School of Business, Economics and IT

International Programme in Politics and Economics

Business-Military Collaboration in Sweden: Enhancing Critical Infrastructure Resilience

Authors: Selena Herbold & Tilde Staff

Bachelor's Thesis, 15 HE credits

Thesis Proposal in Political Science

Spring term 2024

Supervisor: Wayne Stephen Coetzee

UNIVERSITY WEST

School of Business, Economics and IT
Division of Law, Economics, Statistics and Politics
SE - 461 86 TROLLHÄTTAN
SWEDEN
Phone +46 (0) 520 22 30 00
www.hv.se

Abstract

The resilience of critical infrastructure is increasingly emphasised due to rising global security threats, such as Russia's invasion of Ukraine. This single-case study examines how business-military collaboration in Sweden enhances critical infrastructure resilience, explicitly analysing how the Swedish government frames these collaborative efforts. Drawing on McNamara's (2012) public management framework, a qualitative content analysis of government and business documents was conducted. Findings reveal extensive collaborative initiatives across various sectors, including food, energy, cybersecurity, and healthcare, highlighting significant interdependencies between public and private entities. Despite these collaborative efforts, challenges such as unclear regulations and guidelines persist, indicating that while collaboration is essential, it alone does not ensure resilience. The study underscores the necessity of clearly defined roles and responsibilities to enhance the effectiveness of these collaborations. The research contributes to understanding organisational resilience in critical infrastructure by elucidating the practical implementation of business-military collaborations and offering insights for policymakers and stakeholders to optimise future strategies and partnerships.

Keywords: Critical Infrastructure, Resilience, Business-Military Collaboration, Collaborative Public Management, Total Defence

Table of Contents

List of Tables and Appendices

1. Introduction

‘We must be realistic and assume – and be prepared for – a drawn-out confrontation that will continue for as long as Russia flagrantly breaches the UN Charter and the European security order’.

Tobias Billström, 2024

In 2015, Sweden’s security approach changed with the readoption of Total Defence, which includes all ‘[...] activities preparing the society for war and consists of both civil and military defence’ (Government Offices of Sweden, 2021). A key aspect of Total Defence is its emphasis on the continuity of society and societal functions (Swedish Civil Contingencies Agency, 2021). This change was first catalysed by Russia’s aggression towards Ukraine in 2014, with tensions having escalated in February 2022 when Russia invaded Ukraine. Hence, as the contemporary geopolitical frictions in Europe intensify, states are increasing their preparedness for potential war. This preparedness includes deterring complex and evolving modern threats, particularly in the form of hybrid warfare (Szymański, 2020). Hybrid threats encompass a combination of military and non-military tactics. Non-military actions can range from subtle disinformation campaigns to targeted disruptions of critical infrastructure (CI) such as energy supply and financial services (EEAS, 2018). Consequently, the North Atlantic Treaty Organisation (NATO), the European Union (EU), and individual European countries are working urgently on making critical infrastructure resilient, recognising the imperative need to enhance the capacity to withstand and recover from unforeseen hybrid warfare disruptions. According to Woods et al. (2006, p.16), resilience refers to ‘the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operation under both expected and unexpected conditions’. Therefore, the resilience of critical infrastructure can be described as a pillar of Total Defence. Since Total Defence is a comprehensive approach to preparing society for war and ensuring societal functions remain intact, the resilience of critical infrastructure is a key component of this strategy. Critical infrastructures ‘[…] maintain the integrity and functionality of modern societies by ensuring the supply of electric power, gas, water, transportation, telecommunication, and other values’ (Sundelius 2006; see Rhinard, 2020, p. 26). By safeguarding critical infrastructure, which is achieved through their resilience, Total Defence upholds societal stability during times of crisis.

To ensure the resilience of critical infrastructure, various actors must work together, including national and local governments, civilians, and businesses. Nevertheless, as the literature review will show, studies have largely neglected to analyse the contribution of businesses to the resilience of critical infrastructure. The oversight of the private sector's involvement is

particularly striking, considering that its participation is essential. This reality is highlighted by Wither's (2020, p.64) illustration that 'NATO reported [...] 90% of its military transport was chartered or requisitioned from the private sector, over 50% of defence satellite communications were reliant on commercial enterprises [...]'. These significant numbers underscore the increasing reliance on the private sector and the interconnectedness between military and civil actors.

An approach that highlights this interconnectedness of actors is collaborative public management (CPM). As defined by McGuire (2006, p. 33), 'CPM is a process aimed at facilitating and operating in multi-organizational arrangements to solve problems that cannot be solved or easily solved by a single organization'. Therefore, CPM highlights the necessity of shared problem-solving and actors to work together to overcome challenges. This is particularly crucial when dealing with complex issues, such as the resilience of critical infrastructure. Within CPM, collaboration is only one aspect of a broader spectrum encompassing coordination and cooperation (McNamara, 2012). Yet, in this study, our focus is narrowed to examining collaborative processes, specifically within the context of organisational resilience. The latter will be explored by addressing the following research question: *How does the Swedish government frame its collaborative efforts with businesses in the context of critical infrastructure resilience?*

To address the research question, the overall structure of the study takes the form of seven chapters. Chapter two presents previous research conducted on Critical Infrastructure, Resilience, and Collaborative Public Management and elaborates on the contributions of our study within the area of organisational resilience in Sweden. Following this, chapter three delves into the theoretical foundations of the thesis and conceptualises relevant terms such as Resilience and Critical Infrastructure. This chapter also introduces the analytical framework, which draws on McNamara's (2012) interorganisational theory. It consists of two categories – design & formality of the agreement (which will be explained in more detail below) and organisational autonomy. These categories guide the empirical analysis and aid in recognising collaborative efforts between civil and military actors within the context of critical infrastructure resilience. Chapter four specifies the research questions and aim, guiding the overall study. The fifth chapter elaborates and explains the data selection and data analysis of this single–case study, including the introduction of the qualitative content analysis method used to answer the research question. Chapter six presents the research findings, and chapter seven summarises and discusses them. Chapter seven concludes by outlining methodological and theoretical weaknesses and potential future research avenues.

2. Literature Review and Contributions

This section will outline scholarships on Societal Security, Critical Infrastructure Resilience, and Collaborative Public Management. Below, an overview of the most relevant literature will be presented, progressing from a broad perspective to a more detailed examination. It will become apparent that current knowledge on critical infrastructure resilience, in particular within the dimension of organisational resilience, is lacking, and thus, this thesis will draw on and contribute to the literature through an understanding of the framing and implementation of business–military collaboration in contributing to the resilience of critical infrastructure in Sweden. This is significant because business actors can shape the state's ability to manage an armed attack or broader societal crisis.

2.1. Societal Security

Societal security is an extensively studied topic in political science that largely surfaced in the 1990s and 2000s when the notion of "what constitutes" security transformed, largely due to the emergence of the Copenhagen School. The Copenhagen School proposed that security encompasses more than just traditional state-centric territorial and military security. Societal security, according to Sundelius (2006; see Rhinard, 2020, p. 26), can be described as '[...] the ability of the government and civil society to function, the necessity to maintain critical infrastructures, for democratic governance to manifest certain basic values, etc.'. This perspective aligns with the view that critical infrastructure encompasses vital societal functions essential for the functioning and resilience of society as a whole. Thus, the Copenhagen school expanded the concept of security and allowed extended preparedness beyond armed attacks to encompass other potential crises, such as a breakdown of critical infrastructure, amongst other things (Larsson & Rhinard, 2020).

However, in Sweden, and the Nordics in general, societal security already played a role during the Cold War due to their Total Defence approach. Total Defence is a security approach (and policy orientation) demanding that 'all functions of society are engaged in the defence effort, both military and civilian' (Sydow, 2018 see Berzina, 2020, p. 12). This approach involves protecting vital societal functions through close collaboration between the government, the private sector, and the general public (Wither, 2020). Sweden moved away from its Total Defence approach for a period after the Cold War. However, the latter sharply changed with Russia's aggression towards Ukraine in 2014. The EU, NATO, and individual European countries reassessed their security approach and decided to focus on enhancing resilience. Consequently, Sweden readopted its once abandoned Total defence approach in 2015 (Wither,

2020). In practical terms, this meant greater involvement of businesses in security-related activities, including collaborations with military actors. Businesses can support military actors with expertise, resources, or infrastructure for national defence efforts (Malmberg et al., 2023). Consequently, business-military collaboration may strengthen Sweden's security and resilience against evolving threats and potential wars.

2.2. Previous Studies on Critical Infrastructure Resilience

The concept of resilience is a state's ability to 'resist and recover from a major shock such as a natural disaster, failure of critical infrastructure or a hybrid or armed attack' (Nato, 2021 see Frizelle, Garey & Kulalic, 2022, p. 525). Our study will pay particular attention to and focus on the "Resilience of Critical Infrastructure", as indicated at the outset of this thesis. However, there is currently no consensus on what constitutes critical infrastructure. Critical infrastructure, as defined by Labaka, Hernantes & Sarriegi (2016, p. 21), '[...] are essential systems for the safety and economic and social welfare of modern society'. In a similar manner Osei–Kye et al. (2023, p. 1210) point out, 'These complex networks are designed to serve and comply with particular social necessities and must withstand time, to maintain the integrity and functionality of modern societies by ensuring the supply of electric power, gas, water, transportation, telecommunication, and other values'. It becomes apparent that critical infrastructures are systems crucial to society, and a breakdown or interruption of one critical infrastructure would most likely cause multiple critical infrastructures to fail, leading to potentially large and unpredictable consequences. Hence, it is in the interests of the state and society to ensure resilient critical infrastructure. Chapter three will delve deeper into the conceptualisation of critical infrastructure. Nonetheless, the existing lack of consensus on this subject reflects on a broader issue arising within the realm of policymaking. This is similarly applicable to resilience. As many scholars have noted, there is no standardised method of measuring resilience (CSS, 2012 see Frizelle, Garey, and Kulalic, 2022; Pursiainen & Kytömaa, 2022; Carlsson & Melander, 2021). The absence of a universally agreed-upon definition and measurement of resilient critical infrastructure poses a significant challenge for policymakers in producing adequate and effective strategies. That said, there is consensus on the three main dimensions of critical infrastructure resilience: societal, organisational, and technological (Pursiainen, 2018). Firstly, key stakeholders within societal resilience include national and local governments, communities, and households. In these contexts, critical infrastructure frequently intersects with conventional civil protection and collectively responds to various challenges that may occur, such as natural disasters. Secondly, in organisational resilience, businesses play a more central role, particularly those tasked with managing critical infrastructure and maintaining essential functions during crises. Lastly, in technological resilience, key stakeholders encompass critical infrastructure and their facility

operators, along with safety and security manufacturers. It is important to note that these features are not always distinct from one another and can, at times, overlap.

In Sweden, the aspect of resilience that has been most extensively studied is the societal dimension. The societal dimension of resilience investigates the efforts of national and local governments and communities to enhance resilience. As an illustration, one study analysed cross-sector resilience among various government agencies in the transportation, energy, and telecommunication sectors (Rydén Sonesson, Johansson & Cedergren, 2021). This study focused on analysing interdependencies by considering collaboration as a crucial factor. It identified that the analysed documents rarely mentioned collaboration. When they addressed it, they often did so in the form of requesting collaboration. This indicates a deficiency in collaborative efforts. Moreover, the study highlighted that government protocols lacked precise instructions, leading to vulnerabilities in existing collaborations and interdependencies among agencies. A way in which this manifests is in information-sharing challenges such as ‘how to identify what information is needed and from whom’ (Rydén Sonesson, Johansson & Cedergren, 2021, p. 6). The authors recommended fostering close collaboration among infrastructure actors to address such challenges. Similarly, Große & Olausson (2019) analysed the interaction of national and local key actors in the process of Steering Electricity to prioritised power consumers (STYREL). Their analysis shows that vague instructions and weak collaboration are blind spots in the system. It's noteworthy that, although this study specifically addresses Critical Infrastructure Protection (CIP) and not resilience, its findings align with those of the previous study discussed above.

The focus on the societal dimension of resilience carries through to other sectors, such as healthcare. Healthcare research has largely focused on societal and to some extent technological aspects due to their more tangible impacts on healthcare infrastructure (Lyng et al, 2022; Carlsson & Melander, 2021). Nevertheless, organisational resilience is recognised within government-owned hospitals, which operate with management structures and systems for service delivery. Carlsson & Melander (2021) investigate this organisational resilience within the healthcare sector and evaluate metrics and indicators at the organisational level. They emphasise how hospitals and healthcare clinics are and can become more prepared for crises. A similar study on organisational resilience in the healthcare sector by Ignatowicz et al. (2023) examines organisational resilience metrics and indicators, emphasising proactive monitoring and planning, effective crisis management, and a commitment to continuous adaptation to enhance preparedness across the healthcare system. The study analyses resilience by considering external and internal factors that contribute to organisational resilience.

A study by Wallnerström et al., (2020) sheds light on the technological dimension of resilience. The study analyses the reliability of energy supply utilising 15 years of power outage data. To do so, the study measures and derives conclusions from data such as outage times and customers not served. Yet, it is important to distinguish between reliability and resilience. Hence, this study can

only be considered as an indicator of what possible technological resilience may entail and not a study of technological resilience itself. Nevertheless, the study is worth mentioning because of its methodological approach, which may serve as a foundation for technological resilience in critical infrastructure sectors such as energy supply, banking systems, and telecommunications.

Adding to the research on technological resilience Cegarra- Navarro et al., (2023) delve into the resilience of the healthcare system, highlighting its dependence on diverse technological components. They emphasise the necessity of conducting a nationwide Risk and Vulnerability Analysis (RVA) as the initial step in utilising technology to mitigate risks, reduce vulnerabilities, and bolster crisis management capabilities. This analysis involves collaboration among municipalities, country councils, administrative boards, and central authorities to ensure a holistic approach. Cegarra-Navarro et al. (2023) also emphasise the importance of collaboration between healthcare organisations, private sector entities, and community organisations in strengthening healthcare resilience. This collaboration involves knowledge sharing, networking, and technological transfer to enhance adaptability, implicitly defined within healthcare antifragility strategies in the face of challenges like the COVID-19 pandemic.

Whilst the dimensions of resilience often overlapped in the aforementioned studies, they did not specifically include the role of private actors in ensuring resilience. Moreover, some of the previously illustrated literature has utilised the idea of collaboration; however, these studies have failed to identify what they mean by collaboration specifically. In contrast, Berndtsson, Obling, & Østensen (2023) acknowledge the importance of private entities and investigate the growing relationship between business and military actors in Norway. Despite their approach not being resilience-focused, the study shows the growing interconnectedness of private and governmental actors through clearly defined concepts of collaboration, cooperation, and coordination. This important conceptual distinction is rooted in Collaborative Public Management (CPM). Our thesis adapts the Collaborative Public management approach to illustrate how business-military collaboration contributes to the resilience of critical infrastructure and thereby to Sweden’s Total Defence.

2.3. Previous Studies on Collaborative Public Management

CPM ‘is a concept that describes the process of facilitating and operating in multiorganizational arrangements to remedy problems that cannot be solved — or solved easily — by single organizations’ (McGuire, 2006, p. 33).

Collaborative Public Management gained popularity because it addresses the limitations of traditional bureaucratic structures of the 20th century and offers new perspectives on public management by underscoring the increasing significance of collaboration (Agranoff & McGuire, 2003). However, opinions on CPM vary among scholars, with some supporting its potential, while others raise concerns about its necessity. Agranoff (2008) underscores the need for collaboration through networks. He assumes networks to serve as the structural foundation upon which collaborative efforts are built. These networks represent interconnected systems of relationships among stakeholders collaborating to address public challenges. He emphasises the importance of understanding network dynamics and employing effective management strategies to achieve successful outcomes. However, not all scholars agree with this inherent need for collaboration. O’Flynn criticises that collaboration is too often seen as the ‘Holy grail’ (2009, p.112) and that its usage should not be a ‘panacea’ (Huxham, 1996 see O’Flynn, 2009, p. 113). In support of this argument, Elston, Bel & Wang (2023) conducted a study on collaborative excess by examining inter-municipal cooperation, a variation of CPM. They find that inter-municipal cooperation in England is often utilised even when there is no interdependency, creating a ‘collaborative excess’ (Elston, Bel & Wang, 2023, p. 1738).

