digitalization make cybersecurity in the healthcare sector a crucial topic not only in the foreseeable future, but in the immediate present as well.

1.2.1 Problem description

Despite cyber attacks often revolving around utilizing technology, technology should not always be blamed as the root cause of incidents. Cyber attacks may instead be a consequence of factors related to the social aspect of cybersecurity, such as inadequate employee awareness. Defending against cyber attacks is therefore a multidisciplinary inquiry, wherein human behavior and culture are as important as the technology and systems used. Even though a system may be technologically robust, there are numerous human factors that threaten its security. For instance, what if the implemented technology is difficult for employees to use, resulting in a crippling effect on work effectiveness? Would one let their manager and/or patient down, or expose the organization to risk by circumventing policy and procedure? As the numbers show, only 20% of threats are mitigated through solely relying on technology. Most solutions are a combination of social and technical aspects [6].

When investigating the cause of successful cyber attacks, one must observe technology in relation to the people using it. The social aspects of cybersecurity, including how systems are used, often contribute to the success of cyber attacks. This risk can be mitigated through fostering a strong cybersecurity culture. Employees possessing high levels of awareness, knowledge, and expertise of digital threats would themselves provide effective protection. Good cybersecurity culture could lessen significant risk factors, but is difficult to build, maintain, and optimize. Recognizing the importance of the social aspect of cybersecurity motivates

the main topics examined in this thesis: system complexity and cybersecurity culture. Systems composed of several components interacting with each other can be argued as complex, which is the case when investigating cybersecurity in organizations (socio-technical system). The concept of system complexity is important within the adopted paradigm of ST and STS. Through systems thinking, one argues that all variables and internal/external factors must be considered in order to fully understand a system. In other words, to investigate a tree one must also see the the forest, its surrounding ecosystem, and all factors impacting our seemingly simple, individual, tree of choice.

It is believed to be nearly impossible for humans to fully comprehend and understand a complex system [1][2][7]. Understanding system behavior is further complicated when one not only wants to investigate a complex system, but a complex phenomenon such as cybersecurity culture. Cybersecurity culture is the collection of perceptions, attitudes, values, assumptions, and knowledge that guides employee behavior in situations related to the preservation of cybersecurity [8]. The collection of factors determining culture is the result of several other systemic aspects, such as technology, methods, and structure. In consideration of cybersecurity culture's inherent broad and complex nature, examining it within an interconnected paradigm raises one of the main challenges this thesis seek to address. Namely, how a complex socio-technical system, such as the Norwegian National Health Service (NHS), can be analyzed with the aim of identifying issues rooted in cybersecurity culture.

1.2.2 Justification, motivation, and benefits

Norway's healthcare is argued as a complex system as it includes several interconnected components which influence each other. It is highly digitalized, with several aspects affecting the the NHS's cybersecurity culture and resilience against cyber attacks. These aspects reside in both social and technical system constructs. There are organizational modernization efforts conducted on various levels. These efforts include, for example, evolving organizational structures and new legal and regulatory requirements (e.g. through the GDPR affecting personal data, as well as newly-founded governing bodies like the directorate of eHealth). In addition, there is significant diversity among stakeholders in terms of their objectives and role on both the organizational and individual level. The NHS is of significant size, with one state ran hospital region (RHA) having approximately 80,000 employees [9] (Helse Sør-Øst). Further, different stakeholders [10] are involved in governance and decisions related, but not limited, to politics, strategy, finance, and cybersecurity across the NHS. As these decisions influence and govern lower-level institutions like hospitals, this diversity may make it difficult to align stakeholder interests and enact effective policy. Importantly, there may be differences in how these stakeholders recognise the threat of cyber attacks and foster strong cybersecurity culture.

In the healthcare sector, the ability for practitioners to effectively treat patients is crucial. Emerging technological solutions can contribute to enhancing both efficiency and patient care, while satisfying increasing demands for healthcare in our society. As a consequence of ageing populations, the need for healthcare may, in the future, supersede what the system can handle today. Therefore, digitalization is an important method of accounting for the growing needs of populations in the healthcare sector. However, the system as a whole needs to adapt to growing public demand and increased digitalization, including both technological systems and the people who interact with them. It is equally important to build a resilient social structure and strong cybersecurity culture which can balance out technological inventions, increased complexities, modernization, and threats to cybersecurtiy in order to ensure patient care and system security.

The benefit of investigating cybersecurity culture through the proposed paradigm is that it allows the system to be analyzed holistically. This is important, as in situations where a causal relationship is not apparent, an action could have unintended consequences which are hard to identify for the stakeholder responsible for any given change. Through a holistic approach, decision makers can avoid or remedy these consequences by gaining insight into how changing and impacting one system construct or factor may impact others. This understanding reflects the goal of this approach, which is to ultimately unravel the dynamics of cybersecurity culture and find the root causes of interconnected problems and issues.

1.3 Research questions and objective

The research objective describes the expected goal of the thesis and provides a general direction. It specifies an objective which is thought to result in new and useful information for the research community and the investigated system. The research questions (RQ's) provided are more specific in nature and define the questions that need to be answered in order for the author to be able to achieve the objective. Research questions are an essential part of guiding the efforts and activities performed during the thesis, and is discussed in relation to the adopted methodology (3). During the introductory chapter, the RQ's and objective are explained in relation to previously-presented information. It is justified in terms of the value of answering these crucial questions. In addition, information provided within the background section (2) will further justify the selection of RQ's and this text's objective.

Research objective

The main goal of this study is **To identify business alignment problems among stakeholders rooted in cybersecurity culture and propose solutions in order**

to enhance cybersecurity posture in the Norwegian healthcare digital ecosystem.
In a socio-technical system with high complexity, stakeholder diversity, and interaction, it becomes increasingly difficult to achieve business alignment. Business alignment is subject to complications as stakeholder dynamics may limit or influence a stakeholder's ability to achieve its goal. Stakeholders may have a different or limited understanding of problems, resulting in sub-optimal actions —- which are more likely as system complexity and stakeholder diversity grows. This thesis seeks to explore how business misalignment causes problems for cybersecurity, and investigate the culturally-rooted causes of such misalignment. This information can subsequently be used to improve the cybersecurity posture of systems. Cybersecurity culture is argued as a highly interconnected concept and therefore includes several external system aspects which impact its development, strengths, weaknesses, and maintenance. Cybsercutiy culture further includes technological and social influences such as regulation, policy, governance, software solutions, endpoint complexity, cybersecurity knowledge, and awareness. These aspects are influenced by stakeholders on different levels and are subject to cultural influence.

RQ1:

How can the Norwegian healthcare system, which is argued as a complex system, be modelled to investigate business alignment and cybersecurity culture among stakeholders?
Modelling is used as means to investigate complex, interconnected, and dynamic environments. To create an effective model, one needs to determine the modelling approach, system boundaries, and theoretic foundation on which it will be based. These factors need to compliment the overall goal and requirements of the model and be targeted towards the system being investigated.

RQ2:

How do inter/intra dynamics of stakeholders influence cybersecurity culture and expose the system to increasing cybersecurity risk?
To model business alignment, the interactions within the environment must be in focus. These interactions include the socio-technical aspects of the system which are believed to be relevant. For instance, the differences in cybersecurity culture, or other systemic aspects, which negatively affect business alignment across different hierarchical levels of a system and thus result in increased risk. The knowledge gained from investigating the role of different stakeholders, their interrelations with each other, and socio-technical system aspects, can help analyze how the system strengthens or weakens cybersecurity culture, how cybersecurity influences system behavior, and how the behavior of stakeholders are aligned in terms of their overall objective. In other words, interconnectedness comes to fruition when the cause and effect relationship between socio-technical aspects and stakeholders is identified to produce an increased understanding of culture, behavior,

and business alignment.

RQ3:

How can the developed artifact be used to improve cybersecurity culture in the NHS?
The knowledge of how stakeholders and systemic constructs interrelate, within the paradigm of systems thinking, can be used to find vulnerabilities and areas for improvement which are not easily spotted through linear and short-term analysis. As a result, this knowledge is especially useful for improving business alignment and cybersecurity culture. Relationships stemming from fields such as regulation, law, and technology are considered in order to build an interconnected and complex understanding of culture – as well as its maintenance and development. This strategy further facilitates holistic problem identification and possible identification of improvements related to all systemic aspects. Using modelling to facilitate organizational learning is a quintessential component of illustrating how the NHS can improve its cybersecurity culture. A complete model can be used in simulations of scenarios to aid in effective decision making and improve business alignment in regards to cybersecurity. The developed artifact can also serve as a proof of concept, demonstrating that the leveraged modelling tools can be applied to the NHS in order to effectively illustrate issues and potential improvement strategies. While the model may not necessarily provide accurate simulation results, it can nevertheless illustrate general relationships and system behavior.

1.4 Scoping the thesis

Narrowing the scope of this thesis will compensate for challenges such as the broad nature of the adopted paradigm, the fact that the investigated topic of cybersecurity culture involves many aspects of organizational theory and cybersecurity, and the complexity of system-stakeholder relationships. To adequately approach these issues, the system dynamic model will first be limited to identified problems related to the selected topic, rather than attempting to model the entire system. Analysing specific problems related to a given topic can highlight the unique characteristics of the NHS, determine meaningful relations among its stakeholders, and identify the factors affecting its cybersecurity culture. Second, the system will be limited by focusing on a selection of stakeholders specifically regarding the Norwegian Specialist Health Care Services (NSHS) and their multifaceted relationships. The NSHS is the state-ran part of the NHS, and excludes services provided by municipalities. The stakeholders investigated in this text mainly include the government, professional agencies, high-level management in regional health authorities (RHA), and their subordinate institutions (particularly hospitals). Stakeholder relationships are categorized as national, professional, regional, and operational. These labels ensure a holistic approach while preventing the

model from becoming needlessly complex as a consequence of discussing each stakeholder individually.

While the adopted paradigm highlights the importance of a holistic approach, involving everything relevant to a system or problem, it is not realistic given the available time and resources. Regardless of the proposed scope, the information gained through conducting this research may be transferable to additional issues and system stakeholders. Further, the model can be changed and adapted to different scenarios in future work. Including every system aspect – and staying true to a holistic approach – is argued as fundamentally difficult [2]. The scope of this thesis will be further discussed throughout the course of presenting the system in question and its identified problems.

Chapter 2

Background and related work

The background and related work section serves three main purposes. First it will provide a theoretic foundation. Second, the system in question will be presented. Finally, related works are discussed. There is no data collection adding to the empirical foundation after the section is concluded, making the presentation of the system, theoretical framework, and related works essential in order to establish a paradigm with which one can analyze information about the system in question based on its attributes and current challenges. The related work helps the adopted paradigm and provide insight into how the different aspects of cybersecurity interact with one another.

2.1 Background

2.1.1 Theoretic foundation

In the introduction, key concepts such as systems thinking (ST), socio-technical systems (STS), cybersecurity culture, and business alignment are introduced. To create a broader understanding of the underlying principles and models essential to both ST and STS, they will be explained in more detail. In addition, the concept of cybersecurity culture and its connection to human behavior will be discussed by presenting behavioral models. Ultimately, culture and behavior are placed in the context of business alignment. Presenting the theoretic foundation of this thesis will establish a shared understanding of cybersecurity, while also establishing a general method of connecting stakeholder behavior to cultural challenges and business alignment.

Systems thinking

Background and introduction Globalization, digitalization and the Internet, national and international cooperation, global organizations, and complex supply-chains are all characteristics of modern businesses. Compared to the businesses that existed centuries ago, organizational boundaries and complexity have changed.

With this change, a new approach to management and organizational theory referred to as "Systems Thinking" [2] was introduced. Previously, businesses adopted a divide and conquer strategy. Said strategy has brought much wealth and prosperity to the world through the effective manufacturing and production of goods and services. Analyzing an organization while adopting a systems thinking approach means that one considers the larger picture of the "whole" system and its relationships. The philosophy of systems thinking is interdisciplinary and is adopted by scientists across many different fields of study. Perhaps the most significant work relating to management was published by Peter Senge, in 1990 [7].

The essence of systems thinking Peter Senge [7] argues that if we want to understand the entirety of a system, we need to understand all of its parts – not merely its individual components. Interaction between different parts of the system can be delayed in time and its cause and effect relationships are not apparent, despite being connected to the same pattern. Businesses are impacted by interaction and relationships, and the full effect of a change or action may not come to fruition immediately but rather over the course of several years. This makes observing the whole pattern of change difficult. The whole picture is difficult to understand as humans tend to isolate snapshots of systems [7], effectively limiting our ability to analyze and understand organizational complexity.

Systems thinking is an approach to dealing with the system complexity described above. It is a conceptual framework which provides knowledge and tools to make the connectedness of complex systems more clear and provide an analytical tool to help investigate and change them [7]. It is the study of dynamic cause and effect over time. To show how systems thinking is understood and adopted in this thesis the three dimensions and seven principles are presented as they are described in *System Thinking and System Dynamics* by K. E. Maani and R. Y. Cavana. [2].

Dimensions and principles There are three dimensions to the systems thinking conceptual framework. First, the *paradigm*, which determines how one need to think of the world. This paradigm provides a set of principles which collectively provide the foundation on which systems thinking theory and practice is based. It mainly revolves around considering the big picture, component relations, and interaction in order to acknowledge the dynamic nature of systems. Further, the theory acknowledges that cause and effect is not always a linear process. This means that when we have "means to an end," the end (effect) can influence the means (cause). Second, the *language*, which refers to systems thinking as a tool to communicate and understand complexity and dynamic effect. Lastly, the field of systems thinking incorporates and uses different *methodologies* to learn and model the cause and effect relationships of a given system.[2]. All principles describing systems thinking's theoretical foundation is provided by Anderson [11], and explained by [2], presenting them will help to characterize and explain the systems

thinking framework.

- Thinking of the big picture: Regardless of the problems and situations we are faced with, they are always related to interactions and relations coming from the sum of all system parts.
- Balancing short-term and long-term perspectives: Shot-term wins may result in long term losses, and accumulating short-term effects may critically damage an organization over time.
- Recognizing the dynamic, complex, and interdependent nature of systems: Rather than looking at oneself as a victim, one must see the system as the cause of the problems, as a major part of organizational issues are rooted internally. Additionally, the identified problem may be a symptom. Before being able to create a lasting solution to a problem, the real cause must be found. Further building on complexity, dynamics, and inter-dependencies is the notion that factors are seen as interdependent, with bi-directional cause-and-effect, as well as that different factors have different levels of significance.
- Taking into account both measurable and non-measurable factors: Conventional performance indicators give insight into a specific part of a system, giving information about how well an organization is doing. Productivity is affected by the internal health of an organization. Soft indicators, measures of internal health and vitality, create a general baseline for the organization influencing the typical conventional indicators of performance. Morale, burnout, commitment, loyalty etc. is focused and accounted for when one has adopted the systems thinking paradigm.
- Remembering that we are all part of the system in which we function, and that we each influence those systems even as we are being influenced by them, actions with good intentions may have unintended consequences. Today's solutions may be yesterdays problem [7]. This can be a result of may factors, some of witch are mentioned above. However, it is important to also acknowledge that humans themselves, their assumptions, values, and beliefs may well be the problem. After all, our cultures strongly influence our decisions.

Socio-technical systems theory

Introduction and background A system can be defined as "a regularly interacting or interdependent group of items forming a unified whole" [12]. Defining a system as such creates a broad understanding, which is exactly what is conveyed by the systems thinking paradigm. Socio-technical design is to be thought of as a philosophy rather than as a methodology [13]. To further build on how the NHS is perceived in this thesis, the paradigm is complimented by incorporating socio-technical systems thoughts and theory. The relationship between social and technical factors is the main aspect when investigating cybersecurity culture.

Therefore, this relationship is the explicit focus of this thesis, and discussed regardless of the fact that an ST-approach in its foundation would analyze both social and technical aspects of a given system where appropriate.

Socio-technical systems/design was first developed after World War II. Its creators wanted to optimize human intelligence and skills, and associate these social factors with new technology. Further development was a response to jobs in the 60's and 70's being based highly on routin and tightly controlled with few opportunities for personal growth and self-realization [13]. Over the course of history, socio-technical systems have been interpreted differently, however the focus has always been on both the social and technical aspects of a system [1][14].

The essence of socio-technical systems Socio-technical systems theory, as presented by Kowalski [1], seeks to describe the interconnections and interplay within a socio-technical system (2.1). It focuses on the interaction between people and technology. More concretely, by considering the interplay between culture, structure, methods, and machines. The arrows in the model suggest that any change in one of the concepts, or the environment, will affect the others. A secure system wants to be in "equilibrium", meaning there is balance between all components. This representation of systems builds on the foundation on which systems thinking is based. Practically, the connection between the model's concepts mean that vulnerabilities and threats initially rooted in technology can be mitigated and affected by implementing strategies, policies, or interventions that target other aspects of the system. For example, culture, methods, structure, or machines. Additionally, this representation illustrates the importance of an organization having, for example, sufficient cybersecurity culture when introducing new technologies or other interventions.

Systems thinking and socio-technical systems In the context of this thesis, socio-technical system (STS) theory is applied in order to provide a window into the different parts of an organization while adopting the holistic approach depicted though ST. Specifically, it focuses on the social and technical nature of the NHS and cybersecurity culture. To further conceptualize the NHS as a complex system, Kawalski's model [1] is expanded to support the ST principle of the big picture and recognize the dynamic, complex, and interdependent nature of systems and sub-systems. The model is expanded by incorporating the SBC model, societal levels, and sub-system stakeholder interaction. The SBC model [1] was initially used to perform socio-technical analysis of cybersecurity by providing categories within the social and technical subsystems. It can be used regardless of which societal level is being analyzed. The model is applied to many different approaches of analysing socio-technical systems, such as Bilal Al Sabbaghs socio-technical approach to incident response [14]. In many ways, figure 2.2 illustrates the paradigm adopted for this thesis and incorporates the philosophy of systems thinking.

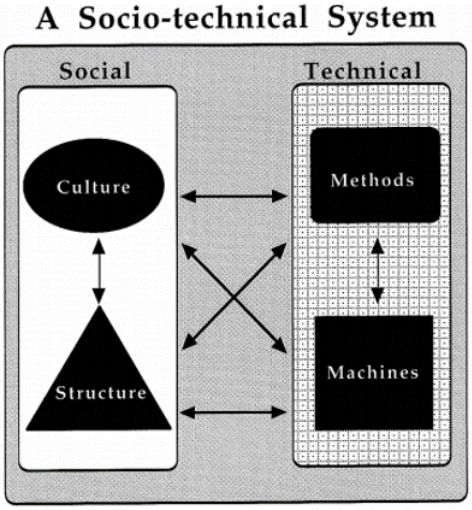

Figure 2.1: A Socio-technical systems, as presented by Kowalski [1], show four main concepts culture, structure, methods, and machines all interacting and impacting the overall system and its security.

First, the model presents the SBC-model and the surrounding socio-technical concepts impacting them. Second, the model is structured in different societal/system levels. Thick arrows indicate that each level impacts the other. Additionally, at each level there are stakeholders (entities) which impact one another. Last, the principles of systems thinking suggest that systems are ecosystems and that thinking "big picture" means seeing the forest and the trees [2]. In other words, a forest (system) consists of several subsystems (trees, weather, animals etc.). Therefore, every entity, regardless of its size, is a socio-technical subsystem. Each societal level, each stakeholder, and every individual is in – on its own – a small subsystem. Together, these subsystems create the system itself, as shown by the figure 2.2. Determining system levels and included stakeholders depends on the systems identified boundaries and the perspective taken when investigating it.

Culture and Cybersecurity

Defining culture and cybersecurity culture One of the primary aims of this thesis is investigating cybersecurity culture, therefore it is essential to discuss culture in relation to cybersecurity and provide definitions. Beginning with organizational culture, which is seen as a combination of artifacts, values and assumptions in an organization that impact and governs organizational action and the behavior of its employees. Cybersecurity culture is defined as: The collection of perceptions, attitudes, values, assumptions and knowledge that guides how things are done in organization in order to be consistent with the Cybersecurity requirements. With

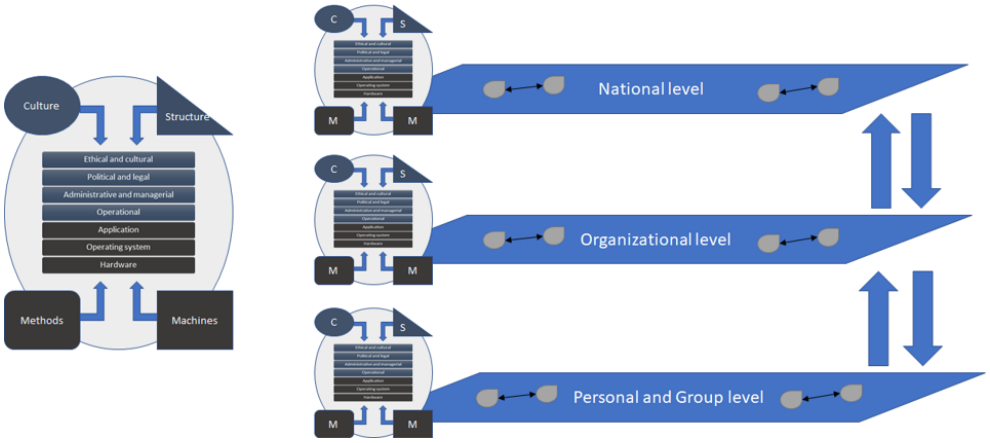

Figure 2.2: Illustrating a system as a system of socio-technical systems on different organizational/societal levels consisting of several stakeholders.

the aim of protecting information assets and influencing employees' security behavior in a way that preserving the Cybersecurity becomes a second nature [8]. By using this definition we can clearly see that culture and behavior are related. The behavior people exhibit in certain situations, their habits, or decisions that has been made in the past determine actions and behavioral patterns, which in-turn can be viewed as expressions culture [15].

One of the main activities performed in this thesis is to identify problem causes rooted in cybersecurity culture and identifying possible stakeholder and system relationships based on previous studies, sector reports and an underlying theoretic foundation. NorSIS [15] discusses the difficulties of measuring culture in the Norwegian society, highlighting the difference between national-level culture and organizational culture. Organizations have defined goals and metrics that help in identifying culture, a nation has not necessarily the same foundation resulting in different approaches to culture. "Different people grab onto different aspects of cybersecurity behavior". NorSIS questions assessing culture as a set of actions which can be altered to increase business value. This approach stand in contrast to the a more interconnected viewpoint of the social and cultural sciences where culture is approached by altering underlying ideas and assumptions. Behavior is only an expression of culture, not culture itself, which is where the focus must be.

Cyber security culture and behavioral models A comprehensive approach to cybersecurity is advised to follow the proposed paradigm of STS and ST, focusing on why organizations/people behave in a certain way rather than the action in itself. One of the concepts of Kowalski's [1] model is culture, indicating that structure, Methods and Machines impact culture. Considering that behavior is culture being expressed [15], these systemic aspects then impact behavior. In the field of social science there are several behavioral models, which seek to understand what

incentivize action and behavior. Some stemming from e.g. criminology, which has inspired both Kowalski's STS model [1] and Mitchie's COM-B model [16]. The latter was brought forward as being suitable to investigate cybersecurity culture when ENISA [17], an esteemed cybersecurity advisory group working to enhance cybersecurity for European Union (EU) member states, analyzed different models applied to the topic. COM-B is a flexible model to assess behavior. Developed by Mitchie et. Al [16] which focused on improving the process of creating policy and making decisions. It builds on the basic principles from behavioral science and US criminology to model behavior. The model show causal relationships between model "components" capability, opportunity, motivation and behavior.

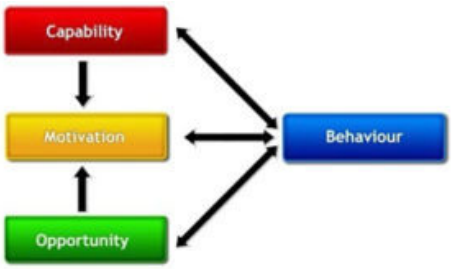

Figure 2.3: The COM-B model, as presented by [16] shows causality between behavior and the components capability, opportunity, motivation.

Mitchie et. Al. [16] define the components of the model as follows: "**Capability** is defined as the individual's psychological and physical capacity to engage in the activity concerned. It includes having the necessary knowledge, and understanding emotional capacity to engage in the activity as well as having the necessary physical skill. Capability governs the thought processes, comprehension, and reasoning needed to behave in a certain way." Capability is linked to behavioral intervention functions such as education, training and enablement. **Motivation** is as defined in the COM-B model as "all those brain processes that energize and direct behavior, not just goals and conscious decision-making. It includes habitual processes, emotional responding, as well as analytical decision-making." Intervention functions targeting motivation are education, persuasion, incentivisation, coercion, environmental restructuring, modelling and enablement. **Opportunity** is defined as "all the factors that lie outside the individual that make the behavior possible or prompt it." It can be achieved through increasing knowledge and understanding to prompt positive feelings about a behavioral target." Opportunity is connected to the intervention functions restriction, environmental restructuring and enablement. Examples of factors effecting opportunity are lack of time or missing economical resources.

Similarly to Kowalski's [1] socio-technical model the arrows in 2.1 illustrate potential influence between the components of the system. In order to change behavior "interventions" are introduced, which is a "coordinated sets of activities

designed to change specified behavior patterns" [16]. An interventions effectiveness is dependent on the interrelationship between the concepts. Models usefulness is enhanced by connecting capability, motivation and opportunity (behavior) to intervention functions, such as education, persuasion, incentivisation, coercion, training, restriction, environmental restructuring, modelling and enablement. The interventions is linked to policies, like communication, guidelines, legislation, regulation etc... The articles final contribution is the behavioral change wheel (BCW) which connects the above concepts. Cane et. al. [18] combine The Theoretical Domains Framework of behavior change (TDF) to the COM-B model. TDF is a theoretical framework rather than a theory. The aim of the Theoretical Domains Framework (TDF) was to simplify and integrate a plethora of behavior change theories and make theory more accessible to, and usable by, other disciplines. Combining TDF domains and COM-B components one get an idea of what domains influence each variable, thus how one can change behaviors. The connection can be seen in the table (2.4).

COM-B component		TDF Domain
Capability	Psychological	Knowledge
		Skills
		Memory, Attention and Decision Processes
		Behavioural Regulation
	Physical	Skills
Opportunity	Social	Social Influences
	Physical	Environmental Context and Resources
Motivation	Reflective	Social/Professional Role & Identity
		Beliefs about Capabilities
		Optimism
		Beliefs about Consequences
		Intentions
		Goals
	Automatic	Social/Professional Role & Identity
		Optimism
		Reinforcement
		Emotion

Figure 2.4: Capability, Opportunity and motivation The COM-B model

The behavioral framework presented is extensive. Further explanations of the TDF domains given in table 2.4 can be found in Cane et. al. paper [18] (table 2), where each domain is defined and its connected constructs.

Business and stakeholder alignment analyzed through using the adopted paradigm, proposed behavioral theories and understanding of cybersecurity culture

As a last entry in presenting the underlying theories and assumptions leading up to our system investigation the concept of stakeholder and business alignment is to be presented. Business alignment can easily be linked to the above mentioned fundamentals of systems thinking, socio-technical systems and behavioral theories. To understand business alignment one must understand the concept of

governance. Information security governance is a very broad term and can be seen as the system by which an organization directs and controls IT security. Theory about information security governance can build on the idea of interventions, and its effect on COM-B model components [16]. A. Da Veiga and J. H. P. Eloff [19] present an Information Security Governance framework, a framework which combines several other frameworks to a single point of reference towards governing information security. Governing cybersecurity can be done through e.g. policy, law and regulation, technology protection and operations, user security management and more. A Security Governance Framework is intended to alter the behavior and security of an organization and its employees, and ensures that management consider a broad spectrum of components to assist in addressing risks to assets on a technology, processes and people level. Knowledge of which behavioral concepts in need of change could result in more effective governance and management, because the governance decisions would be based on the current state of an organization and its employees.

Business alignment is a small, but very important part of governance as executives should focus on business-aligned objectives. Which naturally must be true to achieve good performance and governance of IT security. Rather than plugging individual holes in the cybersecurity though a piece-mental approach companies need to:

> "...develop a holistic cybersecurity strategy that protects the organization's most important assets from the inside out—and safeguards the enterprise across the entire industry value chain, such as from raw materials to consumption." [20]

Accenture [20] reports that business alignment is very important for businesses efficiency. Business alignment means that the goals and strategic direction governing the cybersecurity measures and incentives must be aligned with the general business needs, long term objectives, general purpose and ensure value creation. Current cybersecurity culture is expressed through behavior and is ultimately determined by the composition of the behavioral concepts such as capability, motivation and opportunity. The interventions affecting the behavior can be of different kinds such as legal and regulatory, program organization, policy, guidelines, awareness, education and training, or more operational procedures such as asset management or incident management. Proposed governance activities, or interventions is found in both the governance framework [19] and the behavioral change wheel [16]. The link between the causes of behavior, proposed interventions and measures goes both ways. Behavioral components determine weather or not employees exhibit desired behavior in contact with an intervention e.g. a policy. Ultimately, this leads to a gap between the intended effect of a intervention and the exhibited behavior, widely documented by research on organizational information security [21][22][23][24][25], and through the fundamentals of socio-technical systems and systems thinking.

Business alignment and culture become increasingly complex and difficult to manage due to the nature of the NHS. The sector is of a somewhat decentralised. The operational level is mainly responsible for management of cybersecurity, but stakeholders at other levels influence governance and interventions. It impacts on the operational levels capability, motivation and opportunity to implement measures as well as following the already established structure of information security governance. A realisation which will become increasingly clear as one begin to present the stakeholders of the system and their role. Stakeholder alignment in this sense will therefore mainly revolve around how stakeholders on different levels cause the operational level to govern information security in a way that follow their organizational need and goals regarding total cybersecurity capabilities.

Given the paradigm of systems thinking and socio-technical systems the relationships across levels in the digital ecosystem are acknowledged. As it is initially exemplified, an employee may have limited understanding, knowledge and awareness of cybersecurity risk, resulting in e.g. bad maintenance and/or usage of patient records which can create problems for patient record integrity at the operational level. A cultural problem rooted in the operational level? Maybe, or it could be the result of poor technological solutions, mismanagement of human resources, bad user guidelines, or insufficient high-level influences through i.e. regional level control, pressure and budgeting, or lack of commitment, focus and motivation on a national level.

In other words, culture and the underlying causes of behavior are important factors when assessing stakeholder inter/intra relationships. Top-level stakeholders may have the ability to implement interventions changing the operational level nature of behavior, especially their opportunity as it relies on environmental context, resource availability and other social influences. Opportunity can reduce overall capacity, or motivation, thus creating problems or limiting the operational levels ability to achieve their goals. We therefore have potential business alignment issues as a result of stakeholder behavior and culture.

System dynamics and modelling techniques

Systems thinking is presented as a collection of dimensions, a paradigm, language and methodology. Until this point only the systems thinking *paradigm* has been presented. This section will briefly introduce Systems thinking as a methodology. More information on the adopted methodology in this thesis is given in the "Methodology" section (3).

Introduction and background System dynamics and modelling techniques is a natural extension of the theoretic foundation as it is closely related to System

Thinking. ST is consists of a paradigm, a language and a method. System Thinking as a language to communicate system and world complexity, perspective and paradigm to consider and tools and methods to help guide the process. Systems thinking methodologies are modelling techniques illustrating system interaction and behavior. As the great Peter Senge stated:

> "Systems thinking is a conceptual framework, a body of knowledge and tools that has been developed over the past fifty years, to make the full patterns clearer, and to help us see how to change them effectively." [7]

The most notable approach to a systems thinking methodology was first introduced by Forrester [2][26]. He published the book "Industrial dynamics", which is described in a 1961 M.I.T press article as a "radically new and different approach to the problems of industrial management" [27]. It introduced information feedback systems, a wider understanding of the decision process and mathematical models to simulate complex systems. The methods validity and usage where further highlighted in bestselling book “Limits to Growth” published by Meadows and colleagues in 1972 [28], where systems thinking and system dynamics was used to show behavior in complex socio-ecological systems [29].

In a condensed memoir from Meadows, “Limits To growth” apparently originated from a group of 75 problem solvers called the Club of Rome, with list of 66 world-problems; like poverty, drug addiction and war. How could they investigate the interconnectedness and complexity of the world’s problems, together, and not focus on each problem individually? A member of the group set up a meeting with Forrester, which suggested system dynamics as the solution [30].

Introducing systems thinking modelling techniques There are multiple approaches to model complex systems. However, the end result is more often than not a system dynamics model variation. System dynamics often rely heavily on qualitative data [31] and is well recognized as a valid approach to projects relying on qualitative data to analyze complex systems. Information gathering can be i.e. document analysis, Interviews, workshops or data analysis. Initial modelling and knowledge mapping can be done through e.g. causal loop modelling, which mainly focused in Maani’s ST&M methodology [2], but also other techniques, as discussed in [31]. The most notable being "Influence diagrams" and "Stock and Flow diagrams". To assist in crating the systemic structures in causal loop diagrams the already established system archetypes can be used. Modelling techniques are are explained in more detail in the appendix adding information to the background section 8.

The theoretic framework establish a shared understanding of cybersecurity

The presentation of theoretical framework is aimed to establish a shared understanding of cybersecurity. The methods applied in this thesis are discussed and

presented at a later point. But, the reflections and theoretical frameworks will together with a presentation of the NHS, its stakeholders and cybersecurity capabilities (2.1.2) contribute into justifying choosing an artifact and provide an approach to answering the research objective.

2.1.2 System in question

The Norwegian healthcare system (NHS) was briefly discussed in the introduction (1) where it is presented as a complex system. Its complexity is justified through combining the theoretic framework 2.1.1 with a presentation of the actual system and its stakeholders.

This section consist of two main parts. First, the aim is to provide a general description of the NHS, introduce different stakeholders and describe their role and responsibilities. Second, an introduction to cybersecurity in the Norwegian society and directly related to the healthcare sector will be presented. The intention is to create a case specific introduction to the system, its stakeholders and the problems they face in terms of cybersecurity. The information provided will justify the initial research area, while contributing to defining an appropriate scope and choosing a selection of stakeholders. In-turn, the information provided will serve as a foundation for determining how one can model the system, and to hypothesise cause and effect relating to the interrelated concepts within business alignment and cybersecurity culture. The system will be presented in its entirety, before gradually narrowing down on a selected section of the NHS, which is referred to as the system in question. We first are presented with full picture of the system before it is narrowed down to a more manageable section/function. Scoping is initially introduced in the introduction 1 and is now being built upon and discussed to more detail.

The Norwegian healthcare services

At its core, the Healthcare service Norway provide is split into two main parts, one managed by the municipalities (primary) the other managed by the state (specialized). The government performed the split and decentralized the sector in 1980's moving some responsibility from the state to the municipalities. Still the case in 2020. Primary healthcare services include nursing services (outside of hospitals) such as home aid services and nursing homes, general practitioners (GP's) and health strengthening/preventive work. State-driven specialist care is divided into four regional healthcare authorities (RHA). Their main responsibility in terms of providing healthcare services is operating hospitals, but the RHA also have important tasks related to education, research and patient/next of kin training [10] [32].

Political administration of NHS is done through the ministry of health and care services (HOD) which can be divided in 9 departments with different roles and responsibilities subordinate to the HOD [33]. A tabular representation of all

departments and their main role and function is listed in table (7.1) found in annex 7. The table illustrate how the NHS, or Ministry of health, can be perceived as a set of departments. By investigating the system as a set of departments one can more easily understand the structure of the NHS in its entirety, as well as the responsibilities of the ministry.

The subordinate institutions and organizations To performing the tasks and responsibility depicted in table (7.1) HOD own several subordinate agencies with delegated responsibilities. The subordinate agencies are, among others, the directory of ehealth, directory of health, board of health supervision, institute of public health and national office for Health Service Appeals. The state owned institutions are the Regional Authorities and the Norwegian Healthnet, in addition to the wine monopoly [34]. Roughly, one can say that the NHS consist of professional and executive authorities on respective fields. Entities with professional roles mainly operate on behalf of the nation, where as the executive entities are divided in national, state, and municipality level [35].

