Linköping University | Department of Computer and Information Science
Master’s thesis, 30 ECTS | Information Technology
Spring 2022 | LIU-IDA/LITH-EX-A--22/022--SE

A Comparative Case Study on How the Swedish and British Armed Forces Use Multi Domains in Aspects of Methods, Technology, and Organization

En jämförande fallstudie om hur den svenska och brittiska Försvarsmakten använder multidomänbegreppet i form av metoder, teknologi och organisation

Daniel Keyvanpour

Supervisor: Björn Johansson
Examinator: Ola Leifler

Abstract

The multi-domain operations are vaguely defined and there are a variety of interpretations. In general terms, multi-domain can be described as a means of communication between different joint forces such as land, water, air, cyber, and space. In multi-domain operations, the focus is on how those domains can integrate using technologies, methods, and planning.

By interviewing individuals with long experience in both the British and Swedish Armed Forces and conducting a literature study, the focus has been on understanding how multi-domain operations as a concept are understood, interpreted, and implemented in the respective nation's operations today regarding the technology and organizational structure.

The results were compared with frameworks such as Federated Mission Networking (FMN) and Level of Information Systems Interoperability (LISI). The analysis shows that both the Swedish and British Armed Forces need greater interoperability. In order to have a better ability to cooperate within their forces, a more agile approach to the organization is needed that takes advantage of information and communication technologies. This can be achieved by managing different protocols through the different layers and models and by introducing a cloud service that functions as a cloud service function where the information flow is fast and easily accessible, independent of the domain.

Acknowledgement

First of all, I would like to thank Björn Johansson, as he has always been there for me as an advisor and supported me with valuable input both before this thesis and during the thesis. Björn has been the supervisor for me both at the university and FOI, thus he has done two people's work as he works both as Professor at Linköping University and as research leader at FOI, thank you very much for all your help, Björn! And extra thanks for letting me use your figures to illustrate the concept of multi-domain operations!

Furthermore, I would also like to highlight Ola Leifler who has been the examiner. He has contributed with valuable guidance throughout the writing of this thesis. Furthermore, I want to send a big thank you to my opponent Oscar Olsson who has on several occasions contributed with valuable and nuanced feedback that raised the quality of this thesis! I humbly thank you for that.

Last but not least, I want to thank everyone in FOI and all the people who, with their invaluable knowledge, have put on time to do interviews with me, in order to help me answer my research questions, many thanks to you!

Table of Contents

List of Figures

List of Tables

1. Introduction

The relevance of multi-domain operations has increased worldwide in the last decade since many nations and organizations sought to learn more about how to use modern technology and communicate between different branches of defense [1]. The multi domain operations are vaguely defined, and a multitude of interpretations exist. But in general terms, multi-domain operations (MDO) can be described as a means of communication between different joint forces such as the army, marine, air force, cyber, and space. In multi-domain operations, in these mentioned branches of defense, the focus is on how several domains can in a functionating and smart way both plan and integrate through aspects of technology, methods, and planning [1].

In an age where we are becoming increasingly digital, both the Swedish and British Armed Forces should use technical solutions to understand how to manage the combined threats caused by traditional warfare along with IT threats. This also affects the military organization, where one can see that technology has developed exponentially in recent decades, while the organization has not kept up with the technical development at all. With that in mind, it is becoming more relevant to go beyond the traditional ways (e.g., obedience hierarchies and strict division of responsibilities) of communicating and leading various systems within the military as well. However, the command and control (C2) systems are still relatively unexplored as multi-domain operations and there is ambiguity among most nations and organizations [2]. The thesis will niche itself on two nations that have similar ambitions and foundations in aspects of culture and approach, which are the Swedish and British Armed Forces. There is solid cooperation between these two countries to increase understanding and contribute to a more effective command and control systems in these two countries, which results in the use of technical and methodologic means to achieve interoperable C2 systems [3], [4].

There is today a need to coordinate activities between various kinds of entities, which in this report will be called joint forces. The situation regarding MDO is primarily when many military actions take place in domains that are not usually associated with the military where greater and more sophisticated collaborations between organizations are needed. There is a need to merge and utilize information from any source to integrate planning and synchronize the execution of multi-domain operations in time and space [12].

Additionally, in this report, the term interoperability will be used frequently. The meaning of that term, according to the terminology of the Swedish Armed Forces [5], is the ability and tendency of different actors to use information through communication systems. The Swedish armed forces describe the term using the following words:

> *"Interoperability is the ability to effectively coordinate personnel, systems, units, countries, and organizations to jointly achieve formulated strategic, operational, and tactical objectives"* [5] .

With challenges where many conflicts are taking place in several forms and several domains, it leads to a situation where the interoperability of information systems should be developed with a common standardization process, since the need for interoperability has shown to be of utmost importance today [6]. At the same time, it is important to understand how countries like Sweden harmonize their efforts to achieve comprehensive effects to continue to protect themselves against different threats and warfare. These different threats may show as cyber warfare or influence operations, and in the same way the Swedish Armed forces must communicate through multi-domain operations on both national and international scales to prevent attacks from different threats and warfare [6].

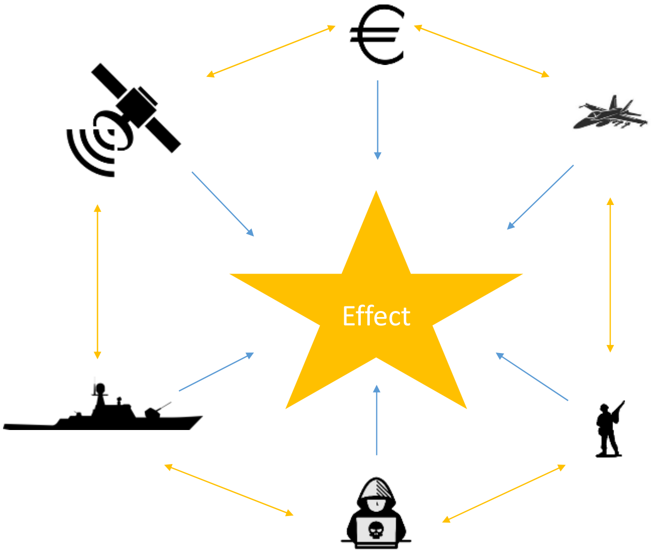


Figure 1.1: Six different examples of warfare that can take place simultaneously, where all activities contribute to a greater effect when they take place together. The six different warfare methods are cyber warfare, influence operations, financial sanctions, proxy combat, special operations, and regular warfare.

Furthermore, there is a shortcoming in how interoperability should work technically to handle the confidentiality that comes with a multi-domain operation. To effectively manage and control C2 multi-domain operations to bring together aviation, army, navy, space, and cyber capabilities to meet the challenges of what joint forces between domains may bring. Frameworks and technical standards that can enable communication and talk to each other in combination with an agile ability to do things differently depending on needs and prerequisites is a challenge that more research should be done on. [7].

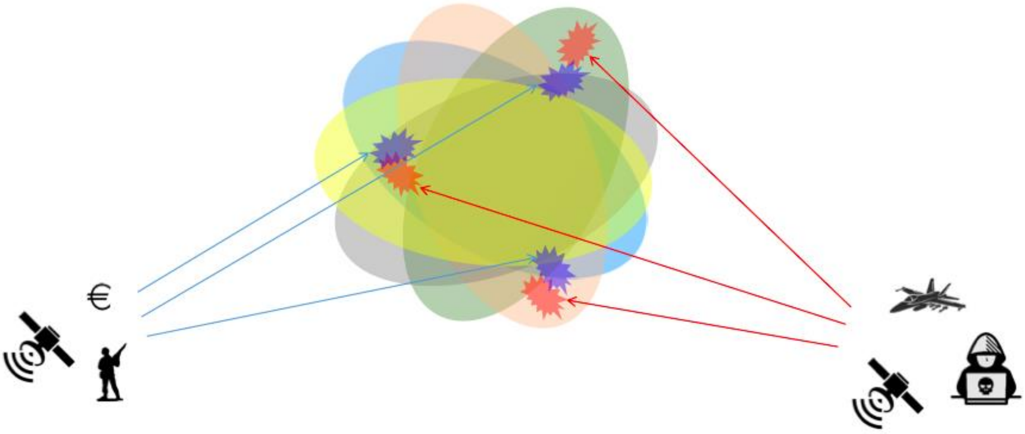


Figure 1.2: Demonstrates how a battle (illustrated in the middle) conducted by MDO can only be fought through MDO

Figure 1.2 has the aim of demonstrating that only MDO can handle MDO in warfare, thus it is important to understand how the Swedish Armed Forces should harmonize their efforts to achieve holistic effects to support themselves against threats and in the same way communicate through multi-domain operations on both national and international scale.

1.1 Motivation

Understanding how the different domains in the military interact with each other efficiently and securely is a matter of course, however, today there are shortcomings in how the operations between different domains work. The fact that military activities are conducted in a time where the complexity of the battlefield is greater since many nations and organizations may act against Sweden through various technology platforms in a way that is outside the arena of what people normally call warfare. This means that the military need ways to deal with different domains such as aviation, navy, army, and cyber. The motivation for comparing Sweden's Armed Forces with UK’s Armed Forces is that the countries have a similar approach from a multi-domain perspective whereas the UK also has the ambition to further develop its joint force and change its armed force so that it can handle multi-domain operations [8].

1.2 Aim

The aim is to investigate and understand the conditions for different countries, in this case, Sweden and the United Kingdom, and understand the possibilities of becoming inter-organizational efficient to handle multi-domain operations. The aim is also to analyze what the prerequisites are for people, organization, and technology to handle multi-domain operations and see how the Swedish and British Armed Forces as an organization are affected when working agile and coordinated. This thesis will use the results of the paper presented by Valaker et al. [9] to clarify what prerequisites there may be in order to handle multi-domain operations. Furthermore, a study on how the military can use technical capabilities to use and enable communication through different domains will also be analyzed and carried out.

1.3 Research questions

In this thesis, there will be an investigation and conduction of a comparative case study of what multi-domain operations mean from a Swedish and British Armed Forces' perspective and what the prerequisites look like from an organizational and technical perspective. The questions are the following:

- How does the Swedish Armed Forces interpret MDO compared to the British Armed Forces, in its approach to MDO?
    - What are the prerequisites in terms of people, organization, and technology?
    - How can the Swedish Armed Forces use frameworks to improve and measure its communication systems?
    - What literature reviews exist that can be used to understand how MDO should work regarding the requirements of interoperability?

1.4 Approach

The intention is to investigate the research questions through a literature review and by conducting interviews with military stakeholders. The approach will thus be a form of a comparative study. More details about the approach are described in the method chapter.

1.5 Delimitations

The multi-domain area is today relatively unexplored, in terms of current research, which contributes to both a wide range of issues in the area that can be researched and to a wider possibility to lay a foundation for MDO should develop in the future. This leads to many delimitations on what is reasonable to implement in terms of technical solutions, given the time and resources for this thesis. Understanding, for example, the conditions for participating in multi-domain operations in terms of doctrine and method is complex and broad. That is why this thesis will focus more on what frameworks there are and what the requirements are for having a large-scale use of interoperability. There will not be any in-depth to this thesis with a prototype implementation, since it requires more time, and there is simply no material to carry out a prototype implementation from an IT perspective, which is why there instead will be a comparative case study. Furthermore, the focus will be on Sweden's and United Kingdom’s perspectives, but there are more nations and organizations such as NATO that this is relevant, but it requires more resources to do this case study for all of them.