Within the context of resilience and critical infrastructure, there is very little research on CPM. Yet, Nohrstedt (2016) highlights that integrating resilience considerations into collaborative public management practices is essential for promoting proactive and adaptive governance approaches to address emerging threats and challenges. The author examines extreme weather conditions in Sweden, emphasising the substantial government investment in public resources to facilitate and strengthen collaboration between public and societal actors in preparedness and response activities. Moreover, he underscores the importance of assessing outcomes at different levels, the role of individual characteristics in shaping collaborative public management, and the need for an analytical method to evaluate collaborative governance in response to complex problems.

A study by Hicklin et al. (2009) explores Collaborative Public Management within disaster response, which is closely linked to the theme of this thesis. One of the study’s aspects investigates the disaster response of school systems in the aftermath of Hurricanes Katrina and Rita to explore ‘[...] whether wicked-problem shocks in natural disaster settings stimulate or

inhibit collaboration (Hicklin et al., 2009, p.102)'. The study's findings suggest that a larger shock stimulates more collaborative interactions. Therefore, these findings reinforce the central theme of our thesis: the collaboration of business and military actors to enhance the resilience of critical infrastructure and effectively respond to and manage potential shocks.

The central theme of business-military collaborations has notably reemerged within the Nordics due to the readopted and transformed total defence approach, which brought on a new wave of '[…] civilian contractors to support military operations […]' (Berndtsson, Obling & Østensen, 2023, p. 398). Hence, exploring this new wave of business-military collaborations within the context of critical infrastructure resilience, especially in the face of potential conflicts and war, is particularly worthy of our attention.

2.4. Contributions

Our thesis seeks to address a gap identified in the existing literature on resilience in Sweden, specifically focusing on critical infrastructure resilience and the role of private actors, particularly in the context of business-military collaborations. It becomes evident that the overall literature on resilience in Sweden focuses largely on the societal and technological dimensions of resilience, leaving organisational resilience somewhat unexplored.

The Total Defence approach highlights a 'whole of society' (Berndtsson, Obling & Østensen, 2023, p. 397) strategy, emphasising maintaining societal functions during a crisis. However, as the literature review demonstrated, prior research on the resilience of critical infrastructure - a pillar of total defence - has somewhat neglected this 'whole of society' (Berndtsson, Obling & Østensen, 2023, p. 397) approach by leaving the role of businesses underexplored. While it is recognised that various actors work together to ensure the resilience of critical infrastructure and thereby strengthen Total Defence, the mechanism of how they do so remain unclear. Yet, one approach that stands out when dealing with 'wicked problems' (Harmon & Mayer, 1986 see McGuire, 2006, p. 34), such as the resilience of critical infrastructure, is collaborative public management. Thus, our study utilises the CPM approach to provide practical insights into the collaborative efforts between business-military actors within the context of critical infrastructure resilience.

Another consideration for this study is that much of the existing literature focuses narrowly on a specific sector of critical infrastructure such as healthcare, energy supply or transport. This limited focus fails to provide a broader and more general perspective, encompassing all functions

critical to society. Hence, this study will utilise a broad perspective by analysing multiple sectors, primarily cybersecurity, telecommunications, and healthcare. While these sectors will be the main focus, other sectors will also be analysed, although to a lesser extent.

To conclude, this thesis aims to contribute to the growing area of resilience of critical infrastructure and the increasing role of businesses within that context. Through a qualitative content analysis, we will investigate how the collaboration of the Swedish government and businesses is framed in official government documents. Additionally, this thesis will explore how business accounts align with the Swedish government's framing of these collaborative efforts. Understanding the present state of business-military collaboration will help future researchers and policymakers to address and optimise collaborative strategies, partnerships, and mechanisms to strengthen Sweden's critical infrastructure resilience and, thereby, Sweden's Total Defence.

3. Theoretical Approach and Analytical Framework

Critical Infrastructure and Resilience are key terms of this thesis, and their interpretation, as used in our study, requires elaboration. Despite the absence of a consensus regarding its exact definition (as argued above), scholars agree that critical infrastructure is of vital importance to modern society, highlighting its interconnected nature (Osei–Kye et al., 2023; Labaka, Hernantes, & Sarriegi, 2016; Boin & McConnell, 2007). There is no definite definition of what categories constitute critical infrastructure. However, the EU in collaboration with NATO identified prioritised sectors as Energy, Digital Infrastructure, Space and Transport (European Commission, 2023). Critical infrastructure embodies various dimensions and is subject to multiple yet often converging definitions. Thus, our thesis does not confine critical infrastructure to any specific category. Instead, we acknowledge the complexity of critical infrastructure and understand it as a critical and vital aspect of society. Consequently, as we indicated above, the empirical analysis will not be limited to specific categories of CI, such as energy or healthcare.

Resilience is another concept that needs clarification. Firstly, it should be mentioned that resilience differs from Critical Infrastructure Protection (CIP). In contrast to CIP, the resilience of critical infrastructure does not solely focus on protection but also contains elements of absorption and recovery (Pursiainen & Kytömaa, 2023). Hence, the resilience of critical infrastructure assumes that protection may fail and puts emphasis on restoration if unforeseen events, such as crises, take place (Pursiainen, 2018; Florin & Linkov, 2016). Given the intricate nature of its components and its relatively new application to critical infrastructure, resilience lacks a universally standardised definition. However, it is commonly conceptualised as 'the capability of a social system (e.g. an organisation, city, or society) to proactively adapt to and recover from

both expected and unexpected disturbances' (Brasset & Vaughan-Williams, 2015 p. 33). Throughout our study, resilience will be conceptualised according to the aforementioned definition.

Our study is inspired by McNamara's (2012) conceptual framework of Cooperation, Coordination and Collaboration, which draws upon and belongs to the Collaborative Public Management scholarship. This framework serves as a lens to investigate how collaboration is framed in government documents. By drawing from McNamara's framework, our study offers practical insights into collaborative public management and the collaboration between business and military actors in enhancing the resilience of critical infrastructure.

McNamara (2012) describes how so-called 'interorganizational arrangements' can be categorised as cooperation, coordination, and collaboration. Moreover, McNamara (2012, p. 391) explains that these three Cs are 'falling along a continuum of increased interaction'. Cooperation is described as a loosely embedded interorganisational interaction characterised by loose connections and minimal integration, while collaboration involves deeper integration and shared goals. Coordination incorporates elements from both cooperation and collaboration, facilitating effective interaction. Yet, it is essential to note that the effectiveness of an interorganisational arrangement is not predetermined. Rather, selecting a specific type of arrangement should be carefully considered based on its alignment with the intended purpose.

It is important to note that our thesis exclusively focuses on collaboration for two main reasons. Firstly, distinguishing between collaboration, coordination, and cooperation is often challenging. Exploring the three Cs would likely lead to unclear results, which would be based on our interpretation of the empirical analysis. Hence, the external validity of this research would be reduced. To avoid the latter, only collaboration has been selected. As previously mentioned, one interorganisational arrangement is not inherently better than another. However, the utility of interorganisational arrangements differs in different situations. As this study aims to investigate the business-military interactions in contributing to the resilience of critical infrastructure, collaboration is the most useful variation of interactions to adopt. Ensuring the resilience of critical infrastructure is a complex and continuous process involving various actors. Hence, it is logical to conclude that collaboration can support this process more optimally because it is the most deeply interwoven form and long-term approach to 'inter-organizational arrangements' (McNamara, 2012, p. 389). In contrast to cooperation or coordination, collaboration 'require[s] much closer relationships, connections, and resources and even a blurring of the boundaries between organizations' (Keast, Brown, & Mandell, 2007 see McNamara, 2012, p. 391). This is important within the context of the resilience of CI, as it is vital to society that these functions are upheld and managed in times of crisis. This is not to say that cooperation and coordination are irrelevant, but in this study, collaboration is the most suitable perspective to adopt.

McNamara's (2012) theory consists of ten categories (Design, Decision making, Formality of the Agreement, Information sharing, Key personnel, Organisational Autonomy, Resolution of turf issues, Resource Allocation, Systems thinking, and Trust), not all of which are suitable for our case. The following part will briefly discuss why certain sections were not utilised in this thesis. However, not all of them will be debated. This section simply provides an example of what had to be considered while making theoretical choices for this study.

Trust can play an important role in collaboration; however, analysing trust is not suitable for our thesis. Firstly, trust between business-military actors may vary on an individual level. In other words, some actors may trust one another, but others may not. Our thesis will not focus on this individual level but on the overall business-military collaboration. Because of the study's design, exploring the category of trust would inappropriately generalise individual actors' trust and, therefore, reduce the study's internal validity. The category of collaborative Systems thinking, which describes that '[...] information systems are often integrated to enhance linkages between organizations (McNamara, 2012, p. 397), is also not appropriate because public documents this study will investigate do not share such sensitive information. Moreover, if the documents provided information on this, the integration of systems may still vary across businesses, and the results of our empirical analysis would lack internal validity. Hence, only sections of McNamara's (2012) theory that supported our research design and internal validity were incorporated into this thesis.

The following categories, we assert, are suitable and adequate for conducting the empirical analysis:

Design, Formality of the Agreement, and Organisational Autonomy.

Initially, these three categories were explored separately from one another. However, as the research progressed, we wanted to sharpen our analytical tools; hence, we decided to utilise an abductive approach - an interplay between induction and deduction. Due to the process of '[...] thinking about data and theory at the same time' (Schwartz-Shea & Yannow, 2012 see Bryman, 2016 p.109), two categories were merged: Design & Formality of the Agreement. By using an abductive approach where conceptual development and empirical investigation mutually inform each other throughout the research process, we were able to redefine the analytical framework, resulting in more relevant findings.

The category of design refers to 'the administrative structure that supports the collective effort' (Thatcher, 2007 see McNamara, 2012 p. 392). In other words, design can be described as the organisational framework that facilitates business-military efforts. Similarly, the category of formality of the agreement illustrates 'the agreed upon determination of the roles and responsibilities of each participating organization in the collective effort' (Thatcher, 2007 see

McNamara, 2012 p. 393). This means that the formality of the agreement can be defined as a contractual framework that delineates the roles, responsibilities, and obligations of each participating actor. The distinction between design and formality of the agreement is subtle, and in practice, these distinctions are even more nuanced. Therefore, as explained above, we decided to merge these categories to demonstrate them better empirically.

Within the context of business-military collaborations, the design & formality of the agreement suggest that actors work with each other largely because they have a shared interest and a shared responsibility. As previously described, ensuring the resilience of critical infrastructure cannot be achieved by a single actor. Therefore, as the resilience of critical infrastructure relies on the contribution of multiple actors, they are to some extent interdependent. Long-term contracts are put in place to effectively manage this interdependence and uphold the responsibilities and commitments of business and military actors.

Lastly, Organisational Autonomy points out 'how independent each of the partnering organizations operates and how many operating procedures and policies have been adapted to the goals of the interorganizational arrangements' (Thatcher, 2007 see McNamara, 2012 p. 393). Within the setting of collaboration, partnering organisations do not operate in isolation. Instead, decisions are made through collective arrangements. These collective arrangements involve joint decision-making processes where all participating actors have a say. In the context of business-military collaboration, collective arrangements ensure that both actors can effectively utilise their capabilities and resources to independently manage their day-to-day operations while contributing to a larger goal– critical infrastructure resilience (McNamara, 2012). Related to collective arrangements are shared rules that actors jointly establish and adhere to, which govern their collective efforts. Shared rules indicate the extent to which actors are willing to adjust their autonomy to achieve common objectives.

As explained above and mentioned from the outset of this study, we will only focus on the interorganisational arrangement of collaboration. As the collaboration between business and military actors will be explored in Sweden, the analysed material in this thesis is in Swedish. Swedish has no distinct words for collaboration, coordination and cooperation. Often, these terms are combined into one (samverkan/samarbete), and the analysed documents do not define these terms. Nevertheless, as our analytical framework will show, the indicators used to investigate material do not include the word collaboration itself. Rather, we will analyse how collaboration manifests through indicators in design, formality of agreement and organisational autonomy. Whilst we cannot be absolutely sure which form of interorganisational agreement samarbete/samverkan initially refers to, we can still distinguish its design & formality of agreement and organisational autonomy.

To conclude, to explore collaboration, the thesis incorporates two categories from McNamara's (2012) conceptual framework because they are both researchable, suitable for the design of this thesis, and adequate to answer the research question. The next part of this chapter will utilise these two categories and present the analytical framework, which is derived from the broader theoretical discussion above.

3.1. Analytical Framework

The analytical framework will guide the empirical analysis of business-military collaborations in the context of critical infrastructure resilience. It is inspired by McNamara's (2012) conceptual approach and explores collaboration through the Design & Formality of the Agreement, and Organisational Autonomy. While these dimensions or categories of collaboration bear traces of McNamara's framework, they are modified to suit the context of critical infrastructure resilience in our study.

The analytical framework below contains two categories of collaboration. These two categories and their respective indicators have been discussed in the theoretical section above. The categories and their corresponding indicators will be used throughout the empirical analysis, which Chapter Five will explain in more detail.

Table 1: Analytical Framework

Indicators of Collaboration	
Design & Formality of the Agreement	**Organisational Autonomy**
'Interdependence'	'Collective Arrangement'
'Working together'	'Shared rules'
'Shared Interest'	
'Shared responsibility'	
'Long-term contracts'	

4. Research Aim & Question

This study aims to address the current lack of research on organisational resilience by investigating the role of businesses within critical infrastructure sectors. More specifically, our thesis aims to deepen the understanding of business-military collaborations and how such collaboration can contribute to and enhance the resilience of critical infrastructure.

The study will be guided by McNamara's (2012) interorganisational framework to identify collaborative efforts and their degrees across two categories: Design & Formality of the Agreement, and Organisational Autonomy. As the investigated documents largely stem from government sources, the main research question points towards empirically investigating: *How does the Swedish government frame its collaborative efforts with businesses in the context of critical infrastructure resilience?*

To delve deeper into the perspectives of business and military actors, the study will identify how this framing of collaboration is reflected in the experience of business actors. This leads the study to ask the following subsidiary research question: *Does the government's framing of collaboration align with business accounts of collaborative efforts within the context of critical infrastructure resilience?*

5. Research Design & Methodological Approach

This chapter discusses the methodology and methods used to examine business-military collaborations in contributing to the resilience of critical infrastructure. The purpose of this chapter is to clarify why certain research methods were used to collect empirical evidence and how the evidence will be analysed. In conjunction with the theoretical approach and the analytical framework set out previously, this chapter aims to illustrate that the research approach (Qualitative Analysis), the research design (Single Case Study), and the choice of methods (Content Analysis) are well suited to answer the main research question of this thesis. Thus, this chapter covers the important aspects of how the study will be conducted, why it is conducted in the manner it is, and to what extent the chosen methodology and methods allow the study to achieve its stated aims.

The chapter proceeds as follows: Section one discusses the research design, and here, justifications are provided for why the single case study is both useful and preferable for examining business-military collaborations in contributing to the resilience of CI. In section two, the discussion turns to the type of methods used to obtain empirical evidence. It is argued here that the Government Offices of Sweden and the Swedish Civil Contingencies Agency act as the primary data sources of this study during the analysed timeframe from 2015 to 2024, which coincides with the period of Sweden's readoption of Total Defence. Additional data stems primarily from LinkedIn and serves to enhance the practical understanding of government data. Section three explains how the data obtained was analysed to draw conclusions, while section four reflects on aspects regarding research ethics.

5.1. A Single Case Study Design

This investigation takes the form of a single case study to explore how business-military collaboration contributes to the resilience of critical infrastructure in Sweden. By concentrating on a singular case, we gain the advantage of conducting an in-depth examination that allows for a more detailed exploration and analysis. This design choice facilitates a thorough investigation, enabling us to uncover nuanced insights and comprehend the complexities of business-military collaboration within critical infrastructure resilience. Yet, single case studies often have limited generalisability because they are set within a certain context (Halperin & Heath, 2017). While acknowledging the potential limitations of single case studies regarding generalisability, it is

important to note that the selected case study offers insights into broader dynamics relevant to business-military collaboration and critical infrastructure resilience. Additionally, this study utilises concepts of resilience, critical infrastructure, and business-military collaboration that are applicable to other contexts. More specifically, this thesis holds the possibility of analytical generalisation because our framework can serve as a tool in future studies focusing on similar patterns of behaviour and processes. Thus, our study acknowledges the inherently limited generalisation of the research design; however, through key concepts and the analytical framework, this study still holds value for researchers exploring similar contexts (broadly defined), such as municipal collaborations in Sweden. Water supply is a locally managed critical infrastructure sector in which some municipalities rely on others for their water supply (Bendz & Boholm, 2018). Hence, an efficient collaboration between municipalities during critical infrastructure disruption is critical. Moreover, the framework of this thesis applies to business collaborations, for example, within the telecommunication sector. Within the telecommunications sector, collaboration among businesses is particularly relevant as a network of companies collaborates to uphold and manage infrastructure vital for communications networks (Chen et al, 2023). When faced with disruptions in critical infrastructure, for instance, cyberattacks or natural disasters, seamless collaboration among telecommunications companies becomes essential for restoring services swiftly and ensuring resilience.