A report published by the Norwegian Digitalization Agency (Difi) investigated the need for directories [36]. Their role and responsibility can be divided in two (as mentioned above), even though there are significant differences between directories. About half of Norwegian directories have an operative level, without an operative level their main role is operating as a middleman between ministries and operational level entities. The two roles are described in [36]:

- **Executing ("gjennomførende"):** Carries out its delegated duty towards inhabitants, organizations and the world of business. Initialize approved measures, projects, plans etc. towards their operative unit, whether it is rooted in municipalities or their subordinate institutions. When the operative level is performed by municipalities, the tasks are often centered around advisory services and providing guidelines.
  If the operative level is delegated to subordinate institutions, such as Regional Healthcare Authorities (RHA), the role typically include systematization and conveying objectives from the ministry, organize lead, develop regional or local institutions and follow up on their compliance.
- **Professional ("faglig"):** This role is aimed at advising the ministry in their decisions regarding e.g. budgeting, law and provide information necessary to make good political decisions. Developing law and regulation (needs ministry approval), and provide professional help to the sector, public administration, media, and the general public.

In both cases the main function is to either perform the actions conveyed by HOD (political and administrative), be mandated to perform tasks on their behalf, and communicate the guidelines all the way down to the operational level, or to other responsible entities. The report also presents four main areas which determine

how good directories are for initialization of politics:
Democratic legitimacy: Translates politics to action and is therefore dependent on being perceived as a professional entity with sufficient knowledge to perform their duty, political and practical understanding and transparency regarding goals, strategy, and openness towards external criticism.
Correct and user-oriented when practising authority: Correctly and efficiently use law and regulation while coordinating efforts to best suit the end-users and organizations.
Professional legitimacy: Directorates are dependent on being perceived as knowledgeable and professional within their respective fields. Show understanding of local factors when advising operative institutions, taking their practical experience into account. Advisory services must be aimed at improving operational-level activities, be targeted and relevant. Important is also their role towards the ministry, in communicating experiences gained from operation level.
Be an enabler for efficiency and coordination: Clearly defined roles and responsibilities, separating different directories, subordinate institutions and ministries. Department must coordinate needs to facilitate and enable balance between operational-level day-to-day and ministry politics, law and regulative changes. Additionally, they must clarify roles and responsibilities between directories when needed.

As the NHS is being introduced one begin to unravel the complexities stemming from stakeholder interaction. The entire system is politically and strategically managed by the Ministry of health and care Services (HOD), which in-tun is divided in 9 departments (7.1). To manage all its tasks HOD has delegated the professional and executing role to its subordinate institutions and organizations, which does not necessarily have to have an operational function. The operational functions within the NHS is either managed and organised nationally, by the state (regional RHAs) or ran by the municipalities. State ran operational functions is referred to the Norwegian Specialist Health Care Service (NSHS) while the services ran by individual municipalities are called Primary Healthcare (PH). The NHS as a whole is influenced by the political, regional and operational levels within the system. Levels and stakeholders can have large differences in terms of their socio-technical system and understanding of each others current situation. Following the adopted paradigm one can assume that the NHS is a system of systems, all influencing each other through i.e. political decisions, strategical direction, level of efficiency, social or structural factors. Until now, the stakeholders mentioned are limited to the the main roles of NHS: professional, executive authority, the specialist healthcare and primary healthcare. In addition to these stakeholders there are National and private suppliers and national/private cybersecurity advisory services. The diversity in services provided, and the complex interactions among stakeholders result in a need to narrow down the system to a more manageable section/function.

The investigated system and proposed system scoping

Fundamental to systems thinking is the principle of thinking of the big picture. We could argue that in order to adopt the big picture one must include all possible factors impacting the system, and every individual stakeholder. This is not feasible, or realistic as there are limited resources and delegated to this project. The thesis strives to look at the system holistically, as a result many factors and stakeholders will be accounted for, while their influences and effect will be examined at the system level of which it originates.

Through the brief presentation of the roles and stakeholders one can identify a system structure, stakeholders that are influencing each other vertically from the ones residing in the political level down to the operational level. The stakeholders can be further categorized as being Political, Professional, Executive and/or local. Thus, the stakeholders are separated by roles and system/organizational levels. To narrow the scope of the thesis a single top-to-bottom vertical path in the NHS system will be examined. This will only partially represent the system, but is is thought to be sufficient to identify business alignment issues rooted in cybersecurity culture for the stakeholders investigated. Although one top-to bottom path excludes large parts of the NHS it provides insight into different major stakeholders residing in their own respective level. The stakeholders mainly focused are the ones integral in providing the Norwegian Specialist Health Care Services (NSHS). Naturally, as the thesis revolves around cybersecurity the main aspects investigated is connected to all socio-technical system aspects presented 2.1 specifically focused on ehealth development and security. As the figure 2.5 suggests our top-to-bottom path consist of The Ministry of Health and Care Services, Directorate of Health, Directorate of eHealth, Norwegian Healthnet, Regional Healthcare Authorities and Health Trusts (Hospitals). These stakeholders represent a system of socio-technical systems dedicated to delivering specialized healthcare services to the general population.

Information about each of the stakeholders mentioned above will help justifying the selected stakeholders. Limiting the scope is very important for the success of this project. However, through the eyes of a system thinker – excluding system aspects and stakeholders – might be perceived as a weakness. Naturally, all stakeholders do impact each other in some degree, weather it is through an established governance structure or unintentional interactions. For this reason we will not disregard influences stemming from stakeholders not specifically listed in the figure, but discuss relationships in relation to the organizational level of which it is rooted.

The investigated stakeholders Insights drawn from the theoretical framework applies to the system in question and investigation of stakeholders. Each stake-

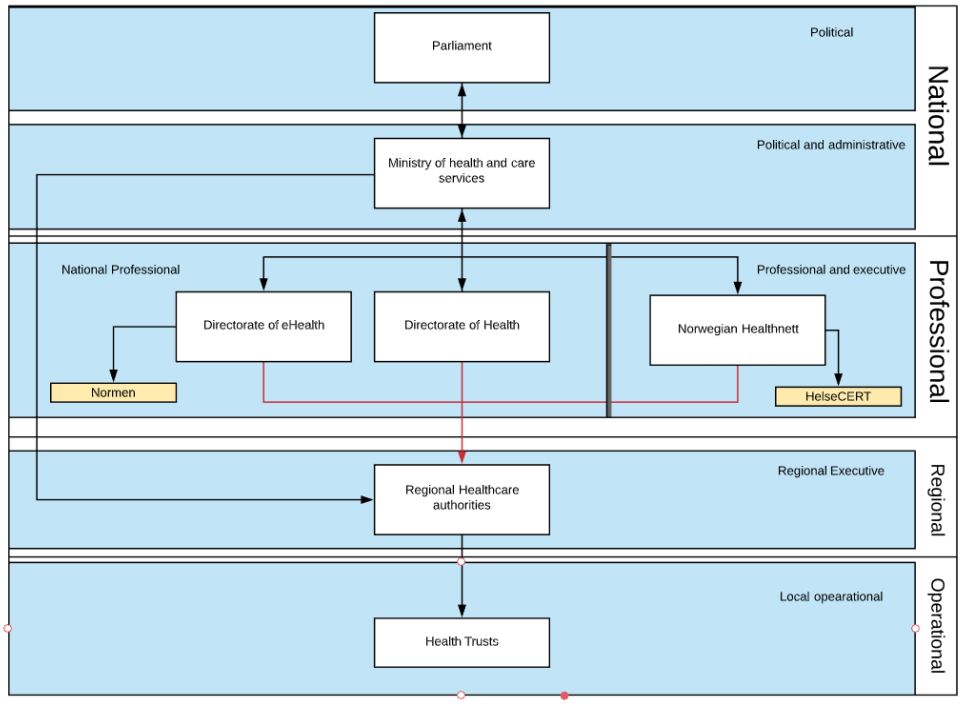

Figure 2.5: The stakeholders mainly focused in this thesis.

holder in the system will horizontally impact the systems/stakeholders on the same level, as well as impacting the levels below and above. These relations and interactions can be identified in defined roles and tasks related to a function or stakeholder, or indirect/undefined relations. One might initially think that political decisions are not impacted by institutions on a lower level. However, the professional role of directories contradicts this by enabling directories to be a middleman between political and operational/regional level. The idea of interconnection among stakeholders in a system where initially introduced in the introductory section (figure 2.2) and is an essential part approaching problems from a systems thinking perspective.

Influences among stakeholders, or the system dynamics, can e.g. be directly observed through a directorates influence on law, regulation and guidelines (professional role). These influences is only confined within one socio-technical aspect. If the new laws, or strategies, result in Hospitals being forced to implement solutions that contradicts their own culture, and already established organizational goals, the solutions could have unintended consequences. Low-level operational systems may also impact the above level systems, through communicating their perspective on the interventions impacting their systems, or as a involuntary effect of their practises. Both scenarios would impact cybersecurity and the quality of care. Attempting to target and change socio-technical aspects through interven-

tions may influence a stakeholders capability, opportunity and/or motivation to behave in a way that strengthens or potentially harms overall cybersecurity. This logic highlight that illustrating the interconnection between a socio-technical systems of stakeholders, business alignment, and the potential interventions initiated to change certain parts of an subordinate systems may lead to interesting findings in terms of how cultural challenges on different organizational levels, and within different stakeholders, affect overall behavior.

Relevant stakeholders Several primary stakeholders are discussed and presented in appendix 7, providing additional information on both primary stakeholders 7.2, and secondary/additional stakeholders 7.3. The tables provide descriptions of each stakeholders role and responsibility. Knowledge of individual stakeholders further adds to our understanding of how the system and its stakeholders interact. Individual stakeholders may reside on the same system/organizational level, making their collective influence the influences of that particular level, when generalized. This is a concept which will be used though-out this thesis, especially related to modelling, as it would be un-feasible to model each stakeholder individually. Therefore, influences will later be generalized to the organizational level of which it originates from. Generalization, in order to holistically investigate a system, is necessary to follow the thoughts and principles in the adopted paradigm of systems thinking. With the system in question discussed at a general level and different stakeholder's roles and responsibilities given, one can begin to unravel the system dynamics, and actual influences related to cybersecurity.

High-level stakeholder influence on cybersecurity in the NHS

Following the generalized presentation of the system in question one can investigate how stakeholders perform and execute their role. This section will provide some concrete examples of public documents governing subordinate organizations, thus providing examples stakeholders acting within their roles. In performing their role the stakeholders impact overall efforts to improve cybersecurity capabilities at different system levels.

National and sectoral level strategic documents published by the national political and administrative level "One digital public sector - Digital strategy for the public sector 2019–2025" is released by the Ministry of Local Government and Modernisation [37]. The document define "the common goals and focus areas for digitalization activities towards 2025, and will support digital transformation throughout the entire public sector". The main goals are Better Services, Efficient public use of resources and increased value creation. To achieve this the main concepts focused are seamless services and user orientation, clear and digitalization-friendly regulations, enabling collaboration across sectors and administrative levels, data sharing, and governance/cooperation enhancement. Collaboration must be between the public and to the private sector, lastly one

must ensure digital competence to optimize the benefits of digitalization, and maintaining trust in the public sectors systems and digital services through good cybersecurity. Cybersecurity is mentioned briefly in the report, and discussed in another strategic document [38].

Cybersecurity in relation to digitalization in the public sector is discussed in the strategy [38]. Difi evaluated information security in central government functions in 2018 and identified a need to increase, and reinforce, governance and control of cybersecurity. All the ministries should improve the monitoring of cybersecurity in underlying agencies. The national cybersecurity strategy highlight the importance of building security competence through the educational system by subjecting more people to cybersecurity in their education. In line with the national strategy of digitalization it highlights the importance of collaboration, during risk and threat analysis, and communication across sectors, private, public and national/internationally. Preventive goals relevant for the public sector are that the organizations must strive for risk aware and good Information Security Management Systems (ISMS), while maintaining and increasing trust between inhabitants, the private sector and the government. The government shall enable collaboration in the public sector, between public and private sector, provide advice and guidance and increase the overall security culture in the general public. The strategy mention identifying and strengthening organizational information security culture. Lastly, the strategy focus on cyberattacks and Norways ability to fight cyber-crime by increasing the governments ability to coordinate, understand and assist during larger incidents. Focusing on collaboration, both internationally and domestically. Each Norwegian organization is themselves responsible to handle attacks on their own enterprise, and share their experiences. To handle larger attacks the government are to develop frameworks, define roles, responsibilities and organization. The government are to enable organizations to run national exercises.

National strategy for security competence (2019) [39] is an extension of one of the five main topics covered in [38]. It highlights a need to target competence and knowledge long-term, focusing on education. In addition it acknowledges the need to increase cybersecurity awareness and knowledge inside organizations, and in the general public. The main focus areas is to increase competence long term, through the educational system, rather than increasing organizational cybersecurity culture.

Normen - A set of Sectoral Norms, either demands or recommendations for privacy and security related practises. Normens main function is first and foremost to be a be a set of demands based on law, especially connected to privacy. Additionally it consists of several suggestive guidelines. Normen is subject to changes, Normen 6.0 [40] is an improvement of the current version of Normen

(5,3) [41] and is currently submitted to open hearing [42]. The main points of improvements are changes to structure, content and language to make it easier to read and enhance reader understanding [42]. Normen has its main "demand/requirement" document, which all entities are pledged to follow through their user agreement with "Norsk Helsenett" (health systems administrator). Normen focus on demands and the demands are formulated in a way that enables self evaluation, where each entity are incentivized to find suitable measures for their organization. Self evaluation is a necessity because of huge stakeholder diversity in terms of organizational size and technological environment as a result of Normen being governing for municipalities, small general practitioner offices and large hospitals [41]. How Normen influence the NSHS is discussed in more detail during the phase of problem structuring (4.1).

2.1.3 The state of cybersecurity in the Norwegian society and the healthcare sector

Cybersecurity is important for digitalization of NHS The Norwegian government and NHS' increased focus on digitalization is the result of the evolving needs of society. Implementing modern technology and systems is seen as a way to increase the efficiency of the health sector – especially as populations age, new medications become available, and new procedures are performed. While modernizing healthcare is a means of overcoming the strain that increased demand places on the sector, increases to population life expectancy (such as through effective care) actually causes an uptick in the need for healthcare. As such, digitalization is sought after as a way of allowing the NHS to try keep up with the cyclical growing needs of Norwegian society. Yet, digitalization comes with its own cost: the increased risk of cyber attacks [43]. This means that cybersecurity must be developed alongside the digitalization of these otherwise-vulnerable sectors. One strategy for aptly increasing cybersecurity is through investments.

Cybersecurity in Norway

To investigate the threat level and trends related to cybersecurity in Norway there are four essential risk and threat reports released each year, published by from The Norwegian Police Security Service (PST), the Norwegian Intelligence Service (NIS), The Norwegian National Security Authority (NSM) and lastly The Norwegian Directorate for Civil Protection (DSB). PST handle domestic intelligence and security, where as e-tjenesten focus on international threats. NSM is a cross-sectoral professional and supervisory authority within the protective security services in Norway. DSB focus on threats and vulnerabilities originating from regional and national preparedness and emergency planning, fire safety, electrical safety, handling and transport of hazardous substances, as well as product and consumer safety [43]. National reports are used by the NHS to aid in their own risk assessments, and are influential for both national, professional and operational level cybersecurity efforts. Additionally, the reports express the importance of investigating cybersecurity in the NHS related to the rate of which the sector digitalize and strive for higher effectiveness.

The national threat assessment [43], released by PST, conclude that state sponsored intelligence operations towards Norwegian political authority, natural resources, business, defence and preparedness, and research and development. Foreign intelligence agents are believed to be targeting the different entities with political influence, from parliament and ministries to media houses, research facilities. Overall such activity can influence the general public's trust towards officials, and negatively impact Norwegian interests. The health sector is a target because of knowledge, research and development in addition to the fact that is is a critical sector making it a security target for sabotage [43].

Focus 2019 [44] is released by NIS, and highlight an increased interest in institutions with unique expertise and technology which includes the healthsector, maritime, space and the arms industry. In addition, increased knowledge and experience of conducting cyber-attacks and state/private availability of malware makes the threat of sabotage higher.

NSM publish Risk2019 [45] and Holistic IKT/digital threat landscape 2019 [46] which is directed at Norwegian businesses, individuals and the society in general. In Risk2019 digitalization is brought forward as a double-edged sword, contributing to innovation and effectiveness at the expense of emergence of new vulnerabilities. The same point is brought forward in [46] where threats as a result of increasingly digitalized businesses and sectors are presented. Increased digitalization needs to be followed by increased security investments and the emerging threats resulting from digitalization is often not fully understood. NSM presents central areas important for organizations to focus on in order to successfully digitalize.

Risk2019 [45] also present 6 main risks, that needs to be focused and be prevented in organizations. As a summarizing one state that the risks mainly revolve around insufficient overview of the risk landscape, lack of investment and understanding of insider threats (deliberate), and lack of holistically assessing the consequence of increased digitalization, digitisation and recent introduction of a new security law. Also, weak security management, control and assessment of security work and missing understanding of different realms of cybersecurity (personnel, physical and digital). Lastly, the inclusion of private companies and consultants is focused. Not only is the risks listed, but also a presentation of national measures to decrease the risks.

The most notable report released from DSB is the analysis of crisis management and preparedness which provides concrete examples of i.e. cyber-attacks. Potentially having an effect on the health sector is a cyber-attack Norwegian ecominfrastructure. The report is not discussed any further as it is not mainly mainly focused in the cyberspace.

In addition to the more specific recommendations and lists given in the reports there are some general conclusions that can be drawn from them. First, one have to acknowledge the health sector as a potential target for cyber-attacks, because of the information the sector hold in terms of research and specific knowledge. Also, the sector is an important part of Norwegian critical infrastructure making it a target for sabotage. More related to internal factors are the increased risk that comes as a result of digitalization. The recommendations mentioned when discussing general societal risk, risk of digitalization or external threats can be used to identify weaknesses in the NHS when identifying cybersecurity problems specific to healthcare.

Cybersecurity issues facing healthcare around the world

Cybersecurity should be on the agenda for all organizations in Norway, especially the NHS, if they are to follow recommendations and be prepared for future and current threats. To continue building understanding of current cybersecurity, especially related health, both domestic and international research on cybersecurity will now be presented. After which cybersecurity directly related to the NHS will be presented through internal reports about cybersecurity issues, and external research conducted on the field.

The cyber threat is growing and it is partly because of digitalization. Kruse et Al [47] identifies cyber security trends in healthcare (2017) through a systematic review. Two main trends associated with risk is: implementation of technology before the organization is ready and increased network integration. Not only because of willingness to adopt new technology but pressure from government through policy, regulation and law (U.S). Digitalization and regulation is a central concept in the risk reports released in Norway and is an important topic when discussing how different stakeholders interact.

Perasklis [48] highlight a gap in the regulatory domain (HIPAA) and actual technological implementation. The paper suggests a new regulatory framework to be implemented and created following three focus areas: Introducing a risk-based, proactive, approach rather than a reactive approach. Identify new trends, risk-based analysis and modelling (current and future trends). Lastly, the balance between regulation and organizational compliance must be optimal, regulation must not be complicated, distracting and expensive but reflect organizational need. The security posture of an organization is determined by a complex mix of technological, operational, and procedural elements that is often difficult to truly understand, let alone improve. What the main focus should be is not always clear, if one should focus on modernisation of technology or strengthening culture and awareness. Perasklis highlight the importance and need for high-level strategies. Although the research is from 2014 it highlights the connection between politics, regulation/law, and operational level management. Which is a central part in the investigated NHS, the dynamics of stakeholders, and the importance of and cybersecurity culture and shared understanding.

A comprehensive report conducted by the Health Care Industry Task Force published in 2017 [49], identify several issues with cybersecurity in the healthcare industry (U.S). Several aspects are discussed, such as the system complexity and diversity and lack of cybersecurity knowledge, ability and maturity. More interestingly, the understanding and mental model of healthcare professionals are discussed. Highlighting non-IT employee lack of cybersecurity awareness, and dif-

ficulties security professionals have with explaining cyber-risk and the long term benefits of focusing on cybersecurity. The need for cultural changes in communication and clinical environments raised as important. Traditionally IT is seen as IT problem, although the cyber-threat needs to be seen as a serious patient care concern [50]. HC-professionals have problems connecting cybersecurity to their patient-first mentality even though it can affect patient-to-hospital trust, and potentially hinder an institution in providing healthcare services to patients in need.

Recent development in law and regulation in Norway suggest that the gap between digital development and regulation is not equal to that in the U.S. at the time of the conducted studies. Even though regulation and law is created, it must be followed up on and implemented in a effective way. How the new law of security affect society can be found in [45] page 23, and is meant to strengthen and modernize security activities. However, the increase in digitalization and network adoption may be a source of problem for the NHS. The gap between adoption of technology and social constructs is a central thought in [1] model of socio-technical systems, implying that organizations introduce new technology at a higher pace that its cybersecurity maturity level suggest they can.

Cybersecurity risks and vulnerabilities as presented by the actors within the NHS

Cybersecurity is an important aspect of the NHS, as a result there are several internal publications on the topic, created by the directories (professional level). As a introduction to cybersecurity within NHS two main reports will briefly be discussed. The directorate of health wrote "High-level risk-and vulnerability assessment for IKT in the health sector" [35]. It was published following previous reports indicating a need to further identify threat and vulnerabilities. This report is on a national level and is therefore generalised. The report utilized existing national level information, investigated and analyzed it cohesively, and used it to create new measures and follow-up procedures for the identified challenges. The foundation of knowledge was 24 reports, some of which are already mentioned in the above sections. Resulting in a picture of IKT cybersecurity, based on old reports, and how the sector has responded to previously proposed measures.

The vulnerabilities believed to pose the biggest risk in today's threat landscape are:

1. Long, complex and difficult to manage value chain.
2. Missing security competence.
3. Inadequate implementation of technical security measures.
4. Outdated software and equipment which is unsupported or non-updatable.
5. Missing and inadequate compliance of information security management systems.
6. Insufficient plans and exercise in managing IKT-incidents.

Based on the key vulnerabilities there are five proposed measures, which all demand resources, prioritisation and support from management.

1. Create national cyber-readiness and response plan.
2. Perform annual exercises on IKT-scenarios affecting the NHS.
3. Strengthen operative IKT-security and through professional agencies. Focusing on basic security measures such as updates, and base proposed interventions on threat and vulnerability assessments.
4. Strengthening the overall impact of cybersecurity institutions, making the directorate of ehealth's influence stronger, their reach longer and influence bigger. Targeted at their role as cybersecurity specialists and performing high-level analysis of cybersecurity in the NHS.
5. Lastly, a strategy for cybersecurity which is governing for the entire NHS is to be created. Should account for challenges specific for the sector and its future development. The strategy should be anchored in national/governing strategies.

The directorate of ehealth also published a report on Information security in the specialist health service. The objective of [51] was to establish a foundation of knowledge, and to identify indicators of cybersecurity. Indicators that on a later stage can be used domestically, and internationally, to monitor development of cybersecurity. A questionnaire was distributed to IKT specialists and management inn RHF, selected HF and regional IKT-Service Providers (ITSP). The result was a high-level report on current cybersecurity culture, management/administration and the structure of work related to cybersecurity. The main findings from the report are:

1. RHF provide guidelines for cybersecurity to the IKT-service providers (ITSP) and HF, which is confirmed by both. Indicating regional support for cybersecurity.
2. Operative security is mainly performed by HF and ITSP. RHA's role is to ensure that cybersecurity has sufficient focus at "subordinate" institutions.
3. Low-level operational IT-security specialists in HF's say there are information security communication at regional level, where they do not contribute.
4. At operational-level (HF) the main responsible party for risk assessment is IT-security specialist. 27% of managers state that they are central contributors to risk assessments.
5. "Normen", a guideline for cybersecurity, is used heavily by all parties.
6. Many have readiness plans but do not have a structured approach to perform excesses.
7. Result indicate that institutions learn from incidents and include management in the process of organizational learning.
8. All respondents show little understanding of the consequence of cyber-incidents.
9. Measurement of cybersecurity culture where lowest in RHA, followed by HF and ITSP.

Based on the report the directorate of ehealth propose 6 recommendations

and suggestions for improvement.

1. Management need adequate security knowledge, expertise and awareness to exercise management, administration and control of information security controles.
2. One should strive for better communication between RHF and HF, and involve the operational level (HF) in regional cybersecurity work.
3. Each individual institution (RHF, HF and IKTSP) must ensure sufficient IT security expertise,
4. One information security exercise annually (at least) which involves RHF, HF and ITSP.
5. Regions should have a structured approach to planning exercises, focusing on inter-regionnal organizational learning and increasing overall level of cyber-readiness.
6. Institutions identify and evaluate security culture and develop measures to improve cybersecurity culture.

As it comes forward, there are work to be done in relation to information security in the NHS which comes mainly as a result of increased digitalization. There are some takeaways from the reports more specific to NHS. First, there is a need to focus on the connection between regional and operational level cybersecurity. Cybersecurity on operational and regional level need to be pulling in the same direction. Also internal cooperation between management level and operational/IT-security experts needs to improve, especially when there is overall need for IT security knowledge to influence decision-makers. Further, the sector need to continue working with increasing the effect and governing power of cybersecurity focused institutions with professional roles, such as the directorate of ehealth. Which will increase the overall focus on cybersecurity. In addition the reports highlight that overall cybersecurity efforts are in need of a more structured approach. Increasing the governing role of stakeholders relevant for development of cybersecurity capabilities will result in a stronger push development of cybersecurity forward.

A main problem identified is the lack of knowledge and competence. There is only going to be more digitalization, more network integration, more technology resulting in increased risk. The need for knowledge on the topic is reflected in all levels, from operational to regional. Insufficient expertise on cybersecurity is not only a problem for the health sector, but Norway in general. Missing competence related to cybersecurity also come forth by the extensive focus on improving health care cybersecurity readiness, planning, and experience. One would also think, as it is pointed out in [51] that knowledge surrounding the costs and effects of cyber-attacks is lacking in the specialist service.

Table 2.1: Furulunds [9] main and sub-categories covered in in-depth interviews with representatives working with cybersecurity in the Specialist healthcare service.

<table>
<tr><th colspan="5">Main category: "Cybersecurity in Norwegian Health Trusts"</th></tr>
<tr><td>Main-categories</td><td>Digitalization</td><td>Cyber-attacks</td><td>Cybersecurity culture</td><td>Digital Risk</td></tr>
<tr><td rowspan="4">Sub-categories</td><td>Dependencies</td><td>Security measures</td><td>Cybersecurity culture today</td><td>Risk assess-ments</td></tr>
<tr><td rowspan="3">Digitalization</td><td>Organizational learning</td><td>Governance structure</td><td>Threats</td></tr>
<tr><td rowspan="2">Future security</td><td>Management focus</td><td rowspan="2">Vulnerabilities</td></tr>
<tr><td>Awareness, training and education</td></tr>
</table>

Adding to the empirical foundation describing cybersecurity in the NHHS

Interviews with specialists in the NHS specialist healthcare documenting organizational cybersecurity maturity Furulund [9] investigated whether the organization (NHS) is prepared to handle the current level of threat based on their organizational cybersecurity maturity. The study takes on a qualitative approach, by analyzing reports and conducting in depth interviews. Furulund concludes that the health sector is not mature enough to defend against advanced professional actors. Although cybersecurity has improved as a result of recent events the main risks are missing competence, resources, business alignment (right focus) and developing a robust cybersecurity culture. The information collected and presented as a result of in-depth interviews in [9] can add to the information this thesis use to investigate cybersecurity in the NSHS. The topics covered in the conducted interviews is represented in table (2.1). The topics are easily connected topics of this thesis, further, the interview subjects are within the proposed scope of this thesis, with them being from different health trusts governed by different RHA's.

The main empirical evidence presented in [9] are divided into the sections and topics presented in table (2.1). The informational foundation used in [9] are reports, public documents and interviews. The knowledge gained from interviews is of particular interest for this study as it does not have any interviews solidifying the information gained from public documents and reports. This thesis will not be overly focused on each individual RHA, rather focus on governance, culture and business alignment interrelation on a higher level.

Digitalization creates new solutions while introducing vulnerabilities. The informants state that there are systems in use that if lost would result in ma-

jor difficulties in maintaining good health services. As a result of digitalization complicating the digital value chain one has more difficulties having a full picture of risk and vulnerability. Informants support the notion of automated and digital work processes pose a bigger threat to cybersecurity than the processes did while being manual. One informant suggest that the coherence between assessments of systems in terms of SLA's vary between different HT's, as well as not necessarily being connected to the actual business impact. Informants highlight the importance of the governments role in providing solutions to the problems digitalization pose, through i.e. national strategies and changes in law/regulation. Hospitals have their contingency plans as an essential measure for handling potential loss of availability. Digitalization could result in more sector personnel and resources working directly with systems, and thus limiting their capability to operate manually. In situations where systems are down, the risk of lacking resources to handle patients physically become more apparent. Digitalization will further complicate the digital value chain as equipment become available at the patients residence and patients are inside the healthcare infrastructure. The digitalization efforts shall be centered around the patients, as it is stated in national digitalization strategy [37]. Digitalization increase endpoint complexity. Making it more difficult to keep services updated, monitoring threat and vulnerability and secure configuration. Additionally, digitalization needs to be accompanied with increased security competence and knowledge. The education must be tailored towards each employee, but it is difficult due to big differences between employees at different HT's. Lastly, one informant highlight collaboration between different organizational levels in the sector as a future problem.

Cyber-attacks Most attacks on the sector are ransomware, e-mail fraud and CEO-fraud. Helse Sør-Øst claim that their detection and systems are good anough to handle small and unprofessional attacks on their systems. Bigger and more sophisticated attacks are much more difficult to deal with, as seen in 2018 (Helse Sør-Øst [3]). There are examples of smaller successful attacks on different regions which had operational and economic consequences. All regions state that the successful attack in 2018 resulted in many changes and organizational learning activities. The region mostly affected experienced good collaboration with professional entities within and outside the health-sector itself, such as HelseCERT, NorCERT and NSM. Other regions implemented improvements on their systems in line with recommendations from NSM, HelseCERT and Sykehuspartner. The attack in 2018 had an important effect on anchoring cybersecurity in higher level management in the HT's and RHA's. Additionally, it solidified the health-sector as a target for cyber-crime. The effect is especially seen in the RHA effected (helse Sør-Øst). The informants from the sector state that it is unrealistic to fully mitigate all risk associated with an Advanced Persistent Threats (APT) and that the strategy of Helse Sør-Øst and Sykehuspartner revolves around detection and response. One region highlight a need to increase resources, both economical and personnel, more security focused systems and better organizational structure. Further, they experi-

ence difficulties in the process of obtaining cybersecurity specialists because of the delayed focus on cybersecurity in the educational system. Information from the informants show that there are differences in maturity between the regions and the individual HT's, as some are smaller and have less resources, such as region Nord with only 10% of the patients in the sector.

Cybersecurity culture The informants are asked about the current state of employee awareness and knowledge, and management governance, focus and guidelines, from this some interesting takes on the culture are presented. Employees have a good understanding of privacy and confidentiality agreements, but not in terms of general security. Due to the size of Helse Sør-Øst (80 000 employees) they have found that regional awareness campaigns are ineffective as Sykehuspartner cant reach out to all employees, thus the lacking culture is compensated for with increased procedural and technical controls. Region Vest have only 50% participation rate on their obligatory e-learning tools, far less logins to their systems than whats expected, and employees does not read their e-mails. Helse Vest also state that privacy is anchored heavily and that the privacy of patients is considered a fundamental principal of healthcare services. The informants point to a narrow view of privacy, and that employees do not connect security related aspects to privacy and confidentiality. For instance, when employees request more rights within the system they do not see how increased availability effect confidentiality and privacy.

The informants where asked about the measures and methods the regions use to educate and raise awareness. Most regions primary tool is an obligatory e-learning course. There are major differences in how they are followed up. In Helse Sør-Øst and sykehus partner they lock users out if they do not complete the course. Other regions are not as strict and the rate of participation reflects it. The rate it is demanded is every 3 years, which may be to to rare considering its importance. it is mainly each individual HT's responsibility to conduct educational and awareness raising activities, however the RHA's assist by having seminars and other activities. This structure of roles and responsibilities have already been discussed while presenting the stakeholders of the system, specifically the relationship between RHA's and their subordinate HT's on the operational level.

Governance structure/management system There are shared regional management systems which describe roles, responsibilities, decision-makers, risk management, policy and contingency. Top-level management at each HT are responsible for establishing the management system. Changing the regional framework can be difficult as it is done in monthly meetings, and the HT's might disagree, which results in difficulties actually implementing changes to the regional framework. The administration described varies among the informants based on which region they are operating within. The management system is however in many cases largely based on "Normen". One informant question the ISMS's alignment

with business strategy and objectives stating that the information security and privacy aspects are not put in context of organizational goals and objectives. All informants state that information security is rooted in management which is a result of recent successful attacks.

Digital Risk One informant state that risk assessments in the region is associated with negativity and are very time consuming. It leads to a risk assessment overly focused on the negative effects of the implementation, rather than balancing risk with gain. Risk assessments are in the way of improvements. It is also stated that risk assessments are not necessarily connected to the business. They are overly focused on complying with law, rather than its effect on providing healthcare, organizational reputation and generally being beneficial to HT's operations. All regions use national threat and vulnerability reports to keep up with the current threat landscape. The sector has begun creating their own risk and vulnerability assessments, but they are largely based on the same openly available national risk assessments. Both technological and social vulnerabilities is brought forward by the informants. Technological vulnerabilities such as lack of modernisation and documentation on old equipment and systems and social vulnerabilities like lacking knowledge and competent personnel. Social vulnerabilities are: lacking resources, need to further anchor security in management and risk management. Old and unsupported systems and equipment put management in an uncomfortable position where one must determine weather delivering health services or having good security is the most important consideration. Additionally, long and complex value chains and interconnectedness between different sectors and organizational entities is also brought forward as a significant threat. Human error is identified as the most prominent threat by the interview subjects.

The interviews add to the information already given and discussed through reports, national threat assessments and international research. Additionally, it provide additional information as to how regions are different, and a discussion of the topics of digitalization, cyber-attacks, Cybersecurity culture and Digital Risk from the perspective of cybersecurity professionals within a region.

2.1.4 A new perspective on cybersecurity in the NHS

The main objective of the background section is to provide context to the research. The theoretical framework section, together with the system in question creates a perspective of cybersecurity and an understanding of the system and its problems relating to cybersecurity. To tie the sections together an holistic presentation of its contents are provided.

- At first, a theoretic framework for investigating the complexity of cybersecurity in organizations has been presented. Effectively establishing a set of thought patterns and concepts the author and reader need to adopt in order to follow the same perspective and paradigm.

- Afterward, the theoretic foundation is build upon by briefly discussing different modelling techniques used within the paradigm of systems thinking.
- Furthermore, one get an overall view of the NHS as a system, the stakeholders and their respective role. This enhance ones understanding of complexity in the system in questions along with increased justification of the problems that fueled the research objective and questions.
- The current societal threats and vulnerabilities in Norway, general cybersecurity issues in global healthcare and cybersecurity challenges specific for the NHS is presented.
- Lastly, the reader is then presented with a selection of the qualitative sources, which together with current threat and challenges and stakeholder roles and responsibility form the informational background on which the interrelationships between the stakeholders and systemic aspects are based.

The aim is to build and consequently adopt a theoretic framework one can use to improve the current understanding of the issues and challenges facing the specialist healthcare. Theory and method can ultimately give previously unknown insight into the actual underlying cases for the identified issues. In other words, we provide a new perspective on cybersecurity in the Norwegian healthcare which is exactly what the research objective and the respective research questions seek to do, by mainly focusing on business alignment challenges as a result of cybersecurity cultural differences between the stakeholders.

2.2 Related work

The aim of this related work section is to present research which apply systems thinking to issues within the field of cybersecurity, thus assessing cybersecurity as a socio-technical phenomena. Additionally, research applying systems thinking and modelling to cybersecurity issues revolving around both management of cybersecurity, behavior and culture and healthcare specific cybersecurity research are of interest. Investigating similar research could justify applying the methodology to answer the research questions, as it will be presented in the section following this one (3), provide insight into the variables and interrelations identified through studies on topics related to organizational cybersecurity, cybersecurity culture, behavior and business alignment and identify healthcare specific relationships which can be linked to our investigated system. Looking into related works also ensures that the research being conducted is unique and could benefit the research community.

2.2.1 Systems thinking and cybersecurity

Systems thinking is a philosophy, and there are many different ways of approaching systems thinking. As it was discussed in the background new waves in Systems theory arose through the renowned works of Forrester and Meadows in the 50's

and 60's [2][26][27][28] which introduced systems thinking to fields with deeply rooted mindsets and methods. Systems thinking as an theoretic foundation and philosophy is widely used in cybersecurity research. The essence of systems thinking can be found in section 2.1.1. The vagueness of the philosophy is discussed by Anderson [11], explained in the sub chapter on System Thinking 2.1.1. Naturally, there is research diversity when it comes to thinking big picture, balance short and long-term investments, recognizing the dynamics and interconnectedness of systems and so on. Systems thinking approaches are, as socio-technical approaches, restricted to a problem/topic and the system in question.