2. Background

2.1 FOI

The Swedish Defense Research Agency (Totalförsvarets Forskningsinstitut, FOI), is an authority under the Swedish Ministry of Defense. FOI's operations can be said to be centered around four different tasks, technology development, method development, investigative work, and research development. It is worth pointing out that FOI does not conduct any intelligence gathering itself, but functions as a collaboration between the Swedish Armed Forces and research conducted at a civilian level. One of FOI's focus areas is the interplay between people, technology, and organization, which is where this thesis is carried out.

2.2 Cloud solutions in the military context

In this thesis, the focus is placed on the human and technology interaction within the military, where the focus is on cloud solutions and how they can affect MDO. According to a paper by Powell [10], the view of cloud services as a service only for commercial and civilian use is being erased and is now becoming increasingly relevant for the military as well. However, there are unique challenges in this, which can be overcome with the right training and the right command and control system.

In an armed forces context, it is thus a matter of enabling communication between different domains but also within a single domain and between different soldiers and officers to be able to quickly take in and process information and orders before it becomes obsolete, incorrect, or has time to become outdated. The fact to consider today is that there is a public cloud today, which is a common definition of cloud computing. In this thesis, the focus is on cloud solutions is already a mature technology and thus the possibility that both the Swedish and British Armed forces start to use it on a larger scale is high [39].

2.3 Frameworks

FMN is mainly emphasized as a central framework where it conceptually contributes to the military being able to synchronize its federated operations through technology, processes, and people. Thus, in this framework, it is included to connect the relationships, technical as well as psychological, between different domains and individuals.

2.4 Warfare and its meaning in this thesis

In this thesis, all kinds of war, indirect or direct armed conflict, will be called warfare, which thoroughly involves engagement or involvement in a conflict or war. The difference in this thesis will be that there will be extra focus on the relationship between peace and war, as a nation can still be threatened by cyber-attacks but not be at war.

2.5 Command and control system, C2 and SWECCIS

Command and control (C2) is a fundamental capability in any armed force. It is the basis for how the military activities are planned, handled, and monitored. The purpose of C2 is thus to arrange activities in space and time to achieve specific goals. Furthermore, the term can be explained in more detail by the fact that C2 works as the majority of processes and attributes that function as a link and a tool for managing both technical and organizational systems to solve problems that arise in both human-to-human situations and human-to-data interaction [11].

3. Related Work

This section will begin with a reflection on the related work, then the topics of this thesis' research questions will be compared with the information of the related work. This is to understand the strengths and weaknesses of the papers are compared with this thesis.

3.1 Organizational interoperability and maturity models

The research on interoperability by Clark and Jones [6] has a strong focus on maturity models and how to use them to build a joint force to meet the challenges of conducting joint operations. Furthermore, the authors highlight the importance of interoperability in operations and how Level of Information Systems Interoperability (LISI) works, which is a model to measure maturity in interoperability. The study aims to explain and highlight the various levels of LISI and get an overall picture of how frameworks such as command and control (C2) work in practice.

In the paper, Clark and Jones [6] provide several metrics for examining and understanding C2 at an organizational level. C2 is a support system for how different military actors can communicate and conduct operations. And in this paper, they describe the various levels of C2, they emphasize that the C2 is task-based, which means that C2 can, according to the authors, be seen to initiate and coordinate a task. Furthermore, they show how the C2 model is built, where the idea is the following, first an event occurs, which triggers a transformation [5].

Based on the paper by Clark and Jones, five different layers of this C2 model are highlighted. These layers divide into two emphasizes, a technical one and one from a human aspect [6].

- The layer that has the most people's emphasis is the C2 framework itself, where the focus is on organization and high-level objectives. The framework is the core and serves as the foundation for the entire process, a process that can be technical, organizational, or legal.
- The second layer, which in this paper is called the C2 process, still has a people emphasis but also a technical emphasis. Here the focus is on identifying which activities individuals and groups operate in operations to build up an intent to adopt common operations.
- The third layer, unlike the two above, is an info bearer and has a focus on both the technology and the people aspects. It is called info management and deals in C2 aspects with managing and retrieving data to use information as a source.
- In contrast to the third, the fourth layer focuses on the technological aspects instead of the managerial where the focus is on information systems that can handle both software and hardware.
- The last layer is called telecommunications and is a so-called data bearer where the focus is on the infrastructure so that information can be sent between different data streams.

Furthermore, there are many different maturity models and how the organizational interoperability maturity mode functions today and what the challenges are with C2 is not yet entirely clear, which is why one of the focuses of this thesis is to go deeper to understand what the requirements are to be able to fully understand this. The conclusion from the authors [6] is that the LISI model has evolved to serve as a model between information systems in terms of interoperability, and requirements can be measured through the different layers and models that are highlighted in the report.

This thesis has built up an understanding of how to approach such models through iterative research cycles that have helped to see LISI from different perspectives, regardless of country or force. This knowledge of how to interpret that model comes from Irani et al. [13]. Where the authors build and highlight methods for analyzing and reflecting on frameworks and models that emerge to promote organizations. This analysis method will be relevant to the method used in this thesis, as it helps to analyze the LISI model correctly.

In addition, another key takeaway is Clark and Jones's [6] proposal for an organization interoperability maturity model, which they believe will serve as material to share in measuring interoperability and examining how the different layers interact with each other. This is interesting as it has contributed to this thesis's understanding of how interoperability can be measured and implemented at an operational level in the military through various information systems. Clark and Jones emphasize how to use this interoperability to build a joint force to meet the challenges of conducting joint operations, which complements this thesis very well as the aim is to understand the requirements of interoperability. These requirements, such as how to conduct joint operations between domains, are not emphasized in Clark and Jones's paper. However, they have a strength in that they in a simple way show five different layers of the C2 model where these layers are divided into two emphases, a technical one and one from a human aspect.

One of the research questions in this thesis is to understand and analyze what the prerequisites of MDO are in terms of people, organization, and technology. Although there is no focus on technical solutions to enable MDO in Clark and Jones' [6] paper, there are some similarities in how they handle the question of organization interoperability, but more on a low level from a C2 perspective. This thesis will on the other hand use that information but also analyze how the Swedish and British Armed Forces can use cloud services and combine it with multi-domain operations.

3.2 Federated Mission Networking (FMN)

In a paper by Runesson [14] there is a strong focus on understanding and exploring how international cooperation can benefit countries such as Sweden in aspects of defense capabilities and through Federated Mission Networking (FMN). Furthermore, digitalization has changed how C2 systems in the Swedish and British Armed Forces need to be updated so it is effective. It is today more complex than ever to conduct military activities to protect Sweden, this can be due to the that the environment in which the military operates has changed, which is a direct consequence of how digitalization has made information sharing and communication more sophisticated. Runesson argues that the Swedish Armed Forces' C2 support system involving cross-domain collaboration has become inefficient and slow [14].

In 2016, Sweden joined the NATO (North Atlantic Treaty Organization) initiative that aims to increase the ability to communicate with each other through control systems. This initiative is called Federated Mission Networking (FMN). FMN is a framework that has been supported by many nations, including the United Kingdom and Sweden. As multi-domain operations become increasingly relevant to build up through solid C2 systems, FMN's main purpose, among others, is to create clear guidelines for how a nation, both internally and externally, can act so that they have a clear process before communicating. The C2 systems, with the help of technology and digitization, will be both smooth and fast with the use of FMN. It should be added, however, that the framework of FMN is still new and at the time of writing is under development, but the basis is there. Further, the Swedish Armed Forces are investing heavily in cooperation at an international level, where one of the keywords in the Swedish Armed Forces is together [14].

The conclusion and the actual product of the paper by Runesson [14] are divided into two parts. The first is that FMN has contributed to increased interoperability in the Swedish Armed Forces due to clearer guidelines on how to communicate more efficiently with the help of computer contexts. The second conclusion is that FMN has contributed to a more dynamic military with increased dynamic communications capabilities. The Swedish Armed Forces have been given a framework to relate to, a framework that has proven to be modular, which means that Sweden can directly copy other countries' control systems but then also adapt and tailor it to the needs and conditions of the Armed Forces. Operations that are common, both nationally and internationally, will become much easier with the help of this framework, this is because it has previously been confusing in terms of communication and control systems as military systems have not followed the digital development to the extent necessary [14].

This paper by Runesson is interesting as it highlights a couple of points that can be linked to the thesis' research questions such as how multi-domain operations (MDO) are becoming more relevant and how to understand the requirements of interoperability. In this thesis, there is also a focus on how Sweden can use (FMN), although the research focuses more on measurement and improvement, while the paper by Runesson has a more focus on the international context of how FMN works on a broad scale, which also is a strength since it gives the reader a clear understanding of the subject. Hence, this thesis is more focused on a specific scale looking at how both the Swedish and British Armed Forces interpret it.

The evaluation and use of information systems and conceptual frameworks have increased in recent years [15], which makes the importance of how understanding the requirements of interoperability even more important. Digitalization has made information sharing more complex and sophisticated, which contributes to the need to understand how to measure complex-dependent frameworks. There are several that can be combined with FMN and one of them is the DeLone and McLean Information Systems (IS) Success Model. This model is based on understanding and processing frameworks to see how they work in the context in which they are used [15], which contributes to this thesis going forward in terms of understanding how FMN is adaptable in order to improve and measure its domain control systems.

3.3 Artificial intelligence and machine learning within MDO

To better understand the technical aspect of MDO, Dinesh and Gregory [16] have placed focus on pointing out that modern warfare is gaining a new standard in terms of moving away from traditional warfighting methods to more digital ones. MDO are a current and efficient way to both manage and integrate the military, so they are coordinated. In the paper by Dinesh and Gregory, there is a tendency to be focused on the army. With that said, AI/ML is a central part of the paper by Dinesh and Gregory, where it is said that it is of utmost importance that there are such solutions for multi-domain operations as armies face much more sophisticated threats today.

It is important to understand how to use modern technology in the form of artificial intelligence and machine learning (AI/ML) to achieve a solid effect in operations in order to read and find patterns [16]. There are many operations in difficult terrain or deep forests where the military can, for example, use smart systems such as AI or ML that can understand and receive information based on the situation and thus give a better statement on how to counteract the enemy.

Therefore, social engineering can be of great importance, and one must understand the reason why these technologies are used to be able to prevent and identify various technical threats. This has been clearly emphasized in the paper by Mann [17], where the author believes that security and technical countermeasures are first and foremost about the individual, which makes it more relevant to understand the individual's role, before proceeding to identify patterns and see how and when multi-domain operations suit who and what.

The paper by Dinesh and Gregory has a strong connection to how AI and ML can identify patterns and see how and when multi-domain operations suit who and what, which gives this thesis' research a strong understanding of how modern technology can be used to improve communication within the military in various domains. One conclusion from this paper is to enable a system and a method to use and understand AI and machine learning to identify when and how to use MDO so that the operation represented can be met. This can be described as a term with the meaning that military operations take place on different terrains that can affect and complicate communication and/or affect storage availability.

Furthermore, there is a tendency in the paper of Dinesh and Gregory that they have a consistent focus on the army, while on the other hand, I want to focus on a joint force between several different domains. This thesis has a mutual focus on technology where Dinesh and Gregory investigate the possibilities with AI/ML while this thesis will focus, from a technical perspective, on how cloud services can be combined with MDO.