Furthermore, the relevance of the thesis extends beyond Sweden's borders, encompassing countries such as the Netherlands, Denmark, and Norway. As Coetzee (2020) noted, these countries are mature liberal democracies with relatively large national security architectures and are characterised by neo-corporatist political cultures. After all, state structures and features matter because the type of state provides a framework of action for the actors and their incentives. The generalisation to be derived from comparative investigations into countries such as Sweden, Denmark, Norway, and the Netherlands could be how the degree and type of business-military collaborations contribute to the resilience of CI.

While acknowledging the relevance of comparative studies involving multiple Nordic countries such as Norway, Denmark, and even Finland, our decision to focus solely on Sweden comes from several strategic considerations aligned with our research objectives. Sweden's recent readoption of the Total Defence approach presents a distinct and timely opportunity to investigate the interaction of public and private security actors in a specific national context. The readoption of a security approach and policy that emphasises interaction between governmental, private, and civil actors (Wither, 2020), is an indicator that Sweden has regained interest in strengthening interaction among actors that are responsible for security. By focusing on Sweden, we can thoroughly examine the interplay between governmental and private actors as they collaborate to contribute to critical infrastructure resilience. As mentioned above, a single case design allows for a deeper and more nuanced analysis of the dynamics and complexities inherent in business-military collaboration within Sweden. By focusing on a single case, we can uncover

contextual factors and arrangements in business-military collaborations that contribute to the resilience of critical infrastructure in ways that may not be readily apparent in a comparative study.

Furthermore, Sweden's strategic geopolitical local and regional influence makes it a particularly relevant and illustrative case for understanding the broader dynamics of business-military collaboration with a broader context of critical infrastructure. Situated in Northern Europe and a strategic position bordering the Baltic Sea, it is a region of increasing geopolitical significance due to its proximity to Russia and the dynamics of broader European security. For a long time, Sweden was a non-NATO member situated in close proximity to Russia and had to navigate a delicate balance between maintaining its neutrality (and military non-alignment) and actively participating in regional security collaboration efforts (Forsberg, 2023). This nuanced geopolitical positioning influenced Sweden's military strategy, defence policies, and collaboration between governmental and private actors, making it an interesting and relevant case to examine. In saying all of that, avoiding selection bias in a single case study is nearly impossible. '[...] Selection bias is always likely to be a problem. We cannot eliminate it completely [...]' (Halperin & Heath, 2017, p. 247). However, the case selection in this study was carefully made and is largely based on Sweden's readoption of Total Defence. By examining this case, we aim to uncover strategies and partnerships that contribute to critical infrastructure resilience, fostering theoretical advances and practical applications in the field.

5.2. Data Selection and Collection

The primary research data in this thesis is drawn from two official government sources, the Government Offices of Sweden (Regeringskansliet) and the Swedish Civil Contingencies Agency (Mynidigheten för Samhällskydd och Beredskap (MSB). Additional research data has been obtained from businesses' LinkedIn profiles and corresponding websites.

The Government Offices of Sweden is a central administrative body of the Swedish government and, therefore, contains official government information and policy documents. The Government Offices of Sweden has a crucial role in shaping and implementing national policies, including those related to critical infrastructure resilience and security. Accessing information from the Government Offices of Sweden typically involves navigating its official website, which provides a comprehensive repository of government publications, reports, and other relevant resources. The second official source is the Swedish Civil Contingencies Agency, which is another central administrative authority organised by the Minister of Defence. MSB is tasked with coordinating efforts across government agencies, local municipalities, and private sector entities to mitigate

societal risks (MSB, 2022). Similar to the Government Offices of Sweden's official website, MSB hosts a wealth of data, reports, and guidelines.

These data sources are deemed the most appropriate for addressing the research question because they align with the thesis's objective to illustrate a wide perspective on this topic. Moreover, selecting two different sources supports the 'overall validity' of this study (Halperin & Heath, 2017, p. 19). Data Collection through surveys or interviews could have been more beneficial if the research focused on individual businesses or certain governmental actors. But by drawing from official government sources, we gain access to comprehensive policy documents, reports and strategic plans that provide insights into the formal government position, which reveals overarching strategies and initiatives driving business-military collaboration. Hence, the choice to utilise data from the Government Offices of Sweden and MSB was motivated by the need to capture an overview of business-military collaboration within the context of critical infrastructure resilience.

As this study primarily draws from government data sources, we can only explore one dimension of business-military collaboration in depth. Nevertheless, this information provides important insights because it illustrates the formal government's position on critical infrastructure resilience and collaboration. This will be discussed in more depth in part 5.3. The government data sources contained some business responses towards policy proposals, which will be incorporated into the empirical analysis. Although the inclusion of business responses compared to government data is relatively limited, it supplements the depth of our thesis, offering a brief overview of the business perspective. Initially, we assumed that these data sources would provide a sufficient answer to the research questions, however upon further examination, we observed that the government documents often did not sufficiently display the current state of business-military collaboration and rather portrayed the potential of those. Hence, we made the decision to include additional data, which was mainly gathered from LinkedIn. We limited this additional data to businesses that participated in the Societal Security Conference 2024 (Mötesplats Samhällssäkerhet). We focused on these particular private businesses because they were likely involved in critical infrastructure activities and thus more inclined to have information on collaborative efforts with government actors, if such collaborations existed. To manage the extensive data available on LinkedIn, we primarily focused our data gathering on a time frame from January 2023 to April 2024. While this is a relatively short time frame, it provides insights on the most recent business perceptions of collaboration and hence provides the additional insights necessary to investigate current collaborative efforts. We examined the companies' LinkedIn profiles to observe their current work and collaboration with military actors. However, occasionally, we had to follow up on the businesses' websites to obtain further details on these collaborations. To maintain transparency, all LinkedIn sources cited in this thesis have been added to the reference list, along with the specific links to the relevant LinkedIn posts. In addition to the LinkedIn sources, our data collection process involved cross-referencing

information obtained from government data sources with the perspectives and insights provided by the relevant companies. At times, the cross-referencing included data from a longer time frame, up to three years, when it offered valuable insights into sustained collaborative initiatives. Data from longer time frames was handpicked for relevance, ensuring that only the most relevant information for our thesis was included in the analysis.

The Government Offices of Sweden have divided government policies into several different categories. The category relevant to this thesis is called 'civil defence'. This category relates to Critical Infrastructure and Resilience because it addresses '[...] society's crisis preparedness and the 'safeguarding the most important societal functions' (Government Offices of Sweden, 2024). The civil defence category contains 307 documents in the form of speeches, articles, and press releases dated from the 1st of January 2015 to the 1st of March 2024. The material from MSB has been filtered through the keyword 'Critical Infrastructure'. This category contains 383 documents in the form of reports, policy documents, and guidelines within the same timeframe spanning from the 1st of January 2015 to the 1st of March 2024.

This particular timeframe was selected due to the readoption of Total Defence in 2015. With its inherent acknowledgement of the interaction between private and public actors, the readoption of Total Defence was one of the main motivators for the case selection. Hence, starting our data collection during the readoption year is only logical. By collecting data over a large timeframe, up to March 2024, we can establish a broad overview of the collaboration between business and military actors following the readoption of Total Defence. Selecting this specific timeframe ensures that the analysis covers a period relevant to answering the overarching research question.

As mentioned above, the initial search result yielded 307 documents in various forms from the Government Offices of Sweden. Upon detailed examination, only 135 of these documents are relevant to this thesis. This lower count stems from press releases often summarising the content of other documents. Excluding these summaries will lead to more accurate analysis as it eliminates duplicates. Additionally, the category of 'civil defence' contained some irrelevant content for this thesis, such as supplying other countries with foreign aid or details for press meetings. These materials were also filtered out as they do not contribute to answering the research question and potentially misrepresent the analysis if included. Moreover, MSB's original search resulted in 383 documents under the category 'critical infrastructure', of which 263 were deemed relevant upon translation and review. The less relevant documents focused on international aid efforts and updates on new Swedish legislation, including the Swedish laws related to critical infrastructure. We ultimately found including these laws redundant for our research because investigating Swedish laws would not significantly contribute to our thesis of business-military collaboration and critical infrastructure resilience. Therefore, we made the

choice to exclude those documents and solely focus on material directly relevant to our research aim.

5.3. Method of Data Analysis – Qualitative Content Analysis

A qualitative approach, more specifically content analysis, is employed to conduct the empirical analysis of this thesis. This approach allows us to '[...] expose the meanings, motives, and purposes embedded within the text [...]' (Weber, 1990 see Halperin & Heath, 2017, p. 376). Qualitative content analysis allows us to systematically analyse the material through the categories and indicators established in the analytical framework. They will aid in distinguishing how collaborative efforts in critical infrastructure resilience manifest (Design, Formality of Agreement, Organisational Autonomy) and capture the nuances of collaborative practices in critical infrastructure resilience. With this information, we can describe how formal government policy frames its collaboration with business actors to contribute to the resilience of CI. Moreover, qualitative methods are concerned with internal explanations, focusing on the 'beliefs of actors whose actions comprise the phenomena to be explained' (Halperin & Heath, 2020, p. 51). Hence, analysing official government documents provides internal explanations of how the government approaches and understands critical infrastructure resilience, as well as the significance it attributes collaboration with the business sector holds. As previously mentioned, this thesis primarily explores the government's stance on collaboration, which holds significance as their beliefs ultimately shape policies concerning the resilience of critical infrastructure.

Selecting a quantitative approach to answer the research question would not have been suitable because the research question of this study is inherently descriptive, and concepts such as collaborations are challenging, if not impossible, to define and analyse numerically. Furthermore, determining the frequency of 'collaboration' within the documents would not give a suitable answer to the research question because it cannot illustrate the role of business-military collaboration and their contributions to the resilience of CI. A quantitative approach can also not distinguish between collaborative aspects such as Design & Formality of the Agreement, or Organisational Autonomy. Therefore, a qualitative approach is the most suitable method for the purpose of this research.

Another benefit of using an unobstructive method, such as qualitative content analysis, is the reduction of biases such as the Heisenberg effect. The Heisenberg effect refers to a change in behaviour when under observation (Halperin & Heath, 2017). The documents utilised in the empirical analysis exist independently of our observation, and they are openly accessible to the public.

To conclude, through the carefully selected method, the findings of our study can accurately describe how business-military collaborations enhance and contribute to the resilience of critical infrastructure. We also decided to include various types of documents in the empirical analysis, such as speeches, articles, press releases, directives, guidelines and reports. This decision allows us to widen the dataset and reduce the possibility that only one type of document corresponds to our findings. By avoiding such narrow research, we enhance the validity of our study.

While we initially planned to conduct the coding manually, we have opted to use Nvivo instead. This decision stems from the large amount of material involved in our empirical analysis. Nvivo allows us to work in a more structured and organised manner compared to the manual coding process (Jackson & Bazeley, 2019). Consequently, this approach will likely ensure that material will not be overlooked, thereby enhancing the quality of our study. A criticism of electronic coding systems is that the software largely fragments the data, and that important context might be lost due to this process (Bryman, 2016). This critique however seems only persuasive if the researcher blindly relies on the coding system. Engaging with an electronic coding system rather than just relying on it will still require the researcher to '[…] think and deliberate, generate codes, and reject and replace them with others that were more illuminating and which seemed to explain each phenomenon better' (Basit, 2003, p. 152). In short, we will thoughtfully utilise Nvivo to ensure that the material can be analysed systematically.

The coding process was conducted as follows:

The translated documents were uploaded into the Nvivo System and organised by business view and government perspective. We then executed the closed coding part, which means that the codes are derived from previous research or theory (Halperin & Heath, 2017). Our codes are based on McNamara's (2012) theory and illustrated in the analytical framework. Hence, the analytical framework served as the coding frame of the analysis. We created folders for each indicator from the analytical framework and went through the individual documents one by one, taking particular care to consider the document's context. Hence, some documents contained an abundance of codes present, while others had none. The open coding was done by comparing the codes and by noticing patterns that did not fit within the previously established coding frame.

This combined approach of open and closed coding benefits this study because it systematically analyses documents while maintaining certain flexibility to discover complementary themes. Nevertheless, the reliability of coding is linked to preventing potential obstacles.

Firstly, reproducibility, or in the context of coding, referred to as inter-coding stability, describes that the text should be coded consistently by different coders (Halperin & Heath, 2017). Our analytical framework supports reproducibility because the analytical framework offers precise keywords that can be identified within the text and hence minimises the scope for interpretation.

This also relates to objectivity – the clear categories and coding indicators offer a robust foundation for objectivity and thus contribute to the reliability of the study. The last issue is Intra-coding reliability. Bryman (2016, p. 692) describes this as ‘The degree to which an individual differs over time in the coding of an item'. While we will conduct the coding separately, we will end the process by comparing and developing a common interpretation. This counters the issue of Intra-coding reliability to a certain extent. Therefore, the obstacles related to Inter-coding stability, Objectivity, and Intra-coding reliability are prevented as best as possible through a careful design of the study and the specific approach to the empirical analysis. By avoiding these three obstacles, we ensure that our study is reliable.

5.4. Research Ethics

Interviews and surveys often raise potential ethical issues such as consent and confidentiality (Halperin & Heath, 2017). However, ethical issues are mostly avoided through a content analysis of publicly available documents. Yet, one issue to be addressed is transparency (Halperin & Heath, 2017). As online documents may change or disappear over time, it is important to ensure transparency regarding the timing and content of accessed documents.

Another point of consideration that requires discussion is bias. Halperin & Heath (2017) describe that there are several different types of biases, such as Selection bias, Confirmation bias, Omitted variable bias, and more. Different methodologies come with different biases. But generally, bias can be described as [...] a deliberate attempt either to hide what you have found in your study or to highlight something disproportionately to its true existence' (Halperin & Heath, 2017, p. 180). The previous part of this chapter has already addressed issues applicable to our case, such as Selection bias. A detailed discussion about decisions was provided, and we explained how the empirical analysis was conducted. We believe that these discussions have made this study's decision-making and research process apparent, and biases have largely been avoided. Nevertheless, to further overcome ethical issues as best as possible, a list of all analysed materials will be attached at the end of the thesis as an appendix to ensure transparency and external validity of the research.

6. Analysis: Business-military collaboration in Sweden's critical infrastructure resilience

The analysis carried out in this chapter helps to answer the research questions by explaining the framing of the interorganisational arrangement between business and military actors and its manifestation. Based on the analytical framework set out in Chapter 3, the chapter proceeds as follows:

Section one examines the design & the formality of the agreement of the interorganisational arrangement. Section two of the analysis examines the category of organisational autonomy, suggesting a coordinative structure.

6.1. Design & Formality of Agreement

The unified category, merging McNamara's (2012) design & formality of the agreement within collaborative interorganisational arrangements, presents the shared power structure and contractual frameworks inherent in such collaboration. The indicators discussed below will demonstrate the existence of some shared power structure between business-military actors and explore underlying assumptions for voluntary agreements between public and private entities.

Interdependence

The primary data we analysed displayed the importance of business actors within the critical infrastructure sectors. The interdependence of business-military actors was particularly noticeable, signalling a form of shared power structure.

We observed indications of a shared power structure through, for example, the electricity grid and its shared ownership. Svenska Kraftnät, a state-owned company, maintains and operates the national electricity grid. However, the local and regional grids and their distribution are overseen by many private companies (Ellevio, 2022). In case of a disruption, private and public actors must, therefore, act together to ensure electricity supply. Consequently, the energy sector is particularly interdependent due to its shared ownership. This shared ownership and interdependence grants businesses some power because the government relies on their contributions.

Similarly, shared power is suggested through the government's acknowledgement of its reliance on the business sector and its practice of 'working with [...] private actors on whom the public

sector is particularly dependent' (117S, p. 217). This is not to say that business and military actors necessarily share an equal power structure. The government still holds significant power since it is responsible for policymaking and imposes rules on businesses, which will be demonstrated later. However, the following analysis will also make it apparent that businesses are crucial contributors to critical infrastructure resilience, and collaborative efforts between these actors are essential. Hence, the interdependence and reliance on businesses to contribute suggests a shared but asymmetrical power structure.