Cybersecurity is often analyzed in a social contexts like management, healthcare, national threat, safety, culture and more. IT-infrastructure and information is at the center of modern society and enterprises, and the link between economical, managerial and the organizational aspects of cybersecurity, as well as the international aspects is becoming more and more prevalent . Although investigated in many different environments, the main theme is reducing risk of loosing information or system availability, integrity and confidentiality. It has gradually moved from being an issue strictly for it IT experts, to an issue affecting the organizations and society at large [19]. Its role and interaction with the social aspects of society means that in order to holistically investigate cybersecurity one need to adopt the perspective of socio-technical systems [1]. By adopting this perspective, the boundaries of the system [52] will be the limiting factor. The social and technical aspects of cybersecurity are very broad concepts, and contain several dimensions. Dimensions can i.e. be the ones highlighted by the SBC model by Kowalski [1], illustrated in figure 2.2.

Nancy Leveson introduced STAMP to systems engineering (System Theoretic Accident Model and Processes) [53], which switch focus from independent component failure towards the more interconnected perspective which included interactions among humans, physical components and the environment. Thus taking a systems thinking approach to safety. The field of safety and security can be related, and the methods transferable. Young and Leveson [54] bridges the gap between safety, security and STAMP in their article on "System Thinking for Safety and Security". The approach taken in safety [53] often contrasts the one taken in security, [54] state that safety focuses on strategy where security tend to focus on tactics. Strategy and tactics are separated by the latter being focused on threat, while the first on the actual outcome. Thus, applying systems thinking to security is shifting the focus from the the threats of the environment, to factors enabling systems to enter vulnerable states. Salim [55] propose using the STAMP methodology [53] to analyze cyber-incidents, which highlighted causal relationships difficult to identify using traditional "technology" focused risk analysis. Salim [55] then questions the "standard" approach to risk management, which revolves around identifying external threat, then implement (mostly) technological measures to deal with the risk. Socio-technical aspects being very important in investigating cybersecurity as one should weight each system aspect and focus on the root problem/solutions

rather than targeting a problem symptom.

Most research, especially research adopting a holistic approach, consider systems as socio-technical. As the parallel between systems thinking and socio-technical systems is apparent works within the field justify adopting it so solve complex problems. AL Sabbagh [14] examines socio-technical concepts surrounding cybersecurity incident response. I.e. modelling individual workers cybersecurity culture through social metrics, applying systems thinking to the complexity of security incidence response to analyze incidents, a socio-technical framework for threat modelling of a software supply chain. Including the organization culture, structure and mental models in incident response enriches information and result in more actionable information. This work illustrate how connecting different aspects of cybersecurity together may enrich the results gained from analysing cybersecurity in a complex system. Da Veiga and Eloff [19] propose a governance framework which connect all critical elements of IT security governance, through inter-relating existing Information Security schemes. The goal is through adopting the framework one can enable the Corporate Executives to make the right decisions considering corporate and IT governance, connecting the viewpoint of management and Information security.

Dutta et. Al.[22] Contribute to a holistic understanding of organizational cybersecurity by modelling interaction between selected technical and behavioral factors which can lead to better decisions in terms e.g. policy and investment. Adopting, as [19], an organizational/business value perspective rather than a psychological/behavioral, or technological. The scope is wide compared to research focusing on one aspect, which enable development of economic models with closed-form solutions. The study is of a high aggregation and is suited for strategic planning and justification of security investments.

In an attempt to holistically investigate organizational cybersecurity behavior Kirlappos [23] explore the concept of "shadow security". Shadow security is the result of employees deploying their own security solutions to combine demands for efficiency and security. Meaning that the socio-technical system aspects is not aligned, the employees behave insecurely. Kirlappos explicitly focus the efforts on security policy, and the effect of it being irrelevant or burdensome. Through interviews the friction between productivity goals and security goals is connected to security misbehavior. Although looking at cybersecurity as a social concept, the approach is limited to just the policy aspects of the socio-technical system. Thus, the paper is limited to insecure behavior and policy. Regardless of its limitations, the concept of "shadow Security" can be used to explain how misalignment between socio-techinical concepts can result in security misbehavior, system insecurity and shadow security. Linberry support humans as a weak link susceptible to social engineering, concluding in the fact that information security must be culturally ingrained through appropriate policy and practise [24].

Researching cybersecurity through the lens of systems thinking, means looking at security in relation to its environment. Thus, what researchers define as the environment, or system boundaries [52], is of great importance. It determines the research scope, similarly to what has been done in this study (2.1.2). In addition to determining the system, the topic can also vary, from making policies, a national strategy, risk management or incident response is just the tip of the iceberg. Cybersecurity touch many aspects of business, organizations, economics, risk, societal functions and individuals. One may take different perspectives effectively including some aspects, and details, while excluding others. Klimburg [56] thoroughly investigate the topic of cybersecurity, on an international and national level, which highlight the important role cybersecurity have in the society, and discuss important factors in need of consideration when creating national and international strategy. Klimburg highlight the four levels of government, political, strategic, operational and tactical (technical) and the fact that they have their own perception of national cybersecurity, thus conceiving and addressing cybersecurity challenges differently. Which, again, may influence organizational or individual cybersecurity to a degree not accounted for in risk analysis frameworks [55], or when e.g. discussing organizational policy [23].

Naturally, the organizational context of cybersecurity include the socio-technical aspect. But, even though a systems thinking approach seek to assess a topic holistically, there will be limitations in approaches to cybersecurity. The reason being that it is in many cases dependent on a plethora of factors, societal, organizational, economical and personal/behavioral, unless the scope or system investigated becomes small enough to be investigated as a whole.

2.2.2 System Dynamics in cybersecurity and organizational research

Systems thinking is naturally connected to modelling techniques [2]. Until now, the research discussed connect cybersecurity to different aspects. Modelling is a common method to apply when conducting systems thinking research. There are many models which can be used, in combination or alone, to illustrate a system, its complexities and interconnections. One of the most common is system dynamics, which in combination with causal loop modelling will form the main methodology of the thesis. The following section will describe the goal, findings and limitation of cyber security research using system dynamics to model cybersecurity issues.

Luna et. al. [21] applied an analytical framework, system dynamics and institutional theory to investigate the success and failure of e-Government projects in Mexico. The approach consider many aspects of the systems in question Luna show interconnection between technology, organizational factors and institutional arrangements in their socio-economic context. The created model represent theory related to development and implementation e-Government projects, from which

simulations of different projects was performed. The research shows that in the e-government projects investigated the project of developing information portals (enacted technology) was interrelated with the agency networks and formalized processes. The researchers concluded that through using a theoretic framework, and system dynamics, one could gain a new understanding of the phenomena investigated (e-government projects).

Jalali et. al. [57] adopts a similar paradigm as [21] and the proposed systemic understanding depicted in systems thinking and socio-technical systems theory [1][7]. Jalali [57] use SD-modeling to unravel the system dynamics of cybersecurity capability development in hospitals, and how dynamics effect total cybersecurity. An iterative causal loop model was developed from variables and the relationship among them. Variables was extracted through inductive coding of in-depth interview data. Lastly, the CLD is transformed to a SD-model. A hypothesised baseline is the starting-point for the simulations. Both papers consider systems as socio-technical, investigate problems in an organizational setting, infers relationships from collected data, hypothesising causal relationships and develop their models by building them over several iterations.

Also following the organizational perspective is Dutta Et. Al. [22]. Dutta set out to create a system dynamics model that illustrate the interplay between technical, organizational and human aspects of cybersecurity and its impact on the business value of an organizational IT system. An attempt to aid management level make good decisions by contributing to a holistic understanding of organizational information security by using an an approach of very high aggregation.

Given that gaining insight into interrelations related to organizational theory, IT and security is one of the purposes of this section concluding remarks from the articles are provided. Dutta [22] found aspects affecting business value. Interesting remarks are that erosion of Percieved risk is a paradoxal effect because good investments and focus can isolate employees from cyber incidents, in turn making "fire drill" type exercises a good measure. Also important for the business value is the risk appetite threshold, and the investment balance between technology and awareness controls and measures. Luna [21] found that strong existing professional network was important, not alone, but in balance with good leadership because the resources needed to be utilized efficiently to create engagement across stakeholders. Jalali [57] concluded that the endpoint complexities at hospitals contributed the most to risk, followed by stakeholder alignment. Jalali also concluded that setting a high goal for cybersecurity can counteract low resource availability.

Dynamics of cybersecurity culture and behavior The human/cultural/behavioral aspect of cybersecurity is not extensively researched using the system dynamics approach. Instead it is applied to problems rooted in the cultural/beha-

vioral/social aspect of cybersecurity, such as "the insider problem". The problem refers to employees intentionally or unintentionally acting insecurely, similar to the "shadow security" concept discussed in [23].

Fagade Et. Al. [58] apply system dynamics to model the complex problem of insider threats. Complexities arise from people, processes and technology. The goal is to model the interconnectedness between three distinct indicators of malicious insiders. The indicators accounted for the personality, behavioral and the technological aspects. The approach focus on the personal and individual level as opposed to the organizational focus in [57] and [21], trying to predict future malicious insider behavior, in the context of business. Effectively meaning that [58] focus on on how the organization enable insider behavior, rather than how insider behavior affects the organization. Interestingly, [58] found that motivation to breach security policy vary within a group of individuals with the same personality traits included. However, the factors which mostly impacted the likelihood of malicious activity where the perception of sanctions, rewards, psychological states and behavior. The research conclude in technical factors having limited effect on the insider threat and that social measures to raise awareness and culture should be created with employee outlook on security in mind.

Although not following the system dynamics approach, [25] Information Security Knowledge Sharing (ISKS) is discussed while acknowledging intrinsic and extrinsic motivation, social influence and facilitating conditions like organizational support. They found that knowledge sharing increase security awareness and lessens the cost of cybersecurity. The most influential factor on ISKS was extrinsic motivational factors such as promotion opportunities, reputation and curiosity satisfaction. A similar conclusion as Fagade [58] came to, only presented in a different wrapper. People-related approaches to mitigate risk is by [59] given as Information Security knowledge sharing (ISKS), security collaboration, Security Cautious Behavior and compliance with policy. [59] provide enablers and barriers associated with each one in addition to discussing their relation. Effective interaction between ISKS and collaboration will lead to cautious behavior subsequently resulting in policy compliance.

The difficulty in performing research in this field of study is on what level of aggregation one should reside. Naturally, there are many levels one can investigate an issue as it comes forth by presenting literature on the topic.

2.2.3 Related work and its implications on the performed study

To conclude the related work segment the presented research will be summarized and this thesis's position among previously performed studies will be discussed. Research on the topic of cybersecurity has changed over the recent years to be investigated in light of several aspects, both social and technical. Additionally, incentives are targeted more towards the organization themselves rather than external threats. This development in research suggests that a holistic socio-technical

approach is preferred over more narrow approaches investigating specific aspects of security. Not only does a holistic approach include ones own organization, but the factors which govern organizational efforts outside of ones control, such as politics, law and regulation. Although cybersecurity benefit from being investigated holistically, adopting the perspective Systems thinking and socio-technical systems, one must acknowledge that investigating to complex systems may lead to subpar results.
Applying systems thinking is often linked to modelling, thus application and results from applying modelling within the paradigm of systems thinking to cybersecurity and organizational research can highlight effective methods and interesting results. The studies using system dynamics all conclude in the methodology being suitable to simulate and model complex systems, complexities from diverse stakeholders or complex technological systems. Considering the system investigated in this thesis a system dynamics model would be considered as a suitable modelling technique.

The related work also provide results that could apply to the system under investigation, regardless of the research applied system dynamics modelling or not. Collaboration and knowledge sharing leads to policy compliance, and policy compliance reduce cost of cybersecurity. That organizational social constructs reduces likelihood of malicious insider behavior to a higher degree than personality traits and technical factors. The paradoxical effect of perceived risk, and effectiveness of exercises counteracting it. Also, that project success not only relies on professional network, but leaderships ability to utilize other stakeholders and engagement in collaboration. In terms of hospital capability development it is stated that endpoint complexity and stakeholder alignment have significant effect on capability development.

This study is related to the adopted paradigm, methodologies and topic of the above mentioned studies. More information on the methodologies the related works have applied in terms of simulation and validation is provided in the validation and verification section in the methodology chapter 3.1.3. This study is different from the related works due to the investigated system and its research objective. System dynamics modelling has not been done on a healthcare system of this size, nor are any of the related works focusing heavily on culture, and business alignment in the context of stakeholder influences. There are limited resources on the topic investigated in this thesis.

Chapter 3

Methodology

The methodology chapter of this thesis will consist of three main parts. The first section will provide a representation of the meta method adopted in this thesis, the design science research method (DSR). In addition to the meta method, the five phase process of systems thinking and modelling will be applied. As the five phase ST&M process is a part of the meta method it will be presented as complimentary methodology. Finally, the two methodologies are altered to suit the needs of this thesis and presented as the methodical steps followed in this thesis.

3.1 Choice of scientific method

3.1.1 The Meta method - Design Science Research Method

The design science research method is a widely accepted method to use in cybersecurity due to the applied nature of the method [60] [61]. The DSR method used in this thesis is based on [60] and [61]. DSR is normally used when combining methods and theories from natural, computer, social and economic science to answer questions occurring in the intersection between technology, information security and organizations [61]. The method revolves around creating knowledge, understanding the problem, and the propose solutions through using an artifact. By analyzing the usage and performance of the artifact one can understand, explain, and often improve a system being investigated. A framework for the design science research method was proposed in chapter 4 of Johannesen and Perjons book "An introduction to Design Science" [60]. It consists of four components:

1. A number of logically related activities, with well-defined input and output
2. Guidelines for carrying out the activities
3. Guidelines for selecting research strategies and methods to be used in the activities
4. Guidelines for relating the research to an existing knowledge base

The DSR-method serve as a high-level framework to follow when performing suitable research, though it must be modified and details needs to be determined

depending on the type of research and needs of researchers. The framework is presented graphically in figure 3.1. Even though the framework is illustrated sequential, the process of creating an artifact is normally a highly iterative process.

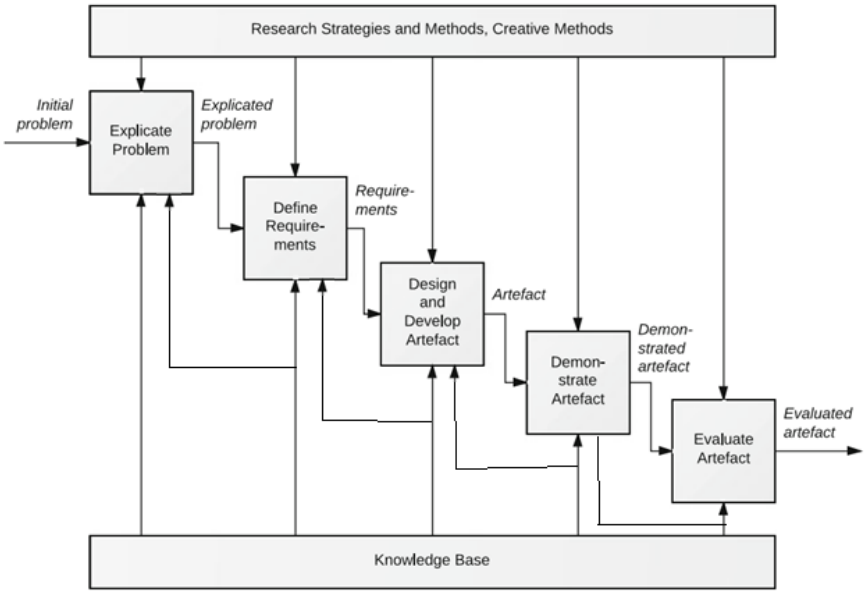

Figure 3.1: DSR method, adopted from [60]. The flow from left to right is the natural flow, arrows show the natural flow and possibility of iterative work within the framework.

The activities above represent a logically connected set of activities that together creates guidelines for trying to solve a given problem. First, one must investigate and analyze a practical problem. Secondly, defining requirements of how to solve the explicated problem. An artifact requires a defined functionality and structure. Step three outputs the artifact, which should address the problem, fulfill the requirements and determine the structure of the model. Demonstration revolves around demonstrating how the developed model functions on a real-life case. Evaluating the artifact determines how well it performs, fulfills requirements and provides insight that could solve the identified problem. The theories and models used to create the artifact, and in-turn answer the RQ's, is the backbone and theoretical framework. This can in part be considered as the knowledge base, which is described as the set of models and theories, from other fields, applied to the given problem. The knowledge base contains information about artifact creation that is similar to the artifact that is being created in this example, found in related works. More information on the different phases in the DSR-method is provided in table (9.1) found in appendix 9. The table present each phase and explain its accompanying activities.

3.1.2 Complimentary methodology - Systems thinking and modelling (ST&M) Methodology

The ST&M Methodology is presented in the book "System Thinking, System Dynamics. Managing Change and Complexity" [2] and is a set of conceptual, and analytical methods. ST&M is split into five distinct but related phases, the phases has specific steps. One do not need to conduct all steps or phases as they can be used separately, or individually, although conducting them all to some degree will add more to the result. Table (3.1), adopted from Maani et. al. [2] ST&M methodology, is as systems thinking and dynamic modelling based on the early work of Forrester's book industrial dynamics [27]. Changing the method in-line with ones own research is reflected in this systems thinking and modelling methodology as well as in the DSR-method.

As it comes forth by table 3.1 the ST&M methodology is a comprehensive methodology that covers phases focusing on planning, initial modelling through causal loop modelling, creation of system dynamics simulation models and steps that focus on using and providing knowledge from the model.

Table 3.1: The five phase process of systems thinking and modelling

Phases	Steps
Problem Structuring	Identify problems or issues of concern to management and main stakeholders. Collect preliminary information and data. Conduct group sessions for creative problem structuring.
Causal loop modelling	Identify main variables. Prepare behavior over time graphs. Develop causal loop diagram. Analyze loop behavior. Identify system archetypes. Identify key leverage point. Develop intervention strategies.
Dynamic modelling	Develop system map or rich picture. Define variable types and construct stock and flow diagrams. Collect detailed information and data. Develop a simulation model. Simulate steady-state/stability conditions. Reproduce reference mode behavior. Validate the model. Perform sensitivity analysis. Design and analyze policies. Develop and test strategies.
Scenario planning and modelling	Plan general scope of scenarios and modelling. Identify key drivers of change and keynote uncertainties. Construct forced and learned scenarios. Simulate scenarios with the model. Evaluate robustness of the policies and strategies.
Implementation and org-learning	Prepare a report and presentation to the management team. Communicate the results and insights of proposed interventions to stakeholders. Develop a micro-world and a learning lab based in the simulation model. Use learning tab to examine mental models and facilitate learning in the organisation.

3.1.3 Adopting a research methodology answering the research questions

The ST&M and the DSR method combined provide the methodical framework this thesis will operate within. Both of which will contribute in the process of answering the research questions. The DSR method operate as a meta methodology. Its purpose is mainly to provide guidance as to how to structure the development of an artifact.

As the artifact created in this thesis is a system dynamics model, a methodology targeted at developing a system dynamics model is preferred. The result of the methodologies combined is a rigid framework to conduct a project, specifically tailored to the goal and objective of this thesis. Both models is presented as detailed, yet they are highly customizable. Thus the proposed methodology can be adapted to effectively answer the stated research questions and fit the researchers available information and time.

The meta framework guide the introductory phases, and provide an overall approach to artifact creation. As the methods overlap, the main methodology will be the ST&M methodology while the DSR-method act as a wrapper surrounding and complimenting the ST&M. To provide a clear structure and illustrate how the methodology leads to answering the research questions each question will be listed and discussed in relation to the proposed methodology. From discussing how the two methodologies is used to answer the research questions a new methodology with the actual steps conducted will be given. Although removing some steps related to creation, demonstration and validation could negatively effect overall quality it is a necessity due to the degree of complexity of the system, available time, resources and available information.

Research questions related to methodology steps and activities

To tie this section together with the overall objective and research questions they will be individually linked to the proposed methodology and the phases it consists of.

Research objective: The research objective is "*To identify business alignment problems among stakeholders rooted in cybersecurity culture and propose solutions in order to enhance cybersecurity posture in the Norwegian healthcare digital ecosystem.*". The underlying intention is to find solutions through adopting comprehensive and interconnected view of organisational cybersecurity culture following the paradigm of socio-technical and systems thinking.

RQ1: How can the Norwegian healthcare system, so argued as a complex system, be modelled to investigate business alignment and cybersecurity cul-

ture among stakeholders?
To answer RQ1 one first need to justify the research topic and objective which is initially done through the first phases of the DSR meta methodology, "**Explicating Problem**". Here we present the system, its stakeholders and the main theoretic foundation the research is going to be grounded on. The knowledge base will provide a framework to approach Business alignment, Cybersecurity Culture and System Complexity. Not sufficient to answer RQ1 completely as the modelling aspect is not completely clarified. Determining a suited modelling approach is covered by phase 2 of the meta methodology "**Define Requirements**".

As the background and related work is presented the most appropriate modelling techniques can be identified. The best modelling techniques depend on the system and problem. As stated the two methodologies overlap, and information gathered during the initial two phases of DSRM is used in the "**Problem structuring**" phase of Maani and Cavanas System Thinking and Modelling Methodology (ST&M Methodology). Phase one of the ST&M methodology introduce identification of specific problems for stakeholders, collection of data related to the stakeholders/problems. By following the the initial steps of both methods one can determine the requirements of the model, thus the appropriate modelling techniques. This process is illustrated in the transition between phase 1 and 2 (3.2)

Consider that one first need to identify a problem, justify its importance and hypothesise its underlying causes. From there propose a modelling technique which can meet the requirements the problem present, in our case related to the system complexity, cybersecurity culture, business alignment and stakeholders. For the sake of document structure the proposed modelling technique and initial problem structuring will be presented within the methodology section (3.2), as it has been thoroughly discussed until this point and presented as a part of the main methodology.

RQ2: How do inter/intra dynamics of stakeholders influence cybersecurity culture and expose the system to increasing cybersecurity risk?

The first research question (RQ1) provides the general theoretical framework, knowledge of the system in question and the modelling technique which act as the empirical foundation. The next step is to use the knowledge and method to investigate the interconnectedness, as it is required within our paradigm of systems thinking and overall research objective. The meta methodology phase "**Define Requirement**" indirectly carries over to the causal loop modelling phase, as the "**Problem structure**" descriptive knowledge is used to extract system/problem variables. The **causal loop modelling** phase is complimented with **influence modelling** influence modelling, a secondary activity. Influence modelling can give more detail to a model, as [29] discussed when comparing conceptualization methods of the “dynamic hypothesis”. Most importantly is the fact that

it can aid the transition from CLD and Influence to a System Dynamics model. This phase, as all the other phases in the applied methodology, is conducted in iterations. It means that modelling the system to greater detail, by opening up for Influences as well as Causal relationships can ease the transition towards a System Dynamics model. Qualitative analysis of the initial model can aid decision-makers and stakeholders to think holistically, thus indicate ways relationships expose the system to increased cybersecurity risk. The initial model is transformed to the final artifact (system dynamics model) consisting of Stocks, flows, quantification of variables and links based on the initial model and inforamtion background. The model can be used to identify increased risks through changing the baseline values of the system then observing its effect on other variables, and illustrate the proposed interrelations.

Going back to the actual RQ. One can clearly tell that by modelling the interrelations based on theoretic and system/stakeholder specific interrelations, and identified problems rooted in culture and business alignment one can illustrate problematic interrelations resulting in increased cybersecurity risk.

RQ3: How can the developed artifact be used to improve cyber security culture in the NHS?
Lastly, the model will be used to illustrate how the modelled relationships influence cybersecurity culture. Simulation of the system and its variables will serve two purposes. Firstly it can illustrate how changing some variables may positively effect overall cybersecurity culture. Altering variables will be rooted in a real-world aspect of the system, thus presenting possible scenarios and variations of the initially proposed system. This process is tied to the "**Scenario planning and modelling**" phase and the **Demonstrate** and **Evaluate** phases from the meta methodology. Even though scenario planning and modelling is a form of Demonstration and Evaluation they are all mentioned for the sake of connecting the two methodologies. An additional note is that the model is subject to change depending on the quality and availability of the preliminary qualitative information used to create it. Thus, even if the simulation model shows weaknesses in terms of its simulation results, its structure and interrelations may still be meaningful, although the variable quantification is weakly rooted in preliminary information, or lack thereof.

The RQ revolves around highlighting how the model can be used to improve the system, not necessarily the exact strategical changes one would need to introduce to the system. Performing a "**Scenario planning and modelling**" phase will lead to an opportunity to finish the modelling process and perform the phase of **Organisational Learning**. **Organisational Learning** is a narrowed down version of the original phase **Implementation and organisational learning** of main methodology (see table(3.1)). The phase includes communicating the results and insights gained from using the artifact, thus potentially leading to potential strategies

which can improve cybersecurity culture in the NHS.

The methodical steps performed in this thesis

Following the presentation of research questions and methodology steps, the methodology used in this thesis is presented.

Problem explication and artifact requirements: Takes the information from the theoretical background and empirical information to clearly define the investigated problem. After which one define the actual requirements of the model, which then determines what modelling technique is going to be utilized.

Problem structuring: This is a very important step as most of the following sections build off the problem structuring. Problem structuring is closely related to the process of problem explication because its input information of empirical information and theoretical frameworks are the same. The main purpose is as in the ST&M methodology to identify problems of concern and present the empirical and theoretical information with the intent to model the system.

- Identify problems and issues of concern for main stakeholders.
- Collect and present preliminary information and data.

Causal loop modelling: Causal loop modelling uses the information given in the problem structuring phase to create a causal loop diagram. Variables are identified and interconnections described in the context of the problem. Loop types and behavior over time is discussed for each individual part as well as the system as a whole, before an holistic analysis of the causal loops effect on the investigated problems.

- Identify main variables.
- Develop causal loop diagram.
- Analyze causal loop behavior over time.
- Identify key leverage points.

Dynamic modelling: Through the *problem structuring* and *causal loop modelling* phases the available information is already given, and relationships described. Information from previous phases are the input, no new information is gathered. The simulation focus on positive and negative influences, and potential changes which can influence overall behavior. Initial simulation model will be a representation of the system in its presumed current state and relationships will determine its development. Rooted in the identified thus representing the reference mode of behavior, or base case.

- Define variable types and determine method and quantification method.
- Develop simulation model.
- Reproduce reference mode behaviors through a base case.

Demonstration and evaluation The process of validation and evaluation of the model is simplified compared to the steps suggested in the ST&M methodology. Simulation validation is continually performed during development, and rooted in previously conducted phases. The concepts discussed in (3.1.3) apply. The main focus of validation are the actual values and structure of the simulation model rather than the accuracy of quantified variables. After the reference mode of behavior is presented the system will be tested through policies (changing one variable) and scenarios (changing several variables) to highlight system functionality and account for uncertainties in the data used in the reference mode. The result of this can improve the model directly, or provide alternative behaviors worth highlighting during discussion and analysis.

- Validation of the model.
- Test and analyze simple policies rooted in real-world scenarios.

Organizational learning: Organisational learning is mainly presented as a phase which will ease use of the model for the stakeholders. In the case of this thesis the main point of this phase is to highlight how the model can be useful for the organisation in question and how it could be used in the future. Additionally, the results and final discussion is presented surrounding the actual results produced as a result.

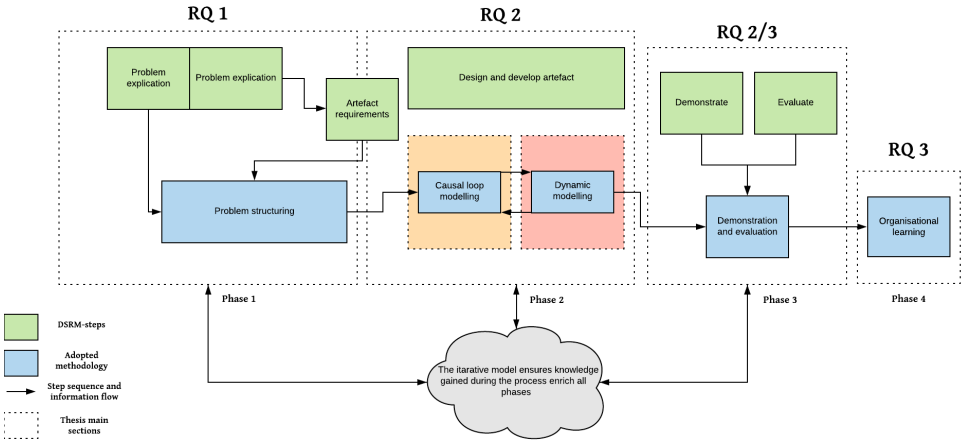

Figure 3.2: DSR method [60] and the revised [2] put in contexts of the research questions, their sequence and main informational flow.

The iterative process and modelling methodology: A system dynamics model is created in sequenced steps, but each steps feed into one another. One continually work with the causal loop model and simulation model, and run tests to validate simulation results along the way. Testing policies and scenarios is integral to developing an accurate model, as the entire methodology is highly iterative. As

indicated by the figure (3.2) one gain knowledge throughout the entire process and modelling could possibly alter the initial problem. The practical result of this is that as one see work done in i.e. phase 3, phase 4 is continually performed.

Validating a system dynamics model Building validity in a model is all about conducting several tests to build confidence in a model. Naturally there are many different ways of increasing the validity of a model. Stermans book [26] on Business dynamics present a compilation of different efforts that can be done, such as seeking face validity, verifying model parameters, checking dimensional consistency, running sensitivity tests, and qualitatively assessing model behaviors. Research applying system dynamics modelling use selection of methods, which together build model validity. Naturally, applying several methods for building validity can strengthen user belief and trust in a particular model. Luna et. al. model validation was based of the variables being grounded in the qualitative information gathered from interviews, a theoretical understanding of technology enactment (theoretic framework), and the fact that it is created through iterations, testing sensitivity and different parameter conditions [21]. Jalali et. al. [57] performed sensitivity tests and grounded the relationships and modelling decisions in the interview data. Using qualitative data to explain system and model behaviors are commonly used in most research applying system dynamic modelling [62]. Fagade et. al. [58] base their interrelations on the theory of planned behavior and personality profiling based on the big five. Dutta et. al. [22] express difficulties in validation and quantification of the effect of smaller incidents as the information is not publicly available, thus leading the study to focus on checking structural fidelity through input of variable values representative of real scenarios. Some of the variables are of quantifiable nature, while others, such as perceived risk are qualitative. Logical arguments are used to link perceived risk to quantifiable variables such as concluding that perceived risk and risk threshold together determine information security investments. Variables such as perceived risk are set to low, medium or high, quantified by values between 0-1, a scaling method used in other studies such as [21][57]. This notion is supported by Luna-Reyes and Anderson [31] when discussing collecting and analysing qualitative information to create system dynamic models.

One step in [2] methodology, and the methodology of which this thesis draw knowledge from regarding how one investigate problems using system dynamics discuss the same concepts as the ones discussed by [26]. More specifically the process of validation begins with getting the model in steady state equilibrium by setting the inflow and outflow to equal out each other. Then one create a base case, or reference mode, reproducing the base case through the model. The same process used in related works. In-turn checking the variables, the iterations and time intervals in the process. The book [2] reference Coyle's suggested steps to build confidence in a model. The CLD must correspond with the statement of the problem. Equations in simulation must correspond to CLD direction and influence

depicted in the CLD. No unrealistic values and the values must be dimensionally valid (translatable to each other). The model must be plausible and one must be able to confirm the level of which it stabilizes, Further, one must maintain the conservation of flow which means that the total quality of a variable that has entered or left the system is still accounted for. Furthermore, [2] describe additional tests that they have found particularly useful. These tests revolves around determining whether each equation is fully justified. Typically done by providing a managerial explanation of the equation, the variables and referencing the source for the variables.

This thesis validity will be based on several different aspects all contributing to increasing the modellers confidence in the system dynamic model. The validity of the causal loop diagram is mainly based of a theoretic framework highlighting how different variables interact, report analysis which can provide a good initial understanding, and second hand interviews and related works investigating similar aspects of cybersecurity. Validity will largely come down to discussing identified problems in light of the theoretical framework and related research. Naturally, as the causal loop diagram is closely related to the System dynamics model, the efforts done to validate and discuss the causal loop model carries over to the system dynamics model.

Validation of the system dynamic model itself follow the methods, tests and steps to build model confidence will be conducted. The model will be built in an iterative fashion, simulation results will be continuously tested and verified through assessing its correspondence to the problem, correspondence with the CLD, model output and variable realism, conservation of flow, dimensional validity and the level of which the system balances. The resulting process will be a combination of the validation techniques utilized in the related works.

3.2 Explicating the problem and defining the artifact requirements

Research question 1 is to be answered by performing the first phase of this thesis. Done through following the steps out this thesis's proposed methodology, adapted from both the DSR and the ST&M methodologies (3.2). The actual design and development of an artifact begins in phase two. RQ1 require a modelling and simulation method, which both must be tied to challenges facing the completion of this thesis, its objectives and RQ's.

ST and STS imply relationships between social system-constructs, such as ethical and cultural, political and legal, administrative and managerial, operational as well as technical constructs related to e.g. applications used, operating sys-

tems and/or hardware related factors. Different organizational units, people and groups all have their respective system and subsystem which all influence eachother and the decisions being made. This leads to system dynamics as a suited approach to create our artifact due to its ability to incorporate several different types of variables and relationships. Explicating the problem, and structuring the problematic relationships are explained in more detail in the problem structuring section 4.1.

3.2.1 Artifact requirements

Initially it has to be stated that this thesis is to follow its paradigm and focus on its topics, which is reflected in the artifacts requirements. Homer et. al. [62] state that challenges of dynamic complexity, non security related, can be solved by utilising system dynamics modelling tools. System dynamics will enable holistic investigation of the NHS as a complex system of diverse stakeholders. Means of modelling must include ways of illustrating the interconnections within the system, both in terms of stakeholder actions, behaviors and decisions and the conditions and states of system variables. NHS is argued as a complex system, and it is well established that system dynamic modelling is an approach to complex systems, problems and stakeholder/system interaction. There are many works presented in the related work section (2.2) which utilise system dynamics in the realm of cybersecurity [57] [22] [58] [25] [19] and organisational/behavioral theory [63] [21]. All of which finding it an effective tool to analyze complex systems, while trying to holistically assess a problem and situation. All the studies examined in [29] express a fondness for the system dynamics approach, also reflected by the above mentioned studies.

The most common approach to initial modelling is causal loop diagrams [2], although there are other methods of conceptualising the system. This thesis will not only apply CLD to the conceptualisation phase, it will also apply influence diagrams. Additionally, Stocks and flows are identified where suited. Brief descriptions of Causal loop diagrams, influence diagrams and stock and flow diagrams are given in the background section (2), and appedix B (8). Causal loop diagrams (CLD) is a way of structuring problems, the system and its delays. Using causal loops may help in keeping the level of detail down, while simultaneously representing the most important system aspects. Influence diagrams can model causal relationships to greater detail than CLDs and open up for including variables impacting variables within the causal loops. One can also distinguish between what kind of influence each variable and link has [29]. Stock and flow diagrams are included in the ST&M methodology [2] and is a good tool to quantify parts of a qualitative model. A good argument for adopting different modelling techniques before actually creating a quantified simulation environment is the degree of qualitative information used [29]. Causal loops and influences are particularly good at being designed to incorporate qualitative information in to a model [29] [31].

It this thesis all these methods will be utilized throughout the modelling phase. The iterative process of modelling means that one continuously improve the model as one goes along, thus having flexibility in therms of how one can model is preferable. Even through increasing the amount of modelling conventions can increase the complexity of conducting the modelling process. Fagade et. al. [58] apply both causal relationships, influences and stocks/flows to create a "dynamic relationship model". Jalali et. al. [57] mainly use causal loops, while combining it with one single stock representing the most interesting variable. Both give their models baseline values before running simulations. Luna [21] use Stocks and Flows, influences and loops. Homer et. al. [62] also illustrate how causal loops combined with stocks and flows and influences can be used. Based on the system in question and the adopted paradigm a similar approach to system dynamics modelling will be applied, as it is illustrated in the proposed methodology (3.2), and its main inspiration [2].

3.2.2 System dynamics simulation

Modelling the system is an iterative approach, continuously evolving in terms of shape, size and degree of qualitative vs quantitative representation. Ultimately one transform the qualitatively focused variables in the CLD/ID in to a quantified model. Stock and flow diagrams are quantitative models, however one can also quantify variables in a CLD/ID model [57] [58]. Baselining is a concept that will be used in this project. After the model is created, starting from modelling causal flows and loops, one iterativly incorporate stocks and flows and quantification of the variables. One can then create a baseline of suitable values for the system, then simulate what happens if one where to change influences or variables inside the causal loop. More information on the process of creating the system dynamic model used in this thesis are given in relation to its creation 4.3, because its creation depend on the problem, available information and variables.