3.4 Command and control (C2), and interoperability

Bengtsson highlights the importance that FMN must be fully compatible with the Swedish Armed Forces [18]. The paper by Bengtsson is also a comparative analysis, much like this thesis. There are many resemblances, with the focus on Swedish command and control systems being able to support the use of basic human-to-human communication services. One of the main aspects of Bengtsson's paper is how and what the implementation of FMN means for the Swedish Armed Forces C2 systems, this thesis will analyze a similar aspect but from a distinct perspective. While Bengtsson highlights how different specifications that provide an understanding of how FMN as a framework and how FMN can be compatible, this thesis will focus more on how Sweden can use FMN to both improve and measure its domain control systems.

The paper highlights 4 different terms that have an acronym that is worth highlighting as they provide an understanding of how the FMN as a framework will help meet the management needs of [18].

- Medical Evacuation (MEDEVAC)

- Situational Awareness (SA)

- Joint Intelligence

- Surveillance and Reconnaissance (JISR)

The specifications of the FMN framework, i.e., how people-to-people communicate with each other, should enable the above function chains to be built [18]. For this to be executed so that FMN becomes part of the Swedish command and control system so that it enables multi-domain operations. Furthermore, the defense gradually reaches three different milestones. The first of which is that there are guidelines for how each operation is handled and that there is an infrastructure for security in communications. The second milestone is that there will be a common infrastructure for all security but that each operation is managed according to judgment. The third and final milestone is that all levels of security and operations have a common infrastructure, across the joint forces [18].

A support system called Swedish Command and Control Information System (SWECCIS) is highlighted repeatedly since this support system is a key that can positively influence the defense from both a technical and an operational perspective. SWECCISS can, with the help of FMN and the milestones required to reach a full command system, is the most suitable system today to make FMN compliant. On the other hand, SWECCIS lacks some communication services today, which makes the realization challenging for the Swedish Armed Forces. The study is interesting as it highlights how interoperability and command and control support systems in the context of FMN can be realized and what is missing for it to become a self-sustaining operation.

A strength of Bengtsson's research is how he in a simple and nuanced way describes FMN as a framework and what it means in practice to be able to be fully integrated so that the Swedish Armed Forces can create a modern and functioning command and control system.

3.5 Network architecture for communications

A paper by Durresi et al. [19] is interesting as it has many similarities with this research. Durresi et al. want to highlight the importance of how today's modern conflicts and warfare take place in more complex ways than a few decades ago. The domains need to communicate confidently and quickly with each other, which the authors call Heterogeneous Multi-Domain (HMD) architecture. Furthermore, different protocols interact and talk to each other through different networks, regardless of the type of terrain or domain [19].

In comparison with previous related work in this thesis, this is more dependent on technology, where the focus is more on the technology and software behind a solid and efficient multi-domain architecture. The paper describes this HMD protocol as a tool where it uses a network with different gateways for communicating. These gateways act as a parabola for communicating and supporting intercommunications between different domains through different protocols so that the, for example, the army and the navy can communicate in multi-domain operations. As for the infrastructure, HMD uses the protocol of a virtual hierarchical one, which is connected to different domains during operations and war. The multiple gateways are crucial in terms of translation in various means of communication such as security and signaling. The conclusion in their paper is above all the development of HMD will help military operations to become more agile and better at meeting today's digitalized warfare, which has been characterized by a lot of cyber and proxy situations [19].

The advantages of HMD protocols are many, partly because it is scalable and promotes based routing, and partly because it supports and satisfies the need for node mobility which in the long term also supports the adaptive networks in aspects of bandwidth. This makes it much easier to satisfy the need for communication in multi-domain operations. In this thesis, there is a focus on understanding the holistic view in MDO where the requirements and the conceptual frameworks for interactions between human-to-human using technological communication services. Furthermore, the technology behind different protocols is not entirely trivial and thus requires work and a certain foundation to stand on. HMD protocol is a tool that is interesting from this context, where you use a network with different gateways to achieve a kind of parabola for supporting intercommunications between different domains through different protocols. Computer networking thus becomes central here to understand why and how various network layers can work in MDO, at the same time as one can then build on with a cloud solution to communicate smoothly and quickly. In the work of Kurose and Ross, this is described in a nuanced way from start to finish where the focus is on how communication and networking work from the application layer to the physical hardware [20].

Another strength is that Durresi et al. describes why today's modern conflicts and wars take place in a more technically complex way than a few decades ago, but also how we can respond to them with the help of technology and digitalization. In comparison to this thesis, it is significant to understand how and why domains need to communicate smoothly and quickly, which is highlighted in Durresi et al. [19]. However, there is a gap in what it looks like on an organizational level, which this thesis complements effectively as my idea is to produce an analysis of how, in military contexts, several different domains can talk to each and how it works on an inter-organizational scale.

To understand the prerequisites for different countries to use MDO to become more inter-organizational efficient, it is important to require an understanding of what it is for abilities that affect MDO from a technical perspective. In order to achieve an overall understanding of the technical perspective, Durresi et al. research will contribute to this thesis to build on those technical aspects. Although the focus will not be on working and doing studies with various protocols in this thesis, Durresi et al. work may be the building block for how this thesis reasons about multi-domain operations [19].

4. Method

In this part of the report, the approach is presented in terms of how I have worked to be able to answer the research questions. The method for this will be presented in chronological order where the method and the feasibility study are first described, and then go deeper into how the data have been collected and how the handling of that data collection took place.

4.1 Research method

The method for the approach of the thesis has been mixed-method research where the focus is on interviews, documentation, and literature review. This thesis will be based on what has previously been presented regarding MDO, and in addition, it will bring up new perspectives and results. Furthermore, the method for collecting and analyzing data will be based on Rowley’s [21] paper. There she shows how and when to use a case study to do research, to answer the questions by using data collection and data analysis, since if there is a subject with a valid theory that has not been fully explored, then a case study is a well-chosen method. She further describes that the key here is to use different types of data collection sources, in order to gather as much independent information as possible.

The following timeline is how the work will go in this master thesis.

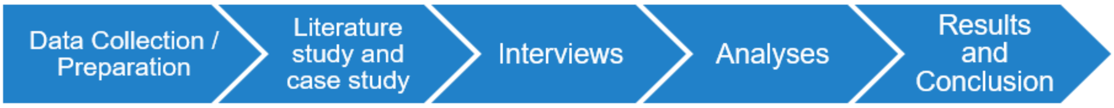

Data Collection / Preparation
Literature study and case study
Interviews
Analyses
Results and Conclusion

Figure 4.1: Showing the timeline of the thesis, starting from left to right

4.2 Pre-study

Since the concept of multi-domain operations is today relatively unexplored [4], while also requiring a lot of work for someone who is not familiar with military terms and doctrines, a lot of preparation was required to understand and find a relevant way to process all literature. Furthermore, the idea was in the pre-studies to divide into two different main parts, where the first is to conduct a comparative case study and the second to analyze the data and information from the case study to understand and answer the research questions. When conducting and following up on the study and way of working in this thesis, it has been based on the material of the guidelines from Kitchenham et al. [22]. The guidelines, in short, means that a systematic review has been implemented where clear goals have been set for what is to be carried out and where the literature study has acted as a cornerstone for the interview and data collection.

Furthermore, the choice of sources has also been influenced by the guidelines. Kitchenham et al. where this thesis has a large selection of sources written by individuals with expertise and recognized expertise in each field, such as individuals with long experience of command-and-control systems in the Swedish and British Armed Forces where the importance of how many, for example, have cited their work, has been of great importance. In other words, this thesis has, in a predominant way, followed Kitchenham et al., by first planning the review itself, and then gathering information and data, which was done through interviews in this case. Finally, an analysis of this review has been made. Given that the area in which this thesis is conducted, is broad and to some extent abstract, a systematic and thorough way of handling all documents and literature was required, and Kitchenham et al., methods have thus been used, as the guidelines. Furthermore, shorter informal interviews have been conducted with people with a background in the MDO to confirm the need for a nuanced picture of MDO and to ensure that people believe that research questions are relevant.

This thesis is built up with the help of existing theory and knowledge from other individuals and research, while it also builds on that theory with assumptions and conclusions such as how cloud services can be integrated or what the conditions are to perform multi-domain operations. Most of the documents in this study has been taken from either the Swedish Armed Forces or FOI, where the focus has been on various C2 reports and doctrines.

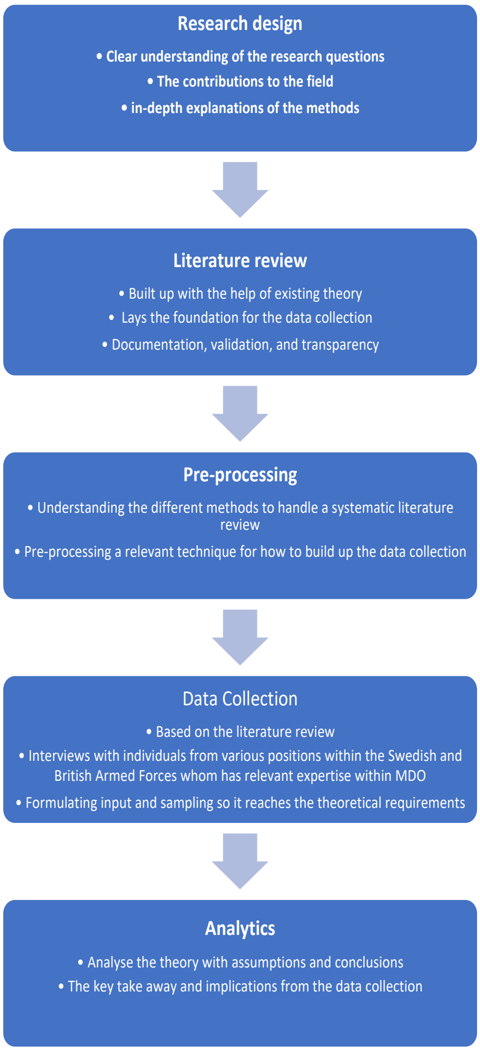

Research design
• Clear understanding of the research questions
• The contributions to the field
• in-depth explanations of the methods
Literature review
• Built up with the help of existing theory
• Lays the foundation for the data collection
• Documentation, validation, and transparency
Pre-processing
• Understanding the different methods to handle a systematic literature review
• Pre-processing a relevant technique for how to build up the data collection
Data Collection
• Based on the literature review
• Interviews with individuals from various positions within the Swedish and British Armed Forces whom has relevant expertise within MDO
• Formulating input and sampling so it reaches the theoretical requirements
Analytics
• Analyse the theory with assumptions and conclusions
• The key take away and implications from the data collection

Figure 4.2: Illustration of the analysis model for this thesis in chronological order.

4.3 Research questions

In this section, the research questions will be broken down into sub-questions, to partly answer the questions in more detailed ones and partly to make them more specified. As this type of research is more theoretical than practical, it leads to an importance in having extra accuracy and clarity about my research questions. The questions can also be changed and developed while the work continues. Therefore, it is very important to break down the questions into smaller components to provide a nuanced picture of what the questions mean in more detail [23].

My thesis is built around understanding and doing a comparative case study where the key is, according to section 1.3, to see how the Sweden Armed Forces compares to the British Armed Forces in its approach to MDO. Why the UK was chosen to compare with depends on three different factors. The first is that the UK may have some similarities with Sweden culturally, the second is the countries' respective defense forces have good relations and the third is that the comparison is relevant as the UK has come further in its process of enabling its MDOs than Sweden, which gives contrasts that becomes interesting to analyze.