Yet, the interdependence of actors expands beyond business-military actors as municipalities, regions, businesses, and voluntary organisations all play vital roles in crisis preparedness and civil defence (105S1). Nevertheless, the role of businesses is particularly highlighted, as the following example shows: 'To a large extent, private actors own and are responsible for many of the most important social functions [...]' (114S, p.130). This quotation and the previous example from the energy sector illustrate that the involvement and contribution of businesses towards critical infrastructure resilience is crucial and that government actors cannot ensure critical infrastructure resilience without the involvement of the private sector.

The business sector holds a similar viewpoint to the government, agreeing on the interdependence of actors. This interdependence is specifically highlighted by their recognition that 'many activities are conducted publicly and privately today. It is important that private enterprises are involved and seen as a resource in efforts to strengthen Sweden's preparedness' (8S2, p.2).

The quotation above highlights one aspect of business-military collaborations well. Due to the shared ownership of critical infrastructure and intertwined relations between private and public actors, businesses see themselves and are seen as an essential resource. Indeed, the government could impose laws on businesses and simply force them to participate in critical infrastructure resilience. However, the analysis will later show that despite existing regulations and rules, there are numerous voluntary initiatives and statements that suggest otherwise. This indicates some underlying assumption about the business sector, which mirrors that of a resource. The business sector is seen as valuable and useful, especially when utilised where its strengths are most applicable.

These examples of interdependence align with Collaborative Public Management theory, which is the basis of McNamara's framework. CPM assumes that addressing 'wicked problems' (Harmon & Mayer, 1986 see McGuire, 2006, p. 34), such as critical infrastructure resilience, requires the involvement of diverse actors. MSB's analysis of collaboration during a crisis similarly expresses this idea: 'When a crisis occurs, a single organization can rarely solve it by itself. Society is intertwined and we depend on each other and that, for example, electricity, electronic communication and transport work even in a crisis' (103T, p.17). Consequently, the

aforementioned example aligns with CPM because it clearly shows that no single entity possesses the resources or capabilities to address complex challenges independently.

Despite the theoretical acknowledgement that complex challenges must be addressed collectively, there are indications that this may fall short of execution. The government highlights the cost-efficiency rationale behind companies' decision not to stockpile, citing it as a vulnerability (128S). Paradoxically, it fails to provide incentives for companies to address the issue of insufficient stock:

> [Our] investigation has […] considered various proposals that could increase the incentives, e.g. protection against qualified cyber attacks, prioritised electricity supply, various financial incentives, the introduction of an official designation for involvement in total defence, etc., but [we have] chosen not to proceed with these (118S, p.14).

If the government is committed to strengthening collaborative efforts, particularly regarding businesses' capabilities, it could offer funding and incentives. While municipalities, regions and government authorities have received funding, no support for companies is mentioned (7S). This example illustrates the challenge of acknowledging a vulnerability in theory but only addressing it to a limited extent in reality. The struggle of theory versus reality is a recurring theme within the analysis and will be discussed throughout the remaining sections of this chapter.

Working together

'Working together' is one of the most prevalent indicators, showing a variety of ways through which businesses and military actors collaborate.

The government bill on Total Defence 2021-2025 highlights a growing interest for businesses to take on important roles in protecting societal functions (118S). A new initiative that came into action in 2023 is the Total Defence Business Council. The council's purpose is to '[...] advise the government on total defence matters and to be a forum for information exchange between the Government Office, relevant authorities and businesses' (118S, p. 167). The council represents different business sectors and has met quarterly throughout 2023. It demonstrates that businesses and government work alongside each other and that businesses act as advisors, offering guidance and information. This collaborative effort, spanning from government down to smaller municipalities and private actors, highlights the significance of effective communication, information sharing and working together. MSB's annual report (79T) states that the goal of collaboration is to ensure that all involved parties thoroughly grasp the current challenges and requirements. This idea is echoed in the statement that both '[…] private actors and government

officials need to share information and experiences with each other both in normal situations and in crises' (115T, p.16).

An example of sharing information and expertise is a joint study by Blackthorn, AquaNoble and the Swedish National Food Agency, who collaborated to create a comprehensive overview and understanding of food supply. Their study analyses how companies can adapt food production levels during times of crisis, thereby addressing the collective need for preparedness (Blackthorn AB, 2024). The value of such an analysis is likely enhanced by having experts from different fields, and thus, it offers an example of how government actors work with and utilise the expertise of businesses.

Within collaborative interorganisational arrangements, the formality of the agreement is both informal and formal (McNamara, 2012). The formal part of the agreement will become evident later on through the indicator ‘long-term contracts’. Yet, our analysis has identified several collaborative efforts based on voluntary agreements. These examples include voluntary forums such as conferences, which serve to exchange information. One of these conferences is the Åre Business Forum. The conference is organised by private actors and includes activities such as networking, workshops, talks and panel discussions. This latest panel discussion concerned companies' contribution to defence issues, with MW Group, a defence company, and the Swedish Armed Forces Research Chief participating. They addressed topics such as ‘Civil-military synergies - innovation, defence and growth’ (MW Group, 2024). Therefore, this year's topic aligns with the core assumption of our thesis: that the collaborative efforts of business and military actors are essential for contributing to total defence, including the resilience of critical infrastructure. Moreover, the conference is an example of business-military collaborations and how exchanging ideas, and information is a key part of their collaborative efforts. However, it is surprising that this event is not organised collectively. To strengthen collaboration and the work of business-military actors, it seems logical to jointly develop events and other initiatives to ensure that both actors can represent their interests accordingly.

During the analysis, two critical infrastructure sectors stood out for their degree of collaboration: cybersecurity and healthcare. Firstly, in the realm of cybersecurity, collaboration has undergone a notable transformation. Historically, the Swedish government held exclusive access to certain information, leaving private actors dependent on government data. However, with the number of IT incident reports increasing since 2016, there has been a growing recognition of the need for closer collaboration between the public and private sectors (93T, p.23). For instance, the government and private actors are increasingly pooling resources and expertise to combat cyber threats. One example is the formation of the Cybersecurity Council (Cybersäkerhets rådet), which is a task force composed of government cybersecurity experts and private sector specialists. The task force works together to analyse emerging threats, share intelligence, and develop coordinated responses (129T, p. 32). By leveraging the unique strengths of each sector,

these collaborations have shown promising results in bolstering Sweden's cyber resilience and minimising the impact of IT incidents, as the following excerpt demonstrates:

> Those of us who work in the cybersecurity industry are currently in the middle of a shift. In the past, everything has been about protecting information and keeping things secret. To keep the cards close to your body and build your own solutions. Now the big word that is manifesting everywhere is collaboration. (Expisoft, 2024)

Although achieving a zero-incident vision may be unrealistic, collaborative efforts between diverse stakeholders offer the best chance to mitigate cybersecurity risk and safeguard critical infrastructure.

Secondly, the sector of healthcare stood out because of its current collaboration, but also because of its request to strengthen collaborative efforts. A government investigation into the resilience of the healthcare sector provides evidence that private-public collaboration must be strengthened:

> It is therefore imperative that municipalities and regions can involve the private actors right from the start in total defence planning. It is not effective for all municipalities and regions to resolve on their own the question of how they should agree with private actors on participation in the total defence [...] (117S, p. 134).

The request for private actors to be involved 'from the start' highlights the inherent need for businesses to participate and contribute to the planning and execution processes. Additionally, it indicates that other actors benefit from working together with businesses. One example of how private actors are and can be further involved within the healthcare sector is the partnership between Medicsolution and Karlskoga Hospital. Medicsolution has created modular facilities that can, for example, serve as operating rooms, as it does in the case of Karlskoga Hospital (MedicSolution, 2015). In times of increased demand, hospitals facing capacity constraints can leverage Medicsolutions' facilities. These units can be transported to various locations supporting hospital capacity with equivalent equipment. During crisis times, this flexibility and additional capacity can become particularly useful and strengthen the resilience of the healthcare sector. The latter shows how innovative ideas can create collaboration and, therefore, contribute to the resilience of critical infrastructure.

Shared interest

The above-mentioned voluntary agreements and the expressed 'common interest' (118S, p.107) suggest that businesses collaborate with the government, driven by a shared interest in making critical infrastructure resilient. This is reinforced by '[...] private-public collaborations are characterised by the fact that they are voluntary based on a common and shared interest of the

participating actors' (118S, p. 107) and '[...] there is an interest in a strong Swedish defence among Swedish companies [...]' (118S, p. 131).

The conference on societal security (Möteplats Samhällssäkerhet) is an example of the interest that business and military actors share. The conference was established in 2015, which aligns with the readoption of Sweden's total defence policy. The conference aims to exchange ideas, exhibit products, and facilitate networking. This exemplifies shared interest because a significant number of participants make an effort to gather during this two-day event alongside important political figures such as the General Director of MSB and the Logistic Manager of the Swedish Armed Forces (Mötesplats Samhällssäkerhet, 2024).

An additional illustration of shared interest is evident in the healthcare sector, particularly highlighted during the COVID-19 pandemic. COVID-19 provided practical insights into the collaborative efforts between government and private actors. MSB noted that many private companies were not legally bound to support the government's crisis management but did so voluntarily (114T). For example, private logistics companies like DHL played a crucial part in ensuring the efficient distribution of medical supplies and equipment nationwide. DHL Sweden collaborated closely with government agencies and healthcare providers to expedite the delivery of critical supplies to healthcare facilities and vulnerable communities (DHL, 2022). The company utilised its extensive network of distribution centres, warehouses, and transportation vehicles to streamline the movement of goods and overcome logistical challenges posed by the crisis.

Another example of business actors shared interest in collaboration and contributing is the case of Amexci, a company specialising in Additive Manufacturing. During the COVID-19 pandemic, the company produced protective healthcare masks using 3D printers to counter a shortage in supply (Doc59S). That said, it must be acknowledged that the company likely gained financial profit from producing the masks. Nevertheless, it illustrates companies' role in contributing to and demonstrating their commitment to aiding in emergencies. Furthermore, this case exemplifies the government's aspiration to engage private actors in collaborative efforts. As outlined in the strategic orientation for defence innovation, the government seeks 'Military risks, problems, and defence needs to [be] addressed by a broader range of actors in society'. By collaborating the government assumes, similar to the assumption of this study that collaboration 'provides opportunities to accelerate and mutually strengthen Sweden's defence capability, resilience, and innovation power'. (17S, p.5).

The previous example aligns with the broader trend observed by the government during the pandemic, where notable collaborations between the healthcare sector and private actors in several different sectors, such as logistics and transportation, development, and manufacturing, took place (262T, p. 48). GrantThornton, a global professional service network with expertise in

risk management, underscores the importance of collaboration and mutual understanding in fortifying healthcare resilience. They emphasise the need for sustained engagement to maintain the positive impact of collaborative initiatives, advocating for continuous collaboration and dialogue:

> [...] to ensure that the beneficial collaboration effect created during the pandemic is maintained, continuous collaboration and dialogue are required. This may include ongoing collaborative projects at both strategic and operational levels, continuous dialogue and communication, as well as the creation of a common strategy for how healthcare (regardless of organizational form) should work to continuously improve patient care (GrantThornton, 2021, p.17).

A practical illustration of such collaboration was the partnership between Karolinska Hospital and the private hospital Capio, which formed a strong alliance to address the challenges posed by the pandemic. Karolinska and Capio worked hand-in-hand to ensure the continuity of essential healthcare services while responding to the surge in patient volumes (Karolinska institutet, 2021). This collaboration went beyond mere resource-sharing; it exemplified a deep mutual understanding of one goal: safeguarding public health and providing optimal patient care. Both hospitals engaged in joint decision-making processes, with both parties contributing their respective expertise and insights. They developed strategies for managing patient flow and staffing problems, allocating resources, and implementing infection control measures.

Furthermore, as mentioned in the indicator above, government agencies and private actors collaborate closely in cybersecurity, indicating a shared interest. Government and private actors have increasingly prioritised their work in cybersecurity over the past decade. Private actors, such as cybersecurity firms and technology companies, are indispensable in enhancing Sweden's capacity to defend against cyberattacks and other IT incidents (129T). Private actors often possess specialised expertise and resources that complement government efforts in cybersecurity. For instance, Ericsson has partnered with government agencies to develop advanced cybersecurity solutions and provide expertise in threat detection and incident response. Ericsson, a global leader in telecommunications, has contributed to Sweden's national cybersecurity strategy by offering advanced network security solutions and collaborating with government agencies to strengthen critical infrastructure defences. On the other hand, the government ensures that the private sector is supported by implementing initiatives to foster private-public collaboration in the information and cybersecurity realm (130T, p. 23).

Almega, an organisation encompassing many companies from different sectors, highlights the shared interest by stating that companies are generally willing to contribute and support Sweden's security (8S2). This willingness and interest from businesses and government actors was largely illustrated through joint initiatives. However, businesses also contribute to critical infrastructure resilience and collaboration independently. An example of this is Combitech's total

defence game. Combitech, a technology consulting firm specialising in defence and security, has developed this tool that allows players, such as companies, to play out different crisis scenarios and aims to enhance preparedness (Combitech, 2024). Additionally, companies take the initiative to engage in knowledge exchanges by hosting meetings and seminars and inviting political figures to exchange ideas and insights. For instance, 4C Strategies hosted a seminar and invited the Chief of Defence to participate (4C Strategies, 2024).

Through these collaborative endeavours, both businesses and government entities aim to tackle challenges comprehensively, with both parties recognising that collaboration can contribute to the resilience of critical infrastructure. Hence, actors understand that certain activities or initiatives should not be solely managed by private or public actors alone:

> [...] The companies cannot and should not run this themselves, we need to do this jointly with the public sphere where they make demands, and we develop the concept further together. There is enormous power in everyone working together and because we have a unique industrial base from it, [...] (103T, p19).

The above is in line with Saab's reasoning to collaborate with public actors, a Swedish aerospace and defence company that asserts that collaboration between public authorities and private companies is both beneficial and essential. Saab is a significant actor within the Swedish military complex that advocates for collaborative efforts, recognising them as the most effective and cost-efficient approach, benefiting both the company and society at large (Saab, 2021). Another example is the National Telecommunication Collaborative Group (NTSG), which is overseen by the Mail and Telecommunications Board (PTS) and serves as a voluntary forum for collaboration within the telecommunications sector. By actively participating in NTSG, businesses and public authorities demonstrate their commitment to mitigating disruptions that could affect both their operations and the broader national infrastructure (224T). The significance of NTSG as a platform for collaboration is underscored by numerous respondents who affirm its role in enabling unified action among stakeholders (225T). This collaborative space ensures that private companies and public authorities can freely exchange information and expertise without exploitation concerns. Regular meetings within this forum further cultivate collaboration and strengthen participant relations. NTSG plays a crucial role in facilitating the seamless sharing of information among member organisations, empowering them to swiftly assess the impact of disruptions and effective response efforts (PTS, 2023). Through NTSG, businesses and public authorities are equipped to navigate challenges collectively and safeguard the resilience of critical telecommunications infrastructure.

The examples above highlight that government actors and businesses share an interest in collaborating with one another and share the idea of making critical infrastructure resilient. Moreover, the examples showed a mutual commitment, which is further reflected in the wish for

‘clear commitments both from the state to the companies and from the companies to the state’ (8S2, p.2).

Shared responsibility

It is evident that the government carries the largest part of the responsibility to ensure critical infrastructure is resilient in Sweden. However, the government shares its responsibility with other actors, including businesses. This is often called the principle of responsibility, meaning each actor remains responsible for its function and readiness during peace and crisis (128S).

Despite the government’s overarching responsibility for ensuring the resilience of critical infrastructure, collaboration with private businesses is essential. Private companies carry a substantial responsibility for maintaining functional telecommunication networks during crises, such as natural disasters, cyberattacks or even war (222T. p 32). For instance, during a severe storm that caused widespread damage to infrastructure, private telecommunications companies collaborated closely with government agencies responsible for disaster response. Together, they mobilised resources, deployed emergency crews and swiftly mobilised their resources to restore connectivity. While private companies focus on repairing damaged infrastructure and establishing temporary communication solutions, government agencies provide support through regulatory assistance, logistical coordination, and access to critical resources. Considering the critical role of telecommunication infrastructure in sustaining communication networks during both peaceful periods and crises, it’s evident that the government invests in building and maintaining a robust telecommunications backbone (239T).