Chapter 4

The Dynamic Modelling Process

The Dynamic Modelling Process is the main chapter and will finalize all four phases of the methodology, beginning with problem structuring and ending with organizational learning. The end goal is to create a system dynamic model that represents the NHS specialist service, and the inter/intra dynamics of its stakeholders in terms of cybersecurity culture and business alignment. By conducting the identified phases, we can ultimately answer the research questions and achieve the research objective.

4.1 Problem structuring

The information used to hypothesise a problem structure can be found in the introduction (1), background (2.1.1), related work (2.2), and appendix 7. The initial chapters of this paper have described how one can investigate cybersecurity problems in a complex system of stakeholders, through applying a methodology suited to the expressed problem and theories that can aid in understanding the investigated topics. Before beginning phase 2 and 3 in the adopted methodology, (3.2) "Problem structuring" must be finalized. Problem structuring is the main analytical section. Information about the system in question, its stakeholders, and their respective roles will aid in identifying the nature of stakeholder interrelations. Coupled with the theoretic foundation and related work, one can hypothesise important variables and system interaction. The identified problem structures leads to model conceptualisation through causal loop modelling, and ultimately the creation of our system dynamics model. As it is stated in the methodology, model conceptualisation can also feed information back into problem structuring.

Problem structuring consists of two main steps: identifying the problems that concern the main stakeholders, and collecting and present preliminary information and data. This section will therefore attempt to initially describe the dynamics of the system by analysing the system and stakeholders in relation to the proposed theoretical framework, system reports, and related works. The main focus while

structuring the problem are aspects connected to cybersecurity culture and management.

4.1.1 Identification of important systemic aspects influencing cybersecurity culture and ultimately business alignment in the NHS specialist care

The research objective will be answered by focusing on the following main concepts that are firmly rooted in the introductory chapter, background, and related work. First, there are differences in cybersecurity culture among the stakeholders in question. This notion is supported by Klimburg's [56] thoughts on levels of government and the fact that they have their own perception of cybersecurity and how to approach it. Further, there is significant diversity between stakeholders in the system under question, which could contribute to differences in culture. Different stakeholder influence each other through their behavior, such as through law, policy, strategic direction, national frameworks, and regional frameworks, which can in turn influence stakeholders at different organizational levels. Second, by adopting the paradigm of systems thinking and socio-technical systems theory, we recognize that cybersecurity culture effects the NHS both locally and globally, as part of the digital ecosystem. This means that misalignment within a stakeholder locally could be a result of global stakeholder influences. Misalignment within a local stakeholder could impact its capability, opportunity, and/or motivation to exhibit behaviors – therefore limiting its ability to meet organizational goals and resulting in business misalignment problems that are rooted in cybersecurity culture. Business misalignment can limit cybersecurity capability development and therefore result in a sub-optimal cybersecurity posture.

With the problem description in mind, it is apparent that one one must identify how culture, structure, methods, and machines influence each other and how different stakeholders can influence other stakeholders within the system. Naturally, this can be discussed on different levels of abstraction and detail. The aspect this thesis mainly focuses on is cybersecurity culture and business alignment, as cultural differences may result influence business alignment. This effect can be observed by investigating how higher level stakeholders (such as political, professional/executive, and regional level stakeholders) influence those at the operative level. The framework proposed in this thesis have discussed analysis of business alignment in relation to socio-technical systems and stakeholders, an analysis which revolves around identifying the influencing factors that determine the behavior exhibited by stakeholders. (2.1.1).

The term "variables" is extensively used when modelling within the paradigm of systems thinking. In causal loop diagrams variables can be qualitative and of varying nature. They can represent problems, challenges, situations, states or actions [2]. Connections between the variables are relationships. This is kept in

mind while discussing the identified issues and and structuring the investigated problem.

Strong culture for digitalization and modernisation

Digitalization is perceived as a double edged sword [35][45][46][51]. It increases the specialist healthcare ability to meet service demands, while also introducing more threats and vulnerabilities to the system at e.g the operational level. Digitalization raises the overall need to develop cybersecurity capabilities at operational level. Therefore, it must be followed by increased security investments [45]. In NHS, the operational level is currently struggling to maintain and update old equipment and is introducing technologies and systems to organizations that are not mature enough to implement them effectively [47][49]. Organizational focus is directed towards enabling digitalization. As a consequence, the available resources to improve existing capabilities is reduced. The identified vulnerabilities in [51] support this argument, which discusses the lack of technological measures and controls – as well as outdated software and equipment. Digitalization is incentivized through a high focus on digitalization and modernization in nation wide strategies and political direction. It creates a political pressure to digitalize as a means of becoming more effective. Digitalization is motivated by the sector's increasing need to provide efficient healthcare services in order to meet current and future demands. In terms of vulnerabilities, increased digitalization creates an increasingly complicated risk landscape, increased endpoint complexity, network integration, further complicating the digital value chain, and possibly makes current law and regulation outdated. Further, increased endpoint complexity is shown to have negative impact on hospital cybersecurity capability development [57]. The effect digitalization has can be described in terms of the erosion of current capabilities or the added system complexity. Both influence the overall level of cybersecurity capabilities and create an increased need to develop and maintain cybersecurity capabilities.

Missing knowledge and expertise in the sector

There are several reports concluding that the Norwegian healthcare system, and the nation at large, struggle with *missing competence, expertise and experience* when it comes to cybersecurity. Naturally, the cybersecurity culture and knowledge is stronger at ITSP, due to the nature of their business revolving around IT [51]. It is however noted that cybersecurity aware behaviors are more related to technical knowledge rather than procedural, as their IT background would suggest. Sector specific threat and vulnerability assessments [35][51] conclude that the healthcare sector is missing overall competence, has low understanding of cybersecurity incidents and their corresponding consequences, low general cybersecurity culture, and missing holistic understanding of all aspects of cybersecurity [9]. NSM clearly stated that [45][46] the threats resulting from digitalization is not understood.

While the sector is already experiencing a serious lack of knowledge, making the system more complicated through digitalization only worsens the effect. Risk 2019 [45] expresses concerns about the ability of organizations to holistically assess consequences of digitalization, lack of understanding of insider threat, and bad holistic understanding of the different realms of cybersecurity. Sufficient knowledge and expertise in the process of governing cybersecurity would positively effect the success of implemented measures and interventions.

Patient-first mentality and the current understanding of cybersecurity at the operational level

Understanding different realms of cybersecurity (personnel, physical and digital) is not only difficult as a result of increased digitalization, but also due to the fact that it is influenced by the current social cybersecurity capabilities of stakeholders. The results of [9] show that employees in all regions are generally considered to have a good understanding of data privacy and the importance of professional-patient confidentiality. Maintaining this principle is perceived as an important part of providing good healthcare services and maintaining the general public's trust in governmental systems and services. However, contrasting this understanding is the lack of holistic understanding of cybersecurity healthcare employees. This narrow understanding of cybersecurity renders it difficult for employees to recognize how patient privacy is impacted by actions which result in elevated privileges, increased access in the system (availability), and/or the poor provision of data confidentiality. This is consequential, as employees may benefit from recognizing the association between security and privacy yet fail to do so. The healthcare industry task force [49] further discussed the lack of awareness of cybersecurity among healthcare employees, and found that IT-professionals find it difficult to explain cybersecurity concepts to healthcare employees. Similarly, [51] uncovered a lack of understanding regarding cybersecurity incident cost among stakeholders in the healthcare sector.

The *patient first mentality* is explained in the introduction: professionals choose options that are centered around patients rather than security. This can be related to the effect of *shadow security* [23], which is discussed in relation to aligning security policy with day-to-day activities and needs. Shadow security is a result of poor business alignment, and issues are partly due to weak cybersecurity culture in the sector. It is a mentality that is ingrained in the minds of healthcare professionals – as their narrow understanding of security suggests. This narrow understanding results in a cognitive difficulty for practitioners to associate patient safety with general concepts of security. Further, related to decisions regarding security v.s. patient safety, it is understandable that the main concern of healthcare professionals is caring for their patients – as their primary role is centered on doing so. As a result, they generally opt for patient-centered solutions. While choosing solutions which support patients and service capacity may appear most appropri-

ate – since doing so reflects the NHS's objective to provide care – decisions must be made by a capable entity with a strong knowledge of not only patient care, but security as well. Further, this entity must possess an appreciation for both the short and long-term consequences of implemented interventions – as stated in Furulund's interviews [9].

Current employee cybersecurity culture and awareness will limit the positive effect of potential interventions and measures performed in order to increase overall cybersecurity capabilities. Not only does awareness and culture effect employees in their day to day activities and decision-making, but also high-level decisions made by managers. Interventions would be more effective, or potentially unnecessary, in environments where a high level of awareness facilitates security-aware behavior. Governance decisions made by managers as a result of strong culture and awareness are ultimately connected to overall knowledge and expertise, and as we already discussed, decisions made on a strong foundation of knowledge would be beneficial to the effect of implemented interventions.

Decentralized management of cybersecurity in the NHS as a whole

Each entity in the NHS specialist service is responsible for maintaining cybersecurity and handling incidents themselves, a responsibility identified in national strategies, the roles and responsibilities of the stakeholders (7.27.3). The main top-level national influence is expressed through law, an effect which will be discussed later in this text 4.1.1. Directorates in the NHS specialist health service hold the professional role, thus linking the executive/operational level to the political level. The executive level is delegated to the RHA's, which further delegates responsibilities to the operational level: individual HT's (hospitals). This structure is emphasized in political guidelines and strategies. RHA's have an established "make sure of" role towards the operational level [51] and provide cybersecurity guidelines which govern their cybersecurity capabilities. Additionally, operational level cybersecurity efforts are governed by law and regulation, and consequently the directorate's (professional level) efforts in translating law and regulations into specific guidelines.

In theory, this systems appears effective as it provide guidelines and procedures which govern the information security on subordinate levels and ensure that the level of cybersecurity is the same in all hospitals. Yet, a fundamental principle is that each individual HT is responsible for individually assessing the need for cybersecurity measures. The guidelines provided on a national level effect everyone, guidelines created at regional level influence the entities within that region, and individual interpretation of the governing frameworks at the operational level result in actual cybersecurity governance. Following this structure, we can see that there may be significant differences between the four regions, and even hospitals within the same region. Differences arrive as a consequence of law and regulatory

frameworks which do not holistically cover all aspects related to governance of information security, and individual HT assessment of the demands/recommendations. Informants in [9] state that the regional frameworks are mostly based on Normen [40][41], and that the sector-norm is largely based on based on law. The relationship between these stakeholders makes each HT largely responsible for their efforts to enhance cybersecurity, especially capabilities outside of those specifically demanded by law. The informants interviewed [9] are connected to different regions and can discuss the result of organisational structure impacting them in different ways. Changing the regional level frameworks can be difficult, as this is done in monthly meetings and disagreements between HT's may result in changes not being accepted. Differences in regional frameworks are shown through, for example, each region having an obligatory e-course which is repeated every 3 years. Further, the way that RHA's ensure operational level participation varies significantly. For example, Helse Sør-Øst has a much higher completion rate than Helse Nord. This is because employees will be locked out of the system if they do not finish the course. Additionally, these informants state that there are different demands when it comes to documenting risk assessments, resulting in differences in the results based on the person conducting them.

The intention of making each HT mainly responsible for capability development is to account for the large differences between them in terms of their size and operations. It enables each HT to implement information security management systems that reflect their business and could potentially increase their ability to reach organizational goals. However, when one considers the general lack of resources, knowledge, and expertise, it becomes appropriate to question the decentralized structure – as information security depends on individual assessment rather than assessments made by a large more competent entity. From a regional perspective and their "make sure of" role, it is difficult for regional level stakeholders to reach out to hospitals within their region with awareness campaigns due to their remarkable size (e.g Helse Sør-Øst with 80,000 employees). Additionally, the large diversity in employee backgrounds and foundations with which to build knowledge upon makes creating effective awareness campaigns more difficult. By providing the operational level with more resources, more cybersecurity personnel, and a higher focus from operational level management, overall cybersecurity capability development could increase. However, the sector's apparent lack of these resources limits the operational level's efforts to increase capabilities. The informants from [9] highlight the difficulties in incorporating different perspectives in decision-making, especially when considering how the patient first mentality and lack of holistic understanding of actions, decisions, systems, and equipment can result in stakeholders sticking to old habits at the cost of cybersecurity.

Ultimately, with the operational level stakeholders' current lack of capabilities in the form of knowledge, expertise, and awareness, one could argue that increasing the level of involvement exhibited by professional agencies could prove

beneficial. Their role is currently limited to being professional, as in helping with knowledge and expertise on relevant subjects – yet they have limited governing power and control over the actual management of cybersecurity. Changing the professional level's role and responsibility has been proposed by the directorates themselves [35] as a measure to increase cybersecurity capabilities, a solution yet to be implemented, and have lasting results. Additionally, a more holistic national strategy which governs the entire NHS is proposed. This strategy could result in more nationwide regulations and guidelines for lower-level stakeholders to follow. These measures can centralize the governance of information security within the NHS and increase the operational level's opportunity, in order to improve the most critical of all vulnerabilities: the lack of social capabilities. By increasing national involvement, we could also make RHA's more aware of potential measures and controls, which could enable them to implement solutions by means of increased resources. Finally, increasing knowledge of cybersecurity at the managerial level, and including operational level IT-security personnel in regional level cybersecurity management, could enable a more holistic and centralised management structure.

Information security management is overly focused on law

Law and regulation govern cybersecurity development through the their ability to mandate that operational level stakeholders comply in certain ways. Normen[41][40][64] is mainly seen as a set of demands of a primarily technical and structural nature. The new security law is specifically tailored to the emerging threats arriving as a result of digitalization [45][46]. Even though this is the case, it may become outdated in the future or be misaligned with the actual business needs of relevant stakeholders. The latter was expressed by informants [9], whereas the fist claim is strengthened by the reactive nature of change as a consequence of large incidents – which will be discussed in the next section. (4.1.1).

Law and regulation, and the demands depicted in Normen, focus primarily on technical and structural demands as a consequence of the social aspect of cybersecurity being more difficult to control and regulate than structural and technological factors. Cybersecurity culture is something that needs to develop over time and be continuously maintained. It is not the same as requiring a specific protection scheme, or bullet-points, to include in risk assessments. National strategies emphasize the need to develop regulatory frameworks in-line with digitalization. It is worth noting that law and regulation must be created to benefit organizations rather than create complicated, distracting, and expensive compliance frameworks [48]. The regional employees interviewed by Furulund discuss misalignment between the regulatory demands introduced by Normen and actual organisational need. Risk assessments are one such example. The process of risk analysis is in some cases perceived as cumbersome, overly time-consuming, and overly focused on the negative consequences of implementing changes. Risk ana-

lysis should asses both cost and benefit, where the potential benefits might be higher than risk [9]. While current demands may not be completely aligned with organizational need, this is not the main focus in this section. Rather, the focus lies with how Normens demands govern cybersecurity efforts.

Normen is based on law and communicates legal frameworks, which makes it is the national level and consequently the professional level's main measure to influence cybersecurity governance on the operational level. As a consequence, their governance is overly based on law and regulation. Normens position it the sector is good [51], and ITSP, RHA's, and hospitals use and follow its mandates/-demands. This is a good thing in and of itself, as it ensures compliance with the law. It can however have an unintended consequence wherein legal demands are given the largest focus, at the expense of organisational needs. This is discussed by [48] and briefly mentioned when discussing the effect of continuous digitalization and increased system complexity. As a result of Normen being overly focused on privacy, structure, and technicalities, the efforts and resources of RHA's, ITSP's, and hospitals largely focus on these aspects – as the law mandates. Yet, the identified weaknesses in the NHS are largely, in fact, rooted more in its social and cultural aspects. Interventions which target social capabilities – such as strengthening cybersecurity culture by increasing knowledge, expertise, increasing collaboration, and/or performing exercises – are overwhelmingly represented in threat and vulnerability reports [35][38][45][49][51], but not demanded in Normen. While national regulation and law are effective at "forcing" change and potential improvement, one can question the holistic nature of Normen and the current influence and interventions system stakeholders have on development of operational level social cybersecurity capabilities. The law has significant impact on stakeholder influence, and can ultimately lead to increased funding. After all, funding is ultimately decided by the focus of regional level stakeholders. Legal frameworks failing to incorporate the social aspects sufficiently ultimately make the funding of cybersecurity capabilities outside of law and regulation limited, resulting in a lack of resources to effectively increase capabilities at the operational level.

The effect of prioritizing capabilities which reflect demands can be seen in the very high number of created and approved IKT-contingency plans – as demanded by Normen – compared to the number of systematic exercises performed in the sector [51]. Every HT and ITSP, and 75% of RHA's, have created and approved plans, but at the RHF and HT only 75% of then perform exercises at a small small/-moderate degree, which is not sufficient. Sector reports and recommendations focus on intensifying the rate of exercises, as well as the importance of performing them while focusing on collaboration between stakeholders. The workforce requests more national level guidelines and demands in order to achieve this goal. When asked if the respondents from RHA's, HT's, and ITSP have investigated the security culture of the organisation in the last three years, the answers are varied

(RHF (25%), HT(45%), IKT supplier(75%)). This is rather low compared to the national average (41%), especially as the nature of healthcare revolves around personal information and critical services/systems [51]. This suggests that organizations follow law and regulation, and do not focus on the identified social and cultural challenges, even though social weaknesses are thoroughly investigated and brought forward in a plethora of risk and vulnerability reports. It also illustrates how the professional agencies are effective in their role when communicating law and regulation. However, they are not as effective in communicating guidelines and recommendations as they are not equally focused in the operational level's efforts to improve cybersecurity capabilities.

The reactive nature of change - a result of large incidents

Perasklis states that healthcare in the United States has a reactive approach to change [48]. Similar conclusions are drawn in Jalali's paper investigating cybersecurity capabilities [57], where incidents and attacks are the catalyst of change. The professionals interviewed in [57] state that successful attacks and incidents increase the pressure to improve cybersecurity capabilities. Leaders become more aware of the threat, and politicians understand its importance. This results in increased motivation, investments, and capability to improve cybersecurity. In [9], interview subjects describe the same effect – especially as a result of the large, successful cyber attack on Helse Sør-Øst [3]. The informants describe this as a before-and after-situation, wherein the attack increased the anchoring of cybersecurity in top-level management at the HT, while also resulting in new law, regulation, and national strategies. Although it resulted in positive changes for the sector, the fact that large successful attacks are the source of such action is not optimal. One should strive to minimize harm through developing a proactive and risk aware approach, rather than an approach that is merely reactive.

An interesting phenomenon related to cybersecurity culture is the levels of perceived risk. When one is subject to an attack, the perceived risk increases – resulting in a pressure to have stronger capabilities [57]. After periods with no serious cybersecurity incidents and/or attacks, the perceived risk gradually lowers. Dutta et. al. [22] described the *Percieved risk* as a paradoxical effect, because well-placed investments and focus can isolate employees from cyber incidents, in turn increasing cybersecurity risk due to employees lowering their guard and engaging in less risk-aware behaviors. General exercises, and "fire drill" type exercises, are identified as an effective measure to counteract this effect. However, there is a general lack of exercises and an initial lack of cybersecurity culture and risk awareness in the healthcare sector, as brought forward by national advisory agencies and sector-specific reports.

Collaboration within the sector, and across different sector in the NHS

Collaboration and capability development increased as a result of the attack on Helse Sør-Øst, both during and in the aftermath. All regions engaged in activities which enhanced their cybersecurity capabilities. Additionally, during the incident, Helse Sør-Øst stated that their collaboration with HelseCERT and other national and private organisation was good, and yielded positive results in terms of increasing their ability to handle the incident [9]. Increased efforts to collaborate as a result of attacks and perceived risk, is supported by Kianpour et. al. [65], which found a strong influence between attack experience and increased collaboration. Regardless of identified improvements, there is still work to be done when it comes to increasing collaboration. After all, it is very important to collaborate in interconnected systems where different stakeholders could benefit from shared information. Collaboration could increase business alignment. For instance, at operational level it is noted that risk analysis is mostly conducted by information security professionals without much involvement from management [51]. This is an issue, as involving management is important to achieve a holistic and shared understanding of risk and cybersecurity. Additionally, the sector lacks the understanding and knowledge to conduct holistic threat and vulnerability assessments themselves. Also, willingness to collaborate deters as the perceived risk decreases [22][65]. The focus on increasing collaboration among the stakeholders is discussed in several risk and vulnerability reports for the sector. Collaboration could increase as a result of current national and professional stakeholder involvement being changed, specifically through providing them with increased responsibilities related to cybersecurity governance.

Misalignment's between strategic direction, law, regional influences and the cybersecurity culture at operational level

At a national strategic level, one can see that the government is interested in digitalization and modernization while maintaining sufficient cybersecurity capabilities. Cybersecurity is a means to optimize the benefits of digitalization and maintaining trust in the public sectors systems and digital services [38]. The main national level strategy to improve cybersecurity culture is focused on increasing cybersecurity focus within educational programs [39], while giving the operational level the responsibility of identifying and improving culture within their organisation. National level strategies also identify the need to reinforce governance and control of security [38] through national influences. However, as discussed, their efforts to reinforce governance have yet to show significant results on the operational level. It is not uncommon, in a general sense, for national level strategies and other socio-political interventions to not follow technological development and consequently the needs of its subordinate stakeholders. Klimburg states in his concluding arguments to assessing national level cybersecurity frameworks that: "Socio-political answers to the questions posed by the rise of cyberspace on the whole significantly lag behind the rate of technological change" [56].

The current national strategies do increase cybersecurity capabilities over time through their educational focus, as increasing the knowledge and awareness of employees through education could reduce their current lack of knowledge and expertise. However, current national strategies are lacking in their focus on how current cybersecurity culture can be improved in terms of internal capability development. National level strategies and interventions are crucial in order to provide incentive for subordinate agencies, as they greatly influence regional and professional stakeholder's actions. For the time being, however, their influences is limited to interventions and practices outlined by current legal frameworks. Perasklis [48] highlights the importance and need for high-level strategies when prioritizing which socio-technical aspects one should focus on improving. The holistic threat and vulnerability assessment conducted by the Directorate of eHealth [35] concludes that there is a need for a holistic IKT-security strategy for the sector, which should be connected to national strategic direction and sector-specific challenges. The strategic guidelines governing the specialist healthcare sector cannot be evaluated as holistic, as the overall responsibility for developing cybersecurity culture lies with the individual regions and hospitals, a method which is not working optimally considering the well-documented under-prioritisation of social measures.

Also highlighted in threat and vulnerability reports are the importance of strengthening the professional and executive role of directorates, and increasing resource availability. Currently, the directorates main influence is based on law. Which is as discussed problematic, because law is not holistically covering best practise, especially in terms of social capability development. The regional level mainly base their management systems on Normen, which provide recommendations covering all aspects of cybersecurity, and demands reflecting regulation. Demands have the largest influence, whereas the recommendations are not followed by the operational level or updated by the secretariat responsible for it. The secretariat and subordinate to the directory of eHealth have limited resources, and therefore mainly focus on the demands rather than recommendations – which are becoming more outdated by the day [42]. This is an understandable decision considering that the demands are the part of Normen which is primarily being used. Informants in Furulund's interviews [9] highlights the importance of the government's role in providing solutions to the problems caused by increased digitalization. We cannot seem to identify the solutions in the current socio-technical system of NSHS.

Our main takeaway from this section, in relation to the research objective, is that the current stakeholder dynamics limit the ability of operational level stakeholders to develop and maintain an acceptable level of cybersecurity capabilities – especially related to the social aspect of cybersecurity. Current stakeholder dynamics and influences are caused by cultural aspects, such as strong digitalization culture, decentralized management structures, and current law and regulation.

As a result of directorates performing their role as professional agencies, the sector has a lot of knowledge of which measures can be implemented, and we can see an increase in threat knowledge and collaboration as a result of recent attacks. However, the proposed measures are not necessarily acted upon due to professional and regional level stakeholders having limited governing power and control. Strong security culture and leadership is not necessarily something that can be regulated in the same way as technological and structural demands, but is rather something that is built and strengthened over time [9]. Further, national level influence should be tailored more towards the social challenges facing the operational and regional levels of the system, by increasing both their opportunity and capability to improve the most critical vulnerabilities. Professional agencies, private actors, and the sectors themselves have identified the challenges but do not have the competency, resources, focus or understanding of cybersecurity to actually incentivize or enable hospitals to implement the necessary changes. Shifting the focus from individual operational level assessment to regional/professional level control and governance could increase overall social capabilities by counteracting some of the most prevalent stakeholder dynamics identified. We conclude that national strategy, regulation, and organizational structure do not enable subordinate organizations to positively influence the operational level. Increasing operational level cybersecurity capabilities reflects the goal of all stakeholders as they would benefit from the sector being secure. After all, it would protect patients and employees from the possible consequence system (in)security. We have therefore identified stakeholder relationships which causes business misalignment. National level stakeholders should – through their power – change current roles, responsibilities, law, strategy, and funding. These changes could change the influence and control exhibited by their subordinate stakeholders (professional/regional), which would ultimately influence the operational level's opportunity, capability, and motivation to increase social capability development.

4.2 Causal Loop Modelling

The analytical section above will be transformed into a causal loop diagram. The two could have been combined, but are separated as an attempt to present the method in a structured way, even though both sections are conducted in iterations. Causal loops tell a story. Creating stories, or rather presenting actual problems and issues of concern related to the research objective, is the first step towards creating a holistic system dynamic model. The causal loop modelling step is focused on identifying potential variables, its structural components, analysis of behavior over time and identification of key leverage points. The model is based on the problem structuring section. Information on the process of creating causal loop models can be found in appendix (8). The causal loop is presented in its entirety in figure 4.1, and should be seen in relation to the sections presenting the CLD sections. Further, the CLD will be the basis of the systems dynamics model, and due to the CLD only serves as a preliminary activity, the primary focus on model

accuracy and structure is done in relation to the system dynamics model rather than the causal loop model.

Key actions or conditions create the best starting variables in CLD's. Variables can influence and be influenced by other variables [2]. Variable names should be be nouns rather than verbs, such as using production rather than producing, one should not include adjectives such as increased, more or less in variable names, limit usage of one variable once in a model and one should present variables in their positive sense, meaning that willingness should be used rather than unwillingness. These principles are not to be mixed with the ability to use variables with a negative association, such as employee burnout.

B1 - Digitalization to meet current and future service demands:

There is a strong culture for digitalization at the national level. Digitalization increase *system complexity*. The political pressure to digitalize the sector will be balanced out by the sector bridging the gap between their *level of service* and *current demand*, because then the need for capacity would be matched by current capacity. Societal development and strategic influence will ensure a continued digitalization in the foreseeable future, due to increase in current capacity demands. The two latter variables are represented as influences rather than being a direct part of the loop. Additionally, it is assumed that there is a delay between identification of needed increase in capacity and actual increase of digitalization efforts.

System complexity and digitalization influence the quality of social capabilities and compliance with law and regulation System complexity is increased by digitalization. The problem structuring phase argue that system complexity increase in-line with digitalization as it introduces new systems, new methods, new equipment, more network integration and result in a more complicated value chain. This expose the system to more cybersecurity risk. Digitalization demand a higher level of knowledge and awareness from the employees. Additionally, digitalization results in law and regulatory changes, increasing demands following implementation of new technology, systems and methods. The CLD show how system complexity negatively influences compliance with law and regulation and the quality of social capabilities as a result of increased digitalization.

B2 - Compliance with law and regulation, development of technological/-structural capabilities and available resources

Being compliant with law, regulation and demands are as argued the main priority for and management at the operational level. Normen is the main influence as it provides sector demands given through law, which the operational level is obligated to follow. Operational level *pressure to follow law and regulation* is caused by regional frameworks and regulations mainly basing their demands on Normens.

Outside of Normens demands there are recommendations given by RHA's and directories, but developing these capabilities is not subject to the same regional, national and national professional pressure and is therefore not implemented to the same degree. Implementation of capabilities outside what law and regulations demand are influenced by variables such as *Available resources* and the operational levels *Capability to improve*.

Increased *compliance with law and regulation* decrease the *pressure to follow law and regulation*, thus balancing *development* and activities conducted to ensure compliance. Continued digitalization and increased system complexity demand more effort from operational level to be compliant and increases overall the costs related to development. Adding to the costs are maintenance of current *Compliance with law and regulation*. Costs associated with law and regulatory compliance depletes the operational levels available resources.

There are identified some problematic effects of organizations being influenced by law and regulation to develop cybersecurity capabilities. First, the fact that law and regulation could be outdated in the future. Secondly, the demands can be misaligned with operational need. *Misalignment with organisational need* decrease available resources. *Available resources* is tied to a *resource gap*, rooted in the identified lack of available resources to develop of cybersecurity capabilities, especially outside of what is currently demanded through law.

Quality and level of social capabilities - Available resources, digitalization, social capability development and current capabilities

The current *Quality and level of social capabilities* are influenced by several variables and cause and effect relationships. In itself it is a goal seeking loop, with system limitations in terms of the *resource gap*, and potential self regulating relationships rooted in awareness and overall capability. The CLD model separate capabilities related to law and regulation and social capabilities. The NSHS is simplified in the sense that the capabilities outside of the ones demanded through law and regulation are social. The separation is rooted in the identified focus of Normen and the current identified cultural issues described in the problem structuring phase.

B3 - Quality and level of social capabilities, target level, capability gap and development First and foremost there is a *capability gap*, which is determined by the total *quality and level of social capabilities* and the *Target level of cybersecurity capabilities*. The target is affected by operational level motivation, a concept introduced at a later stage of the presentation. The current gap represent the needed level of social capabilities, thus giving the operational level incentive to improve and develop their capabilities.

Digitalization and system complexity Digitalization increases *system complexity*. System complexity is connected to the *quality and level of social capabilities*. An increasingly digitalized environment results in processes and methods being exposed to more digital risk, it becomes increasingly difficult to understand the full consequence of digitalization and to gain a complete overview of risk, The result is illustrated simply, the *quality and level of social capabilities* decreases as a result of increased digitalization because digitalization will demand more knowledge and higher levels of awareness of employees.

R1 - Quality of social capabilities reinforces itself through increased capability to improve The *capability gap* has an opposite relation to the operational levels ability to improve, because in order to be able to efficiently *develop cultural and social capabilities* one must posses sufficient human resources, knowledge and expertise. The relationship creates a reinforcing loop, where by increasing social and cultural capability one can further increase efficient development, linking back to the *quality and level of social capabilities*. Ensuring that the operational level posses sufficient knowledge and expertise while managing and governing cybersecurity increases the quality of social capability development. The *capability gap* illustrate missing social capabilities in relation to the identified goal and need of the operational level.

R2 - Cybersecurity awareness and employee cybersecurity culture Increasing the *Quality and level of social capabilities* would increase *Cybersecurity awareness*, which in-turn counteract the negative effects of the current cultural challenges the sector have such as *patient first mentality*. Higher awareness results in more security aware behaviors. It is already discussed that the employees in the sector have difficulties connecting general security concepts to their day-to-day activities. Increasing awareness will result in a higher level of social capabilities due to employees incorporating security in their decisions when faced with increased system complexity.

The current system created mainly incorporate digitalization, compliance with law and regulation, the quality and level of social capabilities, resources and its relationship with itself

Up until this point the CLDs illustrate some essential cause and effect relationships, most importantly it illustrates a continuous need to develop cybersecurity capabilities in-line with digitalization. It highlights how law and regulation create a pressure for compliance, and how its development and maintenance influence the available resources used to increase capabilities outside of what is demanded through law. Capabilities outside of law and regulation are perceived as being of mainly social and cultural nature. Development of social capabilities are not only limited by available resources but the current quality of social capabilities relation

to the operational levels capability to improve and overall employee cybersecurity awareness. The model conveys national influences, professional (directories), regional and operational as they are discussed in the problem structuring section.

Expanding the causal loop model towards a holistic assessment of the interrelations of the system

When we combine the level of *Compliance with law and regulation* and level of social capabilities we have the *Level of cybersecurity capabilities at hospitals* we can illustrate the *Total level of cybersecurity capabilities at hospitals*. The total capabilities are influenced by all the underlying forces driving development of both types of previously examined capabilities.

The *level of cybersecurity capabilities* is related to *system vulnerability*, when the level of cybersecurity capabilities increase the level of system vulnerability decrease. Socio-technical systems theory introduce the concept of system insecurity related to misalignment in systemic aspects, in out case we can identify a misalignment between the technology system complexity and the *level of cybersecurity capabilities at hospitals/the operational level* .

Naturally the level of *system insecurity* is related to the amount of attacks and incidents an operational level entity experiences. There are several consequences of attacks and incidents discussed in this thesis. We have identified a potential decrease in social capabilities as a result of strong cybersecurity capabilities, since they result in less *incidents and attacks*. Less *incidents and attacks*decrease in *attack experience* and *perceived risk* ultimately decreases overall *quality and level of social capabilities*. *Perceived risk* can also increase cybersecurity awareness and employee cybersecurity, as a result of attacks and incidents increasing. This structure is labelled B3, because increasing capabilities ultimately balances out the growth. The delays illustrate the fact that attacks and incidents are a result of system vulnerability over time. The amount of delay is associated with both the degree of insecurity and the incident/attack type. Smaller incidents happen continuously [9], whereas larger attacks occur more rarely.

The sectors reactive pattern of change The amount of *incidents and attacks* has a positive correlation to many different variables. Attacks and incidents build *risk knowledge* and *attack experience*, both of which increase risk knowledge. *Collaboration* between different sectors and stakeholder within a section is increased as a result of attack experience. *System vulnerability* also positively correlate to *Perceived risk*, which in-turn will increase *operational level pressure to have stronger capabilities* and *managerial support*. Larger attacks have a documented positive effect on cybersecurity in the sector through increasing these variables smaller attacks and incidents have much less impact. All the above mentioned variables

add to the *operational level motivation to change behavior*. As it is documented, increased motivation has a positive correlation to increasing the *target level of cybersecurity capabilities*, thus adding to the identified *capability gap*, a variable relative to the current demand of capabilities. Adding to *Operational level motivation to change behavior* will result in an increase in *regional level influence*, which in turn can increase *investments* and *available resources*. However, regional level influence is limited due to their current role and understanding of cybersecurity at the operational level. The effect show how a low level of capabilities is balances out changes as a reaction to larger incidents and attacks.

Operational level opportunity and strategic influences

Throughout the explanation of the CLD the concept of motivation and capability have been presented. To be able to analyze business alignment we need to incorporate all COM variables. The last variable, opportunity, is yet to be presented. Opportunity relates to factors outside of the operational levels control. Changing opportunity is mostly associated with increasing e.g available resources or increase capability. Interventions capable of changing opportunity is e.g. strategic direction, environmental restructuring or other enabling interventions outside of the operational levels immediate control [16].

National level influences are separated between interventions which can directly influence awareness and capacity (External development), and current strategic directions relationship *Operational opportunity*. *External development* can positively effect both cybersecurity knowledge, expertise and general awareness of employees through current high-level educational programs and national level awareness campaigns. National strategy currently focus quite heavily on this as a long term solution to the growing problem of inadequate social capabilities. Noted are the fact that these measures lies within national level role and responsibilities, so they are enacted upon and funded. We also model the negative, or potential positive, effect on *operational opportunity* by changing their current role and responsibilities. Our knowledge of stakeholders and organisational structure suggest that national level politicians and high-level strategic administration exhibit their governing power through subordinate agencies, such as directorates and regional authorities (RHA). The current structure forming the state ran specialist health service use the directories as professional entities. Both subordinate agencies have limited governing power when it comes down to each individual hospital. Hospitals are themselves responsible to assess and implement measures and controls. Resulting in a sub-optimal usage of regional and national professional agencies

Changing current strategic influence would have a positive impact on *Operational opportunity*, which could in turn increase a HT's *available resources* through giving the regional level more influence, as they are important in funding and

governing all hospitals within their region. Changing the role and responsibility of directorates to give them more governing power could also positively influence operational level opportunity. National stakeholders could change law and regulation to be more holistic, or expand directorates current professional role to a more involved one – resulting in their current professional advice and recommendation being followed to a larger degree. Evolving legal and regulatory *compliance demands* could result in increased *investment* and development of capabilities outside of the current demands, which as discussed exclude demands related to social capabilities. Directorates have a strong understanding of how sector risk being able to influence the decision-making process on the operational level or regional level could counteract the operational level's lack of knowledge and expertise (capability). Strengthening the current role of directorates has already been proposed to increase overall cybersecurity in sector reports.