Furthermore, there are three different research questions from section 1.3 in this thesis that will be focused on, in addition to analyzing the general interpretation of MDO, where the first is to do a literature study on the prerequisites in terms of people, organization, and technology are, where focus on the technology aspect is how and when to use collaborative technologies for MDO. In more detail, this means the following:

- What are the prerequisites for Sweden and the UK to apply MDO today, based on what the stakeholders linked to the Swedish and British Armed Forces say?
- What technical solutions are used today and in which scenarios are such services relevant to improve communication?
- How do communication and language between domains affect the ability to apply MDO?

The second question is to see how Sweden can use FMN to improve and measure its C2 systems? This in turn can be explained in more detail in this way:

- Where does Sweden stand today regarding FMN?

The last question is what conceptual frameworks in the form of literature reviews exist that can be used to support MDO and to understand the requirements of interoperability? This research question can be defined as the following:

- Are the concepts of MDO aligned with the needs of the Sweden Armed Forces?
- Are there any differences between Swedish and the British Armed Forces in requirements of interoperability?

With that said, these are only sub-questions to my research questions, which will be a way for me to manage and analyze my data collection and be able to filter literature reviews so that the conclusion answers the research questions in a correct way

4.4 Data Collection

The data collection consists of literature studies and interviews. The literature study is a combination of research and internal documents from the Swedish Armed Forces and FOI.

4.4.1 Literature review

Understanding the whole MDO concept requires a certain amount of familiarity with the subject, which required me to create an overview of research and work that has been done previously in this field. The documents that have been read, are mostly written by FOI and the Swedish Armed Forces, where the focus is on command and control (C2), and interoperability. This has since laid the foundation for what would be my data collection for the interview. The literature study will involve a critical and systematic review of current work done in the MDO sphere with summaries of the relevant articles. Thus, the review is based on a systematic review, which is described in Needleman's paper [24], which means that this thesis has in the following way built up its literature study, where identification of various research and materials in the relevant field has been carried out, to then evaluate and select which are best adaptable to this thesis' research questions. Furthermore, the literature has been found in two different ways, one is through search terms where keywords such as interoperability in the military, have been searched for in various media such as Google Scholar and by searching for material that was created by FOI and the Swedish Armed Forces. The other documents, such as the DGO report [31] was given directly by FOI, where they proposed and gave this thesis several documents, to carry out a systematic literature review.

4.4.2 Semi-structured interviews

To be able to answer the research questions, semi-structured interviews were chosen as a method. Semi-structured interviews mean that the interviews must be prepared with a template and questions, but there should still be plenty of opportunities to speak freely, so it becomes a dialogue instead of a monologue [25]. In each interview this thesis became unique, as it depended on the person’s background, the questions could be changed or revised during the interview. This is important as the subject is still in the development stages and there are many opinions and perspectives on how things can work. The challenge here was to build up questions that allow the stakeholders to highlight their perspectives. To enable this, the questions have been designed so that the questions can quickly change guidelines to be able to match the person's expertise, even more, so that both the validity and reliability of the answers increase. The experience of Hove and Anda [25] also shows that language barriers and the fact that different people in the same subject have different perspectives can contribute to difficulties when conducting semi-structured interviews. This has contributed to the interview questions being designed iteratively to minimize the risk of misinterpretation of the questions.

This method has to some extent been based on Kallio et al. [26] paper where the method has been built up by first understanding and identifying the prerequisites for what is required to use semi-structured interviews, then pilot testing the questions and possibly revising them so that they are better adapted. In this way, it becomes iterative when you go back and see how the method can be improved. The interview material was produced in connection with what my questions were based on, at the same time as there was a mixture of more open questions and questions that are more specified. The focus was placed on the fact that each question has a connection to one of my research questions and that the questions could be answered within a reasonable time, where there would also be room for further discussion.

The selection of interviewees is made so that there will be a mixture of people active in different areas but with the same goal, where the focus was to interview people with different skills but also with a different insight into both the Swedish and British Armed Forces. The interviews took place digitally in Zoom or Skype for all interviews where the questions for the interview had no special order or consequence, rather depending on who the interviewed participant was and what knowledge the participant had. Eight interviews were conducted. Four of the participants have experiences from different fields in the Swedish Armed Forces, one of them has been working in both the Swedish and British Armed Forces and two of them are in the British headquarters, more about the interviewees will be presented under the result section 5.3.

4.4.3 Procedure

As previously mentioned, all eight interviews were conducted digitally, to save time when all the participants in the data collection were in other locations, and some in other countries, simultaneously as there has been a pandemic during 2020-2022. As described in Appendix 1, the interview began with a general background explanation where the focus was on why this interview was conducted and what the purpose of this thesis is. When this was done, the participants described their experiences and what they have done in the military sphere before. The interview material described in the appendix was used to have something to lean on and to have support so that the interview flowed naturally.

The questions had no special order, but for the most part, they ended up in the order best suited for the occasion, for the interview to flow naturally and because many of the questions opened for other topics of discussion. So, to not lose valuable time, prioritization was required to get the most information from the person’s expert area. Furthermore, it was rare that all 16 questions were raised during the interview, instead, the selection of these questions was adapted to the individual who was interviewed and if that person had other experiences that were more suitable for delving into certain other issues, thus some questions were prioritized more than others. Furthermore, every person that was interviewed was continuously encouraged to think freely and give their personal and open opinion as well, especially if they felt that the question that was asked was not in their expert area.

4.4.4 Comparative case study

A comparative case study means that there is a clear case to be studied but that it will also be compared, cases with each other. This type of case study aims to go in-depth within some processes and events, which are then simultaneously compared with various current research. Through this one can see and understand why and how certain things happen and, through the comparison, see what that can do to achieve a certain scenario. Additionally, in a comparative case study, some comparisons are horizontal and vertical that involve both analyses and theories of a particular part of different cases that have the same outcome [27].

4.4.5 Internal documentation

Much of this study is based on documents provided by FOI, these documents include reports and events that describe where Sweden stands today and what is happening. Furthermore, a total of 13 different documents have been provided for this thesis, to get acquainted with the situation of MDO and partly to build on the current literature study. Thus, most of the document was official, such as concept notes, doctrinal documents, and reports

5. Results

5.1 Interpretation of the literature review

In this section, a literature study is conducted where the study focuses on how the conceptual framework works for the development of the operations within the Swedish and British Armed Forces, how the technical solutions for having complex capabilities in the Armed Forces are, and an interpretation of organizational interoperability within the Armed Forces are.

The documentations that will be used in the interpretation of the literature review is primarily based on “Ledningskoncept 2035 - Resultat av 2018 års konceptutveckling” [12], “Från internationellt samarbete till ett nytt svenskt ledningssystem” [14], “Vad innebär införandet av FMN för Försvarsmaktens insatsledningssystem” [18], “Networking, Affiliation Beslut – Försvarsmaktens svarsbrev om Federated Misson” [29], “Doktrin för Gemensamma operationer (DGO)” [25] , and “Future Command and Control and Command Posts – project report 2021” [30].

5.1.1 Conceptual frameworks for the development of operations

To enable MDO in both a national and international environment, well-developed command and control systems are required, as the environment and the arena in which the Swedish Armed Forces carry out operations have changed. With the change, it means that nations today are sensitive to digital attacks, more complex warfare, and increased globalization. The conceptual frameworks that exist today include FMN. Today, the FMN concept as a framework is not fully integrated into the Swedish Armed Forces [18] .

To be able to comply with this framework, it is necessary for command-and-control systems in Sweden to be updated. According to Runesson [14], this concept contributes to the methods for the command systems becoming more transparent by having routines that are the same for other countries within NATO, which also follow the FMN concept. Furthermore, according to the study, this conceptual framework for the development of operations contributes to routines that are mutual throughout the hierarchy, both horizontally and vertically. Which makes it easier to share information and knowledge between different ranks, as routines are created. When information sharing becomes more accessible, it contributes to the Swedish Armed Forces being able to create better conditions for being able to collaborate with others. This collaboration, which is created through better information sharing, contributes to the Swedish Armed Forces being able to handle crises or possible changes better and faster [29].

FMN contributes to information sharing operations, and this takes place across the domain control systems. How the process of information sharing takes place is in an agile way that is carried out iteratively to constantly stay updated while improving the process for each iteration. An illustration of that process is shown in Figure 5.1.1.

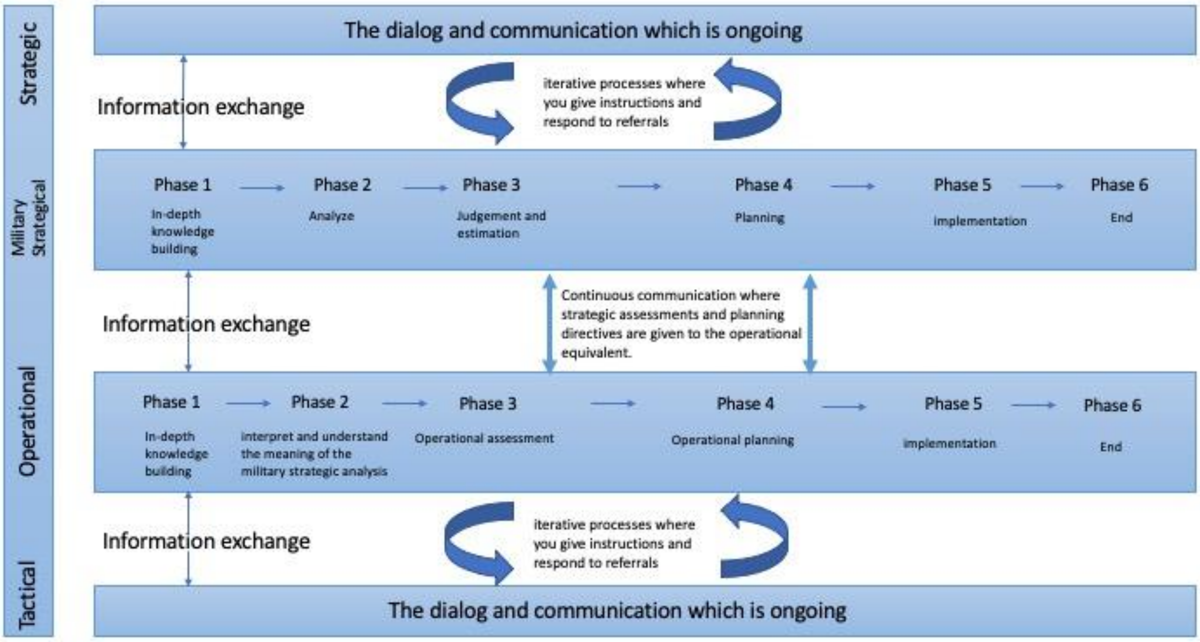

Strategic
The dialog and communication which is ongoing
Information exchange
iterative processes where you give instructions and respond to referrals
Military Strategical
Phase 1
In-depth knowledge building
Phase 2
Analyze
Phase 3
Judgement and estimation
Phase 4
Planning
Phase 5
Implementation
Phase 6
End
Information exchange
Continuous communication where strategic assessments and planning directives are given to the operational equivalent.
Operational
Phase 1
In-depth knowledge building
Phase 2
interpret and understand the meaning of the military strategic analysis
Phase 3
Operational assessment
Phase 4
Operational planning
Phase 5
Implementation
Phase 6
End
Information exchange
iterative processes where you give instructions and respond to referrals
Tactical
The dialog and communication which is ongoing

Figure 5.1.1: A simplified illustration of the flow when doing the planning and information change [28]

In Figure 5.1.1, the framework is demonstrated so that information sharing should be smooth, regardless of which staff you are in. The process for this conceptual framework is that through an in-depth knowledge build-up, an analysis begins and is then sent for assignment review, considerations, and assessments. This leads to phase 4 where planning takes place over an operational concept and an operations plan (OPLAN) [28]. Furthermore, the process leads to an implementation where the focus is on development and evaluation, to then end up in a conclusion and move on to new tasks, hence iteratively. The process for this knowledge building has its foundation in agile work processes where the focus is on coordination and communication between individuals and internal organizations where all phases and levels overlap [28].