As discussed above, the energy sector in Sweden is very interdependent. Hence, private and public actors have a shared responsibility within this sector to ensure the resilience of critical infrastructure. Ellevio, a large private electricity business, has increased its security initiatives such as cybersecurity exercises and ‘[...] several crisis and continuity training sessions together with contractors and other key stakeholders [...] (Ellevio, 2023, p. 93)’ Moreover, the company has increased its security protection and preparedness to be able to ‘strengthen its ability to resist antagonistic influence’ (Ellevio, 2023, p. 12). In pursuit of this aim, Ellevio works together with other actors in the energy sector and authorities. These insights into Ellevio’s work highlight a shared responsibility and demonstrate that private businesses take collaborative efforts and the resilience of critical infrastructure seriously.

To effectively manage this shared responsibility, the government has appointed MSB as a designated point of contact for the business sector regarding supply preparedness (8S13). This provides some clarity for the business sector about whom to contact and engage with within this specific area. However, it’s important to note that this designation only applies to supply preparedness. Despite this and the intention for roles and responsibilities to be shared, there are times when the specifics are lacking, making it difficult to turn into actionable reality. The

government highlights this gap by stating, ‘Cyber security is a responsibility for both public and private actors at national, regional and local level’ (S24, p. 24). Yet, the National Cyber Security Centre, established in 2020, remains a forum for collaboration among government authorities (Nationellt cybersäkerhetscenter, 2023). Hence, presently excluding private actors to share responsibility and knowledge. That said, they occasionally organise conferences for private and public actors, and their goal is to ‘expand our operations to also include collaboration and information exchange with private and public actors in the field of cybersecurity’ (Nationellt cybersäkerhetscenter, 2023).

The government documents and the NSCE goals show a desire for shared responsibility, but the translation into practice falls short at times. Having responsibility but lacking instructions and inclusion to fully take on and manage this responsibility results in an issue for companies.

Long term contracts

Previously, this chapter discussed informal arrangements between business and military actors. Hence, the sections on long-term contracts will now provide insights into the formal aspects of the agreement. The present situation concerning contracts and agreements between business-military actors is lacking clarity. Finding specific information on what contracts and agreements between business-military actors entail has been challenging. This may not have been published within the analysed documents, or these details may not have been fully established. Evidence for the latter can be found in the defence committees' assessment and planning of Resilience 2021-2025, which states that:

> State authorities, county administrations and municipalities must, in collaboration with private actors, plan how companies will be able to contribute and deliver goods and services in the event of more serious disruptions in peacetime or war. As part of this planning, contracts and agreements need to be concluded between the public and private actors concerned. It then also needs to be determined how the costs of these agreements are to be financed (128S, p.139).

The assessment above describes contracts and agreements that will be part of the business-military collaboration; however, any further details are missing. An illustration of what contracts between business and military actors may entail can be seen in the partnership of Volvo, Scania and the Swedish Armed Forces. In 2022, Scania and Volvo provided the Swedish Armed Forces with new 487 vehicles worth about 700 million kronor (Försvarmakten, 2021). Additionally, Volvo has recently signed a 7-year contract to supply the Swedish Armed Forces with machines. Similarly, the Swedish Defence Materiel Administration (FMV) has signed an agreement to purchase a decontamination solution from MW Group, a Nordic defence and security services

provider, to support continuity during contamination in several critical infrastructure sectors (MW Group, nd). Another example of contracts between business and military actors is the city of Västerås purchasing a 10-day food supply for 45,000 residents from Outmeals (Combitech, 2024). These examples show the active participation of businesses within critical infrastructure sectors, in these cases, as suppliers. Almega stresses the particular importance of long-term contracts because they can facilitate 'sustainable preparedness' (8S2, p.3).

Within the context of long-term contracts, a special category of companies emerged – those deemed essential for wartime operations. The government aims to investigate which companies fall into this category and refers to those as K-companies. 'A company approved as war-essential demonstrates through long-term commitment and maintenance of deliveries its responsibility and participation in both civil and military defence' (123S, pp. 277-278). It's important to note that there likely is a large overlap of companies important for war and critical infrastructure such as energy and food supply. However, it seems rather difficult to establish which companies are important in war. Many companies rely on other companies, for instance, for their supply. Therefore, it should not be a single war-relevant company but an entire chain of companies. Additionally, this chain of companies is likely to operate transnationally. Hence, there must be clarity on international supply and business interdependence during crisis times. Indeed, the government mentions these issues, but no clarifications or solutions are specified.

> Globalization has meant that infrastructure systems and supply flows of goods and services have been interconnected with other countries to a greater extent than before. Within society, there is in turn a mutual dependence between different sectors. Most areas are dependent on access to electricity, IT and electronic communications, transport infrastructure, fuel, supplies, financial services, etc. If disruptions occur within one sector, it also affects other sectors. The majority of these areas do not have extensive redundancy but require undisturbed flows for the business to function. However, an undisturbed flow of goods and services both within the country and from other countries will probably not be able to be maintained during war or threat of war. A disruption or interruption in supply flows can thus affect large parts of society (128S, p. 44).

The business sector shares this concern and emphasises the fragmentation and internationalisation of the sectors and warns the government that 'this [fragmentation] results in individual companies struggling to fulfil their obligations concerning preparedness without analysing and ensuring the entire value chain' (8S2, p.2).

6.2. Organisational Autonomy

The last category of our analysis is Organisational Autonomy. It is the first to partly indicate a non-collaborative structure between business and military actors. In collaborative arrangements, actors jointly establish the rules and framework governing their actions. However, as the empirical investigation has revealed, it is mainly the government that imposes policies upon business actors. According to McNamara (2012), if policies governing the arrangement are made by higher authority, it indicates a coordinative structure between private and state actors.

Collective Arrangement

To manage critical infrastructure resilience and the interorganisational arrangements within that context, the Swedish government is considering mandating businesses to participate, rather than relying on collaboration, as previous parts of the analysis indicated.

> Possibilities that can be considered are to set requirements in legislation for private actors to take measures to increase their ability to maintain functionality in the event of disturbances, to have the ability to cooperate and the obligation to contribute to the work of the authorities during disturbances. Such requirements could be combined with one or more authorities being empowered with prescriptive rights and responsibility for supervision and support. A further consideration could be to introduce contingency fees for the private actors in the transport sector in order to use these funds to finance measures that increase the sector's ability to withstand and manage disruptions (128S, p.179)

The excerpt above highlights that the government makes policies governing the collective arrangement without consulting the business sector. As described above, this points to a coordinative structure. The argument aligns with the defence committee's recommendation to create policies requiring private fuel operators to stockpile fuel (114S). However, this result conflicts with the previous section discussing voluntary agreements. Businesses seem to collaborate voluntarily, but the government still wants to impose rules to force those who may not do so. This stance is further supported by '[...] there are already regulations that mean that all businesses can be obliged to participate in total defence planning' (47S, p.32).

Imposing legislation and regulations on business actors, despite businesses voluntarily collaborating, as was demonstrated above, could indicate that such a coordinative structure serves as a safety net due to a lack of trust. Our thesis does not explore the category of trust, but it might be useful to explore how trust shapes inter-organisational structures, which will be

discussed further in the following chapter. Moreover, it is not entirely surprising that the 'collective arrangement' indicator suggests a coordinative structure, given that the government is responsible for creating policies. Yet, there could be closer collaboration and discussion with businesses on how to create more feasible policies. Consulting with the business sector may also help address concerns raised by private actors. Private actors have highlighted '[...] unnecessary uncertainty about responsibilities and roles in the event of a crisis (8S1, pp. 2-3)', and have specifically pointed out a preparedness proposal that is 'perceived as unclear and risks requiring significant resources from companies' (8S7, p.2).

Shared rules

In line with a more coordinative structure is the indicator of shared rules. In 2018, the defence committee assessed that '[...] existing regulations should be the starting point for the dialogue between public and private actors in the preparedness planning [...] the regulatory framework may need to be revised in order for the state to be able to impose requirements on private actors' (126S, p.6). The latter example points to a hierarchical structure and seems to leave little room for collaboration and exchanging ideas around creating rules. Interestingly, the firm tone of imposing rules softened over time. In 2020, the defence committee suggested '[...] that at the local level, municipalities together with private actors need to agree on and conclude agreements' (114S, p. 144). The committee further assesses that information on existing rules should be spread (114S). The Business Council for Total Defence, established in 2023, provides further indication for a more inclusive approach, potentially indicating that the coordinative structure shifted towards more collaboration over time.

As demonstrated above, organisational autonomy leans more towards a coordinative structure, yet the other discussed categories contradict this by indicating a collaborative approach. Overall, the analysed indicators demonstrated various collaborative efforts, although in varying degrees. Nevertheless, these collaborative efforts highlight that business-military collaboration is essential in enhancing and contributing to the resilience of critical infrastructure. This is largely because the actor's work is interdependent, and a joint approach optimises the process of strengthening resilience. Nevertheless, there are unclarified issues on responsibilities and contracts that hinder an optimal collaboration between business-military actors. If the government is serious about strengthening business-military collaborations and therefore the resilience of CI, it must address the unresolved issues and uphold its assertions: 'Civil defence is not primarily a seminar exercise. Awareness must be translated into practical action' (19S).

7. Conclusion

This concluding chapter covers three main points. First, it briefly reviews business-military collaboration and reflects on how the research questions have been answered. Secondly, we reflect on the methodological and theoretical limitations of our study. Finally, we outline the wider implications of our findings and identify future research avenues.

7.1. Business-military Collaborations

This thesis aimed to investigate the role of businesses within critical infrastructure sectors and to deepen an understanding of how business-military collaboration enhances and contributes to the resilience of critical infrastructure. To achieve this, the thesis explored two key questions: *How does the Swedish government frame its collaborative efforts with businesses in the context of critical infrastructure resilience?* and *Does the government's framing of collaboration align with business accounts of collaborative efforts within the context of critical infrastructure resilience?*

The first and overarching answer to the research questions is that business-military collaborations are framed as essential contributors to critical infrastructure resilience. The implementation of current business-military collaborative efforts within critical infrastructure sectors, ranging from food supply, energy supply, and cyber security to healthcare, confirm this, although the collaborations vary in degrees. The energy sector is a prime example of interdependence, highlighting the necessity for collaboration between private and public actors to contribute to critical infrastructure resilience. Moreover, the growing collaboration between public and private sectors in technology and innovation underscores an important example of the effectiveness of business-military collaboration. Strong collaborative efforts were observed within the cybersecurity sector to develop and deploy advanced technologies, improve response capabilities, and mitigate emerging threats. Secondly, businesses serve as suppliers for military actors, as seen in Volvo and Scania, MW Group and Outmeals. These long-term arrangements align with a collaborative structure and allow actors to create a sustainable preparedness, which is particularly highlighted by the business sector. The analysed government documents, however, do not indicate the specifics of contracts between private and public actors. It is important to clarify the obligations and details of such contracts to ensure the current issues around clarity and responsibility are addressed. The current collaborations also reach beyond a simple supply

function, focusing on expertise and knowledge sharing. This became evident through the Business Council for Total Defence, offering a forum for exchange and voluntary conferences and seminars organised by business and military actors. These initiatives illustrate that the actors share an interest in collaboration and critical infrastructure resilience. A compelling illustration of collaborative effort unfolded in the healthcare sector during the Covid-19 pandemic. Both business and public entities rallied together, driven by a shared interest to combat the crisis. The Swedish healthcare system navigated the challenges through collaborative information and expertise-sharing efforts. Additionally, the results suggest that businesses view themselves and are seen by the government as an essential resource for critical infrastructure resilience. They actively engage in various efforts to strengthen preparedness to mitigate risks and ensure continuity during crises, especially in the most suitable areas. Moreover, businesses create initiatives such as hosting meetings and developing innovative solutions like total defence games. Through proactive measures, they underscore the recognition of their role as a key stakeholder. Nevertheless, the private sector is sometimes left out for no apparent reason, as in the example of the National Cyber Security Centre. Another finding of this thesis is that business-military collaborations would benefit from more precise rules and regulations. There seem to be many unclarified issues that need addressing if a strong collaboration is to prevail in times of critical infrastructure disruption. These issues include unclear proposals and tasks for the business sector, establishment of incentives and precise division of responsibilities. Such clarifications should be made during peacetime and as soon as possible to ensure that collaboration runs smoothly. Considering these unclarified issues, it is important to question how Total Defence in practice supports the pillar of the resilience of critical infrastructure. There appears to be a theoretical lack of understanding of what total defence means for the resilience of critical infrastructure and, even more so, how it can be operationalised. This gap needs to be addressed by policy-makers if total defence is to become truly ‘total’ and effectively uphold its aim of maintaining societal functions during crisis time.

Addressing these issues is crucial because collaborative efforts are important in ensuring that actors can act swiftly, decisively, and in a structured manner during a disturbance of CI or war. However, it is important to note that observing and reporting on collaborative efforts do not actually prove resilience; rather, they provide insights into how business-military collaborations aim to achieve resilience. Nevertheless, by observing collaborative efforts, we can investigate the underlying elements of critical infrastructure resilience and make the concept of resilience a bit more tangible.

As mentioned in the literature review, previous studies by Große & Olausson (2019) and Rydén Sonesson, Johansson & Cedergren (2021) found that actors encounter challenges due to insufficient information and procedures. We have shown that this issue also arises within business-military collaborations regarding critical infrastructure in Sweden. Additionally, our

study showed that great emphasis is placed on improving this issue through information exchange at conferences, seminars, and council meetings, though with limited success.

Furthermore, our study found similar results to those conducted by Berndtsson, Obling, & Østensen (2023), which investigated business-military relationships in Norway and found an increasing interconnectedness among business and military actors. Their study also highlighted the difficulty of managing interorganisational arrangements. This is something we have partially seen. For example, through the unclear proposals and the complexity of determining K-companies. However, some parts of the collaboration seem to be running smoothly, such as the shared responsibility within the energy sector.

7.2. Methodological & Theoretical Limitations

Two methodological limitations emerged during the empirical analysis. Firstly, the heavy reliance on government documents often failed to provide precise examples of how current business-military collaboration is conducted. The analysed government documents contained useful information, but often this information described an ideal world rather than reality. Future research should therefore refer to businesses for their data gathering to find tangible examples of how current business-military collaborations are implemented. To balance the theoretical knowledge from government documents, we incorporated additional perspectives from businesses using LinkedIn data. Given the extensive amount of available data, we focused on a specific timeframe, from January 2023 to April 2024. This limitation may affect the study's external validity, as only a fraction of the business-military collaborations existing since 2015 have been included. Nevertheless, this limited time frame provides a snapshot of the most recent business accounts of collaborative efforts with the Swedish government. Moreover, we encountered a limitation linked to the theoretical framework. Overall, McNamara's theory was useful in exploring the interorganisational structure of business and military actors and allowed us to demonstrate degrees of collaboration. However, it was sometimes difficult to differentiate between similar indicators and categories. Consequently, as previously explained, our investigation utilised an abductive approach, allowing us to redefine our analytical tool, resulting in sharper and more relevant findings. Despite this, the currently available framework for analysing collaboration often lacks clear definitions of empirical differences, and therefore, the results are of limited clarity and the reliability of our study may be impacted. Yet, given the constraints of this framework, it represents the most feasible outcome current research can achieve.

7.3. Wider Implications & Future Research Avenues

This thesis solely focused on business-military collaborations and their contributions to critical infrastructure resilience. Future research should consider exploring further dimensions of critical infrastructure resilience, such as business-business collaboration. As described in the analysis, businesses often rely on each other for their supplies and services. Additionally, the examples of Volvo and Scania and Blackthorn and Aqua Nobel show that businesses work together to contribute to the resilience of critical infrastructure. This could provide additional insights into interorganisational arrangements that contribute to critical infrastructure resilience in Sweden.

Another future research avenue is to explore the category of trust between business-military actors. Within the category of organisational autonomy, our analysis showed that the indicators point to a coordinative structure. As touched upon within that section, this may be due to a lack of trust in businesses to continue to collaborate voluntarily. As McNamara described, the categories are treated independently; however, '[...] relationships between elements may exist and are worthy of additional research' (2012 p. 392). Future research is therefore encouraged to add the category of trust within their research to test this assumption and provide a clearer picture of the role of trust in organisational autonomy.

Creating and maintaining the resilience of critical infrastructure is a complex task that takes time. As our study has shown, many issues remain unaddressed, similar to those studied identified already in 2019. Given the significant neglect of civil defence until 2015 in Sweden, it is understandable that these procedures were not immediately in place; however, it has been nearly a decade. To ensure resilient critical infrastructure and resilient business-military collaborations, Sweden should consider speeding up the process, especially since the geopolitical situation that fostered the return of the total defence approach in the first place keeps deteriorating. In this context, future research could aim to provide a snapshot of the current state of societal, technological and organisational resilience in Sweden.