B4 - Current culture and system understanding balance national level influence B4 is an important limiting factor effecting system development. Current *strategic influence* is influenced by the current national culture of decentralized management. Law and regulation, national strategy, directorates and RHA roles and responsibility makes the operational level responsible to implement measures, and increase overall capability. The causal loop limits *operational opportunity*opportunity, thus their ability to improve social cybersecurity capabilities.

The causal loop diagram

Figure 4.1 show the finished CLD. It incorporates the concepts discussed while structuring the problem. The CLD initially tells a story about how digitalisation and system complexity influence development of cybersecurity capabilities. It continues by tying overall capabilities, attacks and incidents, and high-level strategic influence back to variables affecting capability development. The variables and system structure will be improved and tailored to the coming system dynamics model, which will be presented in more detail than the CLD. 4.1.

4.2.1 Analysing causal loop behavior

Both the problem description (4.1) and the causal loop modelling phase (4.2) provide system analysis which enriches our understanding of stakeholder and system interactions. However, we have yet to provide a holistic assessment of how the different causal relations interact over time, identified the key leverage points, and discussed how the model is related to business alignment. The analysis will therefore be developed by combining the theoretical framework, informational background, and modelling methodologies. By applying the theoretic framework in our analysis of the CLD, we greatly enrich the analytical nature of the model regarding business alignment.

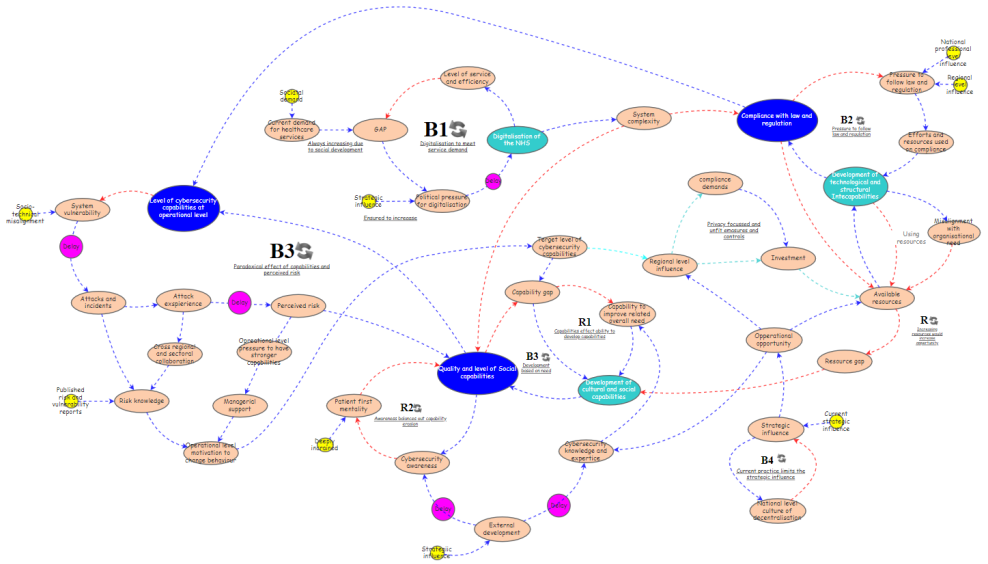

Figure 4.1: Illustrating the a complete causal loop diagram, connecting all causal relationships discussed.

The system and stakeholders effects desired behavior and capabilities through Capability, Opportunity and Motivation

The main problem modelled in the causal loop diagram is how culturally rooted relationships between stakeholders and system variables influence system behavior. Behavior is determined by an actor's capability, opportunity, and motivation. The CLD shows how inter and intra-relationships influence the operational level's behavior through the factors given. Therefore, by investigating and analyzing the identified relationships, we can determine potential interventions and systemic aspects which influence a stakeholder's ability to achieve their behavioral goals. The interventions and systemic aspects could be the result of stakeholders on different system levels, meaning that problematic inter/intra relationships could result in business alignment issues.

Michies work[16] consists of the behavioral change wheel and the COM-B model. To achieve a behavioral goal one must ensure that there are appropriate opportunity, motivation and capability to achieve this. Behavior can be changed by introducing interventions that target the capability, motivation and opportunity (COM-variables, see 2.3). The behavioral system imply that changing behavior can ultimately change the variables. Mitchie et. al. state that:

> "for a given behavior in a given context it provides a way of identifying how far changing particular components or combinations of components could effect the required transformation." [16].

Meaning that the required transformation might be limited by one of the variables

alone, or by variables limiting desired behavior to different degrees. The required transformation of the system is in our case achieving socio-technical alignment and matching cybersecurity capabilities with the increasing digitalization and risk exposure. For more information on the theoretical framework and how it can be used to analyze business alignment see section (2.1.1).

Analysing system behavior over time The system trend is that there is that digitalization correlate positively to system complexity which decreases overall compliance with law and regulation, and the quality and level of social capabilities. The sectors organisational structure and focus makes it so that compliance and regulation is in focus, rather than organisational need and social capabilities. Thus, resulting in hospitals having difficulties developing social capabilities at the pace it is needed to minimize organisational vulnerability. The overall lack of social and cultural capabilities is well documented, and is shown in the CLD.

Vulnerability and attacks have a positive correlation with operational level motivation, resulting in higher goals and targets for cybersecurity social capabilities. In itself, the target represent an organizations identified need to improve as a result of higher motivation. Motivation is linked to increasing total cybersecurity capabilities by increasing the regional level investment. Increase in motivation and its related variables effect on cybersecurity capability development was observed during recent attacks on the sector [9]. Operational level motivation is relatively high and not seen as the COM-variable limiting the operational levels ability to exhibit desired behaviors.

Over an extended period of time the sectors capacity and law and regulatory compliance will balance out at a level close to their respective goals due to national level push for digitalization and the current operational level prioritization of law and regulative compliance. The social capabilities will balance out on level below its goal as a result of the limiting factors of resource availability, capability to improve and level of awareness. While motivation positively influence social capability development it is not sufficient to push social development towards it meeting the desired levels. Social capabilities continue to be lackluster, even after larger attacks, incidents and high levels of motivation. The regional level have limited governing power, thus limited opportunity to change cybersecurity capability development at hospitals. Hospitals are themselves responsible to maintain and develop their own cybersecurity management system and introduce suitable interventions. Balancing out development, in relation to digitalization and increased system complexity, is perceived as the desired behavior due to its focus in sector reports. According to the socio-technical theories we always want to align efforts to different socio-technnical aspects to reduce potential system insecurity. The culturally rooted factors limiting capability is therefore a cause of business misalignment

Opportunity are factors not directly governed and controlled by the operational level. Opportunity have a big role in enabling development of social capabilities and overall increasing cybersecurity capabilities. As highlighted by the CLD, increasing operational level opportunity can result in law or regulative changes decreasing current compliance, or increasing operational levels need to invest by proposing demands outside of current law and regulation. Changes in organisational culture and strategic influence could enable professional agencies more executive control, thus including a capable body of knowledge in the operational levels process of developing social capabilities. The effect of increasing strategic and high-level influences is balanced by the current decentralised culture of information security.

The inter-stakeholder relationships limiting operational level opportunity results in inadequate social cybersecurity development. Resources are lacking as a result of operational level opportunity and law and regulatory focus. This in-turn limit resource availability, thus reducing the operational levels ability to focus on cybersecurity surrounding organisational need. Operational level initial lack of social capabilities, and insufficient effort to improve it, result in low levels of knowledge, expertise and awareness. Lacking social capabilities lower overall social capabilities over time. Seemingly, as a result of sector risk assessments, strategic direction, incidents and attacks the sector have sufficient motivation to improve capabilities. The factors discussed, in conjunction with a continuous increase in system complexity, results in a decline in the operational levels social capabilities over time. Overall sector capacity and law and regulatory compliance are going to increase towards their intended levels.

The key leverage point of the model Leverage points are key actions or interventions which can have a lasting impact on the system, reversing trends or breaking a vicious cycle. The focus should be on identifying the problem rather than symptoms of the problem [2]. On a high-level one can say that the key leverage point of the model are operational level opportunity, altered by changing the organisational and managerial structure of the system. One could to some degree state that limited capabilities, and development of capabilities are a symptom of inadequate regional, directorate and national influences in the process of governing and managing cybersecurity. The operational levels limited capability to successfully maintain appropriate levels of social capabilities is not easily changed by targeting capability alone as it relies heavily on opportunity. Increasing operational level opportunity is not limited to increasing operational level investment, but changing the role and responsibilities of different stakeholders in the system. This could increase investment and help individual hospitals in their governance decisions, thus increasing capabilities as well as investment. Due to its high opportunity is perceived as the key leverage point in the model. Capability could also increase overall level of social capabilities, but without more resources, and regional/national influence the sector will have difficulties keeping up with current

increase in system complexity

Analysing cultural problems resulting in bad business alignment Analysing a causal loop model should be focused on both the CLD in itself, development over time and how the model relates to the overall research objective. Business alignment is as stated in section (2.1.1) linked to COM-B, socio-technical aspects and interventions. "Business alignment means that the goals and strategic direction governing the cybersecurity measures and incentives must be alignment with the general business needs, long term objectives, general purpose and ensure value creation." By looking at the causal loop diagram from the perspective of business alignment one can see how inter and intra stakeholder relationships influence the effectiveness operational level cybersecurity management and governance. The desired behavioral goals, increasing cybersecurity capabilities, is reflected at all organisational levels. Directorates propose measures to enhance social capabilities inline with digitalization, private actors highlight culture as a problem, the regional level acknowledge the situation and the operational level want to increase the overall level of capabilities. However, there are balancing structures rooted in cultural understanding that limits the operational levels potential to achieve their goals in terms of cybersecurity, as discussed when presenting national level culture and understanding the main leverage point of the model.

According to the adopted behavioral theories we can say that capability, opportunity and motivation all have the possibility to influence each other. Either positively or negatively. Behavioral concepts are present at all levels in the systems, but our analysis is mainly based on surrounding stakeholders effect on operational level behavior. We can see that the long term goals and objectives, and strategic direction of the primary national influence is not necessarily complimenting operational need, resulting in business alignment issues rooted in national level ability to increase operational level opportunity. As a result of their organisational culture and culture for law and regulation being the main governing factor. Additionally, the subordinate entities have limited governing power and control resulting in missing resources given through regional levels influence. For the operational level to be able to follow their needs it is necessary to increase both opportunity and capabilities. Stakeholder influences which limit operational levels ability to achieve desired behavioral goals represent the factors contributing to business misalignment.

4.3 System Dynamic modelling

The system dynamics model (SDM) will be presented in more detail than the CLD by introducing small and isolated structural parts, which will be continuously added to, over the course of this section. Problem structuring and causal loop modelling have presented influences and discussed how, and why, variables influence

each other. The Systems dynamic model is an extension of the CLD and will look different due to the way simulations work. Some sections will be simplified, other sections might be more complicated and detailed. The System Dynamics model is mainly based on the concepts described in the Problem structuring section, and incorporates ideas and variables from the CLD. Before presenting the SDM the model primitives, general structure and modelling approach will be presented. After which the SDM is presented with the primary focus of explaining each primitives quantification method and the modelling structure.

Defining variable types used in the simulation model In order to create a system dynamics model one have to determine the variable types and the different modelling mechanisms utilized. The primitives used in this SDM are stocks, flows, variables, links and converters. A brief explanation is given based on Maani and Cavanas book on Systems Thinking and System Dynamics [2].
Stock: Stocks are accumulated quantities or smoothed statistical data. Stocks describe the condition of the system and would continue to exist even if the flows stopped. Examples of accumulated quantities are e.g. cash or population. Smoothed statistical data could illustrate an average between in-flow and outflow, such as average sales or birthrate. The main purpose of choosing stocks are their ability to describe the state of the system related to the problem modelled and investigated but they can be used in circumstances where something is generated over time.
Flow: A Flow moves material between stocks. For instance, in the case of a bank account you could have an inflow of deposits and an outflow of withdrawals.
Variables: Variables are dynamically calculated values or constants. In the bank account model you could have a variable representing the interest rate. It could be a fixed value or be governed by an equation that changes over time.
Links: Links illustrate transfer of information between variables, stocks, flows, and all other system primitives used. If two primitives are linked, they are related and the value a given primitive has is accessible to the primitive it is linked to.
Converters: Converters are used in this simulation model. Converters are primitives which takes an input and gives an output. The input and output is governed by a user-created table/graph of X's and Y's, connecting a given X value to a given Y value depending on the graph/table.
Influences: Influences are represented as smaller yellow circles. These have an initial value, and is not changed over time, but their initial value can be changed before a simulation run.

How the simulation will work in this system dynamic model The variables used in the causal loop diagram are generally difficult to quantify with a specific value representing them, there are also difficulties when one need to quantify how they relate to one another. As it has been done in previous works the main philosophy behind quantification of all primitives are percentages and rates. Therefore

Table 4.1: Variable and influence scheme showing examples of connecting low, medium and high positive and negative influence to variable rates.

Influences	Change and correlation factor
High positive influence	1.8
Medium positive influence	1.5
Low positive influence	1.2
High negative influence	0.2
Medium negative influence	0.5
Low negative influence	0.8

the model only work with rates, and thus percentage increase or decrease, depending on desired simulation behavior. Stocks are in some cases represented as percentages of what one ultimately want or need, in other words, degrees of a concept related to a maximum goal of 100%. Stocks will always represent the current state of the system. However, keep in mind that not all stocks are part of a goal seeking loop with a maximum of 100%, but rather represent the current state of e.g. investment, motivation or pressure, where 100% is the current state, and increasing it would result in the stock increasing to above its current level.

Variables are linked to other variables, before ultimately influencing the in-flow or out-flows of stocks. Variables are as stated quantified through rates, examples of using rates are given in table 4.1 where we can connect qualitative values to a quantitative increase in flow.

Imagine, for example, that a stock's current value is set to 80, and that the value (flow) added to the stock on each iteration is 10. On an iteration without any variable influence the in-flow is 10*1. However, if the flow was affected by a variable influence of say 20%, it would be 10*1.2=12 instead of 10.

In addition to having the initial variable value influence other connected primitives, one can further weight its influence. Or, the variable could possibly influence one primitive positively while negatively influencing another. This can be done by manipulating an e.g. 1.2 variable rate to influence a connected variable by 50% (1.1), or by positively influencing one variable by 1.2 while negatively influencing another by 0.8. Stocks always have an initial value representing the state of the stock at the beginning of the simulation. Variables, on the other hand, can be created during simulation, change over the course of the simulation, or have an initial value at the beginning of a simulation. They are not restricted to being changed as a result of flows.

4.3.1 Developing a system dynamics simulation model

The modelling software used in this thesis is "Insightmaker", which offers free modelling and simulation within the browser. As mentioned the presentation of

the SDM is divided in smaller structural parts, which means that primitives related to simulation parts not yet presented are set to have no influence on the system. Or else, the values presented would not make sense to the reader as they are caused by variables yet to be presented. However, after all parts are presented they will be connected to each other and the simulation results will represent all system interactions. Naturally, to facilitate simulation some of the variables identified and used in relation to the causal loop model are altered, and the model has some structural differences. The simulation model is used to illustrate expected behaviors related to the problem structuring phase, CLD modelling, and CLD analysis.

Meeting increased service need by digitalization

The first part of the system dynamics model simulates the sector working towards their capacity goals. It illustrates the current degree of capacity in the healthcare sector, the target and gap, whereas the gap is filled by digitalization/increased capacity. Additionally, it incorporates a continuous erosion of capacity due to increased needs as a result of societal development.

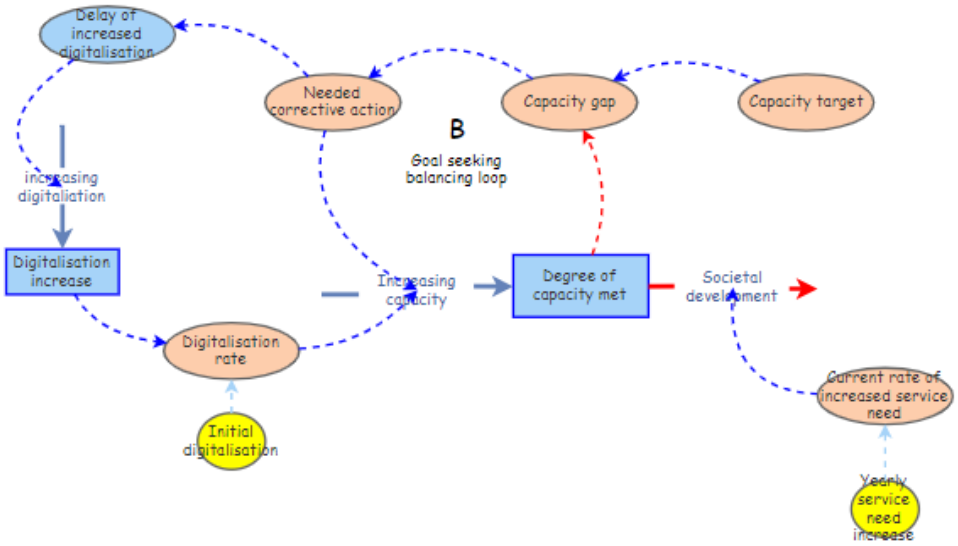

Figure 4.2: The simulation structure of the sector digitalizing to meet service capacity goals

Presenting the primitives and flows: The model is primarily a goal-seeking balancing loop, which comes from the current *degree of capacity met*, the *Capacity target* and *Capacity gap*. The gap determines, among other factors, the yearly increase in capacity as a result of the in-flow *Increasing capacity* which adds to the stock at each iteration.

Yearly *Increasing capacity* is determined by *Capacity gap* and the *Rate of digitalization*. The initial value of the *Digitalization rate* is determined by *Initial Digitalization* as it is documented that the healthcare system today uses digitalization as tool to increase service capacity. Over time the healthcare system will slowly increase the *Digitalization rate* in pulses every two years, based on the capacity gap at that point in time. Illustrating how the identified missing capacity results in further digitalization as a result of national pressure. The *Digitalization rate* influences the in-flow by determining the % amount of the gap being filled, as the in-flow is linked to both the *digitalization rate* and the *Capacity gap*/*Needed corrective action*. As time moves on the *Digitalization rate* increases due to the identified gap, which means more digitalization, and consequently a bigger part of the gap is filled due to the current *Digitalization rate*. However, as this is a goal seeking loop, the *Degree of capacity met* gets closer to its goal of 100% as the simulation continues. When digitalization increases the gap decreases. This relation keeps the in-flow of *increased capacity* at a relatively stable level. The reasoning behind this is simply that as the capacity gap begins to close, the effectiveness of digitalization in terms of *Increasing capacity* decrease, even though the current *Digitalization rate* stays the same.

The outflow is rooted in the fact that societal development will continuously demand more capacity, as discussed throughout the thesis. Thus, *Societal development* reduces the degree of met capacity by a given percentage each year.

Quantifying the primitives towards a system baseline: The most important initial variable values set are *Initial Digitalization*, the *Degree of capacity met*, and the *Yearly service need increase*. Initial digitalization is set to be 25%. This is due to the fact that the sector currently focuses on digitalization heavily as means to increase capacity and meet future demand. The yearly increase in capacity need is set to 7%, with initial digitalization, and then the digitalization rate set to 25% and therefore closes the gap by 25% yearly. With digitalization at this level we can see from table 4.2 see that the current degree of capacity met increases only slightly, as we increase capacity by 7.5 and decrease it by 7, as a result of social development. However, increases in digitalization will make the simulation move towards its goal over time. The initial level of capability is set to 70% of current demand, as the sector is believed to not fully cover societal needs at the current point in time. As a result of societal development, we can see that demand for healthcare would increase by approximately 50% in ten years. The current level suggests that there is a big need to provide more effective services, which is currently being done through digitalization. Table 4.2 shows how the values develop over time the first ten years.

Simulation behavior: The two graphs presented (4.3 and 4.4) show behavior over 15 years. The total level of capacity shows a goal seeking behavior moving

Time ↑	Degree of capacity met	Increasing capacity	Societal development	increasing digitaliation	Digitalisation increase	Digitalisation rate	Capacity gap
0	70	7.5	7	0	1	0.25	30
1	70.5	7.375	7	0	1	0.25	29.5
2	70.875	7.28125	7	0.29125	1	0.25	29.125
3	71.15625	9.311123047	7	0	1.29125	0.3228125	28.84375
4	73.467373047	8.565063638	7	0.26532627	1.29125	0.3228125	26.532626953
5	75.032436685	9.715979141	7	0	1.55657627	0.389144067	24.967563315

Table 4.2: The first 5 years of simulation. Shows value of primitives over time, as a result of initial variable quantification.

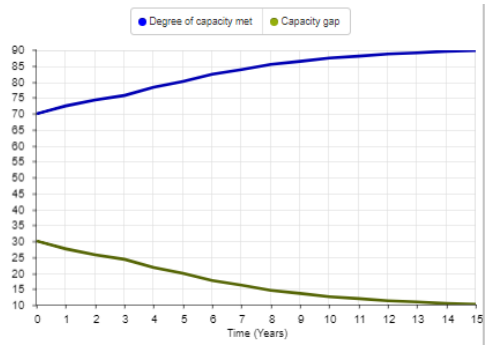

Figure 4.3: Showing *Degree of capacity met* following a goal seeking behavior over time.

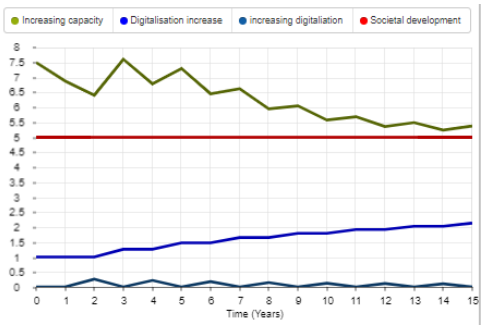

Figure 4.4: Showing *Increased Capacity* over time, total *digitalization increase*, *Social development* and the "Pulsing" behavior of *Increasing digitalization*.

towards 100% met capacity. More importantly, 4.4 shows how yearly increase are higher than yearly erosion, which fills the gap over time. As the gap is filled, it results in a higher level of digitalization overall due to national level stakeholders increasing the current level of digitalization.

We can see by looking at the simulation after the first 15 years that the sector becomes more efficient due to the increase in digitalization. As the gap is larger in the beginning, the increase in capacity is higher, over time it balances at the level of which the society develop. Every second year the sector increase their level of digitalization which ultimately makes the simulation get closer to its goal. The total level of increased digitalization over time is shown by the variable *Digitalization increase* and tells something about how much the system must be digitalized before the sector meets their capacity goals.

Digitalization increase system complexity

The sectors continuous efforts to digitalize and increase capacity have an effect on system complexity, a concept and relationship thoroughly investigated in previous sections. The increased system complexity is a natural result of amount of increased capacity, which as discussed is influenced by the digitalisation rate and the capacity gap. Yearly *System complexity increase* to is connected to the stock

out-flows (erosion) of both the *Degree of social capabilities* and *Degree of law and regulatory compliance*.

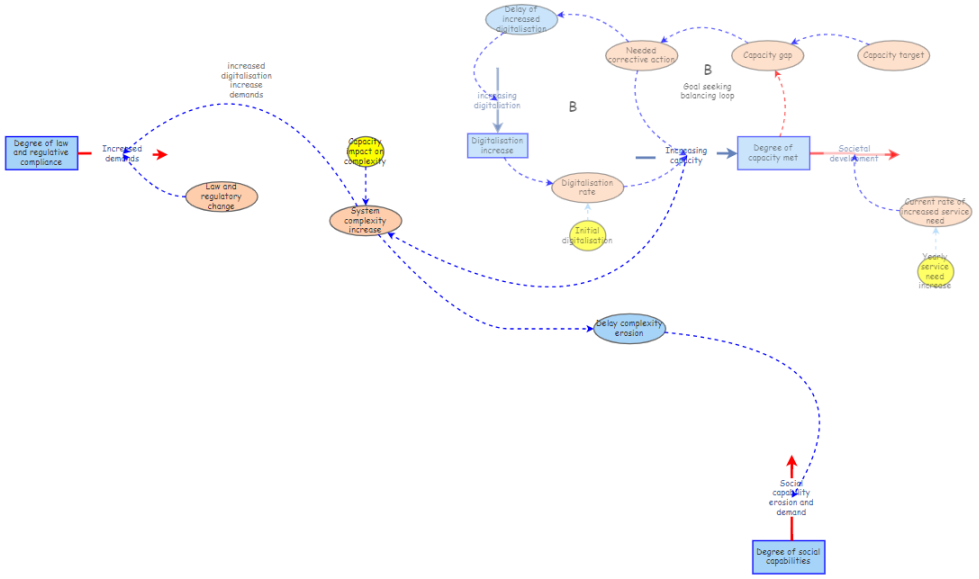

Figure 4.5: Showing the initial simulation structure influencing system complexity and erosion of cybersecurity capabilities.

Presenting the primitives and flows: This transitional part of the simulation attempts to quantify the results of the initial simulation of "Meeting increased service need by digitalization" to increased system complexity and eroding cybersecurity capabilities. The stocks *Degree of social capabilities* and *Degree of law and regulatory compliance* follow the same logic as the stock *Degree of capacity met*. Where an initial value is set, between 1 and 100 with 100 being a very good level of capabilities. The simulation and in-flows of these stocks are to be explained at a later stage, this section focus merely on their out-flow, as a result of digitalization and increased system complexity.

The increased system complexity is given by the yearly *increasing capacity*. We already established that the flow in question represents the level of *Initial digitalization* and *Digitalization increase*, which is limited by the actual *Needed Corrective action*. Thus, this variable is fitting to give a general sense of how much system complexity increases at each time iteration. Naturally we could apply the techniques used to change and weight variable influences given in 4.3 to increase or decrease *increasing capacity's* relation to *System complexity increase*.

Quantifying the primitives towards a system baseline: Quantification of the variables discussed in this section are only determined by weighting yearly *system*

complexity increase, as a result of *Increasing capacity*, which determines the yearly percentage increase in the out-flow (erosion) related to the stocks of *Degree of law and regulatory compliance* and *Degree of capacity met*.

As digitalization increase overall demands to be compliant, through i.e. performing risk assessments related to new technology, or following the law and regulatory demands related to privacy it will continuously demand work equal to the *System complexity*. Additionally, over time one can expect national level stakeholders to introduce new laws and demands following the technological development. Thus, in addition to the system complexity increase, the erosion of law and regulative compliance is added to every fifth year, where the demands increase by 50%, with the first pulse starting after three years.

The same principle apply to erosion of social capability. Continuous increase in complexity cause a decline in the current level of social capabilities, due to yearly erosion. For structural reasons there is a delay of one year for the erosion, as development of social capabilities first occur after one time-iteration in the model, which is seen as a reaction to previous actions. Increasing complexity effects the social capabilities in a plethora of ways as it is portrayed in this thesis. Thus, the effect that *System complexity increase* has on the erosion is weighted by a factor of 1.2. Table 4.3 show how the values develop over the first ten years.

Time	System complexity increase	Social capability erosion and...	Increased demands
0	7.5	0	7.5
1	7.375	9	7.375
2	7.28125	8.85	7.28125
3	9.311123047	8.7375	13.96668457
4	8.565063638	11.173347656	8.565063638
5	9.715979141	10.278076366	9.715979141
6	8.659071971	11.659174969	8.659071971
7	9.158994003	10.390886365	9.158994003
8	8.198731703	10.990792803	12.298097555
9	8.45981255	9.838478044	8.45981255
10	7.743253599	10.15177506	7.743253599

Table 4.3: The first 10 years of simulation. Shows value of primitives over time, as a result of initial quantification of system complexity, and the erosion of social capabilities and erosion of law and regulatory compliance.

Simulation behavior: The graph presented (4.6) show behavior over 15 years. Aside from the additions and changes discussed the erosion mainly follow the *Increasing capacity*, and thus has a similar development as 4.4.

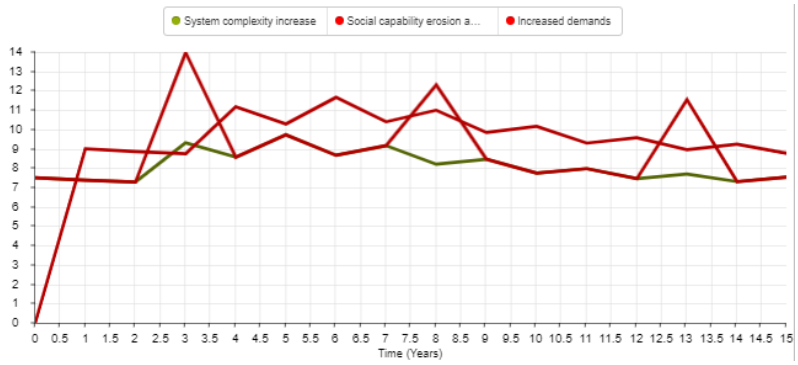

Figure 4.6: The first 15 years of simulation. Shows value of primitives over time, as a result of initial quantification of variables. Red line of highest value is *Social capability erosion and demand* , the red line with "pulses" is the *Increased demands*, the green line is partly hidden behind *Increased demands* and represent *system complexity increase*.

Degree of regulatory compliance, development, maintenance and erosion

This section of the simulation aims to model how the *Compliance gap* is filled due to an increase in *Operational level incentive to follow law and regulation*. Over time the gap is filled due to a pulsing *Delayed pressure to follow law and regulation* impacting operational incentive.

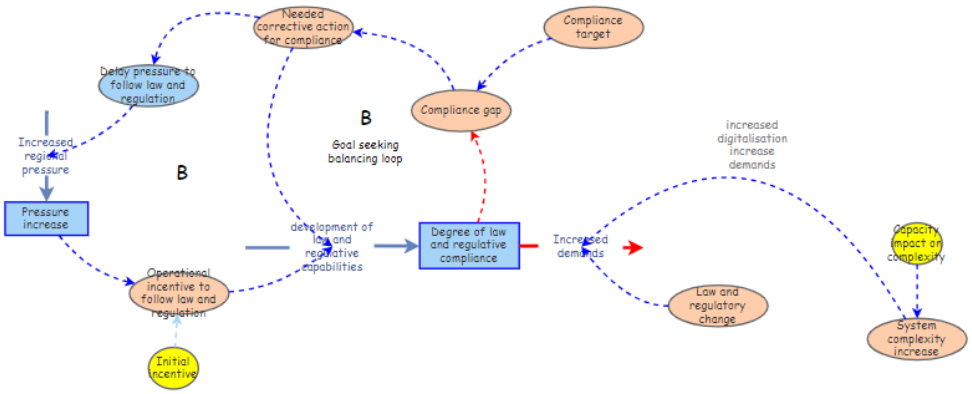

Figure 4.7: The simulation structure of the sectors degree of regulatory compliance.

Presenting the primitives and flows: There are similarities between the simulation structure given in relation to the *Degree of capacity met* (4.2) and the model determining the *Degree of law and regulative compliance* (4.7) in that both struc-

tures are goal seeking, and that the corrective action is subject to pulsing delays. The *development of law and regulatory capabilities* are limited by the *Operational levels incentive to follow law and regulation*, initially set by a given amount of *Initial incentive*. Incentive is a variable determining the development of capabilities and is relative to the current gap. Naturally, the stocks out-flow *Increased demands* is the same as previously discussed.

Quantifying the primitives towards a system baseline: There are mainly three primitives relevant for the simulation of the *Degree of law and regulative compliance*, the starting value of the stock, the pulse frequency of *delayed pressure to follow law and regulation* and the *Initial Incentive*. The current level of regulatory and legal compliance is documented to be quite good, as a result the *Degree of law and regulatory compliance* is initially set to 80%. The operational level management are motivated to follow law and regulation, its importance is thoroughly rooted and there are measures such as "Normen" created to make following law and regulation easier. Initial incentive is set to 70%. The actual *Operational Incentive to follow law and regulation* are increased every two years. The table (4.4) show the primitives, where in addition to these variables can observe the effect of increasing demands.

Time	Degree of law and regulative...	Compliance gap	Increased regional pressure	Operational incentive to follo...	development of law and reg...	Increased demands
0	80	20	0	0.7	14	7.5
1	86.5	13.5	0	0.7	9.45	7.375
2	88.575	11.425	0.11425	0.7	7.9975	7.28125
3	89.29125	10.70875	0	0.779975	8.352557281	13.96668457
4	83.677122711	16.322877289	0.163228773	0.779975	12.731436214	8.565063638
5	87.643495286	12.156504714	0	0.894235141	10.870773707	9.715979141
6	88.998289852	11.001710148	0.110017101	0.894235141	9.838115825	8.659071971
7	90.177333707	9.822666293	0	0.971247112	9.54023627	9.158994003
8	90.558575974	9.441424026	0.09441424	0.971247112	9.169955819	12.298097555
9	87.430434238	12.569565762	0	1.03733708	13.038876647	8.45981255

Table 4.4: The first 9 years of simulation. Shows value of primitives nine years of simulation related to development and erosion of law and regulative compliance.

Simulation behavior: The two graphs presented (4.8 and 4.9) show behavior over 15 years. The total level of law and regulatory compliance show goal seeking behavior moving towards 100% compliance. More importantly, 4.9 show how yearly increase are higher than yearly erosion, which fills the gap over time. As the gap is filled the result is an overall higher level of law and regulatory compliance, as a result of high levels of incentive to fill the gap.

In both graphs the effect of pulsing *Law and regulatory change* can be seen because it increases out-flow and thus the *Compliance gap* follows, and ultimately the in-flow increase as a result. Changes in system complexity would influence the behavior of the model as yearly erosion increases.

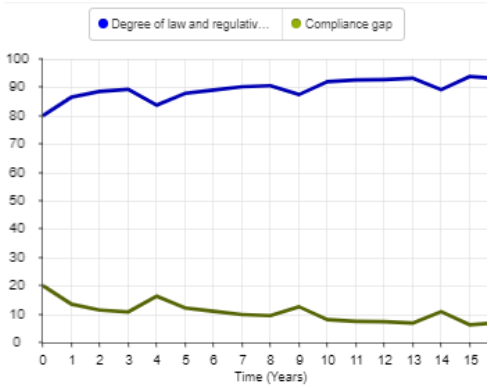

Figure 4.8: Showing *Degree of law and regulatory compliance*. Illustrating its goal seeking nature.

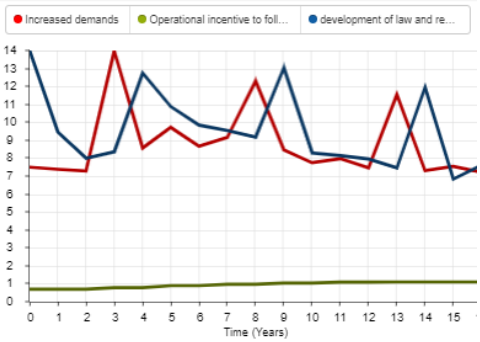

Figure 4.9: Showing out-flow *Increased demands*, in-flow *development of law and regulative capabilities* and *Operational incentive to follow law and regulation*.

Available resources as a result of costs associated with development and maintenance of capabilities aimed at the law and regulatory compliance

The result of the sector being overly focused on law and regulation is a depletion of operational level resources, as the total amount of available resources are used for development and maintenance of law and regulatory capabilities. Not only are the total amount of resources used to comply with regulation, but it is used for social capability development as well. The overall structure is shown in figure 4.10.

Presenting the primitives and flows: The simulation illustrating the resource usage mainly revolves around the stock *Available resources* which follows an alternative structure to the stocks that have been presented thus far. *Available resources* is initially set to 100%, which represents the total resources available at the beginning of the simulation. The *Cost of compliance* and *Cost of development* is given through a percentage of the available resources. *Investment* determines the *Yearly investment*, which is initially set to add to the stock by 100%, as this is the current level of investment. *Resources available for social development* is defined as the available resources after the *Cost of compliance* and *Cost of development* is subtracted from the *Available resources*. This simulation structures makes it so that the available resources is first used for law and regulatory compliance and the resources left are used for capability development outside of what is mandated though law.