For the Swedish Armed Forces to use FMN and improve communications systems, it is an important factor in quickly making decisions faster than the enemies does. Thus, FMN becomes a framework for being able to handle decisions more timewise and more efficiently than the opponent. Something that is important is the concept of modular control where FMN is seen as a framework to be able to be adaptable and thus shape each unique case according to the needs of each unique operation [29].

The Swedish Armed Forces' goal is to have a fully realized FMN concept by 2023 and fully integrated it into operations [30]. At the same time, the study shows that there is still a lot to do, especially in the digital and technical sphere, today there is mostly support for services that include human-to-human interaction because in FMN there are different specifications, while Sweden has only full reached the level that is at a communicative level such as informal messaging services and audio-based collaboration services. One of Sweden's C2 systems, SWECCIS, still has some spiral specifications left to support, where a common denominator is the technical aspects to make Sweden's command and control system more integrated and useful [28], [31]. Furthermore, each development step toward a fully compatible FMN is described as an FMN spiral, wherein each step the focus is on the architecture, technology, communication process, and standards.

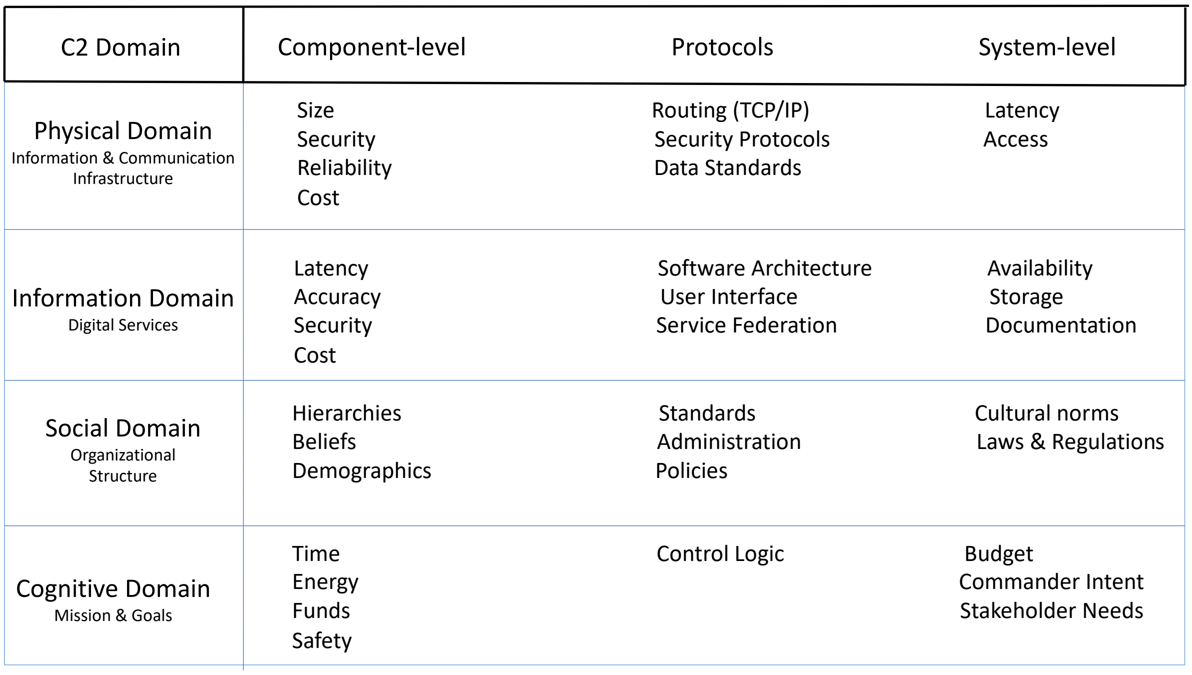
In the UK, it is different as they have a much greater global experience than Sweden has as they have built solid experience from their operations in Afghanistan which required them to have a more FMN-compatible military at the same time as they have become forced to act in joint forces in several domains. Within these experiences, they have both managed and configured spirals 1 and 2 where they built a network through The New Style of IT (NSoIT) program that provides solutions for communication through network systems and communication that simplifies federated networks [32].

5.1.2 Technology solutions and information systems within MDO

To fully be able to integrate into the framework and make MDO a realization, the technical parts must be in place. Hence, technical solutions and measurement systems such as cloud services and LISI within MDO are a must to realize such operations.

An essential part of the command and control systems is based on an information system, where there is a framework that revolves around different levels of networks. To enable MDO within the Swedish and British Armed Forces, there must be an architecture for implementing and promoting the technical communication between different domains [29].

Table 5.1.2: Adapted table which shows the different architecture for four domains as described in [33]



C2 Domain	Component-level	Protocols	System-level
Physical Domain Information & Communication Infrastructure	Size Security Reliability Cost	Routing (TCP/IP) Security Protocols Data Standards	Latency Access
Information Domain Digital Services	Latency Accuracy Security Cost	Software Architecture User Interface Service Federation	Availability Storage Documentation
Social Domain Organizational Structure	Hierarchies Beliefs Demographics	Standards Administration Policies	Cultural norms Laws & Regulations
Cognitive Domain Mission & Goals	Time Energy Funds Safety	Control Logic	Budget Commander Intent Stakeholder Needs

From Table 5.1.2 we see what Eisenberg et al. [33], has developed to show how C2 revolves around different levels of networks where each C2 domain (not to be confused with domain in the MDO context) has different requirements for its infrastructure and component constraints. To achieve a full MDO where everyone in the Swedish and British Armed Forces experiences a synergy in their interoperability, it is required that each C2 domain achieve the goals described in Table 5.1.2.

Interoperability as a concept can also be described in smaller components such as Levels of Conceptual Interoperability Models (LCIM). By building up the concept and describing it through seven equal network levels, all to make it clearer to the user how and what is required to achieve adequate interoperability. According to Tolk et al. [34], LCIM has contributed to a framework that relates to a standard that can demonstrate and act as a basis for how the Swedish and British Armed Forces can handle challenges to be able to cooperate through information systems. In this model, three layers should be met and understood to achieve interoperability that can be simulated and implemented with the help of information systems:

- The technical
  - The focus here is on the infrastructure connected to networks that will then assist the Swedish and British Armed Forces with integrability
- The syntactic
  - The focus is on the interpretation of messages and the data format, which differs depending on the country
- The semantic
  - Focus on how different levels and/or individuals within the organization exchange information with each other through language and text

All the above layers require a deeper technical foundation where information and software can be exchanged and shared through different networks and at the same time via interfaces where middleware can be used [34].

Semantic interoperability has been clearly described as an important part of achieving complex and adequate communication for the exchange of data, where the information from the data only arises when it is interpreted, i.e., it is only with the receiver or transmitter that one can talk about information. The need for this type of interoperability comes from ambiguous information exchange. However, semantic interoperability is still today only in the concept stage but is an important pillar for achieving good interoperability where one can transform information through predetermined ontologies.

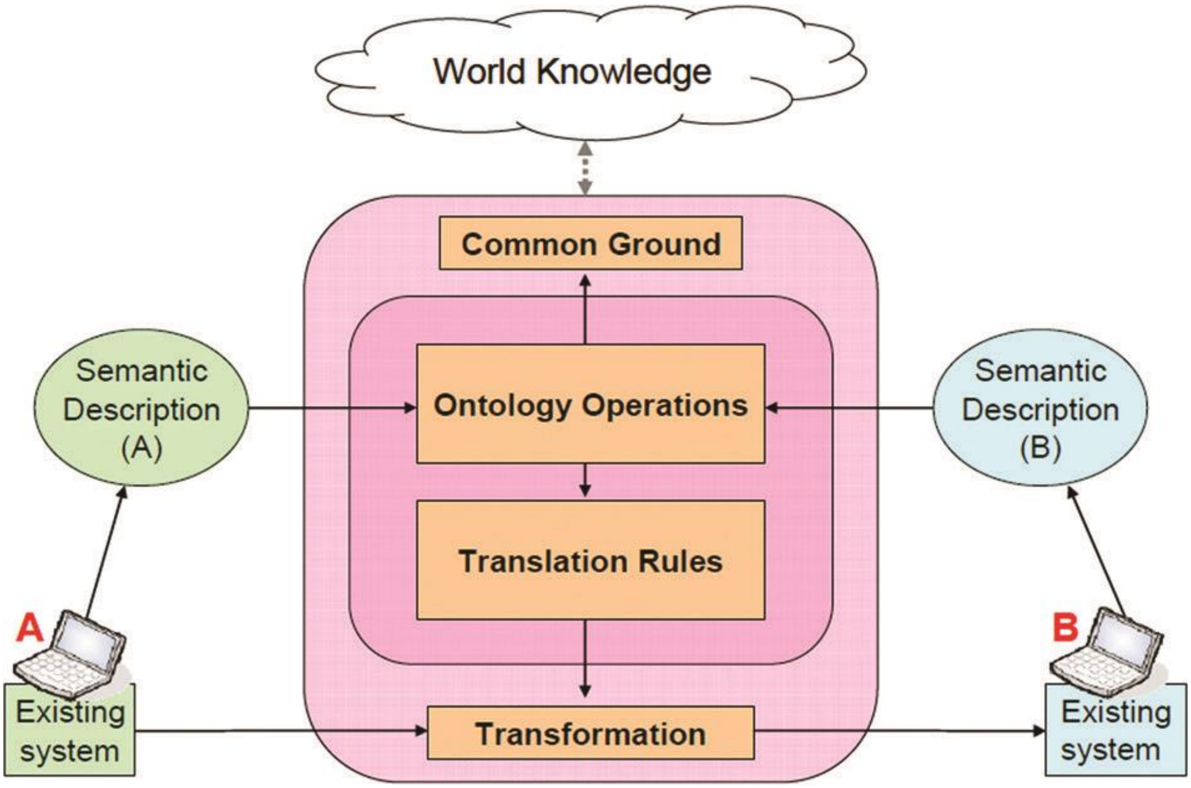


Figure 5.1.2: Shows how semantic interoperability works on a conceptual level, retrieved from [35]

Semantic interoperability assumes that there are two or more systems or individuals interacting with each other and where there are already established rules regardless of where or who you are. There a manual intervention interprets the meaning of the information so that the exchange of information becomes understandable regardless of whether you are out in the field or sitting behind a desk [35].