The interorganisational arrangement between business and military actors in Sweden largely aligns with a collaborative structure. A recurring theme from the empirical analysis is the necessity of business-military collaborations, which serve as essential drivers of Sweden's critical infrastructure resilience. However, these collaborations alone do not ensure resilience, especially when unresolved issues and unclear government proposals can sometimes hinder the process. Yet, if policymakers address these issues and transform theoretical knowledge into practical solutions, it could potentially enhance the resilience of critical infrastructure.

8. Reference List

4C Strategies. (2024). [LinkedIn]. Available: https://www.linkedin.com/posts/4c-strategies_yesterday-we-had-the-honor-of-welcoming-activity-7181584742952165379-LtCn?utm_source=share&utm_medium=member_desktop. [2024-04-20].

Agranoff, R. & McGuire, M. (2003). *Collaborative Public Management: New Strategies for Local Governments*. Washington, D.C.: Georgetown University Press.

Agranoff, R. (2008). Intergovernmental and Network Administration, Accountability and Performance: Symposium Introduction. [Electronic] *Public Performance & Management Review*, vol. 31(3), pp. 315-319. Available: JSTOR [2024-03-05] DOI:10.2753/PMR1530-9576310300.

Basit, T.N. (2003). Manual or electronic? The role of coding in qualitative data analysis. [Electronic] *Educational Research*, vol. 45(2), pp. 143–154. Available: ERIC [2024-04-16] DOI:10.1080/0013188032000133548.

Bendz, A. & Boholm, Å. (2019). Drinking water risk management: local government collaboration in West Sweden. [Electronic] *Journal of Risk Research*, vol. 22(6), pp. 674–691. Available: Business Source Ultimate [2024-05-02] DOI: 10.1080/13669877.2018.1485168.

Berndtsson, J., Obling, A. R., & Østensen, Å. G. (2023). Business-Military Relations and Collaborative Total Defence in Scandinavia. In Berndtsson, J., Goldenberg, I., Von Hlatky, S. *Total Defence Forces in the Twenty-First Century.* Montreal & Kingston: McGill-Queen's University Press, pp. 397-420.

Berzina, I., (2020). From “total” to “comprehensive” national defence: the development of the concept in Europe. [Electronic] *Journal on Baltic Security*, vol.6 (2), pp. 7–15. Available: Directory of Open Access Journals [2024-04-24] DOI:10.2478/jobs-2020-0006.

Billström, T. (2024-01-08). *The future of Sweden’s security policy – speech by Minister for Foreign Affairs Tobias Billström at the Folk och Försvar Annual National Conference.* [Electronic]. Available: https://www.government.se/speeches/2024/01/tobias-billstrom-at-the-folk-och-forsvar-annual-national-conference/. [2024-02-07].

Blackthorn AB. (2024). [LinkedIn] Available: https://www.linkedin.com/posts/aqua-nobel_omst%C3%A4llning-av-livsmedelsproduktion-vid-kris-activity-7157756851437113345-cUSV?utm_source=share&utm_medium=member_desktop. [2024-04-27].

Boin, A., & McConnell, A. (2007). Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience. [Electronic] *Journal of contingencies and crisis management*, vol.15(1), pp. 50-59. Available: Wiley Online [2024-03-04] DOI.org/10.1111/j.1468-5973.2007.00504.x.

Brasset, J. & Vaughan-Williams, N. (2015). Security and the Performative Politics of Resilience: Critical Infrastructure Protection and Humanitarian Emergency Preparedness. [Electronic] *Security Dialogue*, vol.46(1), pp. 32-50. Available: SAGE Journals [2024-02-01] DOI: 10.1177/0967010614555943.

Bryman, A. (2016). *Social research methods*. 5. ed. Oxford: Oxford University Press.

Bryson, J. M., Crosby, B. C., & Stone, M. M. (2006). The design and implementation of Cross-Sector collaborations: Propositions from the literature. [Electronic] *Public administration review*, vol.66, pp. 44-55. Available: Wiley Online [2024-03-01] DOI: https://doi.org/10.1111/j.1540-6210.2006.00665.x.

Carlsson, F. & Melander, G. (2021). *Risk and vulnerability analysis management for increased crisis preparedness and resilience.* [Electronic] Stockholm: KTH. (Independent thesis Advanced level 30hp, 2021 Department of Technology and technologies) Available: https://www.diva-portal.org/smash/get/diva2:1591696/FULLTEXT01.pdf [2024-02-14].

Cegarra- Navarro, J.G., Chinnaswamy, A., Garzia-Perez, A., Marinez-Caro, E. & Sallos, M. (2023). Resilience in healthcare systems: cyber security and digital and technological transformation. [Electronic] *Technovation v*ol.121, pp. 1-11. Available: ScienceDirect [2024-02-14] DOI: S0166497222001304.

Chen, S., Ding, F., Hao, M., Gao, C. (2023) Exploring the global geography of cybercrime and its driving forces. [Electronic] *Humanities and Social Sciences Communications*, vol. 10(71) pp.1-10. Available: Nature Springer [2024-04-20] DOI: 10.1057/s41599-023-01560.

Coetzee, W.S. (2020). Doing research on ‘sensitive topics’: Studying the Sweden-South Africa Arms Deal. *Scientia Militaria*, Vol. 48(2), pp. 65-85. DOI: 10.5787/48-2-1278.

Combitech. (2024). [LinkedIn] Available: https://www.linkedin.com/posts/combitech-ab_combitech-faemrsaemrjningsberedskap-krisberedskap-activity-7178273367345553408-gIM2?utm_source=share&utm_medium=member_desktop. [2024-04-20].

Combitech. (2024). [LinkedIn] Available: https://www.linkedin.com/posts/combitech-ab_totalfaemrsvarsspelet-totalfaemrsvar-civiltfaemrsvar-activity-7188469174665433088-D2vl?utm_source=share&utm_medium=member_desktop. [2024-04-20].

DHL. (2021-12-12). *Trends in logistics, Shaping the way we work and live.* [Electronic] Bonn, Germany. Available: https://www.dhl.com/global-en/delivered/globalization/trends-in-logistics.html [2024-04-29].

Ellevio. (2022). *Annual and Sustainability Report.* [Electronic] Stockholm: Ellevio. Available: https://www.ellevio.se/globalassets/content/finansiell-information/2022/web-pdf-eng/market-and-drivers_ellevio-annual-report-2022_web.pdf [2024-05-24].

Ellevio. (2023). *Annual and Sustainability Report.* [Electronic] Stockholm: Ellevio. Available: https://www.ellevio.se/globalassets/content/finansiell-information/2023/ellevio_annual_report_2023_web.pdf [2024-05-25].

Elston, T., Bel, G., & Wang, H. (2023). If it ain't broke, don't fix it: When collaborative public management becomes collaborative excess. [Electronic] *Public Administration Review*, vol. *83*(6), pp.1737-1760. Available: Wiley Online [2024-03-05] DOI: 10.1111/puar.13708.

European Commission (2023-06-29). *EU-NATO Task Force: Final assessment report on strengthening our resilience and protection of critical infrastructure.* [Electronic]. Brussels. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3564. [2024-02-12].

European Union External Action (2018-06-13). *A Europe that Protects: Countering Hybrid Threats.* [Electronic]. Brussels. Available: https://www.eeas.europa.eu/node/46393_en. [2024-02-05].

Expisoft. (2024). [LinkedIn] Available: https://www.linkedin.com/posts/expisoft-ab_vi-som-verkar-i-cybers%C3%A4kerhetsbranschen-st%C3%A5r-activity-7173618800494297088-sbxg?utm_source=share&utm_medium=member_desktop.[2024-04-21].

Florin, M.V., & Linkov, I. (2016). *IRGC resource guide on resilience.* [Electronic] Lausanne: EPFL International Risk Governance Center (IRGC). Available: https://infoscience.epfl.ch/record/228206?v=pdf [2024-02-12].

Forsberg, T. (2023). Finland And Sweden’s Road To NATO. [Electronic] *Current History*, vol. 122 (842), pp. 89-94. Available: Elsevier [2024-03-15].

Försvarmakten (2021-11-02). Hundratals nya lastbilar till Försvarsmakten från 2022. [Electronic]. Stockholm. Available: https://www.forsvarsmakten.se/sv/aktuellt/2021/11/hundratals-nya-lastbilar-till-forsvarsmakten-fran-2022/ [2024-04-28].

Frizzelle, B., Garey, J. & Kulalic, I. (2022). NATO's national resilience mandate: challenges and opportunities. [Electronic] *Defence Studies*, vol. 22(3), pp. 525–532. Available: Academic Search Premier [2024-02-06] DOI:10.1080/14702436.2022.2082954.

Government Offices of Sweden (2021-06-21). *Development of modern total defence.* [Electronic]. Stockholm. Available: https://www.government.se/articles/2018/06/development-of-modern-total-defence/. [2024-02-05].

GrantThornton (2021). *Den privatdrivna sjukvårdens erfarenheter av Pandemin; En obereonde studie på uppdrag av Vårdföretagen.* [Electronic]Göteborg: GrantThornton. Available: https://www.almega.se/app/uploads/sites/3/2022/02/den-privatdrivna-vardens-erfarenheter-av-pandemin-final-2022-01-18.pdf [2024-05-01].

Große, C. and Olausson, P.M. (2019). Blind spots in interaction between actors in Swedish planning for critical infrastructure protection. [Electronic] *Safety Science*, vol.118, pp. 424–434. Available: ScienceDirect [2024-02-16] DOI:10.1016/j.ssci.2019.05.049.

Hicklin, A., O'Toole Jr, L.J., Meier, K.J., & Robinson, S.E. (2009). Calming the Storms: Collaborative Public Management, Hurricanes Katrina and Rita, and Disaster Response. In O'Leary, R. & Bingham, L. (ed.) *The Collaborative Public Manager: New Ideas for the Twenty-First Century*, Georgetown University Press, pp. 95- 114.

Ignatowicz, A., El-Sawy, D., Lasserson, D., Mannion, R. & Tarrant, C. (2023). Organizational resilience in healthcare: a review and descriptive narrative synthesis of approaches to resilience measurement and assessment in empirical studies. [Electronic] *BMC Health Services Research* vol. 23(1), pp. 1-24 Available: Springer Nature Journals [2024-02-19] DOI: 10.1186/s12913-023-09242-9.

Jackson, K. & Bazeley, P. (2019). *Qualitative data analysis with NVivo.*3.ed. London: SAGE.

Karolinska Institutet (2021) *Annual Report* [Electronic] Stockholm. Available: https://ki.se/media/232094/download?attachment [2024-04-29].

Kun, L. (2008). Protection of health care and public health infrastructure and key assets. [Electronic] *IEEE Engineering in Medicine and Biology magazine,* vol. 27(6), pp. 8-13.

Available: British Library Document Supply Centre Inside Serials & Conference Proceedings [2024-02-19] DOI: 10.1109/MEMB.2008.930615.

Labaka, L., Hernantes, J., & Sarriegi, J. M. (2016). A holistic framework for building critical infrastructure resilience. [Electronic] *Technological Forecasting and Social Change,* vol. 103, pp. 21-33. Available: ScienceDirect [2024-02-24] DOI:10.1016/j.techfore.2015.11.005.

Larsson, S., & Rhinard, M. (2020). *Nordic societal security: Convergence and divergence*. New York: Routledge.

Lyng, H.B., Fagerdal, B., Guise, V., Haraldseid-Driftland, C., Macrae, C., Schibevagg, L., Wiig, S. (2022) Capacities for resilience in healthcare; a qualitative study across different healthcare context. [Electronic] *BMC Health Services Research,* vol. 22 (1), pp.1-14. Available: Springer Nature Journals [2024-02-26] DOI: 10.1186 s12913-022-07887-6.

Malmberg, P., Eriksson, M., Jansson, O., Ottosson, J. (2023) The role of Industry in Sweden's Total Defence: Past, Present, and Future. [Electronic] *KKRVA Handlingar och Tidsskrift,* vol.9, pp. 1-7. Available: Kungl Krigsvetenskapsakademien [2024-03-19].

McGuire, M. (2006). Collaborative Public Management: Assessing What We Know and How We Know It. [Electronic] *Public Administration Review,* vol. 66, pp. 33–43. Available: JSTOR Journals [2024- 02-27].

McNamara, M.W. (2012). Starting to Untangle the Web of Cooperation, Coordination, and Collaboration: A Framework for Public Managers. [Electronic] *International Journal of Public Administration,* vol. 35 (6), pp. 389 - 401. Available: British Library Document Supply Centre Inside Serials & Conference Proceedings [2024-02-13] DOI: 10.1080/01900692.2012.655527.

MedicSolution. (2015-10-27). *Leverans av operationssalar till Karlskoga.* [Electronic]. Available: https://www.medicsolution.com/sv/press/leverans-av-operationssalar-till-karlskoga/. [2024-04-26].

Mötesplats Samhällssäkerhet. (2024). *Om Mötesplats Samhällssäkerhet.* [Electronic]. Available: https://www.samhallssakerhet.se/sv/om/. [2024-04-21].

MW Group (nd). *MW Group signs agreement with the Swedish Defence Materiel Administration (FMV) to deliver a pilot decontamination solution.* [Electronic]. Available: https://mw.group/mw-group-signs-agreement-with-fmv/. [2024-04-27].

MW Group. (2024). [LinkedIn] Available: https://www.linkedin.com/posts/mw-group-ab_arebiz-nordensdavos-activity-7184630000006905857-1e9r utm_source=share&utm_medium=member_desktop. [2024-04-27].

Nationellt cybersäkerhetscenter. (2023). [LinkedIn] Available: https://www.linkedin.com/posts/nationellt-cybers%C3%A4kerhetscenter-ncsc-se_ncsc-%C3%A4r-en-plattform-f%C3%B6r-samverkan-mellan-activity-7096828029280133122-NBBz?utm_source=share&utm_medium=member_desktop. [2024-04-25].

Nohrstedt, D. (2016). Explaining Mobilization and Performance of Collaboration in Routine Emergency Management. [Electronic] *Administration & Society*, vol. 48(2), pp. 135-162. Available: SAGE Journals [2024-03-05] DOI:10.1177/0095399712473983.

O'Flynn, J. (2009). The cult of collaboration in public policy. [Electronic] *Australian Journal of Public Administration*, vol. 68, pp. 112-116. Available: Wiley Online [2024-03-03] DOI:10.1111/j.1467-8500.2009.00616.x.

Osei-Kyei, R., Almeida, L.M., Ampratwum, G. & Tam,V., (2023). Systematic review of critical infrastructure resilience indicators. [Electronic]. *Construction Innovation*, vol. 23(5), pp. 1210–1231. Available: Emerald Insight [2024-03-03] DOI:10.1108/CI-03-2021-0047.

PTS. (2023) *Robusta åtgärden: Nationella telesamverkangruppen (NTSG)*. [Electronic]. Available: https://www.pts.se/sv/bransch/internet/Om-robust-kommunikation/robusthetshojande-atgarder/nationella-telesamverkansgruppen/ [2024-05-02].

Pursiainen, C. (2018). Critical infrastructure resilience: A Nordic model in the making?. [Electronic] *International journal of disaster risk reduction*, vol. 27, pp. 632-641. Available: ScienceDirect [2024-02-20] DOI: 10.1016/j.ijdrr.2017.08.006.

Pursiainen, C., & Kytömaa, E. (2023). From European critical infrastructure protection to the resilience of European critical entities: what does it mean?. [Electronic] *Sustainable and Resilient Infrastructure*, vol. 8, pp. 85-101. Available: Sociology Source Ultimate [2024-02-20] DOI:10.1080/23789689.2022.2128562.

Rhinard, M. (2020). Societal security in theory and practice. [Electronic] *NordSTEVA Nordic Societal Security,* pp. 22-42. Available: SwePub [2024-02-20] DOI:10.4324/9781003045533-3.

Rydén Sonesson, T., Johansson, J., & Cedergren, A. (2021). Governance and interdependencies of critical infrastructures: Exploring mechanisms for cross-sector resilience. [Electronic] *Safety*

Science, vol. 142, pp.1-11. Available: ScienceDirect [2024-03-05] DOI: 10.1016/j.ssci.2021.105383.

Saab AB. (2021). *Kraften i goda Samarbete.* [Electronic]. Available:https://www.saab.com/sv/markets/sweden/om-saab-i-sverige/innovation/samarbeten [2024-05-01].