Quantifying the primitives towards a system baseline: The variables in need of weighting and quantification are the actual *Cost of compliance* and *Cost of development*. Development costs are naturally related to actual *development of law*

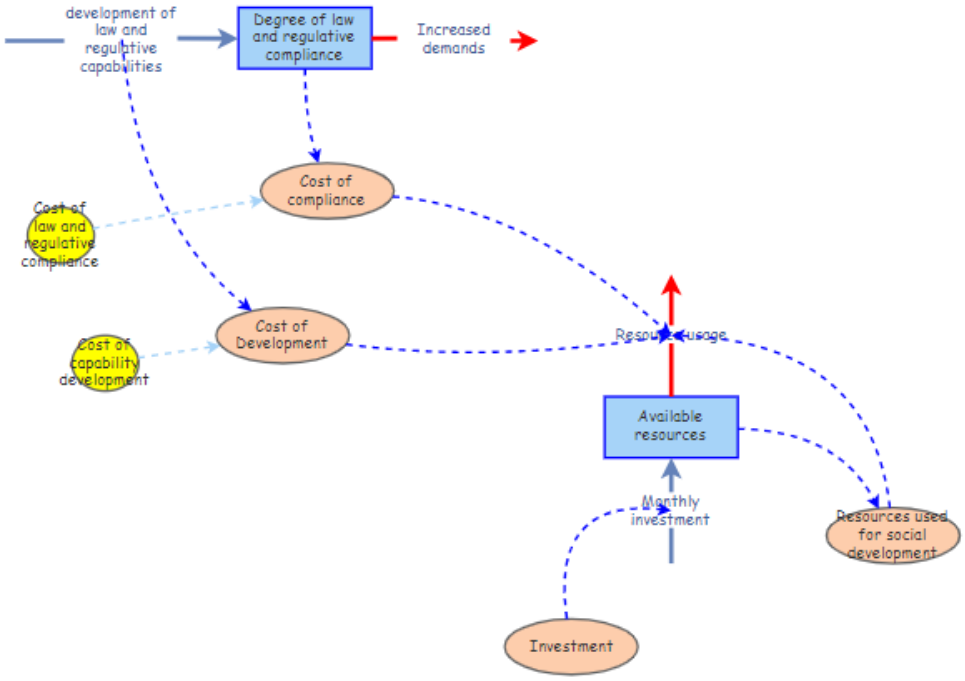

Figure 4.10: Illustrates the simulation structure considering resource availability and depletion.

and regulative capabilities, and maintenance is related to the *Degree of law and regulatory compliance*. Both costs are based on the same type of variable: a percentage representing law and regulative compliance. It is fair to assume that development of new capabilities come as a response to yearly increase in erosion, and that developing capabilities to meet new regulative demands are more costly than maintaining current compliance. For this reason, the development costs are increased by 25% and maintenance is decreased by 20%. This means that the cost of compliance is 80% of the current degree of law and regulatory compliance, and development costs are 125% of the yearly development of law and regulatory capabilities. Resource usage is illustrated in table 4.5.

Simulation behavior: It is assumed that the national and regional focus on law and regulatory compliance results in operational level stakeholders having sufficient resources to perform the activities needed to keep the level of compliance high. Given their high motivation to fill the gap due to increased pressure and operational level incentive, the *Cost of development* and *Cost of maintenance* increases as the sector increase their level of compliance through development. However, we observe that cost of development is high in the beginning of the simulation, as the gap is high, but is reduced once the gap gets smaller. Both costs add to the out-flow from *Available resources*. The remaining stock is invested in the development of social capabilities, which in the end, also adds to the out-flow of total

Time	Available resources	Cost of Development	Cost of compliance	Resources available ...	Yearly investment	Development of soci...	Degree of law and re...
0	0	17.5	64	0	100	0	80
1	18.5	11.8125	69.2	18.5	100	7.4	86.5
2	18.9875	9.996875	70.86	18.9875	100	7.57974924	88.575
3	19.143125	10.440696602	71.433	19.143125	100	7.602361194	89.29125
4	18.126303398	15.914295267	66.941698169	18.126303398	100	7.150463067	83.677122711
5	17.144006564	13.588467134	70.274796229	17.144006564	100	6.89038933	87.843495286
6	16.136736637	12.297644782	71.198631882	16.136736637	100	6.591544192	88.998289852
7	16.503723336	11.925295338	72.141866965	16.503723336	100	6.956353653	90.177333707
8	15.932837697	11.462444774	72.446860779	15.932837697	100	6.823115055	90.558575974
9	16.090694447	16.298595809	69.944347391	16.090694447	100	7.039564386	87.430434238

Table 4.5: The first 9 years of simulation. Shows value of primitives determining the resources used, and the available resources which can be used to improve cybersecurity outside of law and regulatory compliance

resources, effectively making available resources 0, before a new yearly investment is provided.

The amount of available resources relies heavily on how one calculate the total cost of increasing, and maintaining law and regulatory compliance. The remaining resources balance out at the same pace and level as the overall *Degree of law and regulative compliance*, as both *Development of law and regulative capabilities* and *Degree of law and regulatory compliance* settle at a level relative to the *Increased demands*. Changing variables are done when demonstrating and validating the proposed model.

Degree of social capabilities limited by resource availability, capability to improve, awareness, and external influences

Simulating the *Degree of social capabilities* is slightly more complicated than the system structures presented thus far. In itself it is a goal seeking loop, however the systems efforts to fill the gaps are limited by *Resources available for social development*, their current *Capability to improve* and the out-flow is affected by *Awareness of employees* as well as digitalization and system complexity.

Presenting the primitives and flows: The stock of *Degree of social capabilities* follow the same logic as *Degree of capacity met* and *Degree of law and regulative compliance*, where it illustrates the current state of the system. *Development of social capabilities* determine the in-flow, directly related with *Operational level social capability development*. For now, three factors determine development: *Resources available for social development*, *Capability to improve* and the *Identified effort needed*. The "converter" *Capability to improve* outputs a factor which can increase or decrease *Development of social capabilities* based on the gap, rooted in the fact that the operational level knowledge and expertise can influence capability development.
The out-flow is connected to the *System complexity increase*, a variable discussed previously. Additionally, it is subject to change as a result of employee awareness.

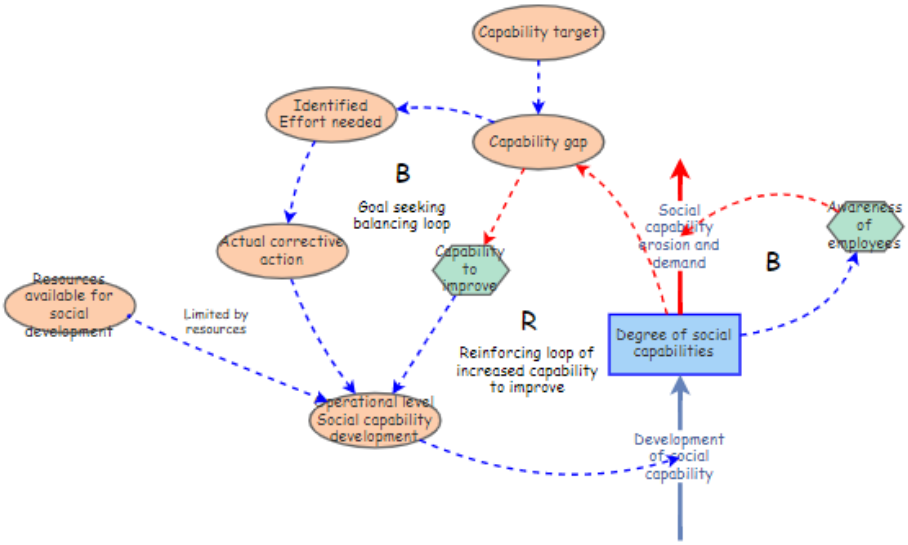

Figure 4.11: The simulation structure created to simulate *Degree of social capabilities*, consisting of a stock, flows, two converters, several variables and links.

Employee awareness is based on the capability gap because if the *Capability gap* is low the employee awareness would be high. Higher awareness results in more security aware behaviors, thus reducing the actual negative erosion *Increased complexity* has on overall *Degree of social capabilities*.

Quantifying the primitives towards a system baseline: This simulation structure contains converters, which changes a particular input to an output, in our case both converters have different inputs and outputs. The converter *Capability to improve* is expressed through affecting the operational levels ability to utilize the available resources effectively. Currently, their lack of knowledge and expertise is perceived as a fairly large limitation to development. The converter is set to result in values between 1.5, and 0.5, where the positive rate is a result of a low gap and 0.5 a high gap. First, when the gap is reduced to 25%, the resources are utilized to a 1:1 ratio, at 0 its used more effectively 1.5. The ratios for gaps higher than 25 result in negative resource effectiveness (See figure (4.12).

Awareness of employees reduces the effect of erosion as a result of the *Degree of social capabilities*. The current level of awareness has the capability to enhance the negative effects of digitalization, as well as reduce them. If the current level of awareness goes below 50% the effect of system complexity would increase. If overall *Degree of cybersecurity social capabilities* is higher than 50%, the effect of system complexity can be reduced. Quantification is as seen values between 1.2

Input Value	Output Value
0	1.5
25	1
50	0.8
75	0.65
100	0.5

Figure 4.12: Showing the converter results of input value from *Capability gap* and output values transferred to *Operational level social capability development*.

Input Value	Output Value
0	1.2
25	1.1
50	1
75	0.85
100	0.7

Figure 4.13: Showing the converter results of input value from *Degree of social capabilities* and output values influencing the outflow of the stock based on employee awareness.

and 0.7 where the positive effects of awareness is thought to potentially be bigger than the negative effects (See figure (4.13)), while not being as influential as the overall effect of *Capability to improve* is on capability development.

Outside of the two converters, the initial stock value of *Degree of social capabilities* must be determined. Initially it is set to 50, as the sector is lacking quite heavily in their overall degree of social capabilities as brought forward throughout this thesis. Last, the actual calculation of *Operational level social capability development*. It is a simple mathematical formulae, multiplying the *Actual corrective action* (stemming from the gap), with the limiting rate *Resources available for social capability development* and the rate given through the converter *Capability to improve*. It determines, as the other in-flows similarly structured, development as a percentage of the identified gap.

Time	Degree of social capabili...	Capability to improve	Operational level Social capabi...	Resources available for soci...	Social capability erosion and ...	Awareness of employees	Capability gap
0	50	0.8	0	0	0	1	50
1	50	0.8	7.4	18.5	9	1	50
2	48.4	0.7904	7.74398352	18.9875	8.90664	1.0064	51.6
3	47.23734352	0.783424061	7.912913061	19.143125	8.834054844	1.011050626	52.76265648
4	46.316201737	0.77789721	7.569630746	18.126303398	11.337989091	1.014735193	53.683798263
5	42.547843392	0.75528706	7.439276563	17.144006564	10.584451705	1.029808626	57.452156608
6	39.40266825	0.736416009	7.20099375	16.136736637	12.153399549	1.042389327	60.59733175
7	34.45026245	0.706701575	7.645201756	16.503723336	11.037188589	1.06219895	65.54973755
8	31.058275617	0.686349654	7.53912064	15.932837697	11.823531075	1.075766898	68.941724383
9	26.773865182	0.660643191	7.784090241	16.090694447	10.752517314	1.092904539	73.226134818
10	23.805438109	0.642832629	8.738254641	13.7570568	11.215460261	1.104778248	76.194561891

Table 4.6: The first 10 years of simulation. Shows value of primitives used to simulate *Degree of social capabilities over time*

Simulation behavior: The two graphs presented, (4.14 and 4.15), show behavior over approximately 15 years. Even though *Degree of social capability* is in itself a goal seeking loop, its ability to fill the gap is limited by various variables. Most notably resource availability, current awareness and knowledge and expertise. Erosion is as we can observe generally higher than development resulting in a continuous decrease in the stock. This behavior reflects the difficulties opera-

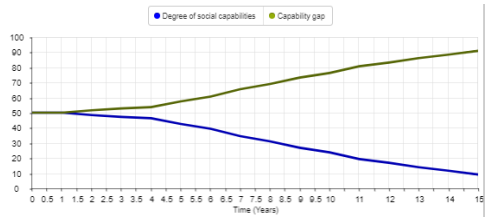

Figure 4.14: Showing *Degree of social capabilities* and the *Capability gap* over time.

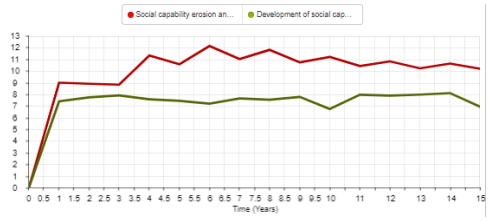

Figure 4.15: Showing out-flow and in-flow. Illustrating how development is lower than erosion, reducing overall capabilities

tional level employees express due to digitalization, system complexity and focus on regulation and law as well as lacking knowledge and awareness.

Total level of cybersecurity and following system vulnerability, small incidents and big attacks

We continue to add to the model in line with both the problem structuring section and the causal loop diagram. The coming sections will add relationships which influence the previously given variables, thus changing the simulation results. The coming system dynamics relationships will be presented in a slightly simplified way and is caused by the system structures presented thus far.

Total level of cybersecurity and system vulnerability: Following the logic from our causal loop diagram the *Degree of law and regulative compliance* and *Degree of social capabilities* together make up for the *Total level of cybersecurity*, which is as we know related to incidents and possible attacks. *Total level of cybersecurity* is divided by 2, in order for its value to be within the range of 0-100. When presenting the structure *Degree of law and regulative compliance* and *Degree of social capabilities* are ghosted, a functionality within "insightmaker" which creates an exact copy, done to ease model readability. This explains their position in the model structure, and the fact that they are duplicated in the coming figures. *System insecurity* is determined by the gap between *Total level of cybersecurity* and 100, representing missing cybersecurity capabilities (4.16). System insecurity grows as social capabilities decrease, because the decrease is higher compared to the increase in degree of law and regulatory compliance.

Incidents and attacks affecting perceived risk and motivation to change: System insecurity, a term based the concept of system (in)security from socio-technical systems theory, results in *small incidents* and *large incidents*. Incidents and attacks are a natural consequence of system vulnerability, the simulation represent this simple, as some variables included in the CLD are not added. The amount of *System insecurity* determine the amount of *Small incidents* and *Large incidents*. The

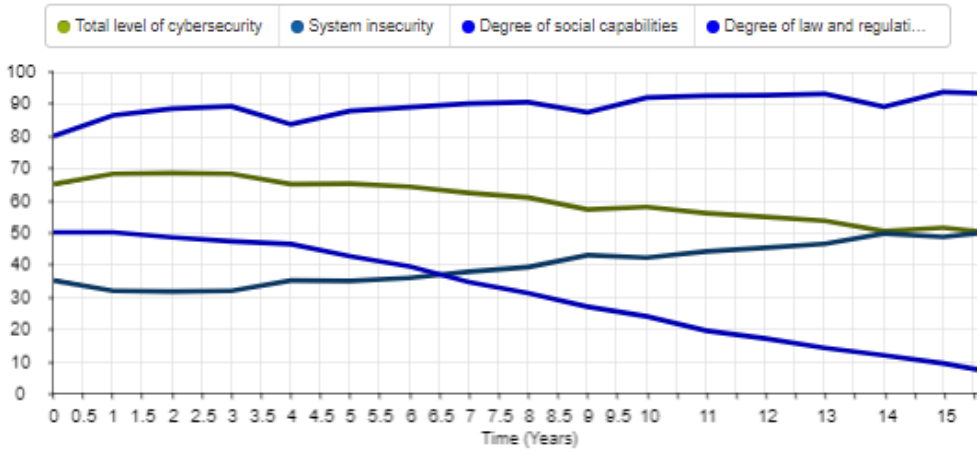

Figure 4.16: Graphical result of the primitives *Degree of law and regulative compliance*, *Degree of social capabilities*, *Total level of cybersecurity* and *System insecurity*. Two stocks are dark blue, the one with the pulsing behavior and higher levels are *Degree of law and regulative compliance*.

two latter variables are directly used as ratios because of their effect on *Perceived risk increase* and *motivation to change behavior*. Both small and larger incidents result in increased motivation to change behaviors, whereas only large incidents increase the perceived risk.

The effect of increasing perceived risk: *Perceived risk* increases as a result of large incidents. Large incidents, incerasing perceived risk in the system, do not happen very often, but when they do it can have positive consequences for different aspects of cybersecurity. Currently, attacks are set to happen in pulses. *Large incidents* are set to occur every four years, beginning in two years. The attacks actual effect on *Perceived risk increase* is based on the total level of *System insecurity*, 30% system insecurity results in the *Large incident effect* to be 1.30. Done under the assumption that system insecurity effects the consequence and size of an attack, thus its effect on perceived risk. *Perceived risk increase*, as a result of larger attacks and incidents, have three effects, it increases operational level *Motivation to improve*, it increases overall employee awareness thus reducing the erosion of social capabilities (similarly to *Awareness of employees* converter effect), lastly it creates higher pressure on the regional level to invest in information security (Figure 4.17).

Quantifying the effect of *Perceived risk increase* Table 4.7 show primitives affected by the *Perceived risk increase*, as well as what causes the *Perceived risk increase* to begin with. Its effect on *Social capability erosion* is not easily spotted due to other influences also effecting the out-flow. Further, the erosion is reduced by half of the current increase in perceived risk meaning that an increase in per-

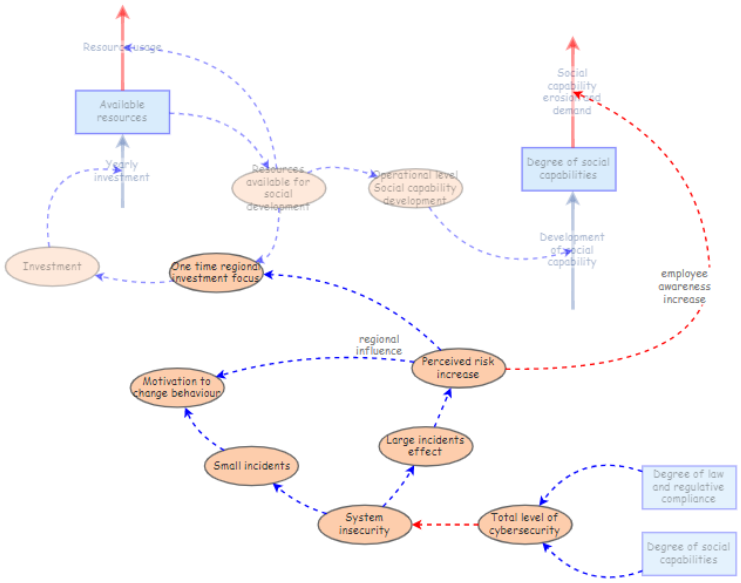

Figure 4.17: Introduces the newly introduced primitive, and put them in context of the rest of the model.

ceived risk of 30% will result in a 15% reduction of eroded capabilities that year. *One time regional investment focus* show that increased risk may cause an increase in resources. The actual increase in resources is based on the perceived risk % increase, and the *Resources available for social development* from last year, where *one time regional investment* increase by the percentage given by the *perceived risk increase*. The result of this is increased overall resources and increased *Operational level Social capability development*. The effect of *Perceived risk increased* are hypothesised to have a larger impact on the employees and people responsible for cybersecurity, as implemented through it effecting regional investment more compared awareness and decreased erosion.

Time	Large incidents effect	Perceived risk increase	System insecurity	Social capability erosio...	Resources available for...	One time regional inves...
0	0	1	35	0	0	0
1	0	1	31.75	9	18.5	0
2	1.31850125	1.31850125	31.850125	8.93054385	18.9875	6.047542484
3	0	1	32.382559479	8.879270095	25.190667484	0
4	0	1	34.603875047	11.302282403	18.126303398	0
5	0	1	34.587343639	10.566610031	17.144006564	0
6	1.35739598	1.35739598	35.739597981	12.147810331	16.136736637	5.767204801
7	0	1	37.760698967	11.043381312	22.270928138	0

Table 4.7: Showing values affected by *Perceived risk increase* over the first 7 years, accounting for two attack pulses

.

Motivation to change behavior and its effect on identified effort needed As it comes forth when presenting the problem we cannot see that the operational

level have any significant problems with identifying its weaknesses in terms of social capabilities, as they are thoroughly presented in sector reports. Thus the level of motivation is relatively high to begin the simulation. *Smaller incidents* mainly result in effects associated with acknowledging the current capability gap.

Presenting the primitives and flows To illustrate and model the connection between *system insecurity*, *small incidents*, overall motivation and the *identified efforts needed* one need to account for the total increase in *Motivation to change behaviors*. Thus, the *Motivation to change behavior* continuously flow into the stock *Motivation*. Motivation is capped at 100% which means that the operational level acknowledge the entirety of the *Capability gap*. Larger incidents also contribute to operational level motivation.

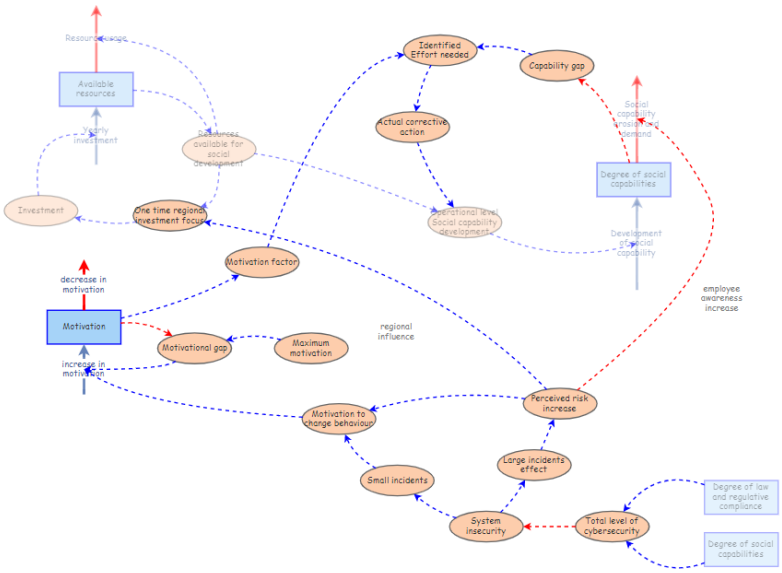

Figure 4.18: Adds overall motivation as a result of system insecurity and smaller incidents

Quantifying the primitives towards a system baseline: We have established that operational level motivation is high to begin with and affected by a continuous increase as a result of incidents. Therefore, the operational level motivation closes in on the gap relatively quickly, thus making the *Identified effort needed* close to the actual *Capability gap*. Table 4.8 show principle development over the first 8 years of the simulation.

Time	increase in motivation	Motivation	Identified Effort needed	Capability gap
0	0.875	90	45	50
1	0.724296875	90.875	45.4375	50
2	3.557591287	91.599296875	47.88376144	52.27525
3	0.392080893	95.156888162	51.438358554	54.056368959
4	0.385057297	95.548969055	50.530950751	52.884872805
5	0.35157807	95.934026351	54.699838286	57.018182564
6	1.777999248	96.285604421	58.231112754	60.477485813
7	0.182799197	98.063603669	64.426543811	65.69873164
8	0.166715213	98.246402866	65.446753446	66.614910609

Table 4.8: High level of motivation results in most of the gap being identified by the operational level.

Simulation behavior combining all relationships currently presented: Until this point several system constructs have been presented.

- National stakeholders striving towards the capacity goal through increased digitalization.
- Digitalization's effect on overall system complexity and erosion of operational cybersecurity capabilities.
- Overall effort to maintain and develop law and regulatory compliance and its effects on resource availability.
- Development and erosion of social capabilities, limited by available resources and affected by the current level of social capabilities.
- The sectors reactive pattern of behavior as a result of incidents and attacks, and the effect of system insecurity related to investment and increased operational level motivation.

At this point we can investigate how the main variables develop over time as a result of the currently presented inter/intra relationships among stakeholders. Each primitive have been given a baseline value where appropriate, and the interconnections between different variables are quantified. As hypothesised in the previous chapters the current system baseline makes it so the operational level is unable to increase cybersecurity capabilities to the desired levels. It also suggests that the drive to meet service demand, and the following increased system complexity results in declining in cybersecurity capabilities. We know that operational level focus on law and regulatory compliance, and that these capabilities do not account for all aspects of cybersecurity, thus resulting in a overall cybersecurity insecurity. Illustrated by figure 4.19 and 4.20.
To further investigate social cybersecurity capabilities figure (4.20) represent the development and erosion of capabilities. On average, one can see that erosion is higher than development. When seen in relation to investment and resources a clear increase in development can be observed as a result (4.21) of increased investments. However, the current amount of regional level investment and interference with operational level business is not sufficient to stabilize social capabilities at a acceptable level. Further, we have simulated and observed how the current level of social capabilities limiting growth and development.

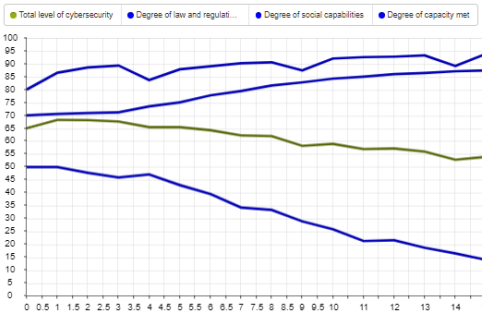

Figure 4.19: Holistic representation of main stocks and system insecurity

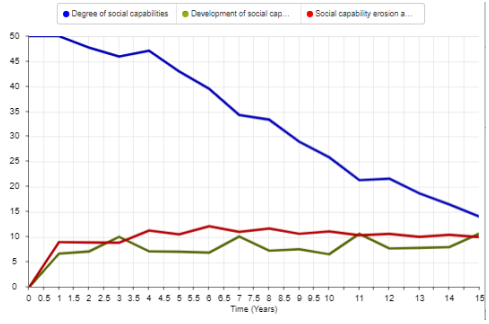

Figure 4.20: Degree of social capabilities and development/erosion of capabilities

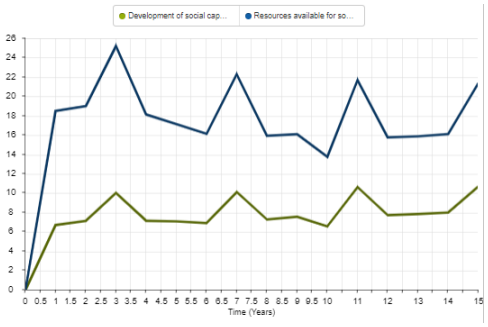

Figure 4.21: Interrelationship between resource availability and social capability development

High-level influences changes opportunity and influence capabilities

The last part of this system dynamics simulation model is opportunity and additional high-level influences, these are influences which can change overall behavior and change the trends currently present in the simulation. The causal loop diagram connected opportunity to resource availability, overall capability to improve, the role of both regional and professional levels, in addition to already established measures which can improve overall cybersecurity capabilities.

National strategies focusing on education National level strategies are brought forward as measures that can increase overall employee awareness through including cybersecurity in educational programs. This measure will counteract the effects of lacking awareness as well as provide the sector with more knowledge and expertise in terms of actual development. Assuming that the workforce consists of people between 25-65 of age, thus needing to replace 1 in 40 due to pensions each year. This suggest that 2.5% of the workforce is replaced each year. Given that these employees possessed the required degree of knowledge, expertise and awareness it could add up to a 2.5% out of 100. However, this proposition is not likely. The educational focus will first and foremost be to how one provide healthcare services. Adding cybersecurity to education is a long-term project and will take some time before showing results. Additionally, exhibiting desired behavior is a result of the environment as well as knowledge of cybersecurity. Regardless, the effect is added through 1% addition every year, after a 3 year delay, added directly to the stock *Degree of social capabilities*. Regardless of its presumed limitations it shows promise as over several years most of the older workforce are replaced with younger employees which can more easily understand technological solutions and the security related to this. Its effect can bee seen by comparing figure 4.23 with 4.19, where it is observed that the *Degree of social capabilities* stabilize at a higher level as a result of the educational measure.

Opportunity Increasing opportunity can, as discussed leading to the system dynamics model, have several effects on overall operational level cybersecurity. Opportunity is inherently linked to overall national level involvement, as well as the implementation of interventions enabling its subordinate organizations (i.e. professional and regional level) to improve. In previous sections, the possibility of changing both system structure and the roles and responsibilities of professional actors was discussed. It could result in more knowledge and expertise being applied in the decision-making process. Thus increasing *operational level social capability development*, since it is limited by currently possessed knowledge and expertise. Second, it could increase the influence, governing power, and capability of the regional level. This would result in a higher level of *Regional level influence*. For now, investments are mostly used to comply with legal mandates, as they are

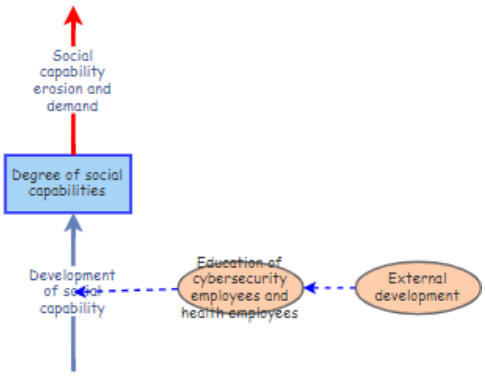

Figure 4.22: Simulation model including the effect of education

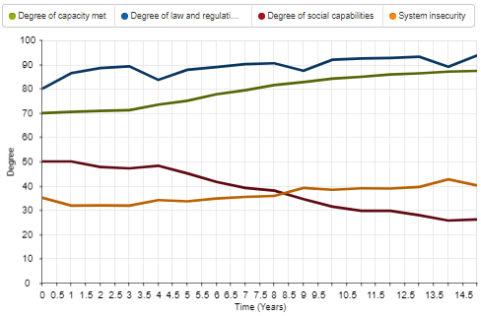

Figure 4.23: Education increases overall social capabilities

the primary form of national influence at the current point in time.

Opportunity is simulated through using a stock representing the current level, as stocks where used to represent *Available resources*. Opportunity is kept at the same level due to the current cultural understanding of the national level. If one were to decrease the decentralised management culture it would make the national-level influences bigger, thus positively influencing its connected variables. Without increasing operational level opportunity, the simulation will stay the same. Opportunity can be seen as a solution loop, as it can heavily influence the limiting factors of the system. Its effect will be examined at a later stage. The representation is slightly simplified, mostly because one can increase opportunity through other interventions rather than by changing the decentralized management structure (e.g. through changing law and regulation). Figure 4.24 show the simulation model as opportunity is added as a structural component to the model.

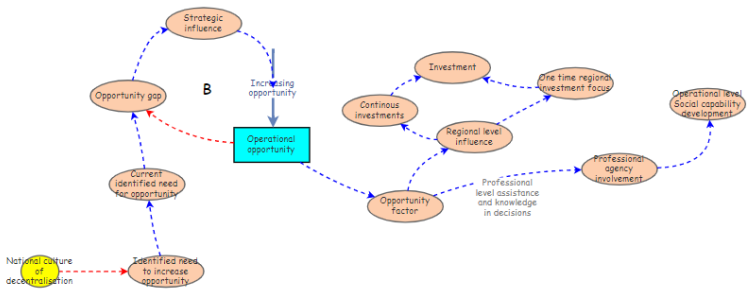

Figure 4.24: Structure showing how current level of opportunity is balanced by national culture, while it could increase the opportunity factor and its connected variables.

Quantification of opportunity: The stock *operational opportunity* results in an *opportunity factor*, which is positively related to *Regional level influence* and *Operational level social capability development*. Initially the *Opportunity factor* is set to being 1, as this is the perceived baseline value. By changing the *identified need to increase opportunity* one in turn increase the *Opportunity factor*. Quantifying the actual influence opportunity and national level culture of decentralisation, have on *Investment* and *operational level social capability development* is very difficult. The model has implemented the change in opportunity as a factor, reflecting the percentage increase in opportunity as a result of changing *National culture of decentralisation*. Increasing *Regional influence* will increase their *One time investments* which is initially rooted in the *Perceived risk increases*. Additionally, it adds yearly continuous investments. The variable *Regional influences* are multiplied by four, considering that reducing *National culture of decentralisation* by i.e. 20% initially only increase a relatively small investment every four years by 20% as well as only increasing the yearly budget by 1.2. each year. The effect is believed to be higher, resulting in increasing the variable. The effect of *Professional agency involvement* is calculated by multiplying the variable *Capability to improve* within the formula for calculating overall *Operational level social capability development*. The result of changing opportunity will as stated be examined in the demonstration and validation phase.

Reproducing reference mode behaviors through the base case

Every element of the simulation model has now been presented. We are left with a simulation model, incorporating many elements discussed leading up to the creating of both our causal loop model and system dynamics model. The variables and stocks are determined based on a hypothesised base case of values. The base case has been shown and demonstrated throughout the simulation models presentation. Figure (4.25) shows the structure of the presented simulation model with all its primitives present, and figure (4.26) illustrate the graphical simulation of the system in its reference mode of behavior (base case).

The holistic representation of the simulation model 4.25 shows that there are differences between the CLD and SD models. However, it does not differ in terms of relationships or general structure. Neither does it reflect concepts and interconnections differently that what was discussed in the problem identification phase. As the SD model is the main contribution, it is of higher quality and generally more detailed. It is also structured in a way that enables simulation, as opposed to the CLD model where simulation was not the main goal.

4.3.2 Demonstration and evaluation

This section consists of two main sections "Validation of the simulation model" and "Testing and analysis of simple policies rooted in real world scenarios". These two phases seeks not only to validate simulation behavior, but also demonstrate and evaluate its functionality. Confidence in the model will firstly be built by the

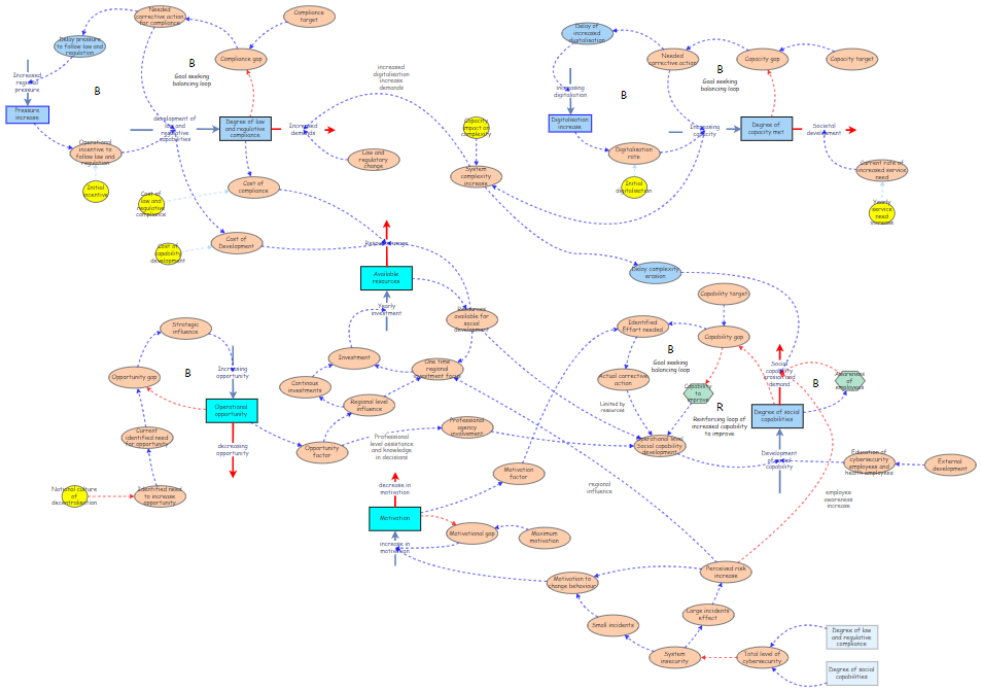

Figure 4.25: Connecting every part of the simulation.

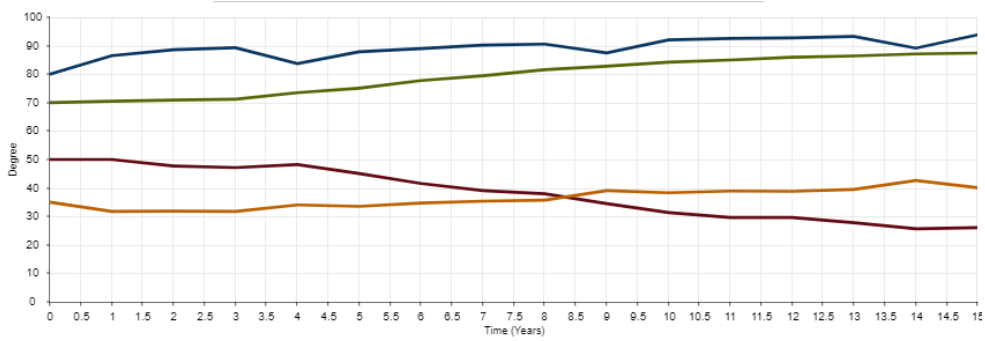

Figure 4.26: Simulation results showing development of three main stocks and system insecurity.

section dedicated to validation then through the process of demonstrating different scenarios and policies, while simultaneously illustrating model relationships. Issues with the model and inconsistencies were identified by performing demonstration and evaluation. They have been corrected and changed accordingly.