The information systems that come with FMN are both complex and require a change in Swedish Armed Forces' structure. Information systems that have been affected by FMN's introduction have different security levels, where all levels have their network and information infrastructures (NII). In this infrastructure, information is thus exchanged, both through domains and through networks where the purpose is to retrieve information through a logical domain and quickly return the information with a flow that is continuous [18]. In such systems, that are integrated with FMN's concept, however, it makes a difference whether it is at a low or high tactical level. In the lower levels, the focus is on the exchange of information in the form of easier technical solutions such as chat, email, and replication. While in the higher operational technical level, SWECCIS is to be adopted and used. The technical description of SWECCIS, which is available for sharing and exchanging information, has been built up so that it can be integrated and synchronized with softwares at the same time [18].

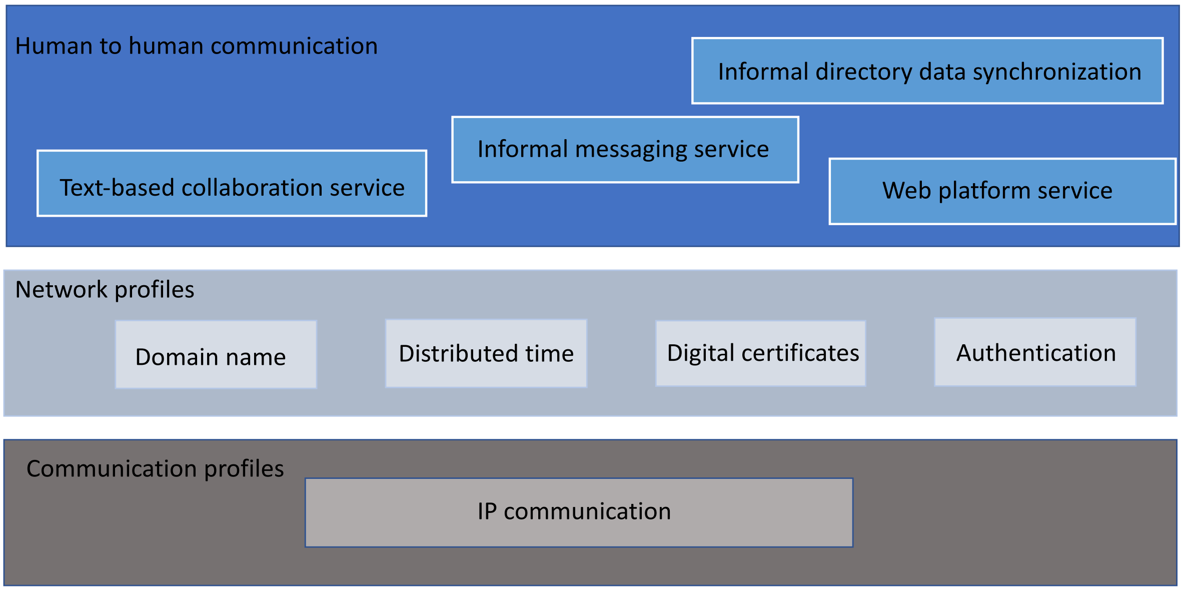
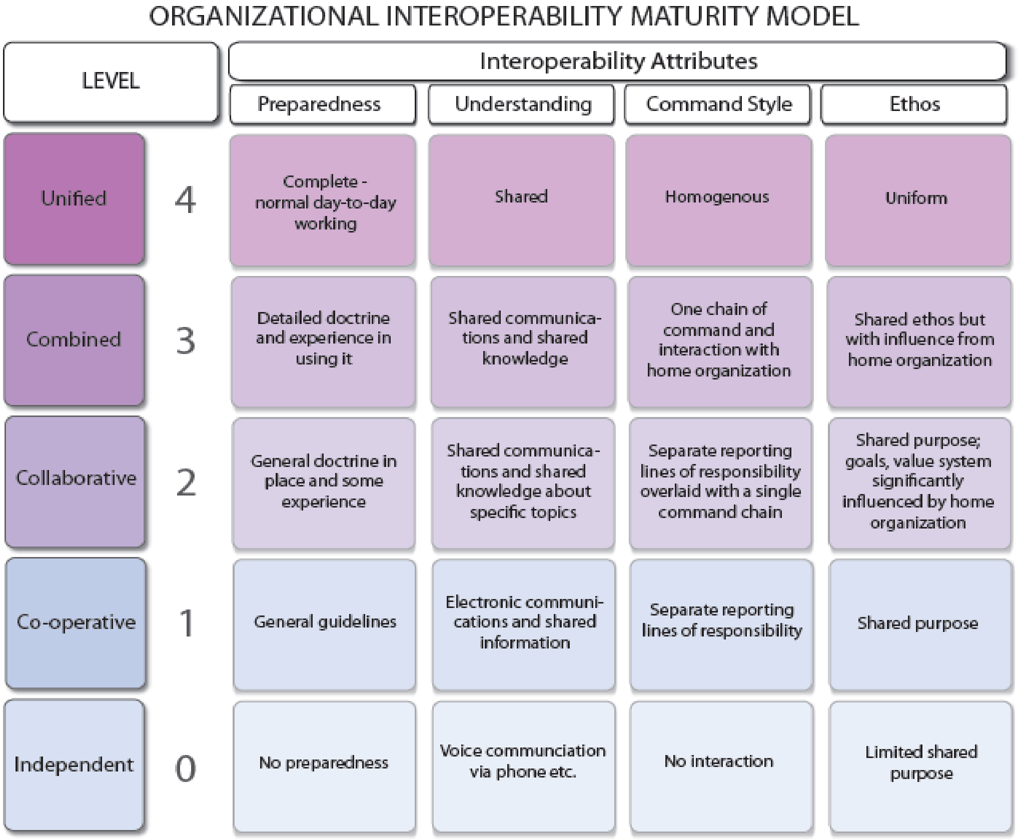


Figure 5.1.3: An adapted illustration of what SWECCIS architecture looks like, from an FMN spiral 1 perspective [18]

5.1.3 Organizational interoperability

Rules, policies, and security are three keywords that are emphasized in the study when the interoperability in aspects of information sharing becomes relevant. FMN has made guidelines and standards regarding these aspects of security, but how each country adopts them is not entirely clear in an era of technological development where different militaries have made different advances in technology and infrastructure. However, there is a deficiency in terms of who should have access to what and how the exchange, legally takes place between different nations [36].

Regarding organizational interoperability, a recurring model in several studies is LISI, which is described in section 3.4. From Figure 5.1.3 in Anderson et al. [37], organizational interoperability is highlighted as a model of maturity to assess and see where an organization is, and to classify the interoperability capability.



ORGANIZATIONAL INTEROPERABILITY MATURITY MODEL

LEVEL		Interoperability Attributes			
		Preparedness	Understanding	Command Style	Ethos
Unified	4	Complete - normal day-to-day working	Shared	Homogenous	Uniform
Combined	3	Detailed doctrine and experience in using it	Shared communications and shared knowledge	One chain of command and interaction with home organization	Shared ethos but with influence from home organization
Collaborative	2	General doctrine in place and some experience	Shared communications and shared knowledge about specific topics	Separate reporting lines of responsibility overlaid with a single command chain	Shared purpose; goals, value system significantly influenced by home organization
Co-operative	1	General guidelines	Electronic communications and shared information	Separate reporting lines of responsibility	Shared purpose
Independent	0	No preparedness	Voice communciation via phone etc.	No interaction	Limited shared purpose

Figure 5.1.3: An illustration of what the different attributes and levels look like in aspects of the interoperability of LISI, retrieved from [37].

Furthermore, LISI is a model for managing interoperability between different systems and not between users. This is because the system as a model is based on only assessing the information systems' interoperability, which can then be evaluated to see and evaluate whether one's information system is sustainable from an organizational perspective [38].

5.2 FOI and its current work

The current work that FOI has performed regarding MDO, interoperability, and command and control systems, will be interpreted and explained through observations and comparisons. Something that is emphasized [31] is the fact that organizational system thinking is required to achieve an MDO context. Furthermore, the organizational system thinking is more relevant from the Swedish Armed Forces perspective, while the British counterpart, focus more on orchestrating collaborations. In this context, orchestrating collaborations means that the Swedish Armed Forces, through integration, performs well-planned activities and measures.

Furthermore, in aspects of C2, there has been some focus on how AI can change and influence the Swedish Armed Forces in multi-domain contexts [31]. Something that is highlighted earlier in this thesis' literature study is information and data sharing, where there has highlighted several hypotheses about how AI can affect data sharing possibilities. These possibilities are reflected as a kind of "information broker" by managing and analyzing all the data that comes in and making it adapted for the operating and tactical receivers. This can be compared to targeted ads that are commercially available [39].

Furthermore, the theme around C2 agility and agile forms of system working have developed and become much more vital today in terms of MDO. The idea for C2 agility was developed by NATO STO's research groups SAS-065, SAS-085, and SAS-104, where the focus was on how information sharing can be streamlined and made more accessible, which has been a current issue as the organizational structure of a military organization is hierarchical and traditional. The empirical study shows that the British Armed Forces have shown more commitment to introducing agile thinking within their organizations where decisions and ideas are not divided according to rank but according to competence and needs [39].

The following figures will be regarded as a demonstration and clarification of what MDO means, as it has been interpreted from the DGO [31] and which this thesis has since collected and reproduced in its interpretation.

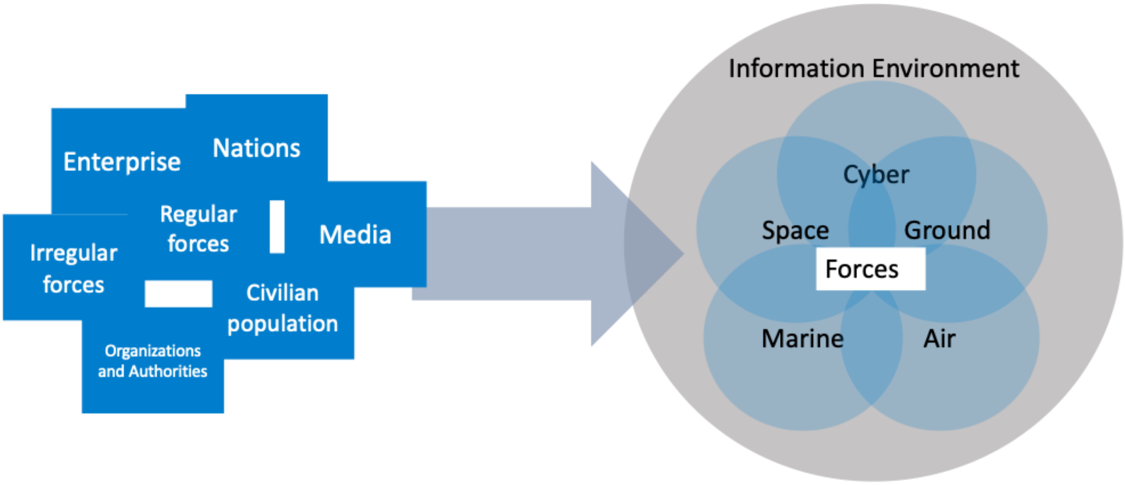


Figure 5.1: This shows how the domain concept tries to achieve synergies by acting together in the information environment, here it will be independent of which branches of defense the forces belong to, but it will be that of joint forces, independent of units or domain, coordinate attacks.

5.3 Results from the data and interview collection

In this section, results from this thesis' interviews will be taken up and presented. The results will be further divided, where the answers from participants that are considered to be most relevant for this thesis, will be interpreted and translated, and then presented where first the question itself will be addressed and then the description made by the participants will be presented.