Swedish Civil Contingency Agency, (2021). Total defence – all of us together [Electronic]. Available: https://www.msb.se/siteassets/dokument/amnesomraden/krisberedskap-och-civilt-forsvar/stod-till-kommuner/krisberedskapsveckan/kampanjmaterial/material-2021/faktablad-totalforsvar/faktablad_totalforsvar_engelska.pdf. [2024-06-08].

Szymański, P. (2020). Towards greater resilience: NATO and the EU on hybrid threats. [Electronic] *Centre for Eastern Studies*. Available: Archive of European Integration [2024-02-07].

Volvo (2024-05-07). *Volvo CE supplies first wheel loaders to Swedish Armed Forces in SEK 1.2 billion 7-year deal.* [Electronic]. Göteborg. Available: https://www.volvoce.com/global/en/news-and-events/news-and-stories/2024/volvo-ce-supplies-first-wheel-loaders-to-swedish-armed-forces-in-sek-1-2-billion-7-year-deal/ [2024-05-09].

Wallnerström, C.J. Dalheim, M., Seratelius, M., & Johansson, T. (2020). Power outage related statistics in Sweden since the early 2000s and evaluation of reliability trends. *2020 International Conference on Probabilistic Methods Applied to Power Systems (PMAPS), Probabilistic Methods Applied to Power Systems (PMAPS),* pp. 1–6. Available: IEEE Xplore [2024-02-09] DOI:10.1109/PMAPS47429.2020.9183500.

Wither, J.K. (2020). Back to the future? Nordic total defence concepts. [Electronic] *Defence studies*, vol.20(1), pp. 61–81. Available at: British Library Document Supply Centre Inside Serials & Conference Proceedings [2024-01-30]. DOI 10.1080/14702436.2020.1718498.

Woods, D., Hollnagel, E., Leveson, N. (2006). *Resilience Engineering: Concepts and Precepts*. [Electronic] Aldershot, England: CRC Press Available: eBook Index [2024-02-19].

9. Appendices

9.1. Articles

Document Code	Document Identifier	Accessed Date
Doc5S	https://www.regeringen.se/artiklar/2024/02/nationell-samordning-av-sjuktransporter-en-viktig-del-i-samhallets-hantering-av-terrorattentat/	25-03-2024
Doc6S	https://www.regeringen.se/artiklar/2024/02/uppbyggnaden-av-totalforsvaret-ar-en-angelagenhet-for-hela-samhallet/	25-03-2024
Doc15S	https://www.regeringen.se/artiklar/2024/01/totalforsvaret-kan-inte-vanta--flera-satsningar-presenterade-pa-folk-och-forsvar/	28-03-2024
Doc16S	https://www.regeringen.se/debattartiklar/2024/01/sveriges-beredskap-starks-pa-flera-omraden/	28-03-2024
Doc23S	https://www.regeringen.se/artiklar/2023/12/forsvarsberedningen overlamnar-totalforsvarsrapporten-kraftsamling/	28-03-2024
Doc37S	https://www.regeringen.se/artiklar/2023/06/varden-ska-fungera-aven-i-kris-och-krig/	29-03-2024
Doc38S	https://www.regeringen.se/artiklar/2023/06/forsvarsberedningen-overlamnar - den-sakerhetspolitiska-rapporten-till-forsvarsminister-pal-jonson/	29-03-2024
Doc 40S	https://www.regeringen.se/artiklar/2023/06/forsorjningsberedskap-i-fokus-nar-naringslivsradet-traffades/	29-03-2024
Doc56S	https://www.regeringen.se/artiklar/2023/03/forsta-motet-i-det-tvarsektoriella-naringslivsradet-for-totalforsvar-och-krisberedskap/	31-03-2024
Doc57S	https://www.regeringen.se/artiklar/2023/03/totalforsvarets-tillvaxt-pa-agendan-nar-pal-jonson-och-carl-oskar-bohlin-besokte-karlstad/	31-03-2024
Doc58S	https://www.regeringen.se/artiklar/2023/03/sjofartens-roll-for-det-civila-forsvaret-i-fokus-nar-carl-oskar-bohlin-besokte-goteborgs-hamn/	31-03-2024
Doc59S	https://www.regeringen.se/artiklar/2023/03/teknikutveckling-och-totalforsvar-pa-agendan-nar-carl-oskar-bohlin-besokte-3d-skrivarforetag-i-karlskoga/	31-03-2023
Doc68S	https://www.regeringen.se/artiklar/2023/02/ministrar-besokte-nationellt-cybersakerhetscenter/	01-04-2024
Doc70S	https://www.regeringen.se/artiklar/2023/01/carl-oskar-bohlin-besokte-dalregementet-och-beredskapsdepa-i-borlange/	01-04-2024
Doc74S	https://www.regeringen.se/artiklar/2023/01/civilplikten-pa-agendan-nar-carl-oskar-bohlin-besokte-storstockholms-brandforsvar/	01-04-2024

Doc75S	https://www.regeringen.se/artiklar/2023/01/de-viktigaste-nyheterna-fran-forsvarsdepartementet-pa-folk-och-forsvar/	01-04-2024
Doc76S	https://www.regeringen.se/artiklar/2023/01/ett-tvarsektoriellt-naringslivsrad-ska-tillsattas-for-att-starka-forsorjningsberedskapen/	01-04-2024
Doc77S	https://www.regeringen.se/artiklar/2023/01/aktivering-av-civilplikt-for-raddningstjansten-ska-forberedas/	01-04-2024
Doc80S	https://www.regeringen.se/debattartiklar/2023/01/allas-nyarslofte-bor-vara-battre-hemberedskap/	01-04-2024
Doc81S	https://www.regeringen.se/artiklar/2022/12/civilt-forsvar-och-cybersakerhet-pa-agendan-nar-carl-oskar-bohlin-besokte-lansstyrelsen-ostergotland-och-foi/	01-04-2024
Doc1T	https://rib.msb.se/bib/Search/Document?id=30558&h=&q=kritisk%20infrastruktur&search=1	26-03-2024
Doc2T	https://rib.msb.se/bib/Search/Document?id=29818&h=&q=kritisk%20infrastruktur&search=1	26-03-2024
Doc7T	https://rib.msb.se/bib/Search/Document?id=30575&h=&q=kritisk%20infrastruktur&search=1	26-03-2024
Doc9T	https://rib.msb.se/bib/Search/Document?id=30599&h=&q=kritisk%20infrastruktur&search=1	26-03-2024
Doc19	MSB2262	27-03-2024
Doc21	MSB2156	27-03-2024
Doc22	MSB2263	27-03-2024
Doc23	MSB2273	27-03-2024
Doc24T	https://rib.msb.se/bib/Search/Document?id=30447&h=&q=kritisk%20infrastruktur&search=1	27-03-2024
Doc26T	https://rib.msb.se/bib/Search/Document?id=30487&h=&q=kritisk%20infrastruktur&search=1	27-03-2024
Doc27T	MSB2178	27-03-2024
Doc31T	MSB1408	27-03-2024
Doc32T	MSB2260	27-03-2024
Doc34T	MSB2248	27-03-2024
Doc36T	FOI-R-5516--SE	27-03-

		2024
Doc53T	FBD2022/23	28-03-2024
Doc60T	https://rib.msb.se/bib/Search/Document?id=30585&h=&q=kritisk%20infrastruktur&search=1	28-03-2024
Doc63T	MSB2073	28-03-2024
Doc64T	MSB1974	28-03-2024
Doc65T	MSB1994	28-03-2024
Doc66T	MSB1915	28-03-2024
Doc68T	MSB1938	29-03-2024
Doc73T	https://rib.msb.se/bib/Search/Document?id=30382&h=&q=kritisk%20infrastruktur&search=1	29-03-2024
Doc75T	FOI-R—5260—SE	29-03-2024
Doc77T	https://rib.msb.se/bib/Search/Document?id=30139&h=&q=kritisk%20infrastruktur&search=1	29-03-2024
Doc81T	MSB1774	29-03-2024
Doc82T	MSB1519	29-03-2024
Doc85T	https://rib.msb.se/bib/Search/Document?id=29931&h=&q=kritisk%20infrastruktur&search=1	29-03-2024
Doc87T	MSB1457	29-03-2024
Doc88T	MSB1979	29-03-2024
Doc92T	https://rib.msb.se/bib/Search/Document?id=29922&h=&q=kritisk%20infrastruktur&search=1	29-03-2024
Doc94T	MSB1515	29-03-2024
Doc95T	MSB1849	29-03-2024
Doc96T	MSB1701	29-03-2024
Doc99T	https://rib.msb.se/bib/Search/Document?id=29594&h=&q=kritisk%20infrastruktur&search=1	29-03-2024

Doc101T	MSB1365	30-03-2024
Doc102T	MSB1802	30-03-2024
Doc103T	MSB1835	30-03-2024
Doc105T	MSB695	30-03-2024
Doc108T	MSB1806	30-03-2024
Doc111T	https://rib.msb.se/bib/Search/Document?id=29715&h=&q=kritisk%20infrastruktur&search=1	30-03-2024
Doc116T	MSB1682	30-03-2024
Doc117T	MSB1743	30-03-2024
Doc119T	MSB1829	30-03-2024
Doc120T	MSB1705	30-03-2024
Doc122T	MSB1566	30-03-2024
Doc124T	MSB1862	30-03-2024
Doc125T	MSB1901	30-03-2024
Doc127T	MSB1813	30-03-2024
Doc128T	MSB1655	30-03-2024
Doc131T	MSB1646	30-03-2024
Doc132T	MSB1720	30-03-2024
Doc134T	RiR: 2021:7	30-03-2024
Doc135T	MSB1709	30-03-2024
Doc144T	MSB1776	31-03-2024
Doc148T	DNR; 2021/00384	31-03-

		2024
Doc159T	FHS/930/2011	31-03-2024
Doc161T	https://rib.msb.se/bib/Search/Document?id=29489&h=&q=kritisk%20infrastruktur&search=1	31-03-2024
Doc162T	MSB1478	31-03-2024
Doc165T	MSB 2019-04982	31-03-2024
Doc167T	MSB1521	31-03-2024
Doc175T	MSB1600	31-03-2024
Doc176T	tps://rib.msb.se/bib/Search/Document?id=29470&h=&q=kritisk%20infrastruktur&search=1	31-03-2024
Doc181T	MSB1469	31-03-2024
Doc185T	SoS-2020-1-6569	31-03-2024
Doc188T	ttps://rib.msb.se/bib/Search/Document?id=29952&h=&q=kritisk%20infrastruktur&search=1	31-03-2024
Doc189T	https://rib.msb.se/bib/Search/Document?id=29409&h=&q=kritisk%20infrastruktur&search=1	31-03-2024
Doc192T	RISE-2020:11	31-03-2024
Doc193T	MSB1681	02-04-2024
Doc195T	https://rib.msb.se/bib/Search/Document?id=29455&h=&q=kritisk%20infrastruktur&search=1	02-04-2024
Doc196T	MSB1496	02-04-2024
Doc197T	FOI-R—4992—SE	02-04-2024
Doc199T	MSB1618	02-04-2024
Doc200T	MSB1619	02-04-2024
Doc202T	MSB1181	02-04-2024
Doc203T	MSB1179	02-04-2024

Doc204T	MSB1178	02-04-2024
Doc205T	MSB1198	02-04-2024
Doc207T	MSB1252	02-04-2024
Doc209T	MSB1194	02-04-2024
Doc211T	MSB2017-1624	02-04-2024
Doc214T	MSB1285	02-04-2024
Doc219T	MSB1290	02-04-2024
Doc222T	MSB932	02-04-2024
Doc225T	MSB1163	02-04-2024
Doc226T	MSB1190	02-04-2024
Doc227T	MSB1199	02-04-2024
Doc229T	MSB1275	03-04-2024
Doc230T	FOI-R—4588—SE	03-04-2024
Doc232T	RiR-2018:6	03-04-2024
Doc236T	MSB1172	03-04-2024
Doc240T	https://rib.msb.se/bib/Search/Document?id=28796&h=&q=kritisk%20infrastruktur&search=1	03-04-2024
Doc241T	MSB1081	04-04-2023
Doc242T	MSB2016-6304-7	04-04-2023
Doc243T	MSB1128	04-04-2023
Doc244T	MSB1076	04-04-2023
Doc247T	MSB1144	04-04-

		2023
Doc248T	MSB1131	04-04-2023
Doc249T	MSB860	04-04-2023
Doc255T	MSB1084	04-04-2023
Doc256T	MSB1048	04-04-2023
Doc259T	https://rib.msb.se/bib/Search/Document?id=28257&h=&q=kritisk%20infrastruktur&search=1	04-04-2023
Doc262T	MSB998	04-04-2023
Doc263T	MSB916	04-04-2023

9.2. Assignments

Document Code	Document Identifier	Accessed Date
Doc3S	Ku2024/00322	25-03-2024
Doc10S	Fö2024/00054	28-03-2024
Doc29S	KN2023/04096	29-03-2024
Doc32S	LI2023/02842	29-03-2024
Doc35S	S2023/02002	29-03-202
Doc48S	S2023/01527	30-03-2024
DocS50	KN2023/02999	30-03-2024
Doc61S	S2023/00380	31-03-2024
Doc71S	Fö2023/00118	01-04-2024

Doc83S	S2022/04550	01-04-2024
Doc84S	S2022/04258	01-04-2024
Doc85S	S2022/04257	01-04-2024
Doc89S	Ju2022/02313	01-04-2024
Doc90S	Ju2022/02219	01-04-2024
Doc93S	Ju2022/01976	01-04-2024
Doc94S	Ju2022/01292	01-04-2024
Doc95S	Ju2022/01209	01-04-2024
Doc96S	Ju2021/03620	01-04-2024
Doc100S	Ju2021/02771	01-04-2024
Doc102S	I2021/01905	02-04-2024
Doc103S	Ju2021/02005	02-04-2024
Doc106S	Ju2021/01243	02-04-2024
Doc107S	Ju2020/04658	02-04-2024
Doc112S	Fö2019/01330	02-04-2024
Doc113S	N2020/02693	02-04-2024
Doc115S	N2020/02294	02-04-2024
Doc120S	Ju2019/02477/SSK	02-04-2024
Doc129S	Fö2017/00688/MFI	02-04-2024
Doc131S	Ju2016/07782/SSK	02-04-2024
Doc132S	Ju2015/09907/SSK	02-04-

		2024
Doc14T	https://rib.msb.se/bib/Search/Document?id=30593&h=&q=kritisk%20infrastruktur&search=1	27-03-2024
Doc30T	MSB2225	27-03-2024
Doc70T	MSB2029	28-03-2024
Doc113T	MSB5430	29-03-2024

9.3. Directives

Document Code	Document Identifier	Accessed Date
Doc2S	S2024/00390	25-03-2024
Doc52S	Ds 2023:12	31-03-2024
Doc53S	Dir. 2023:51	31-03-2024
Doc63S	Dir. 2023:30	31-03-2024
Doc82S	Fö2022/00125	01-04-2024
Doc87S	Dir. 2022:119	01-04-2024
Doc88S	Dir. 2022:121	01-04-2024
Doc92S	Dir. 2022:72	01-04-2024
Doc97S	Dir. 2021:80	02-04-2024
Doc99S	Dir. 2021:65	02-04-2024
Doc104S	Dir. 2021:30	02-04-2024
Doc109S	Dir. 2021:20	02-04-2024

Doc110S	2020/21:FPM72	02-04-2024
Doc111S	2020/21:FPM7	02-04-2024
Doc124S	Dir. 2018:79	02-04-2024
Doc125S	Dir. 2018:77	02-04-2024
Doc126S	Dir. 2018:64	02-04-2024
Doc130S	Dir. 2017:31	02-04-2024