Validation of the simulation model

The general approach to model validation is described in the methodology chapter (3), where related works are discussed and general steps to build validity presented. Several steps ensuring the validity of the model have been conducted during its creation. In-flows and out-flows have been continually tested and simulations have been continuously ran to investigate how variables and formulas effect its connected flow. This process is partly documented by presenting the model in steps, where simulation results differ before and after introducing relationships and variables. The presentation show only a small part of this process as the concepts have been more thoroughly applied during model construction. The steps used to build validity in this thesis are the ones described by Maani et. al. [2], based on theory and work in the field of system dynamics.

- **The causal loop diagram must correspond to the statement of the problem.**
  The causal loop models correlation to both the explicated problem and problem structuring, and its underlying purpose of identifying cultural reasons for business alignment issues have been discussed previously. The causal loop diagram, and problem structuring phase, is the basis of which the simulation model is created, thus the same properties apply to the system dynamics model.
- **The equations must correspond to the causal loop diagram, in particular the relationships.**
  The system dynamic model follow the connections depicted in the causal loop diagram in terms of how primitives influence one another. There are no inconsistencies in terms of system relationships between the causal loop diagram and the system dynamic model. However, it must be mentioned that there are differences between the two models. Some structural adjustments, and addition/removal of variables. It does however not differentiate in its intended relationship influences.
- **The model must be dimensionally valid, which enable converting variable dimensions (units of measurements).** As this model utilizes percentages rather than tangible measurements dimensional validity is not problematic. All percentages and rates are given pr/year, and one can revert variable influence and equations back and forth. However, one can question the quality of the quantification of variables, as a 20% increase in i.e. motivation does not necessarily translate seamlessly to a similar percentage increase in identified problems. Although quantification and variable

dimensions is implemented in a simple fashion, it does not jeopardize dimensional validity.

- **Has each equation in the model been adequately documented?**
  Each variable and interconnection has been documented throughout the thesis. This has mainly involved managerial explanations and discussing the assumptions underlying them. Because of the nature of this thesis the explanations and assumptions are based off theories, related work and additional sources of information describing the topics under question.
- **The simulation does not produce any unrealistic values.**
  This is confirmed through the presentation of simulation results during the model creation. Under the current circumstances the model does not produce any particularly unrealistic values such as negative capabilities or resources. Changing key variables in a controlled manner does change the results, but do not result in unrealistic values.
- **Behavior of the model should be feasible - what is does should be what we expect it to do.**
  The base case run, as well as the intermediate runs demonstrate the stability of the model under different circumstances and influences. It does not behave abnormally compared to what one would expect, and its behavior is feasible.
- **The model should maintain "conservation of flow", meaning that the total quantity of a variable, which has entered and left the system, together with what is still there should be accounted for.**
  Checking this consists of carefully examining simulation results during model creation, ensuring that all variables are accounted for at each time iteration. Ensuring and presenting "conservation of flow" is made easier by presenting the model in steps, ensuring that the variables are successfully transferred through the intended links and relationships.
- **Does each equation make sense when inputs take on extreme values?**
  The model is not created explicitly to handle all kinds of variables, but if the variables are kept within logical reasoning the model will simulate the behavior. This means that the simulation can handle extreme input for variables such as, for example, resources and investments. However, increasing the capability gap past 100% of possible capability does not make logical sense and would greatly impact simulation behaviors, and therefore does not support extreme variables to the same extent. By doubling the yearly budget for cybersecurity one would in reality increase the resources used on social capabilities by 500%, as they initially are ca. 20% of the total budget of 100%. In doing this social capability development would skyrocket the first years, and be comfortably maintained over time. As shown in figure 4.27. If one were to change compliance target to 200% – which does not make any sense as one could only achieve 100% compliance – the result would be capabilities growing towards the goal of 200%. As a result, the development/maintenance costs would be to high to facilitate any social devel-

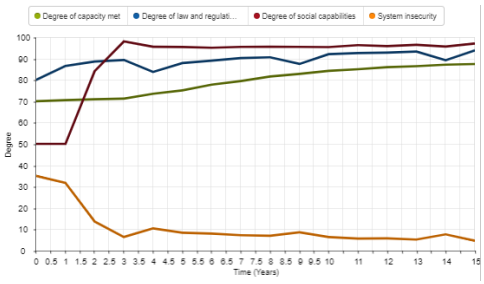

Figure 4.27: Showing simulation results with "extreme" variable inputs, increases investment in social capability development by 500%

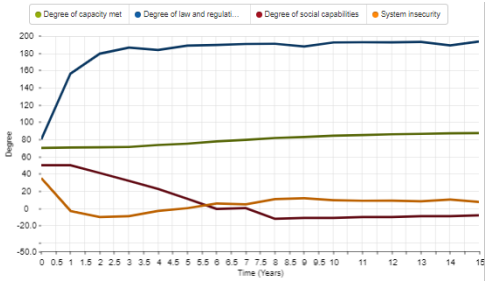

Figure 4.28: Illustrate "extreme" variable value aimed at making the simulation illogical.

opment, as seen in figure 4.28. The second example is more detrimental to the simulation results than the first, as one can see in the figure that the extremes circumvent the model's ability to effectively stop negative values.

Problems with simulation model validation This models main weakness in term of validity is the foundation on which it is built. With limited information and resources on the topic, and no possibility to specifically ask for the information needed the way in which variables and interrelationships are quantified suffers from weak justification. The topics of limitations and future work will be discussed when presenting limitations and future work (6).

Test and analyse simple policies rooted in real-world scenarios.

Simulation models are often subjected to policies and strategies. Policies revolves around changing one variable and showing how the system reacts, strategies are a set of policies changed at the same time. Policies are applied continuously during the development process to analyse current system behavior. Testing different policies are source of validation, as well as being a tool to help present the results from the model. This section will firstly provide some variations to the current system baseline, showing how different variables influence the entire system, further validating its behaviors and connecting current simulation setting to the real world. Secondly, the simulation will be exposed to changes which intend to highlight system interactions and stakeholder influences.

Using and changing the model provides insight as to how one can utilize and improve the model in the future, in addition to increasing validity and illustrating interconnections. Even with the validation efforts conducted in this thesis, the actual accuracy of the proposed model is still under question due to the data on which it is built. However, this does not take away from the fact that one could use such an artifact to improve overall cybersecurity culture in a system such

as the NSHS, and NHS as a whole. With more accurate data one could alter the relationships, variables and equations with the aim of making them more accurate.

Varying the system baseline by changing the overall dynamics and variables

The variables subjected to analysis and change are variables thought to be uncertain and influential in terms of system behaviors. The primitives that are changed are the initial value of *Degree of law and regulative compliance*, *Degree of capacity met* and *Degree of social capabilities*. Additionally, the variables determining *Cost of compliance* and *Cost of development* are of high influence due to its connection to *Resources for social development*. Lastly the effect of the operational levels *Capability to improve* is examined. Changes are mainly investigated in its effect on the three main stocks of the system, *Degree of law and regulative compliance*, *Degree of capacity met* and *Degree of social capabilities*. For comparison to the base case the reader is directed to the graphical representation corresponding to system development when in its reference mode behavior (4.26).

Changing the initial value of *Degree of capacity met*: By reducing the overall degree of capacity met the *system complexity* increase as a result of more to fill the capacity gaps. In turn, this would increase *Increased demands* related to law and regulatory compliance and *Social capability erosion and demand*. When *Development of law regulative capabilities* increases so does the *Cost of development* enhancing the negative effect on social capability development. Figure 4.29 show overall simulation development.

Changing the initial value of *Degree law and regulative compliance*: Changing this initial stock value mostly effects the associated costs, decreasing *Cost of compliance* while increasing *Cost of development*. Due to development being more costly than maintaining compliance *resources available for social development* decrease slightly. The effect of reduced *Degree of law and regulative compliance* is not significant, because of the fact that several factors influence *Operational level social capability*. The increased gap is filled fast due to high levels of *Operational incentive to follow law and regulation*.

Reducing both *initial incentive* and initial value of *Degree of law and regulatory compliance* If we were to reduce both operational level incentives and initial compliance, the costs of both development and compliance would drastically decrease, as the operational level would not focus mainly on law and regulative compliance leaving resources to be used on *Social capability development*. Figure 4.30 shows the result of decreasing *Initial incentive* to 30% and initial *Degree of law and regulatory compliance to 50%*. The graph suggests that the *System insecurity* would be higher initially, before stabilizing at a lower level than the reference mode. *Degree of social capabilities* would be developed at a higher pace, while law and regulatory compliance would more slowly climb towards its goal.

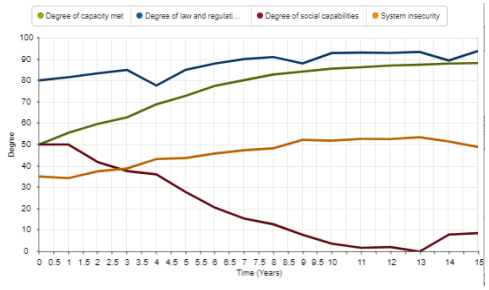

Figure 4.29: Illustrate overall stock development when initial capacity is set to 50% as opposed to 70%

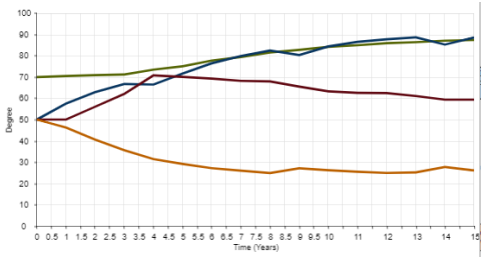

Figure 4.30: Show development as a result of lower initial levels of *Degree of law and regulative compliance* and lower initial incentive and pressure to follow comply to law and regulation

Changing the *Cost of compliance* Changing compliance variables illustrates how changing variables affecting the *Resources available for social development* significantly influences the operational level's ability to develop social capabilities. The costs can be altered without influencing the actual *Degree of law and regulative* and *Initial incentives*. Although operational focus on law and regulatory compliance, and its limited resources, is firmly rooted in previous sections, the actual simulation of costs are created on an overall expectation of simulation behavior and logical reasoning. If we were to say that the maintaining compliance only costs 50% of the total level of compliance, as opposed to 80%, and the development and erosion stayed the same the *Resources available for social development* would increase significantly. Baseline costs are given in table 4.5 and the costs as a result of the changes are given in figure 4.31, the graph showing holistic system results in terms of graphs are shown in figure 4.32.

Time	Available resources	Cost of Development	Cost of compliance	Resources availabl...	Yearly investment	Development of so...	Degree of law and ...
0	0	17.5	40	0	100	0	80
1	42.5	11.8125	43.25	42.5	100	15.44875	86.5
2	44.9375	9.996875	44.2875	44.9375	112.352476172	15.266244909	88.575
3	58.068101172	10.440696602	44.645625	58.068101172	100	17.962914687	89.29125
4	44.913678398	15.914295267	41.838561355	44.913678398	100	11.930383103	83.677122711
5	42.247143378	13.588467134	43.921747643	42.247143378	100	9.71757735	87.843495286
6	42.489785223	12.297644782	44.499144926	42.489785223	107.08211632	10.539196374	88.998289852
7	50.285326612	11.925295338	45.088666853	50.285326612	100	10.922093707	90.177333707
8	42.986037809	11.462444774	45.279287987	42.986037809	100	9.650287671	90.558575974
9	43.258267239	16.298595809	43.715217119	43.258267239	100	8.474348692	87.430434238

Figure 4.31: Shows overall financial status after altering the *Cost of compliance*

Changing the the influence of current *Degree of social cybersecurity capabilities* *Operational level social capability development* is highly influenced by resources and affected by the current *Degree of social capabilities* through the converter's *Capability to improve* and the *Awareness of employees*. Their baseline values are given in figure 4.12 and 4.13, these are attempts at quantifying the effect of

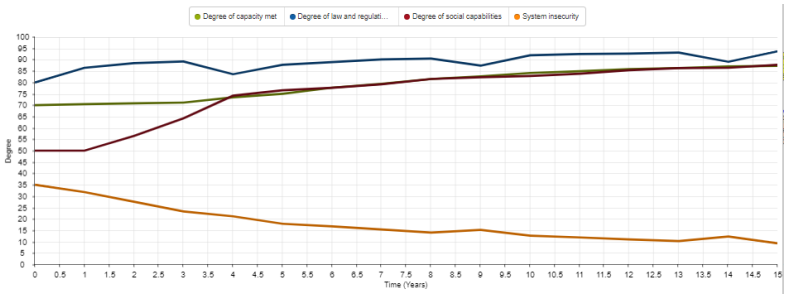

Figure 4.32: Graphical simulation results after decreasing *Cost of compliance*

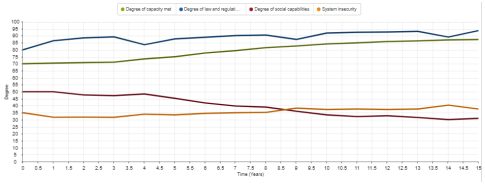

Figure 4.33: System development excluding the influence of awareness while including the influence of capability to improve.

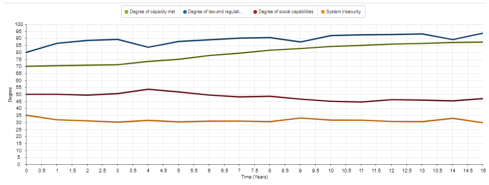

Figure 4.34: The result of only having the influence of *Employee awareness* relevant

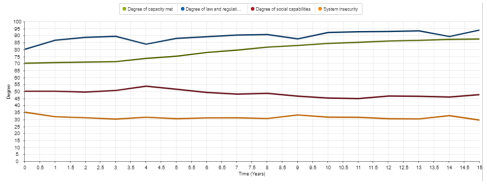

Figure 4.35: System development without the influence of awareness and capability

knowledge and expertise and overall awareness within an operational entity. By removing both influences one can see their actual influence on the *Degree of social capabilities*. With both influences removed the results are as seen in figure 4.35. With the effect of *Capability to improve* impacting *Degree of social capabilities* the corresponding graph is shown in figure (4.33). With the *Degree of social capabilities* stable around 50% the awareness does not show any significant effect, but any increase or decrease in capabilities would be stronger due to the level of awareness. The same principle apply to *Capability to improve*, the main difference is that is is perceived to have a bigger impact overall. Thus, with a gap of 50, *Development of social capabilities* would decrease as a result. We observe that poor *Degree of social capabilities* results in an even worse *Degree of social capabilities* at the next time iteration, if the *Degree of social capabilities* were to be good the effects are reversed.

Changing the initial value of the stock *Degree of social capabilities* Changing the initial value of *Degree of social capabilities* would result in *Capability to improve* to increase development and *Awareness of employees* to decrease erosion. However we do not see development being able to maintain the high initial level as the *Actual corrective action* relative to the *Capability gap* is low. The system does however stabilise at a generally higher level than if the capabilities where lower to begin with. With an initial value of 80 *Degree of social capabilities* is ca. 40% after 15 years compared to 26% in the baseline simulation. This behavior suggests that the amount of erosion is higher than the *operational level social capability development*, as a result of insufficient resources to maintain a very high level of social capabilities.

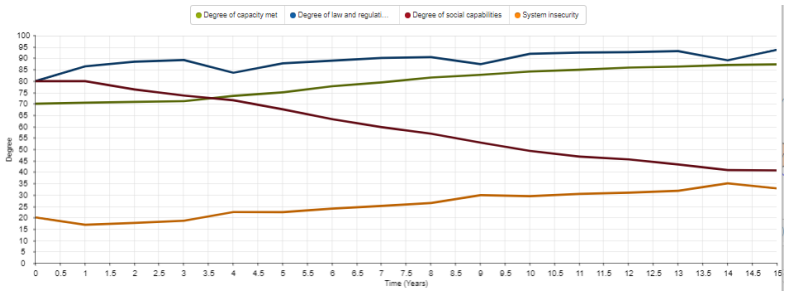

Figure 4.36: Simulation results with the initial value of *Degree of social capabilities* set to 80.

Changing the national level influences increasing operational level opportunity. Opportunity has, until this point, been considered as an influence capable of changing the overall simulation behaviors. It is present in all simulations, although its value is static. This section will showcase how the system reacts to increases in the stock *Operational opportunity*. The effects are examined separately. *National culture of decentralisation* will be reduced by 20% twice, in turn increasing *Capability to improve* and therefore the overall *Degree of social capabilities*. The same policy changes are conducted for *Regional influence*, excluding the effect of incorporating professional level knowledge and expertise *Operational level social capability development*. Increasing regional influence revolves around increasing their investments occurring every 4 years due to the effect of large incidents, as well as providing a steady stream of investments.

With both *Regional level influence* and *Professional agency involvement* active, we observe how one can alter system behavior in order to close in on a desired level of cybersecurity social capabilities. The results come from decreasing *National culture of decentralisation* by 30%. Figure (4.41) is a graphical representation of the main stocks. Figure (4.42) illustrates how *Continuous investment* and bigger *One time regional investments* increase the amount of *Resources available for social development*, making *operational level social capability development* higher than the *social capability erosion and demand*. Figure (4.42) also show the *Oppor-*

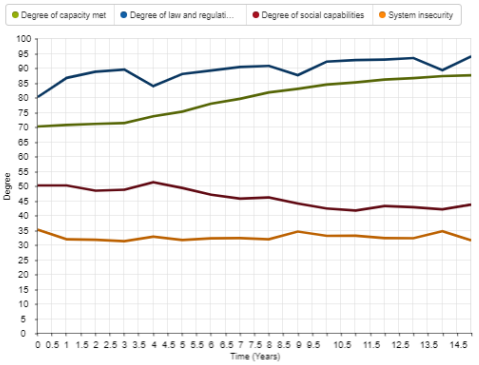

Figure 4.37: Reducing *National level culture of decentralisation by 20%*accounting for the effect of *Professional agency involvement*

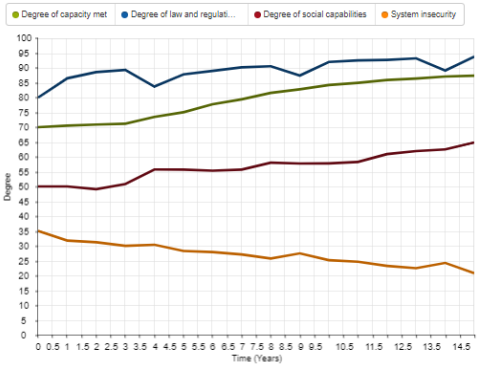

Figure 4.38: Reducing *National level culture of decentralisation by 40%* accounting for the effect of *Professional agency involvement*

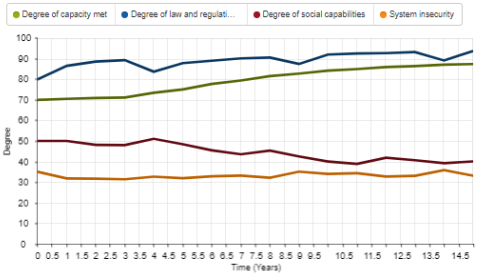

Figure 4.39: Reducing *National level culture of decentralisation by 20%* accounting for the effect of *Regional influence*

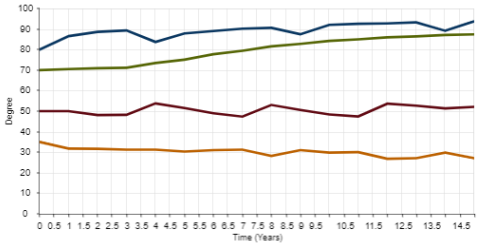

Figure 4.40: Reducing *National level culture of decentralisation by 40%*, accounting for the effect of *Regional influence*

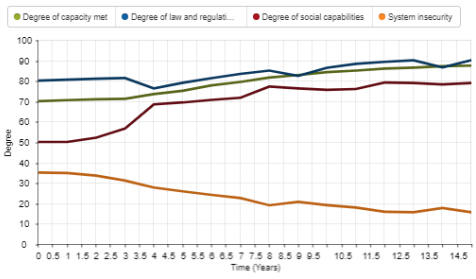

Figure 4.41: Graphical development of main stocks with an 30% decrease in national culture of decentralisation

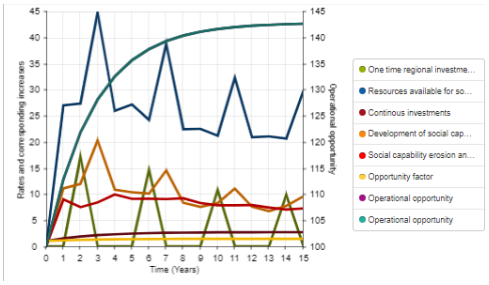

Figure 4.42: Graphical representation of the variables mainly responsible for creating overall increase in cybersecurity capabilities as a result of 30% decrease in national culture of decentralisation.

tunity factor which is used to increase *Capability to improve by a given percentage* based on the *Operational opportunity*.

Demonstration and validation provides the basis of further analysis and strengthen our confidence in the simulation model

Through performing both subsections, confidence in the model's behavior has increased. In the general tests to build validity, there no significant issues were identified with the steps. However, validity arrives in degrees and there are many additional tests which can be utilized to build model validity. This model's validity can be questioned when it comes to adequate documentation such as when the justification is weak (i.e. weighing a variable). Some of the steps discussed in the validity chapter were further built on and illustrated during policy implementations. Through changing variables, one illustrate overall variable and formulae influence. Results under different circumstances, especially where the variables are of an uncertain nature or of high general influence demonstrate how current quantification and overall variations effect the simulation. Not only does this further illustrate validation steps, but it also provides a basis for analysing the results and implications that culturally-rooted cybersecurity challenges can have on overall social cybersecurity capabilities and business alignment. Additionally, it provides a basis for analysing how the thesis answers the identified research questions, especially in relation to how it can be used to help relevant stakeholders improve cybersecurity culture.

4.3.3 Organisational learning

The main purpose of this section is to describe how the model can be useful for the organisation in question, and how it may be useful in the future. While this step is more important in cases where one more closely collaborates with the organ-

isation in question, it is nonetheless relevant for answering the RQ3, as it targets how one can use the artifact to enhance cybersecurity culture. There are two main areas in which the model is useful. First, where it models identified problems in the sector – mainly those rooted in cybersecurity culture, as well as the effect identified relationships have on cybersecurity cultural development at the operational level. By highlighting the relationship between stakeholders in the system, one can identify areas that are important to improve in order to enable other stakeholders to do the same. Not only are relationships between stakeholders of different system levels modelled, but relationships within ones own organisation are as well. If we consider the simulation to be accurately portraying aspects of cybersecurity within the system as a whole, the problems and results shown in the section which demonstrates and validates the model can be used to identify weaknesses. Additionally, the simulation shows that inter and intra relationships between stakeholders in a complex environment can be modelled. If the modeller uses more accurate data surrounding the topics investigated – especially related to quantification – they could improve and tailor the model to be more accurate. Lastly, while the accuracy of the variables and simulation results can be questioned, the illustrative nature of modelling can still help enhance the overall understanding of concepts used to investigate cybersecurity. These concepts include, but are not limited to, theories such as COM-B behavioral theories and socio-technical systems.

Chapter 5

Discussion and implications

5.1 Main findings from the System Dynamics simulation model

Sections leading to the development of the simulation model, such as background and related work, problem structuring, and causal loop modelling, have presented issues rooted in cybersecurity culture and stakeholder influence. As a result of investigating the problems and challenges from a holistic perspective, and connecting them through modelling techniques, several interesting relationships were discovered and illustrated by using the simulation model. It illustrates how system behaviors, in the simulation base case, results in a steady decrease in operational level social capabilities. Initial decrease, and ultimately system balance at inadequate social capabilities, is a result of continuous digitalization, increased system complexity, lack of resources, lacking knowledge and expertise, and poor employee cybersecurity awareness. Development of social capabilities continues to decrease, even though current national, professional, and regional influence is accounted for. The model base case incorporates a continuous addition of knowledgeable and aware employees, as a result of national-level educational programs and the sector's reactive pattern of change.

The operational level's lack of resources is connected to management of cybersecurity being overly focused on law. Demands created with the foundation of law are followed to a relatively high degree, ensured by RHA's incorporating the demands in their cybersecurity frameworks. The developed capabilities – outside of those mandated by law – are governed by individual hospitals, and is not subjected to the same pressure or funding from RHA's. The simulation model has shown that, by reducing operational level incentive to comply to law and regulations and lowering initial of law and regulatory compliance, resources which can be used for social capability development are freed. Then, less resources would be used as a result of lower maintenance and development costs, which would enable social capability development.

As this research illustrates, changing the base value of healthcare capacity severely impacts the ability of stakeholders on the operational level to maintain and develop their degree of social capabilities. This impact is a consequence of increased pressure to meet current and future capacity demands. Increasing capacity is achieved through digitalization, as the government has a strong culture for digitization as means of modernization. Digitalization is perceived as a double-edged sword: it increases efficiency while simultaneously increasing system complexity. In turn, increased system complexity increases erosion of social capabilities, as well as law and regulatory capabilities. As a result of these diminished law and regulatory capabilities, the system prioritizes their development. This further adds to development costs and reduces the availability of resources used to develop social capabilities. The effect of decreased social capability is further increased by the operational level's internal relationships – particularly concerning the capability to improve and level of awareness. In other words, by increasing the level of system complexity we severely impact and limit social capability development.

The simulation model illustrated how changes to initial social cybersecurity capabilities will affect the system over the time. It is concluded that the operational level does not have the ability to maintain high levels of social capability over extended periods. However, the system stabilizes at a higher overall level of cybersecurity capabilities. This thesis further investigated the effect of removing capability and awareness from the simulation results. This investigation demonstrated that awareness does not significantly influence the simulation while in its base case, due to the level at which it stabilizes. However, removing the effect of capability in the simulation base case results in higher levels of social capabilities. By removing a factor, which limits development of social capabilities in the simulation base case, we increased development overall.

Lastly, by indirectly changing operational level opportunity through, for example, giving professional agencies more governing power and influence in the decision-making process at hospitals, their capability to improve increases. Additionally, operational level opportunity is tied to regional level influence and willingness to invest. Increased investments could be a result of changes to current law and regulation, or increasing their ability to change funding and budgeting. Regional level influences increase available resources through larger investments as a result of large incidents and attacks, and a continuous stream of added resources. Opportunity is initially limited due to the organisational structure, roles, and responsibilities determined due to a culture of decentralised management on the national level. By individually demonstrating both regional influence and professional level involvement, we can observe that professional involvement has a higher positive effect than regional influence does. Incorporating both influences naturally results in positive development of capabilities and significantly less system insecurity.

The simulation model highlights how culturally rooted issues influence the operational level's capability, opportunity, and motivation in order to exhibit the desired behavior of increasing social cybersecurity capabilities. The main limiting factors have been identified as capability and opportunity through the causal loop modelling phase and problem structuring. These factors were then consequently illustrated in the system dynamics model. Inter/intra-stakeholder influences and relationships prohibits the operational level's ability to achieve goals, by limiting capability and opportunity. We can therefore state that the identified issues pose a business alignment problem where national, professional, and regional influence and interventions do not enable stakeholders at the operational level to achieve their goals.

5.2 Answering the identified research questions and achieving the research objective

The research objective and questions were initially presented in the introduction (1), where their motivation and function were stated as well. They describe the expected goal and define the specific tasks that need to be completed in order for the objective to be achieved. This section is dedicated to answering the proposed research question and discussing how the research goal is met. First, the objective and following research questions are given:

- **Research objective:** To identify business alignment problems among stakeholders rooted in cybersecurity culture and propose solutions in order to enhance cybersecurity posture in the Norwegian healthcare digital ecosystem.
- **RQ1:** How can the Norwegian healthcare system, which is argued as a complex system, be modelled to investigate business alignment and cybersecurity culture among stakeholders?
- **RQ2:** How do inter/intra dynamics of stakeholders influence cybersecurity culture and expose the system to increasing cybersecurity risk?
- **RQ3:** How can the developed artifact be used to improve cybersecurity culture in the NHS?

The proposed methodology highlights how these questions will be answered in this thesis (3.2). By conducting the steps provided in the methodology, these research questions can be answered and the goal of the thesis can be achieved.

5.2.1 RQ1 - How can the Norwegian healthcare system, so argued as a complex system, be modelled to investigate business alignment and cybersecurity culture among stakeholders?

Throughout the problem explication, artifact requirements, and problem structuring sections, it was established that by following a methodology for creating

a system dynamics simulation model one could investigate the impacting factors on business misalignment that are rooted in the cybersecurity culture.

The adopted perspective portrayed in socio-technical systems theory and systems thinking enabled a holistic assessment of systemic aspects, as well as their influence on culture. Business alignment is seen in relation to behavioral theories connecting the factors, capability, opportunity, and motivation for exhibited behavior. The factors determining behavior are subject to influence as a result of interventions and measures implemented on different organizational levels. This influence can ultimately be rooted in culture, and determine a stakeholder's ability to exhibit desired behavior, as in reaching their organisational goals. The theoretical framework enables the analysis of stakeholders, cultural influences and business alignment. Through establishing a holistic theoretic framework of analyzing systems, culture, and business alignment, the general method used to model the system could be established. Additionally, this text limits its questioning of the NHS to the Norwegian specialist healthcare service (NSHS). By narrowing this scope, we compensate for challenges such as the broad nature of the adopted paradigm, the fact that the investigated topic of cybersecurity culture involves many aspects of organizational theory and cybersecurity, and the complexity of system-stakeholder relationships. The primary stakeholders considered are government bodies, professional agencies, and regional health authorities (RHA) and their subordinate institutions – especially hospital trusts. Influences are discussed in relation to the following organizational levels: national, professional, regional, and operational. Lastly, the system and stakeholders are presented and identified in a way that enables us to model and investigate their inter/intra dynamics.

5.2.2 RQ2 - How do inter/intra dynamics of stakeholders influence cybersecurity culture and expose the system to increasing cybersecurity risk?

RQ2 is answered by performing the dynamic modelling process, which produces the system dynamic model. This artifact was identified as suitable to model the proposed system, its stakeholders, cybersecurity culture and business alignment. This system dynamics model was designed specifically for investigating stakeholder dynamics, influencing cybersecurity culture, and relating the simulation results to system insecurity (risk). Culturally rooted stakeholder dynamics were in focus throughout this thesis. However, as the adopted paradigm suggests, this approach does not exclude issues related to areas such as – but not limited to – policy, law, and digitalization.

The simulation model illustrated aspects of stakeholder dynamics that are exposing the system to risk. The thesis concludes that a current lack of awareness, knowledge, and expertise influences the social capabilities at the operational level. Furthermore, this thesis concludes that high-level strategies, as well as a decent-

ralised management culture, limit the operational level's opportunity in a way that weakens their cybersecurity culture. The main limiting factors are insufficient resources, low regional level involvement, continuous increase in system complexity due to digitalization, high focus on law and regulation, and limited professional agency involvement in cybersecurity governance and operational level decision-making. Limited capability development is ultimately connected to risk and system insecurity. Whereas limited operational level opportunity is mainly caused by high-level national influences as a consequence of current strategy and legislation enforced by the ministry of health and care services. More detailed findings from the simulation model are discussed when presenting the main findings from the system dynamic simulation model 5.1.

5.2.3 RQ3 - How can the developed artifact be used to improve cyber security culture in the NHS?

In relation to organizational learning, this thesis discussed how the artefact developed throughout this research can be used to increase cybersecurity culture. Organizational learning can arrive as a result of the sector and its stakeholders acknowledging the identified challenges discussed in relation to RQ2. By acknowledging issues, one can design and implement interventions targeted at resolving them. The model can alternatively be used to analyze how a proposed intervention would affect cybersecurity and social capability development.

Using these results, or the model directly, implies that we have sufficient confidence in the model, which might not be the case. However, one can facilitate organizational learning simply by using the current simulation as a baseline, and improve its accuracy. More accurate data would enhance overall model validity and build confidence in its simulation results, which enable the model to be used in conjunction with decision-making. Lastly, modelling can present complex systems in a more comprehensible way, which can in turn help stakeholders who are unfamiliar with cybersecurity understand the underlying concepts used in this thesis. The way cybersecurity is presented can aid in educational activities aimed at increasing stakeholders' understanding of socio-technical systems, systems thinking, and behavioral theory in relation to cybersecurity, business alignment, and culture.

5.2.4 Research objective - To identify business alignment problems among stakeholders rooted in cybersecurity culture and propose solutions to enhance cybersecurity posture in the Norwegian healthcare digital ecosystem.

The research objective is split in two main sections:

The first half of the objective is to identify the factors negatively impacting business alignment that are rooted in cybersecurity culture. When studying these

factors, cybersecurity culture is the primary focus. This is because the majority of the identified factors revolve around how current culture and understanding influence stakeholder behavior and cause potential issues. While answering RQ1 and presenting the theoretic framework (2.1.1), this thesis states that stakeholder interventions influencing the COM-B variables of a particular stakeholder can result in business misalignment.

Further, the model simulates how stakeholder influence and interventions such as policy, law, national strategies, organizational structure, stakeholder roles, and responsibilities influence operational level capability development. It identifies several stakeholder interactions that influence the ability of operational level stakeholders to exhibit desired behavior and reach their organizational goal. All issues and relationships discussed in this thesis are linked to underlying cultural causes and factors determining behavior (such as capability, opportunity, and motivation). As a result, this thesis has successfully identified business alignment issues rooted in cybersecurity culture. As a conclusion to the first half of the objective, this thesis presents the simulation results while finding that the main behavioral factors limiting business alignment is opportunity, followed second by capability.

The second half of the research objective, on the other hand, is centered on identifying solutions in order to enhance overall cybersecurity posture in the NHS. Identified potential solutions are inherently related to factors that limit business alignment, such as operational level opportunity and capability. This model strongly suggests that operational level opportunity is the largest problem, as it could potentiality influence both the capability of hospitals to improve, and the overall availability of resources. Opportunity is not something that the operational level stakeholders themselves can easily change, as it relies on external influences.

One of the main principles of the systems thinking paradigm is recognizing the dynamic, complex, and interdependent nature of systems. This includes, but is not limited to, understanding that an identified problem may turn out to only be a symptom. To enable lasting solutions, the root issue must be identified and addressed.

Through demonstrating simulation behaviours, this paper discovered several interesting relationships. Further, by utilizing the insights gained from the model, we could find and target effective solutions in order to address the actual root cause.

The first proposed solution to enhance overall cybersecurity posture is to increase regional level influences, enabling regional level stakeholders to increase their investment and ensure greater focus on increasing operational level cybersecurity culture. The second solution is that one could change the role and governing power of professional agencies, which could increase the capability of hospitals

to improve. Giving professional agencies more governing power could incentivize hospitals' social capability development, as professional entities have proposed solutions which target the issue of lacking social capabilities, though proposed solutions are yet to be implemented. Further, giving them a more active role could increase operational level capability, thus mitigating the effect of lacking knowledge and expertise. Lastly, this thesis illustrates how decreasing the amount of digitalization could reduce added system complexity, and how changing operational level incentives to follow law and regulation could free up resources to increase social capability development. Both are solutions worth investigating, but come at the cost of decreased healthcare capacity (in the case of decreasing digitalization as a means to modernize), and lower regulatory compliance (in the case of increasing available resources for social capability development).

In conclusion to the second half of the research objective, the potential solutions offered are all tied to opportunity, which mainly changes as a result of national level involvement. This effectively makes the limiting factors of national level involvement – identified as culture of decentralized management, strategic direction, and law – the root issue. With national influences perceived as the root issue, solutions aimed at changing this influence in ways that indirectly achieve the previously-mentioned solutions should be a priority. However, considering the negative effects of decreasing capacity and regulatory compliance interventions, they should be thoroughly evaluated. Better, lasting solutions may need to take the form of interventions that target the underlying issues which prevent national level stakeholders from increasing their regional and professional level influence. Through employing these interventions, one could enable operational level stakeholders to achieve their organizational goals and achieve business alignment across all organizational/system levels. This is crucial, considering the fact that all stakeholders ultimately want patients to be secure and safe.

Chapter 6

Conclusion and future work

Conclusion This thesis consists of several activities aimed at analysing culturally rooted issues that effect business alignment. First, it presents the background of the work, which introduces the adopted paradigm that enables the observation of cybersecurity and systems. The two leading perspectives and theories utilized are systems thinking [2][7] and socio-technical systems [1]. Both frameworks enable cybersecurity to be viewed as a complex and interconnected phenomenon. Cybersecurity culture is the topic of main interest in this thesis. It is placed within the context of behavioral theories, such as the COM-B model [16], in order to enable an analysis of its implications and effect on business alignment. The paradigm, models, and theories result in a theoretic framework used to analyze and identify system interactions, and provides a strong background for applying modelling to analyze complex problems.