Clarification of notation

All eight individuals who participated in the study will be presented with an ID code before their input and answers are presented. The second column presents whether the individual works for the Swedish or British Armed Forces, or whether the person has insight into both. The third column superficially presents the individuals' experiences in the form of the number of years in the military or other factors that may be interesting to know. Furthermore, all the results from the interview will be called for the participant followed by a parenthesis with its ID code where the answers will be in quotation marks and indented paragraphing, to make it clearer. All excerpts I present are based on my notes. Many times, these types of excerpts are based on verbatim transcripts from recordings, and that is not the case here. Each excerpt will be divided into a number, to facilitate references when analyzing the text.

Table 5.3 Information about the participants of the interviews

ID-code	SWE/UK	Experience and background
A	Swedish	10-15 years' experience within interoperability and FMN
B	Swedish	20+ years within the FMV, experience within interoperability
C	British	20+ experience, UK military. Expertise within concept dev. and MDI
D	British/Swedish	Worked at the Swedish and UK HQ, expertise in C2 systems
E	British/Swedish	Stationed in the UK military, 10+ years of expertise in concepts & doctrines
F	Swedish	30+ years' experience in the military and FMV. Expertise in C2 systems
G	Swedish	15-10 years' experience within interoperability and FMN
H	Swedish	35+ years in various positions in the Swedish armed forces.

5.3.1 General aspects of MDO

The three participants (C, D, E) with insight and experience of the British Armed Forces had the same starting point regarding their view of how they define domain and multi-domain in an armed forces perspective, whereas one participant (D) developed it on the following way.

1) "There are five domains, the concept of system engineering vocabulary where a domain should have a purpose and a delimitation is under development. There are today 5 operational domains, which differ between countries. The UK has decided to merge the electromagnetic spectrum and cyber into one domain. These domains are used for planning and seeing where you as an organization can get the most effective. With that said, it is more conceptual thinking. Suppose that there is the land domain, which should not necessarily be the army, but the land domain is an abstraction that makes us influence each other. Nevertheless, the traditional domains are off the land, maritime air and then space and cyber and electromagnetic."

The participant then develops his reasoning with an example

2) "To operate from the ground domain for example with the help of air defenses. The meaning is that you stand on the ground and shoot air missiles at an aircraft in the air and then you have worked from one domain to another. And in the same way, we can coordinate combat in the naval domain by firing naval target robots both from aircraft, boats, and ground-based robot installations towards the same target in the domain. And in this way we coordinate combatants. Some domains depend on some. So, for example, to get up in the air, you need to take off in an airplane on the ground. So what is our new domain?

When discussing whether the participants think the concept of multi-domain operations is important, there were mixed answers, however, all agreed that the concept itself was important, the participant (C) described it as the following,

3) "So, my personal view is that a lot of people use the phrase multi-domain integration and I do not think anyone has any particular precise meaning behind it, so MDI can mean a lot of things to many people, for me, I think it is a buzzword.

While (D, E) had a different approach to the issue where they expressed it as follows,

4) "What is important is the coordination that takes place because the UK does not have sufficient capacity if you were to select an individual system where you only choose one system which should affect an opponent. But if we merge the systems so that they work together and we call it a conflict with systems that work together, then you can achieve a higher effect than the individual systems individually, i.e., that you achieve synergy effects."

Regarding the conditions for the UK to participate in multi-domain operations, both internally and together with other nations, the same participant (E) described overall in the following way,

5) "We have cultures to take into account and then we have the system support itself to have technical conditions to cope with this and that there are also limitations in it as well. Getting this coordinated management is thus a challenge."

While participant (D) describes and compares with Sweden in a more detailed *way*

6) "It is more difficult for the UK because their management structures are different as it mostly leads operations abroad. But in Sweden, they lead everything from the operational staff, which makes Sweden more suitable. Compared with the UK, Sweden has come to different distances between different branches of defense in how interoperable we are with other nations. If you look at it purely doctrinaire, at the command-and-control system, how do you handle future management in a complex environment in MDO, how can you then use the effect? If we are imagining a larger ship with a helicopter taking off, then what domain belongs to the helicopter? Air or marine? Marine commanders in the future may become domain commanders over the effect in marine domains."

Two other participants (D, E) emphasized the importance of having challenges from an IT and organizational perspective. One of the participants (D) expressed it in the following way,

7) "Legislation is an important part of this. Common data standards and security are important to look at. Further, the language around it is important as well. If you are sitting on the other side and receiving a classified message, it is not entirely trivial that it is interpreted correctly. Then we have compromised some information in that sense that the data is compromised, so having common data standards and security classifications is important to under each other."

Worth considering was when participants with Swedish input were compared with the British equivalent, was that the British participants had a different view of MDO and instead called it MDI (multi-domain integration). When asked what the difference between MDO and MDI from a British perspective is, one participant (C) answered with the following,

8) "MDO comes from the US Army and was an approach to how to handle A2AD (area denial weapon or anti-access / area denial) for the army. MDI is more than an army force operation in an A2AD bubble, this is about using the entire keyboard of "state power, where the allies and the military domains should achieve the desired effect. Both countries are aiming for the same thing, but the fact that the UK has come a long way in their approach to composite operations means that they have a slightly different focus on how to integrate in a digital architectural way."

5.3.2 Needs and requirements

Regarding what MDO looks like in the relationship between war and peace from a multi-domain perspective, a participant from the UK described his perspective in the following way,

9) "The distinction between war and peace is less relevant than it used to be. Activities that looked like warfare, but maybe aren't war and not a declaration of war in the official sense to the below level of war. Historically, the UK has liked to have power and influence globally. That, that history has a legacy, and it has a legacy that the UK continues to wish to continue. In other words, what is war or peace today is a gray area, as much is done through agents or financial sanctions, in a way that did not happen 30-40 years ago. What made this possible was digitization, the information age.

Regarding what the UK needs from a primarily technical perspective to collaborate and communicate to be able to coordinate different help and support from other units, the answer was the following from participant (E),

10) “It is today rather hierarchical in the military, and it can take a long time for the information exchange to reach down to the soldier from the officer, this is mainly a cultural challenge and not technical. On the other hand, it will be a challenge to what people and data integration should look like. With the digitalization of the Armed Forces, there will be more and more gray areas around who takes what concerning the data, this way of thinking is something we work with, and we call it C2 Agility”.

One participant (C) pointed out that from the multi-domain perspective, there is a need for interoperability in the British armed forces' command system,

11) “If we want to work together with others, we must adapt to others as well. Although we can have the best solutions because we are at the forefront when it comes to technology and engineering, it does not matter if we do not have interoperability. Therefore, in some respects, we must adapt to others. Interoperability is a key for us to be able to work together with others and then we must adapt.”

Another participant (D) said that the need for interoperability in the Armed Forces' command system is great,

12) "The UK has over the years, worked in many exercises together with NATO, so they have certain systems that are compatible for FMN. Observe that the systems are not just technical but also a lot of method-thinking. If you look more closely at the need for technology in this interoperability, there is an approach to automating functions so that domains can smoothly talk to each other. A keyword here is intelligent age warfare where you, with the help of digital networks and smart processes controlled by AI, want to be able to simplify conflicts.”

5.3.3 The future and its infrastructure

In aspects of what the needs are, today and in the future, related to infrastructures for C2 systems to be able to operate in MDO contexts, two of the participants (D, E) answered the following,

13) "Redundancy, robustness, and solutions that do not necessarily utilize the commercial, are important. There are development projects that do that, that use the commercial initiatives, and then you must build the security in a different way for the military. It becomes important to do work with encryption and how to store the information. Furthermore, the UK needs to continue to process protocols and facilitate and plan for how the technical equipment will be developed so that it can be moved easily. The information exchange works so that domain-wide synergy effects contribute to an interoperable and multimodal base in the military. "

As for the future of MDO in the UK, all three individuals (C, D, E) with insight into the British Armed Forces have a somewhat synchronized idea, where one of the participants (D) answered in the following way,

14) "As for multi-domain integration and I think that within 20 or 30 years, we will just talk about the multi-domain in the same way that we talk about joint today. With globalization and the information age we live in, we will have to act multi-domain, in one way or another. Then what the word is called will probability change, but the digital development will be enormously important."

5.4 Results from the interview: MDO from a Swedish perspective

5.4.1 General aspects of MDO

All Swedish participants defined domain and multi-domain in an armed forces perspective, where they argued that multi-domain can be defined as operations where more than one combat force participates and that Sweden has five different ones: army, air, sea, cyber, and space. Furthermore, one participant (E) means that,

15) "As so often before, we have borrowed the word domain from abroad. Their (UK) need to define domains is clearer than in Sweden because many nations do not have a task force but only work under NATO, they simply have a joint level that we in Sweden do not have. We define it as an "arena" where everyone should work at the same time. By multi-domain, we mean that we should attack the right domain and avoid the domains where the enemy is strong. Synergies are achieved by attacking multiple domains simultaneously. The armed forces operate in cyber, land, marine and air, but not yet in the space domain, which the UK does."

Furthermore, all Swedish participants also reasoned that the concept of MDO is important and that it is a new label for old problems. Sweden must have an armed force able to work together. Sweden is so small that everything must work together. Furthermore, a participant (A) says the following,

16) "The concepts must be changed for us to be able to take this into account. We end up in the downpipes far too often and we must get away from this. It is a process that hurts and will take time. We can make almost any decision, but if you can find ways to circumvent these, you will perform complex operations between domains much faster."

Another participant (F) has the following perspective on the multi-domain concept,

17) "If you go back a few years and look at interoperability and think about how we send out a JAS aircraft to collaborate in an exercise area that all other nations do, it requires a system, one that works together with the other nations. The standard we use must work with other people's systems. Otherwise, we cannot implement close air support (CAS), which requires that Sweden have a system integration that I easy to build on and have joint flights that are compatible with an unbreakable bond."

Regarding how Sweden thinks in its approach to multi-domain operations, a participant (A) gives his perspective and an example of how Sweden thinks through the following reasoning.

18) "When you carry out an operation, you plan the effect in the information arena. Thus, there is a great deal of effort as the systems thinking that exists in the Swedish Armed Forces is not fully compatible with other nations in NATO."

Furthermore, one participant (B) believes that information ownership is seen quite differently by different nations.

19) "Connecting different networks with different information that is classified is quite difficult. A NATO-adapted structure means that Sweden has some organizational compatibility. But knowledge, technology, and methods are also needed to be interoperable."

5.4.2 Needs and requirements

Several of the participants (A, B, F) described the conditions for MDO in Sweden as very good, were two of the most prominent reasons were due to that Sweden has had a good tradition of conducting joint operations and that Sweden has in some meaning a NATO adapted structure. One of the participants (A) answered in this way regarding the conditions for Sweden to be able to conduct operations with several domains,

20) "We have a task force that is strong and experienced and can create holistic operations. We are not fully aware of the target process. We are perhaps best at working multi-nationally within a domain than we are at working in multidomain. This is explained by our tradition of collaborating internationally. We have not had the conditions to practice multi-domain so much before. The important difference is that many do not have an operational staff, those who have worked a lot in NATO have a great habit of cooperating but that does not mean they can work multi-domain in aspects of data-driven operations and joint fire."