9.4. Government Bill

Document Code	Document Identifier	Accessed Date
Doc12S	Prop. 2023/24:60	28-03-2024
Doc17S	https://www.regeringen.se/contentassets/38380ae279be406a9775a6d54002503e/strategisk-inriktning-for-forsvarsinnovation.pdf	28-03-2024
Doc62S	Prop 2022/23:77	31-03-2024
Doc73S	Prop 2022/23:45	01-04-2024
Doc114S	Prop. 2020/21:30	02-04-2024
Doc119S	https://www.regeringen.se/rattsliga-dokument/lagradsremiss 2019/08/skydd-av-sveriges-sakerhet-vid-radioanvandning/	02-04-2024
Doc122S	Prop. 2018/19:127	02-04-2024
Doc133S	Prop. 2015/16:67	02-04-2024
Doc134S	Prop. 2014/15:109	02-04-2024
Doc257T	https://rib.msb.se/bib/Search/Document?id=28389&h=&q=kritisk%20inf	04-04-

	rastruktur&search=1	2024

9.5. Press release

Document Name	Document Identifier	Accessed Date
Doc4S	https://www.regeringen.se/pressmeddelanden/2024/02/myndigheter-ges-i-uppdrag-att-bilda-ett-rad-for-skydd-av-kulturarv/	25-03-2024
Doc7S	https://www.regeringen.se/pressmeddelanden/2024/02/78-atgarder-starker-det-civila-forsvaret---regeringen-presenterade-en-samlad-lagesbeskrivning-om-det-civila-forsvaret/	28-03-2024
Doc9S	https://www.regeringen.se/pressmeddelanden/2024/02/mats-persson-och-carl-oskar-bohlin-inviger-cybercampus-sverige/	28-03-2023
Doc11S	https://www.regeringen.se/pressmeddelanden/2024/01/regeringen-samlade-berorda-myndigheter-med-anledning-av-storskalig-cyberattackregeringen-samlade-berorda-myndigheter-med-anledning-av-storskalig-cyberattack/	28-03-2023
Doc13S	https://www.regeringen.se/pressmeddelanden/2024/01/i-dag-aktiveras-civilplikten/	28-03-2024
Doc14S	https://www.regeringen.se/pressmeddelanden/2024/01/naringslivet-far-forstarkt-roll-vid-kriser-och-hojd-beredskap/	28-03-2024
Doc18S	https://www.regeringen.se/pressmeddelanden/2024/01/atgarder-for-effektivare-beredskaps--och-forsorjningsplanering-aviserade-pa-folk-och-forsvar/	28-03-2024
Doc20S	https://www.regeringen.se/pressmeddelanden/2023/12/regeringen-aktiverar-delar-av-civilplikten/	28-03-2024
Doc21S	https://www.regeringen.se/pressmeddelanden/2023/12/starkta-krav-i-myndigheternas-regleringsbrev-kring-informations--och-cybersakerhetsarbetet/	28-03-2024
Doc22S	https://www.regeringen.se/pressmeddelanden/2023/12/regleringsbrev-med-nyheter-inom-halso--och-sjukvardsomradet-har-beslutats/	28-03-2024
Doc25S	https://www.regeringen.se/pressmeddelanden/2023/12/nationella-sakerhetsstrategin-diskuteras-i-naringslivsradet/	29-03-2024
Doc26S	https://www.regeringen.se/pressmeddelanden/2023/12/regeringen-har-tagit-emot-forslag-som-ska-starka-den-konstitutionella-beredskapen-for-kriser/	29-03-2024
Doc31S	https://www.regeringen.se/pressmeddelanden/2023/07/en-okad-	29-03-

	spridning-av-desinformation-riktas-mot-sverige/	2024
Doc33S	https://www.regeringen.se/pressmeddelanden/2023/06/socialtjanstens-och-halso--och-sjukvardens-beredskap-ska-styras-och-foljas-upp-genom-statsbidrag/	29-03-2024
Doc34S	https://www.regeringen.se/pressmeddelanden/2023/06/400-miljoner-kronor-till-regionerna-for-att-starka-sjukvardens-forsorjningsberedskap/	29-03-2024
Doc36S	https://www.regeringen.se/pressmeddelanden/2023/06/trafikverket-ska-utreda-en-eventuell-reservhamn-pa-gotland/	29-03-2024
Doc41S	https://www.regeringen.se/pressmeddelanden/2023/06/metod-ska-utvecklas-for-att-regelbundet-mata-oppenvardsapotekens-tillhandahallande-av-lakemedel/	29-03-2024
DocS49	https://www.regeringen.se/pressmeddelanden/2023/04/regeringen-vill-utreda-hur-civilplikten-kan-utokas-till-fler-samhallsviktiga-branscher-och-verksamheter/	30-03-2024
Doc51S	https://www.regeringen.se/pressmeddelanden/2023/04/sveriges-katastrofmedicinska-beredskap-ska-starkas/	31-03-2024
Doc54S	https://www.regeringen.se/pressmeddelanden/2023/04/regeringen-starker-forsorjningsberedskapen-inom-livsmedels--och-dricksvattenomradet/	31-03-2024
Doc55S	https://www.regeringen.se/pressmeddelanden/2023/03/halso--och-sjukvardens-formaga-att-hantera-masskadehandelser-ska-starkas/	31-03-2024
Doc60S	https://www.regeringen.se/pressmeddelanden/2023/03/regeringen-uppdrar-till-msb-att-erbjuda-effektivare-informationssakerhetsarbete-till-naringslivet/	31-03-2024
Doc64S	https://www.regeringen.se/pressmeddelanden/2023/02/regeringen-bjuder-in-deltagare-till-naringslivsradet/	31-03-2024
Doc67S	https://www.regeringen.se/pressmeddelanden/2023/02/socialstyrelsen-ska-kopa-in-och-lagra-sjukvardsprodukter-som-behovs-for-traumavard/	01-04-2024
Doc72S	https://www.regeringen.se/pressmeddelanden/2023/01/statsbidrag-till-regioner-for-att-hoja-driftsakerheten-pa-halso--och-sjukvardens-fastigheter/	01-04-2024
Doc79S	https://www.regeringen.se/pressmeddelanden/2022/12/regeringen-har-beslutat-om-fortsatt-arbete-for-att-bygga-upp-en-livsmedelsberedskap/	01-04-2024

9.6. Responses

Document Code	Document Identifier	Accessed Date
Doc8S1	https://www.regeringen.se/contentassets/0357ac82c7c94bdbbd1544ade0ccf6ac/adda.pdf	25-03-2024

Doc8S2	https://www.regeringen.se/contentassets/0357ac82c7c94bdbbd1544ade0ccf6ac/almega.pdf	25-03-2024
Doc8S3	https://www.regeringen.se/contentassets/0357ac82c7c94bdbbd1544ade0ccf6ac/apotek-produktion--laboratorier-ab.pdf	27-03-2024
Doc8S4	https://www.regeringen.se/contentassets/0357ac82c7c94bdbbd1544ade0ccf6ac/apoteket.pdf	27-03-2024
Doc8S6	https://www.regeringen.se/contentassets/0357ac82c7c94bdbbd1544ade0ccf6ac/bankgirot.pdf	27-03-2024
Doc8S7	https://www.regeringen.se/contentassets/0357ac82c7c94bdbbd1544ade0ccf6ac/ericsson.pdf	27-03-2024
Doc8S8	https://www.regeringen.se/contentassets/0357ac82c7c94bdbbd1544ade0ccf6ac/euroclear-sweden-ab.pdf	28-03-2024
Doc8S9	https://www.regeringen.se/contentassets/0357ac82c7c94bdbbd1544ade0ccf6ac/euroclear-sweden-ab.pdf	28-03-2024
Doc8S10	https://www.regeringen.se/contentassets/0357ac82c7c94bdbbd1544ade0ccf6ac/stokab.pdf	28-03-2024
Doc8S11	https://www.regeringen.se/contentassets/0357ac82c7c94bdbbd1544ade0ccf6ac/svemin-branschorganisationen-for-gruvor-mineral--och-metallproducenter-i-sverige.pdf	28-03-2024
Doc8S12	https://www.regeringen.se/contentassets/0357ac82c7c94bdbbd1544ade0ccf6ac/telenor-sverige-ab.pdf	28-03-2024
Doc18S13	https://www.regeringen.se/contentassets/0357ac82c7c94bdbbd1544ade0ccf6ac/svensk-forsakring.pdf	28-03-2024
Doc8S14	https://www.regeringen.se/rattsliga-dokument/lagradsremiss/2023/11/en-telesamverkansgrupp-for-fredstida-kriser-och-hojd-beredskap/	28-03-2024
Doc28S	https://www.regeringen.se/remisser/2023/09/remiss-av-promemorian-aktivering-av-civilplikt-inom-den-kommunala-raddningstjansten-och-elforsorjningsomradet/	29-03-2024
Doc42S	https://www.regeringen.se/remisser/2023/09/remiss-av-promemorian-aktivering-av-civilplikt-inom-den-kommunala-raddningstjansten-och-elforsorjningsomradet/	30-03-2024
Doc43	https://www.regeringen.se/pressmeddelanden/2023/06/operativ-krisledning-vid-allvarliga-driftstorningar-i-den-finansiella-sektorn-ska-forbattras/	30-03-2024
Doc44S	https://www.regeringen.se/pressmeddelanden/2023/06/regeringen-vill-sakra-god-beredskap-for-skolan-vid-kris-eller-krig/	30-03-2024
Doc45S	Ju2022/00440	30-03-2024
Doc91S1	Ju2022/00440	01-04-2024
Doc91S2	Ju2022/00440	01-04-

		2024
Doc91S3	SOU 2021:25	01-04-2024
Doc101S	https://rib.msb.se/bib/Search/Document?id=30180&h=&q=kritisk%20infrastruktur&search=1	01-04-2024
Doc15T	https://rib.msb.se/bib/Search/Document?id=30359&h=&q=kritisk%20infrastruktur&search=1	27-03-2024
Doc16T	https://rib.msb.se/bib/Search/Document?id=29656&h=&q=kritisk%20infrastruktur&search=1	27-03-2024
Doc137T	https://rib.msb.se/bib/Search/Document?id=30359&h=&q=kritisk%20infrastruktur&search=1	29-03-2024
Doc178T	MSB1544	30-03-2024

9.7. Reports

Document Code	Document Identifier	Accessed Date
Doc24S	https://www.regeringen.se/contentassets/0decd61162c24c73a9ca443328ccd9dd/sammandrag-av-kraftsamling-ds-202334	28-03-2024
Doc27S	SOU 2023:75	29-03-2024
Doc39S	Ds 2023:19	29-03-2024
Doc65S	SOU 2023:11	31-03-2024
Doc86S	SOU2022:57	01-04-2024
Doc98S	Skr. 2021/22:6	01-04-2024
Doc105S	SOU 2021:25	02-04-2024
Doc116S	SOU 2020:29	02-04-2024
Doc117S	SOU 2020:23	02-04-2024
Doc1	SOU 2019:51	02-04-

18S		2024
Doc121S	SOU 2019:34	02-04-2024
Doc123S	Ds 2019:8	02-04-2024
Doc127S	SOU 2018:26	02-04-2024
Doc128S	Ds 2017:66	02-04-2024
Doc135S	SOU 2016:13	02-04-2024
Doc3T	https://rib.msb.se/bib/Search/Document?id=30557&h=&q=kritisk%20infrastruktur&search=1	26-03-2024
Doc6T	https://rib.msb.se/bib/Search/Document?id=30596&h=&q=kritisk%20infrastruktur&search=1	26-03-2024
Doc10T	https://rib.msb.se/bib/Search/Document?id=30582&h=&q=kritisk%20infrastruktur&search=1	26-03-2024
Doc11T	https://rib.msb.se/bib/Search/Document?id=30623&h=&q=kritisk%20infrastruktur&search=1	26-03-2024
Doc18T	MSB2174	27-03-2024
Doc20T	MSB2265	27-03-2024
Doc28T	MSB2267	27-03-2024
Doc29T	MSB2283	27-03-2024
Doc37T	MSB2194	27-03-2024
Doc40T	FOI-R8094—SE	27-03-2024
Doc52T	MSB1825	28-03-2024
Doc61T	MSB1867	28-03-2024
Doc62T	MSB1940	28-03-2024
Doc71T	MSB1923	28-03-2024
Doc76T	MSB1916	28-03-2024

Doc79T	MSB1915	28-03-2024
Doc80T	MSB242	28-03-2024
Doc89T	https://rib.msb.se/bib/Search/Document?id=29974&h=&q=kritisk%20infrastruktur&search=1	28-03-2024
Doc100T	MSB1880	29-03-2024
Doc106T	MSB1804	29-03-2024
Doc110T	MSB1855	29-03-2024
Doc112T	MSB1783	29-03-2024
Doc114T	MSB1851	29-03-2024
Doc118T	https://rib.msb.se/bib/Search/Document?id=29483&h=&q=kritisk%20infrastruktur&search=1	29-03-2024
Doc123T	MSB1845	29-03-2024
Doc126T	MSB1796	29-03-2024
Doc130T	FM2021-l 7683:2	30-03-2024
Doc142T	FOI-R—5230—SE	30-03-2024
Doc147T	FOI-R-5247—SE	31-03-2024
Doc150T	MSB1745	31-03-2024
Doc151T	MSB1778	31-03-2024
Doc158T	https://rib.msb.se/bib/Search/Document?id=30296&h=&q=kritisk%20infrastruktur&search=1	31-03-2024
Doc163T	MSB1526	31-03-2024
Doc164T	https://rib.msb.se/bib/Search/Document?id=29595&h=&q=kritisk%20infrastruktur&search=1	31-03-2024
Doc169T	MSB1547	31-03-2024
Doc1	MSB1524	31-03-

72T		2024
Doc174T	MSB1501	31-03-2024
Doc177T	https://rib.msb.se/bib/Search/Document?id=29399&h=&q=kritisk%20infrastruktur&search=1	31-03-2024
Doc179T	https://rib.msb.se/bib/Search/Document?id=29472&h=&q=kritisk%20infrastruktur&search=1	31-03-2024
Doc180T	MSB1456	31-03-2024
Doc186T	MSB1594	31-03-2024
Doc187T	https://rib.msb.se/bib/Search/Document?id=29431&h=&q=kritisk%20infrastruktur&search=1	31-03-2024
Doc191T	https://rib.msb.se/bib/Search/Document?id=29394&h=&q=kritisk%20infrastruktur&search=1	02-04-2024
Doc194T	https://rib.msb.se/bib/Search/Document?id=29610&h=&q=kritisk%20infrastruktur&search=1	02-04-2024
Doc206T	MSB1304	02-04-2024
Doc208T	MSB2017-2825	02-04-2024
Doc213T	MSB1222	02-04-2024
Doc216T	MSB1294	02-04-2024
Doc223T	MSB1282	02-04-2024
Doc224T	MSB1177	02-04-2024
Doc228T	MSB1223	02-04-2024
Doc231T	MSB1156	03-04-2024
Doc235T	https://rib.msb.se/bib/Search/Document?id=29249&h=&q=kritisk%20infrastruktur&search=1	03-04-2024
Doc239T	MSB1245	03-04-2024
Doc245T	MSB1098	04-04-2024
Doc246T	MSB1086	04-04-2024

Doc251T	MSB1116	04-04-2024
Doc253T	MSB1080	04-04-2024
Doc258T	MSB2016-6701	04-04-2024
Doc261T	MSB1140	04-04-2024

9.8. Speeches

Document Code	Document Identifier	Accessed Date
Doc19S	https://www.regeringen.se/tal/2024/01/anforande-av-minister-for- civilt-forsvar-carl-oskar-bohlin-vid-folk-och-forsvars-rikskonferens-2024/	28-03-2024
Doc78S	https://www.regeringen.se/tal/2023/01/tal-av-minister-for-civilt-forsvar-carl-oskar-bohlin-vid-folk-och-forsvars-rikskonferens-2023/	01-04-2024

9.9. Guidelines

Document Code	Document Identifier	Accessed Date
Doc108S	Ju2020/04658	02-04-2024
Doc17T	https://rib.msb.se/bib/Search/Document?id=30373&h=&q=kritisk%20infrastruktur&search=1	27-03-2024
Doc25T	FOI-R-5359—SE	29-03-2024
Doc33T	MSB2213	29-03-2024
Doc54T	MSB2095	29-03-2024
Doc55T	MSB1943	29-03-2024
Doc58T	FOI-R--2022-639—SE	29-03-2024
Doc67T	MSB1945	29-03-2024

Doc74T	https://rib.msb.se/bib/Search/Document?id=29918&h=&q=kritisk%20infrastruktur&search=1	29-03-2024
Doc86T	MSB1978	29-03-2024
Doc93T	MSB1519	30-03-2024
Doc98T	MSB1635	30-03-2024
Doc115T	MSB1803	30-03-2024
Doc138T	MSB1792	31-03-2024
Doc157T	https://rib.msb.se/bib/Search/Document?id=29679&h=&q=kritisk%20infrastruktur&search=1	31-03-2024
Doc201T	MSB1180	02-04-2024
Doc254T	MSB1083	03-04-2024

9.10. Others

Document Code	Document Identifier	Accessed Date
Doc1S	Fö2023/01701	25-03-2024
Doc69S	S2023/00487	01-04-2024
Doc30S	Dir 2023:116	29-03-2024
Doc46S	LI2023/02525	30-03-2024
Doc47S	Fi2023/01681	30-03-2024