After the theoretic foundation is provided, the thesis' focus shifts toward presenting the system in question, namely the Norwegian healthcare system. This section details how the management of cybersecurity is structured within the system and presents different stakeholders, along with their current roles and responsibilities. Each stakeholder is assigned to a system level, those being: national, national professional, regional, and operational. Seeing stakeholders in relation to their system level is important, as the adopted paradigm suggest incorporating different organizational levels when analyzing socio-technical systems. The system is argued as complex given its number of stakeholders and the multifaceted relationships between them, which is used to argue that the required system scoping only includes stakeholders within the Norwegian specialist healthcare service. By presenting the system stakeholders, and considering them in context of the previously presented theoretic framework, we begin to unravel their complex relationships. Stakeholder dynamics are identified through presenting their defined roles, responsibilities, and observing how interventions (such as national strategic documents, policies, and guidelines) influence stakeholders. To further highlight relationships, identify problems, and justifying the research, cybersecurity issues are identified in sector reports, international research, and other sources of qualitative

information. Problems identified where, for example, there is a lack of cybersecurity awareness and knowledge, the operational level overly focuses on law and regulatory compliance, there is increased digitalization and system complexity, and/or they are beholden to a reactive pattern of change. The identified problems are seen in the context of stakeholder involvement, as well as through their cause and effect on stakeholders and overall cybersecurity capabilities.

The theoretical foundation and system in question have been presented, and the general area of research has been justified in a way that provides insight into current cybersecurity problems and highlights the relationships between stakeholders. The next step is therefore to present and discuss related works that apply systems thinking to cybersecurity, system dynamics to the the field of cybersecurity or organisational research, and investigate the dynamics of cybersecurity culture and behavior. These related works provide valuable insight into influences within the field of cybersecurity and organizational behavior, in addition to the methodology and simulation techniques used. Some of the related works adopt comparable paradigms and follow similar research methodologies. However, this thesis differentiate itself by way of its research objective and holistic approach to the system in question, its stakeholders, and its analysis of business alignment.

After the background and related work is presented, it is then opt to discuss the application of research methodology. This thesis follows an adapted version of the Design Science Research (DSR) method [60], and the Systems Thinking and Modelling (ST&M) Methodology [2]. Both methodologies are highly adaptable. When combined, they create a methodology suitable for this thesis. Deciding which steps to incorporate from the DSRM and ST&M is achieved through discussing the methodologies in relation to the research objective and questions presented by this thesis. The result was a less comprehensive version of the ST&M Methodology, used mainly for problem structuring, causal loop modelling and system dynamics modelling, and application of the DSRM methodology as a meta-methodology, defining phases and steps not extensively covered by the ST&M methodology. Essential to the methodology is the creation of an artifact: in this case a System Dynamics simulation model, which was created on the basis of problem structuring and causal loop modelling. All phases in the methodology was improved in iterations, where information from a later phase could feed information to phases conducted previously.

The dynamic modelling process consists of structuring a problem, creating a initial causal loop model, translating it to a functional system dynamics simulation model, creating a base case, validating it, and presenting variations and changes to its variables. All phases of model creation rely on information to be presented in the background and related works section, and only elaborated and explained in the context of model creation through problem structuring, causal loop modelling, and ultimately system dynamic model simulation. The resulting simulation

tool represents previously discussed problems and stakeholder interactions. The quantification of simulation variables is mainly based on assumptions as to how variables influences each other. The simulation results are ultimately connected to how the organisation in question could benefit from using the model, such as by incorporating the results in their body of knowledge or fine tuning and adapting the proposed model to better suit business needs. The simulation results illustrates identified cultural challenges in light of its effect on business alignment and demonstrates how inadequate operational level opportunity, as a result of a national culture of decentralised management, law, and digitalization, limits the actual development of social capabilities. Counteracting this limitation could potentially increase cybersecurity culture at the operational level, and therefore limit the system's exposure to risk.

Scientific contribution There are several scientific contributions to this thesis. First, the thesis illustrates how system dynamic modelling can be used to model the Norwegian specialist healthcare service. The NSHS is a highly complex socio-technical system with stakeholders residing within different system levels (national, national professional, regional and operational) influencing each other. The adopted paradigm does not limit influences to being those that effect stakeholders externally, and acknowledges that the socio-technical systems that are internal to one stakeholder also influences overall system behavior and development. Second, culturally rooted cybersecurity challenges are placed in context of one another, as well as in the context of overall business alignment. Simulation results could be used to justify changing the system in a way that facilitates a more healthy cybersecurity posture, and illustrates how high-level stakeholders are partly responsible for current operational level development. Additionally, the simulation model can be used as a baseline to further improve its validity and accuracy in determining the variable values and formulas that drive system development.

Limitations While the scientific contributions of the thesis are listed above, there are limitations that could potentially inhibit the usability of the simulation model.

Empirical background and model validity: The main limitation of this work is based in its empirical foundation, as this foundation impacts model validity. Initially, this thesis was intended to be complimented by in-depth interviews of employees who work at different organizational levels, such as national, national professional, regional, and operational. This would include employees working in the ministry, directorates, RHA's, and individual hospitals. Additional efforts could have been taken to interview employees working in different IT service providers. Conducting interviews is believed to greatly enhance overall model validity and

strengthen the process of quantifying variables. It could also strengthen quantification of variable-relationships, and determine equations within simulation model. However, conducting interviews became difficult due to the ongoing Covid-19 pandemic, which made physical interactions reckless, unethical, and largely unfeasible per the resources available to this project. It was particularly impractical to conduct such interviews with the specified population, as would-be interview subjects work in a sector affected greatly by this global pandemic. Therefore, this thesis withheld from placing further strain on managerial positions in a sector that was already under significant stress as a consequence of the global situation. While it may have been possible to conduct online interviews, this was considered ethically inappropriate considering the level of strain placed on the required interview subjects – many of whom work in the Norwegian health sector. As a backup solution considered more appropriate at the current point in time, related research, public documents and reports were investigated in order to find the necessary information that would justify stakeholder and variable relationships and enable the creation of the system dynamic simulation model. While not optimal, it provided sufficient information to answer the research questions and objective to some degree, at the cost of model validity.

Report analysis is mainly a tool used to create an initial problem understanding, rather than serve as the main source of knowledge and feedback. Although, coupled with a theoretical framework and additional information provided by related works – as well as qualitative interview data from related research – the lack of model validity is noticeable. After structuring a problem, additional information should ideally be added in order to strengthen the simulation model. Causal loop modelling is often a method conducted with stakeholders present. While the empirical foundation takes away from model confidence, it still stands as a baseline which can be used by stakeholders to enhance their system understanding. Further, it serves as a model that can be improved once given more relevant data and information. The model could also be used to facilitate organisational learning by illustrating concepts related to cybersecurity, culture, and business alignment.

Model complexity: Due to the size and complexity of the system in question, it becomes increasingly difficult to represent all relationships and variables in the model. As the adopted paradigm suggests, the overall goal is to acknowledge system complexity. It include as many relevant variables as possible in order to inform the model. Which could lead to the thesis being perceived as falling short in its effort to holistically investigate the cybersecurity of the NHS by adopting the paradigm of systems thinking. This thesis does not represent every individual stakeholder. Instead, it is based on general systemic levels and the influences which resides within them. Additionally, it does not model every relationship between the systemic levels. Rather, the primary focus is in how higher level stakeholders influence lower level stakeholders, with the intent of finding relationships limiting cybersecurity capabilities. The thesis identify the primary

relationships and model them, while some relationships may not be accounted for.

Future work The presented simulation model provides a base case. By using the model to discuss the relationships and problems with stakeholders directly, one could greatly increase its overall base case validity. Therefore, future work is suggested in this area in order to open the current simulation and causal loop model to direct feedback from the stakeholders themselves. By discussing the identified problems, variables, and relationships directly with stakeholders, differences in their understanding of cybersecurity could be highlighted alongside the circumstances and influences that are not identified in the current empirical background.

Bibliography

[1] S. Kowalski, *IT Insecurity: A Multi-disciplinary Inquiry*. Stocholm, 1994, p. 314.

[2] K. E. Maani and R. Y. Cavana, *Systems Thinking, System Dynamics: Managing Change and Complexity*. New Zealand: Pearson Education, 2007, pp. 1–278, ISBN: 978-1877371035.

[3] A. S. Sæther, *Datasystemene til Helse Sør -Øst angrepet*, news, Jan. 2018. [Online]. Available: https://www.vg.no/i/0E4W4G.

[4] NRK, *Dataangrepet mot Helse Sør-Øst*, Jan. 2018. [Online]. Available: https://www.nrk.no/nyheter/dataangrepet-mot-helse-sor-ost-1.13873606.

[5] M. Field, 'WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled', *The Telegraph*, Oct. 2018, ISSN: 0307-1235. [Online]. Available: https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/.

[6] Cisco, 'Cisco Cybersecurity Report', Annual {CSR}, 2018. [Online]. Available: http://cs.co/9007BNiAx.

[7] P. M. Senge, *The Fifth Dicipline: The Art & Practice of The Learning Organization*. Doubleday/Currency, 1990.

[8] A. AlHogail and A. Mirza, 'Information security culture: definition and a literature review', in *2014 World Congress on Computer Applications and Information Systems (WCCAIS)*, Jan. 2014, pp. 1–7. DOI: 10.1109/WCCAIS.2014.6916579.

[9] S. Furullund, ' Er cybersikkerheten god nok? En studie av organisatoriske forutsetninger for cybersikkerhet i helsesektoren', Master's thesis, Nord universitet: Fakultet for samfunnsvitenskap (FSV), 2019. [Online]. Available: https://nordopen.nord.no/nord-xmlui/handle/11250/2616993.

[10] A. K. Lindahl, D. Squires and Å. Ringard, *Norway : {International} {Health} {Care} {System} {Profiles}*, 2016. [Online]. Available: www.commonwealthfund.org/international-health-policy-center/countries/norway (visited on 02/02/2020).

[11] V. Anderson and L. Johnson, *Systems thinking basics*. Cambridge, MA: Pegasus Communications, 1997, pp. 1–14, ISBN: 9781883823122.

[12] M. Webster, *System | Definition of System by Merriam-Webster*, 2019. [Online]. Available: www.merriam-webster.com/dictionary/system (visited on 16/01/2020).

[13] E. Mumford, *The story of socio-technical design: Reflections on its successes, failures and potential*, Oct. 2006. DOI: 10.1111/j.1365-2575.2006.00221.x. [Online]. Available: http://doi.wiley.com/10.1111/j.1365-2575.2006.00221.x.

[14] B. Al Sabbagh, 'Cybersecurity Incident Response : A Socio-Technical Approach (PhD dissertation)', *Department of Computer and Systems Sciences*, s. 133, 2019. [Online]. Available: http://urn.kb.se/resolve?urn=urn:nbn:se:su:diva-167873.

[15] B. Malmedal and H. E. Royslien, 'The Norwegian Cyber Security Culture', NorSIS, Tech. Rep., 2016.

[16] S. Michie, M. M. van Stralen and R. West, 'The behaviour change wheel: A new method for characterising and designing behaviour change interventions', *Implementation Science*, vol. 6, no. 1, p. 42, Dec. 2011, ISSN: 1748-5908. DOI: 10.1186/1748-5908-6-42. [Online]. Available: http://implementationscience.biomedcentral.com/articles/10.1186/1748-5908-6-42.

[17] European Union Agency for Network and Information Security (ENISA), 'Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity', 2018. DOI: 10.2824/324042. [Online]. Available: www.enisa.europa.eu.

[18] J. Cane, D. O'Connor and S. Michie, 'Validation of the theoretical domains framework for use in behaviour change and implementation research', *Implementation Science*, vol. 7, no. 1, pp. 1–17, Apr. 2012, ISSN: 17485908. DOI: 10.1186/1748-5908-7-37.

[19] A. D. Veiga and J. H. P. Eloff, 'Information security governance framework', *Information Security Management*, vol. 24, no. 4, pp. 361–372, 2009, ISSN: 15437221. DOI: 10.1145/1655168.1655170.

[20] K. Bissel, R. LaSalle and K. Richards, 'The Accenture Security Index - Redifining Security and how to achieve it', Tech. Rep., 2017. [Online]. Available: www.accenture.com/us-en/insight-accenture-security-index.

[21] L. F. Luna-Reyes and J. R. Gil-Garcia, 'Using institutional theory and dynamic simulation to understand complex e-Government phenomena', *Government Information Quarterly*, vol. 28, no. 3, pp. 329–345, Jul. 2011, ISSN: 0740-624X. DOI: 10.1016/j.giq.2010.08.007.

[22] A. Dutta and R. Roy, 'Dynamics of organizational information security', *System Dynamics Review*, vol. 24, no. 3, pp. 349–375, Jun. 2008, ISSN: 08837066. DOI: 10.1002/sdr.405. [Online]. Available: http://doi.wiley.com/10.1002/sdr.405.

[23] I. Kirlappos, S. Parkin and M. A. Sasse, '"Shadow security" as a tool for the learning organization', *ACM SIGCAS Computers and Society*, vol. 45, no. 1, pp. 29–37, Feb. 2015. [Online]. Available: http://dx.doi.org/10.1145/2738210.2738216.

[24] S. Lineberry, *The Human Element: The Weakest Link in Information Security*, 2007. [Online]. Available: https://www.journalofaccountancy.com/issues/2007/nov/thehumanelementtheweakestlinkininformationsecurity.html (visited on 09/03/2020).

[25] N. S. Safa and R. Von Solms, 'An information security knowledge sharing model in organizations', *Computers in Human Behavior*, vol. 57, pp. 442–451, Apr. 2016, ISSN: 07475632. DOI: 10.1016/j.chb.2015.12.037. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0747563215303083.

[26] J. Sterman, *Business Dynamics, System Thinking and Modeling for a Complex World*. Jan. 2000, vol. 19, ISBN: 9780071179898. [Online]. Available: https://www.researchgate.net/publication/44827001_Business_Dynamics_System_Thinking_and_Modeling_for_a_Complex_World.

[27] D. E. Porter, 'Industrial Dynamics. Jay Forrester. M.I.T. Press, Cambridge, Mass.; Wiley, New York, 1961. xv + 464 pp. Illus. $18', *Science*, vol. 135, no. 3502, pp. 426–427, Feb. 1962, ISSN: 0036-8075. DOI: 10.1126/science.135.3502.426-a.

[28] D. H. Meadows, D. L. Meadows, J. Randers and W. Behrens, *The limits to growth : a report for the Club of Rome's Project on the Predicament of Mankind*, 1st edition. Universe Books, 1972, p. 205, ISBN: 0876639015.

[29] S. Elsawah, S. A. Pierce, S. H. Hamilton, H. van Delden, D. Haase, A. Elmahdi and A. J. Jakeman, 'An overview of the system dynamics process for integrated modelling of socio-ecological systems: Lessons on good modelling practice from five case studies', *Environmental Modelling and Software*, vol. 93, pp. 127–145, 2017, ISSN: 13648152. DOI: 10.1016/j.envsoft.2017.03.001.

[30] D. H. Meadows and D. Meadows, 'The history and conclusions ofThe Limits to Growth', *System Dynamics Review*, vol. 23, no. 2-3, pp. 191–197, 2007, ISSN: 08837066. DOI: 10.1002/sdr.371. [Online]. Available: http://doi.wiley.com/10.1002/sdr.371.

[31] L. F. Luna-Reyes and D. L. Andersen, 'Collecting and analyzing qualitative data for system dynamics: methods and models', *System Dynamics Review*, vol. 19, no. 4, pp. 271–296, 2003, ISSN: 0883-7066. DOI: 10.1002/sdr.280. [Online]. Available: http://doi.wiley.com/10.1002/sdr.280.

[32] Ministry of Health and Care Services, *Helse- og omsorgsdepartementet*, 2020. [Online]. Available: www.regjeringen.no/no/dep/hod/id421/ (visited on 06/02/2020).

[33] Ministry of Health and Care Services, *Departments*. [Online]. Available: www.regjeringen.no/en/dep/hod/organisation-and-management-of-the-ministry-of-health-and-care-services/Departments/id448/ (visited on 06/02/2020).

[34] Ministry of Health and Care Services, *Etater og virksomheter under Helse- og omsorgsdepartementet*, no, Feb. 2020. [Online]. Available: https://www.regjeringen.no/no/dep/hod/org/etater-og-virksomheter-under-helse--og-omsorgsdepartementet/id2345206/ (visited on 25/02/2020).

[35] 'Overordnet risiko- og sårbarhetsvurdering for IKT i helse- og omsorgssektoren - ehelse', The Directorate of ehealth, Oslo, Tech. Rep., 2019. [Online]. Available: https://ehelse.no/publikasjoner/overordnet-risiko-og-sarbarhetsvurdering-for-ikt-i-helse-og-omsorgssektoren.

[36] D. Solumsmoen, I. Botheim and A. Hildrum, 'Merverdi eller unødig omvei? Om direktoratenes rolle i gjennomføring av nasjonal politikk', DIFI, Tech. Rep., Nov. 2013. [Online]. Available: https://www.difi.no/sites/difino/files/merverdi%7B%5C_%7Deller%7B%5C_%7Dunodig%7B%5C_%7Domvei%7B%5C_%7D1.pdf.

[37] Ministry of Local Government and Modernisation, *One digital public sector*, Jun. 2019.

[38] 'Nasjonal strategi for digital sikkerhet', no, Justis- og beredskapsdepartementet and Forsvarsdepartementet, Tech. Rep., Jan. 2019.

[39] Justis- og beredskapsdepartementet and Kunnskapsdepartementet, *Nasjonal strategi for digital sikkerhetskompetanse*, no, 2020. [Online]. Available: https://www.regjeringen.no/contentassets/073749ab881a4360877027cfca4ea580/nasjonal-strategi-for-digital-sikkerhetskompetanse---endelig.pdf.

[40] 'Normen 6.0', no, The Norwegian Directorate of eHealth, Standard, Jan. 2019. [Online]. Available: ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren.

[41] 'Normen 5.3 - Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren - ehelse', no, The Norwegian Directorate of eHealth, Standard, 2020. [Online]. Available: https://ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren.

[42] Å. Hetland, *Normen 6.0 - åpent høringsseminar*, no, Sep. 2019. [Online]. Available: https://www.youtube.com/watch?v=fOOjptIxhqY.

[43] 'Nasjonal trusselvurdering 2020', no, The Norwegian Police Security Service, Report, 2020. [Online]. Available: https://pst.no/globalassets/artikler/utgivelser/2020/nasjonal-trusselvurdering-2020-print.pdf.

[44] 'FOCUS 2019 - The Norwegian Intelligence Service's assessment of current security challenges', The Norwegian Intelligence Service (NIS), Report, 2019. [Online]. Available: https://forsvaret.no/fakta_/ForsvaretDocuments/focus2019_english_web.pdf.

[45] 'RISIKO 2019 - Krafttak for et sikrere Norge', no, The Norwegian NationalSecurity Authority (NSM), Report, 2019. [Online]. Available: https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2019_final_enkeltside.pdf.

[46] 'Helhetlig digitalt risikobilde 2019', The Norwegian National Security Authority (NSM), Report, 2019. [Online]. Available: https://www.nsm.stat.no/globalassets/rapporter/2019---nsm-helhetlig-digitalt-risikobilde.pdf.

[47] C. S. Kruse, B. Frederick, T. Jacobson and D. K. Monticone, 'Cybersecurity in healthcare: a systematic review of modern threats and trends', *Technology and Health Care*, vol. 25, pp. 1–10, 2017. DOI: 10.3233/THC-161263.

[48] E. D. Perakslis, 'Cybersecurity in health', *The New England Journal of Medicine*, pp. 395–397, Jul. 2014. DOI: 10.1056/NEJMp1404358.

[49] 'Report on improving cybersecurity in the health care industry', Health Care Industry Task Force, Report, 2017. [Online]. Available: https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.

[50] M. P. Jarret, 'Cybersecurity—A Serious Patient Care Concern', *American Medical Association*, vol. 318, no. 14, pp. 1319–1320, Sep. 2017. DOI: 10.1001/jama.2017.11986.

[51] 'Informasjonssikkerhet i helse- og omsorgstjenesten 2019 - ehelse', The Directorate of ehealth, Oslo, Report, Nov. 2019. [Online]. Available: https://ehelse.no/publikasjoner/informasjonssikkerhet-i-helse-og-omsorgstjenesten-2019.

[52] H. V. Haraldsson, *Introduction to system thinking and causal loop diagrams*. Jan. 2004, p. 49. [Online]. Available: https://www.researchgate.net/publication/258261003_Introduction_to_system_thinking_and_causal_loop_diagrams.

[53] N. G. Leverson, *Engineering a Safer World: Systems Thinking Applied to Safety*. Cambridge: The MIT Press, 2011, ISBN: 9780262016629. [Online]. Available: https://mitpress.mit.edu/books/engineering-safer-world.

[54] W. Young and N. Leveson, 'Systems thinking for safety and security', in *ACM International Conference Proceeding Series*, New York, USA: ACM Press, 2013, pp. 1–8, ISBN: 9781450320153. DOI: 10.1145/2523649.2530277.

[55] H. M. Salim, 'Cyber Safety: A Systems Thinking and Systems Theory Approach to Managing Cyber Security Risks', Master's thesis, Massachusetts Institute of Technology, 2014.

[56] A. Klimburg, *National cyber security framework manual*. [Talinn, Estonia]: NATO Cooperative Cyber Defense Center of Excellence, 2012.

[57] M. S. Jalali and J. P. Kaiser, 'Cybersecurity in Hospitals: A Systematic, Organizational Perspective', *Journal of Medical Internet Research*, vol. 20(5), 2018. DOI: 10.2196/10059.

[58] T. Fagade, T. Spyridopoulos, N. Albishry and T. Tryfonas, 'System Dynamics Approach to Malicious Insider Cyber-Threat Modelling and Analysis', T. Tryfonas, Ed., Cham: Springer International Publishing, 2017, pp. 309–321, ISBN: 978-3-319-58460-7. DOI: 10.1007/978-3-319-58460-7_21.

[59] N. S. Safa, R. V. Solms and L. Futcher, 'Human aspects of information security in organisations', *Computer Fraud and Security*, vol. 2016, no. 2, pp. 15–18, Feb. 2016, ISSN: 13613723. DOI: 10.1016/S1361-3723(16)30017-3.

[60] P. Johannesson and E. Perjons, *An Introduction to Design Science*, P. Johannesson and E. Perjons, Eds. Springer International Publishing, 2014, ISBN: 978-3-319-10632-8. DOI: 10.1007/978-3-319-10632-8_4.

[61] P. Pandey, *Using Theories from Economics and Finance for Information Security Risk Management*. 2016, ISBN: 978-82-326-1713-5. [Online]. Available: https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2396727.

[62] J. B. Homer and G. B. Hirsch, 'System dynamics modeling for public health: Background and opportunities', *American Journal of Public Health*, vol. 96, no. 3, pp. 452–458, Mar. 2006, ISSN: 00900036. DOI: 10.2105/AJPH.2005.062059.

[63] Marc-Andre Chavy-Macdonald, Kazuhiro Aoyama and Kazuya Oizumi, 'A model framework for determining dynamic architecture goals in a System-of-Systems', in *Conference on Systems Engineering Research*, 2017, pp. 238–254. [Online]. Available: https://www.researchgate.net/publication/315680223_A_model_framework_for_determining_dynamic_architecture_goals_in_a_System-of-Systems.

[64] Direktoratet for ehelse, *Normen - ehelse*, 2020. [Online]. Available: https://ehelse.no/normen (visited on 26/03/2020).

[65] M. Kianpour, H. Øverby, S. J. Kowalski and C. Frantz, 'Social Preferences in Decision Making Under Cybersecurity Risks and Uncertainties', in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11594 LNCS, Springer Verlag, Jul. 2019, pp. 149–163, ISBN: 9783030223502. DOI: 10.1007/978-3-030-22351-9_10.

[66] The Norwegian Directorate of Health, *Dette gjør Helsedirektoratet*. [Online]. Available: https://www.helsedirektoratet.no/om-oss/dette-gjor-helsedirektoratet (visited on 06/02/2020).

[67] Ministry of Health and Care Services, *Hovedinstruks for directoratet for ehelse*, 2020. [Online]. Available: https://ehelse.no/om-oss/om-direktoratet-for-e-helse.

[68] Helse- og omsorgsdepartementet, *De regionale helseforetakene*, no, 2020. [Online]. Available: https://www.regjeringen.no/no/tema/helse-og-omsorg/sykehus/innsikt/nokkeltall-og-fakta---ny/de-regionale-helseforetakene/id528110/ (visited on 26/03/2020).

[69] Norskhelsenett, *Norsk Helsenett SF - Vår historie*, no, 2020. [Online]. Available: https://www.nhn.no/om-oss/vaar-historie/ (visited on 26/03/2020).

[70] Helse- og omsorgsdepartementet, 'Oppdragsbrev til Norsk Helsenett SF for 2020', no, Report, 2020. [Online]. Available: www.hod.dep.no.

[71] 'Nordmenn og digital sikkerhetskultur', Norsk senter for informasjonssikring (NORSIS), Report, 2019. [Online]. Available: https://norsis.no/norsis-publiserer-rapport-om-nordmenn-og-digital-sikkerhetskultur/.

[72] E. F. Wolstenholme, 'Towards the definition and use of a core set of archetypal structures in system dynamics', *System Dynamics Review*, vol. 19, no. 1, pp. 7–26, 2003, ISSN: 0883-7066. DOI: 10.1002/sdr.259.

Chapter 7

Appendix A - Describing the system in question

Appendix A is to be seen as additional information to the background and related work section and provides additional information about the NHS and its stakeholders.

7.1 Ministry of Health and Care - departments

Table 7.1 illustrate how the NHS, or Ministry of health, can be perceived as a set of departments. By investigating the system as a set of departments one can more easily understand the structure of the NHS in its entirety, as well as the responsibilities of the ministry.

7.2 Stakeholders in the Norwegian Specialist Healthcare

This section serves as additional information regarding stakeholders within the system, as an addition to the presentation of the system under question. The reason for moving table 7.2 and 7.3 is that each individual stakeholder is not individually included in the modelling phase, which rather focus on organizational level. For the sake of striving for a holistic perspective, more stakeholders than the ones initially identified as the primary stakeholders are given, all stakeholders together determine the influence of their organizational level. Moreover, the stakeholders are limited to the ones most relevant for the Norwegian Specialist Health Service. The stakeholders presented are from all main organizational levels (national, national professional, regional and operational). However, most are associated with different functions on the national professional level.

Table 7.1: Ministry of Health and Care - departments

Department	Role and responsibilities
The Department of Public Health	The area of focus is promoting good health, and preventive medicine. Keeping an eye on the populations health registers, nutrition food safety and drug/alcohol use/abuse.
The Department of Specialist Health Care Services	Responsible for financing specialist healthcare services and developing the services in-line with the societal needs.
The Department of Hospital Ownership	Governance over the regional health authorities (RHA) and Norsk helsenett.
The Department of eHealth	Overall responsibility of the digitalization process of the healthcare sector. Has a broad area of responsibilities, covering development and is integral in the cyber security related aspects in digital solutions.
The Department of Health Legislation	Responsible for the law and regulations that applies in HOD area of practice.
The Department of Municipal Health Care Services	Responsible for developing policy measures related to health services administered by the municipalities, also referred to as primary healthcare services.
The Department of Budgetary and Financial Affairs	Works relating to central government funding (statsbudsjett) and has overall responsibility for finance and funding in HOD.
The Department of Administration	Responsible for shared tasks and coordinating HOD, making sure that HOD operate inline with overall goals, objectives, guidelines, law and policy.
The Communications Division	Responsible for communication towards media and other outlets in addition to managing communication during crisis.

Table 7.2: Main Stakeholders and their organizational level and role in the NHS

Stakeholder	Organizational level	Role and responsibility
Ministry of Health and Care Services	National	Strategic responsibility and top-level responsibility for providing the population equal access to health care services. The ministry delegate responsibility for different functions in NHS to subordinate agencies and institutions. In addition, the ministry govern the NHS through legislation and budgeting. [32]
Norwegian directorate of Health	Professional	Mandated by HOD, being a external organization/subordinate agency, its main goal is to improve the nations health through its role as: Professional agency, executor of health and care policy, administrator and interpreter of legislation and executioner of politics. The directory preform a specialist/professional role, between Ministry and Operational/executing levels, thus it guides subordinate departments [66].
Directorate of e-health	Professional	An important national authority, premise setter and enabler of digitalisation and ehealth solutions. Responsible for national management, administration and coordination of ehealth solutions. Influences all of NHS for RHA, municipalities, specialist communities and other health institutions. Develop and follow-up incentives connected to information security and privacy, and holds as directorates often do a professional role.[67]
Regional healthcare authority (RHA)	Regional	Responsible for a given region in Norway, Helse Sør-Øst, Helse Vest, Helse Midt Norge and Helse Nord. RHS's provide the specialist medical services in Norway [68]
Health Trusts	Operational	Hospitals delivering different services, subordinate to one regional healthcare authority.

Table 7.3: Secondary Stakeholders or subordinate entities qualifying for a mention and their organizational level and role in the NHS

Stakeholder	Level	Role and responsibility
Parliament	National	The legislative authority, making laws, determining the state budget and control the government.
Relevant Ministries	Political	Provide strategic guidance for all members of the public, the NHS included. Examples of their influence can be found in governing documents like "One digital public sector" [37], published by the Ministry of Local Government and Modernisation and the "National Cyber Security Strategy for Norway" [38] which is published collectively by "Norwegian Ministries".
Norwegian Healthnet (NHN)	Professional	Overall objective is to enable maintenance and development of ehealth infrastructure, facilitating effective inter/intra stakeholder collaboration. NHN seek to simplify, improving effectiveness and quality of electronic services, to benefit patients, employees and the population at large. Services such as electronic prescription, core journal, basic data (grunndata) and helsenorge.no. [69] [70]
Secretariat for responsible for "Normen"	Professional	"Normen" is an important part of the directorate of ehealth's effort to improve information security across the entire health sector. It is a document seeking to guide cybersecurity and privacy for all stakeholders in the NHS based on current law and regulation. [64][41][40]
HelseCERT	Professional	A national center for information security, a sector of NHN. Main task is to detect, prevent and handle cyber-incidents. Act as a professional actor, spreading IKT-security knowledge of threats and measures and network monitoring.[69] [70]
Cyber advisory companies	National and independent	Several private or state ran, independent from the NHS, advise and conduct tasks related to cyber security and security on behalf of the public interest and exclusively for the NHS, such as threat assessments and risk analyses[43] [45] [46] [71] [44].
Private service providers	National, Regional, Operational, local	The NHS uses many different private service providers for different services, ranging from server operations to health equipment, as the NHS do not have the capacity to deliver all the services it needs.

Chapter 8

Appendix B - Adding to the Theoretic foundation and thesis background

Causal loop modelling After identifying a problem, and justifying it, causal loop modelling can be applied as a first step towards creating a system dynamics model. The main focus is to identify relationships among identified variables and illustrating their behaviour over time through causal loops. Causal loops being a loop containing cause and effect relationships [2]. Causal loops tell a story. Creating stories, or rather presenting actual problems and issues of concern related to the a problem can be the first step towards a holistic system dynamic model.
A hypothetical relationship between team building and team spirit can illustrate a very simple causal loop. When efforts to *Team building* are introduced the *Team building* variable increase, resulting in its related variable *Team spirit* also increasing. The two variables create a *Reinforcing* loop where engaging in team building increase team spirit, increased team spirit prompts more engagement in team building. Effectively meaning that both values will reinforce the other.
Loops can also be *balancing* which are self regulating loops. Given a hypothetical example with variables *security goal gap*, *security investment* and *actual security level* one can say that when *security goal gap* increase so does *security investment*. When the hypothetical business makes a *security investment* the *actual security level* increase, given that the investment was effective. Ultimately meaning that the *security goal gap* decreases again. Balancing itself by closing the gap between actual and desired level of security.

Causal loops follow principles of non-linear cause and effect [26] variables are grouped together to form loops linking the starting variable back to itself. Each loop should tell a story. Causal loop modelling is the most common steppingstone in analysing systems following the systems thinking approach [30]. The causal loop diagram is often much more complex than the single loops presented (8.1) as the model could have connected several different balancing and reinforcing

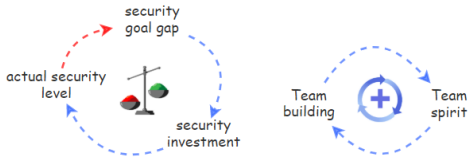

Figure 8.1: Balancing and reinforcing Causal loops. Blue means that the variables change the same direction, red indicate opposite. Some literature use O's and S's and + and - to indicate weather the *link* and variables move in the opposite or same direction.

loops together.

Influence diagrams Adding influences to the causal loop model opens up for a higher level of detail. In addition to mapping the causal loops it enables the modeller to connect un-looped variables that effect variables within the causal loops. The result of applying this method is that one is closer to being able to operationalize the model after the initial modelling phase in completed. For instance, what influences team spirit? Well, lets just assume its the amount of employees present, amount of vacation and satisfaction with the environment. These variables are not necessarily a part of the loop, at least not in this hypothetical scenario, but they enable the modeller to show what influences the team spirit variable. While modelling one can introduce different colours on the links between variables to imply different types of influences.

Stocks and flows Stocks are quantities that change over time as a result of flows. Programming functions and mathematical expressions define the amount of in-flow and out-flow each step in the simulation. The flows incorporate the variables connected to them, which often is based on what connections are conveyed in the causal loop and relationship model. Creating a stock and flow diagram is a part of [30] methodology, and is built and developed from a causal loop model.

System archetypes To help with creating causal loop diagrams there have been created basic general structures, system archetypes. These can be used as a foundation to build upon. Archetypes are modelling structures representing specific dynamics within a system. Archetypes are discussed in many different presentations of system dynamics modelling [2][72]. Wolstenholme [72] reduce previously proposed system archetypes to four general problem/solution archetypes: "Under-achievement, where intended achievement fails to be realised. Out of control, where intended control fails to be realised. Relative achievement, where achievement is only gained at the expense of another. Relative control, where control is

only gained at the expense of others." These system archetypes propose a basic systemic structure to common organisational problems.

Dynamic modelling and simulation System Dynamics (SD) is grounded in System Thinking (ST) and is a natural part of modelling a complex system while adopting the ST-paradigm. SD-models are used to represent, explore and simulate a system and all interactions among system entities, practises, actions, measurements and more. Although, following a system dynamics approach often require one to continuously work on and improve a model until one finally end up with a model which can be simulated. Not always true as some project simply seek to illustrate the model qualitatively rather than continuing on the path to quantifying the model.

The appendix have introduced some of the modelling methods which are used in applying system dynamics to complex systems. Further, related work (2.2) will build an understanding of how system thinking and system dynamics are used in research. After which the simulation and modelling approach (3.2.1) will be described in further detail when the thesis methodology is presented. There are many works applying system dynamics to the realm of cybersecurity, organisational theory and behavioural theory.

Chapter 9

Appendix C - Adding to the methodology section

9.1 Additional explanation of the DSR methodology

Table 9.1 explain each DSR phase and its activities. The table are to be seen in relation to the methodology and can add to the readers understanding of the DSR-methodology.

Table 9.1: DSR-method phases/activity explanations

Activity	Explanation
Explicate Problem	For a problem to be worth researching it has to be important. It must be precisely defined, and it needs to be put in context. Explicating the problem is largely done by discussing theories and perspectives on cybersecurity, healthcare, culture and behavior. Creates the perspective, justifies the research and describes the problem. Which is going to contribute and justify making the artifact.
Defining requirements	Identifying what type of artifact, and what the requirements need to be for the model to answer the explicated problem. It is an outline of the model largely based on descriptive knowledge. Requirements can be structural, environmental and functional. Introduction, background and explicated problem is input to this phase.
Design and develop the artifact	The design and development of the model follows the specified requirements, in terms of non-functional and functional requirements. Information used to model the system are from a variety of sources, including relevant research and documents, theories and methods and other sources of qualitative information collected and analyzed.
Demonstrate	Demonstrate that the model can be used on a real-life case, therefore indicating that it can provide new knowledge about a system. This is also a way of identifying ways to improve and work iteratively with previous phases. The demonstration must focus on the main aim of the thesis, and explain exactly why the case and model works.
Evaluate artifact:	There are several different ways of evaluating a model, depending on the amount of resources available. Theoretically, the model can work in all cases as it is shows to work in the demonstration phase, however this is a weak form of evaluation. Several different use-cases can be demonstrated, and the explored cases and simulations may have known outcomes enabling evaluation of the simulation results. All in-all a tool to evaluate and improve the model.

Jakob Vagle

Investigating Business Alignment Issues Rooted in Cybersecurity Culture

NTNU
Kunnskap for en bedre verden