Furthermore, Sweden is not a member of NATO today, however, the Swedish Armed Forces have several preconditions for conducting and participating in operations with several domains together with other nations, which the participants (A, B, D, F, G) agree on. Since most of our systems are NATO-friendly and are structured in a way so that the Swedish Armed Forces have been able to contribute to the international military forces in, for example, Afghanistan, and thus Sweden has some organizational compatibility.

There are many challenges regarding MDO, especially regarding the IT aspect, which all participants believe. One participant (G) described the challenge as follows,

21) "The biggest challenge is to be able to exchange classified information with others. The more people who have access to information, the greater the risk that someone who should not receive it will receive it. Technically, we can always solve with enough money, but the handling is much more difficult. Sweden must go from protecting all information to protecting relevant information. The most important thing must be protected, the rest of the information must be possible to share with partners we trust. Today's situation is unsustainable because if Sweden is to handle the information that is technically available, all information must be classified with metadata, which we do not do today."

While two other participants (A, and B) had different approaches to the IT challenge,

22) "As far as the IT perspective is concerned, the multi-domain challenges are the same as the domain-internal challenges and that is to digitize the armed forces. Today we have an IT system that is not at all adapted to handle even a domain in terms of data handling capabilities. It does not have to do with multi-domain but that we tend to buy platforms and where we forget that we must dress it with support systems such as transmission. We do not use the capabilities of the platforms because of this."

Furthermore, there is a focus among the participants on what the technical interoperability means, where one participant (E) developed the reasoning with,

23) "The idea is to be interoperable, to be able to help and get help from others. In total defense, one must also share data within the nation. What is agreed upon, are the function chains where certain roles need information. But if you look at service instructions that provide information on how to go about it, each nation has its use case. Sweden must think about how difficult it will be to follow what is decided in the federated work with procedures and instructions."

From an organizational perspective, there was a focus on how information sharing takes place and the art of working agile, which is a challenge according to all participants. One participant (E) reasoned about FMN and how we must create doctrines to create interoperability.

24) "We also must look at how we store and transmit the information as we need to be able to carry out data-driven operations. To be able to carry out operations in a digitized way, we need interoperability, above all on a combat technical and tactical level. Both nationally and internationally, the challenge is to have interoperable combat technology systems. The biggest obstacle is the law and adopting FMN so that it becomes technically and organizationally compatible with the Swedish Armed Forces."

5.4.3 The future and its infrastructure

Three of the participants (A, F, E) emphasized that the needs related to infrastructure for implementing MDOs look much like commercial systems. Where a nation has data centers, such as Amazon or Google. One of the participants (F) said more concretely that communication will become even more important in the future,

25) "Something the military did a long time is talking on the radio. There are some points to it and that is that if you have a good radio connection then you can hear who is on the other side and you can also hear how the person is feeling, thus interpreting their expressions in stressful situations. If you are in a combat operation, it is important to know if the individual on the other side is breaking down or how to formulate yourself to interpret the person's voice. This can be simplified in chat mode. There is much less bandwidth, and you get over the language barrier much easier. It does not matter if you speak Scanian or Norrlandic. It can even facilitate communication. Suppose you have a Frenchman trying to speak English, then it can be difficult. But it can be even worse if you have a Scot trying to speak English with you through the radio. Regarding how we can use chat functions in the military on a tactical and operational level, First, we must practice running radio and chat in parallel to understand what it gives in effect, to then decide which means of communication is best"

The digital security aspect is something that several participants also highlighted as an important segment of the infrastructure, where one participant (B) highlights what he thinks about the future regarding MDO,

26) "I sincerely hope that we will have data that can be communicated to those who need it. We must allow it and have solutions that make it possible. The projects that the military has today may not allow the possibility to share data that one would like, between the branches of war. An effort is put into optimizing the weapons type through service-to-service. However, there are technical possibilities, but once again it falls on safety aspects."

Another participant pointed out the following regarding the digital infrastructure,

27) "Above all, it becomes important to handle transmission in the field by using data transfer protocols that are connection-oriented and that do not cause delays. And then we have the aspect of storage that is a challenge from a military perspective. It will always be a challenge. What we are bad at are information management and information classification. If we can sort it out, we can solve a lot in technical aspects."

5.5 Results from the interview: Cloud solutions within MDO

When it comes to cloud solutions to promote MDO and make the Swedish and British Armed Forces more digital, the reasoning was many, where two participants (C, D) said that,

28) "A lot of restructuring is needed about the UK's ability to store and process data. The data information should be used both vertically and horizontally (purely organizationally) where there are operational capabilities in creating a so-called data lake, which will act as a platform for managing cloud storage. Here, automated integration and customizable information displays become an important source to be able to achieve this. Further, the data lake is more accurate instead of calling it for the cloud. A data lake will act instead of the traditional data servers and thus become an environment that will bring types of data processing that have not been used before and storing and using the same repository for handling different data.

Furthermore, another participant (B) says that,

29) "Cloud services can be quite important, but it is also extremely important that those who are at the end of the front, that if they lose contact with the cloud service, there is a backup in the form of traditional means. We will probably make extensive use of cloud services, those who do not may end up at an information disadvantage. But they must be able to function without the broad information highway."

Furthermore, another participant (B) says that,

30) "Cloud services can be quite important, but it is also extremely important that those who are at the end of the front, that if they lose contact with the cloud service, there is a backup in the form of traditional means. We will probably make extensive use of cloud services, those who do not may end up at an information disadvantage. But they must be able to function without the broad information highway."

Furthermore, the same participant believes that the focus should also be on the availability of data servers,

31) "Somewhere the cloud is realized on some server, you must be aware of that. The information does not float in a cloud, it is somewhere. Trust and security are important aspects. There are many involved here, and it can be difficult to know who has access to data."

It was highlighted by two of the participants from the UK (C, D) how they view the difference between interoperability and intraoperability where the following was said by a participant (C),

32) "You can also build a closed cloud service in a closed network, there is no connection to the internet. The question then is how to ensure multi-level information security. The CIO at the HQ in the UK is looking at this with cloud services and trying to understand what this could mean, but has not delved into anything yet, at least not on a large scale. First, we need to analyze how cloud services can improve our interoperability and our intraoperability between our forces where the foundation of the data exchange between systems is integrated. An important aspect that must not be overlooked. Because if I do not trust my colleagues, it will not work. There are many benefits to cloud services, but there are also many trust capabilities issues, who owns the cloud? Within FMN, not everyone has all the technical abilities. Cloud services can allow things to be split up. If you put yourself in a situation and think of radio systems that act as a boundary for which levels can work together, how far down should you speak English? Individual systems may require very far-reaching interoperability."

Another participant (D) developed the reasoning about cloud services and chats in the following way,

33) "I do not think we have any alternative. We must have cloud services. We cannot have a technology solution that society generally does not use. We must relate to the outside world. When the air force was founded, the IT development was driven by the air force, but that is no longer the case, the digitization is driven by civil society. It is imperative to create cloud services. The question is how to do it. A start is to handle joint fire and develop so that several domains fight for the same goal at the same time. Weapons from air, sea, and land interact. You collect intelligence (ISR)and store data so that it can be processed and analyzed for several domains at the same time. In military terms, it is important to remember that data is not always IT. For data-driven operations, we have always been thorough, but now we have extremely much more data in more platforms to handle. Therefore, we need to digitize to be able to do this."

Confidentiality in the use of intermediate services and the use of gateways to act as translators is something that several participants (D, E, G) pointed out as important in cloud services to be able to participate in multi-domain operations. One participant (E) developed his reasoning with the following,

34) "We are looking at a way to use some form of gateway, that is, translator between different JREs (JREPs) which is an IP protocol that translates link 16 data from radio to IP. This will be a type of micro cloud service where we have a centralized gateway that translates between different languages. Where you deliver your location picture and your information into a cloud service that you can subscribe to, and in that way, you get information based on the domain you are in. Furthermore, you must investigate how long you keep the confidentiality regarding the security aspect. Information that is classified is always linked to a time when the confidentiality has a time perspective that it is no longer confidential. And that is probably what is difficult about cloud services, to be able to set up and maintain confidentiality. Tee time before someone has cracked the information. Therefore, cloud services are a risk. At the same time, if we do not take advantage of the opportunities that exist today with technology, we will fall behind."

6. Analysis

The analysis chapter contains information and an in-depth understanding of the central elements of this thesis. This chapter will answer if the purpose of the report has been answered relative to the research questions and whether the results from the literature (concept notes and doctrines) and the interviews have been conducted in a way that answered this thesis's main questions. Thus, the analysis is built upon the answer of the participants from the interview study and the literature study.

6.1 Prerequisites in terms of people, organization, and technology

The most important aspect when looking at prerequisites is command and control, in the form of the holistic aspect of how to conduct coordinated operations. Today’s prerequisites for conducting MDO from a people, organization, and technology perspective are many in terms of coordinated operations, according to the answers from my interview study. Culture becomes an important aspect here that must not be underestimated. An MDO will require cooperation between several different branches of defense by the Armed Forces, those that do not usually cooperate at a level required for the MDO.

From the literature study, it is seen that synergy effects are something that must be achieved in an MDO [33], because it is a fact today that the traditional method of warfare, i.e., war armed directly against each other is only a fraction of different methods of war. Today there are more influence operations, financial sanctions, and proxy wars. For a nation like Sweden to be able to defend itself against these, it is required that the nation has a clear workflow that works multi coordinated while individuals are adapted and receive solid training in how to work transversely between different domains to achieve synergies.

When engaging in combat with systems in collaboration, both the Swedish and British Armed Forces can then achieve a higher effect. System coordination thus becomes important in aspects of leading and developing prerequisites in terms of people, organization, and technology. However, there are limitations in how to get to the coordinating management. Looking at the answers from the participants from the interview study (4, 13, 15) the experience is that coordinated combat has repeatedly been carried out in Sweden, but without getting the synergy effect wanted. It is thus possible to analyze whether the Swedish Armed Forces has made attempts at joint efforts by different domains having different windows to work in but against the same goal.

Regarding how technology and humans interact, one can from the participants' perspective think about what it looks like to have weapon systems coordinate without them interacting with each other. Because in a perspective in terms of individuals and organizations, Sweden is relatively small in terms of volume, which makes that difficult.

C2 agility is an important aspect to consider here, partly to investigate how the conditions are linked to the background literature, and partly to see what the issues surrounding the conditions look like. In order to be able to approach a good C2 system, there should also be an agile mentality in order to be able to work dynamically so that collaboration and information flow becomes easily accessible to handle and share. C2 agility is more established in the British Armed Forces than it is in Swedish Armed Forces. If you look at how the structure is structured between these countries, there is no major difference in what the countries have achieved in technology, however, there is a completely different ambition for the British Armed Forces to learn and work agile than what the Swedish counterpart has.

From the participants, it is possible to see that the technical conditions are there and if they do not, it is easy, financially to acquire them. But to enable an Armed Forces that act in multi-domain operations, culture is once again the challenge, which is because the armed forces have a strong hierarchy that is characterized by vertical coordination in the organization. Hence the introduction of C2 agility will thus also be a challenge. So as digitalization progresses and the military continues to develop digitalization, new methods are also needed to work within the organization, especially in terms of how people and data integration should go, as the participants from the interview study emphasize.

Looking at the Swedish Armed Forces' view on C2, it is the main theme from the interviews (6, 10, 14) that changes are required to be able to implement MDO. When the IT systems are introduced as a step to perform joint and complex operations, it also means that various questions arise, where groups and individuals will need to change how they work and look at regulations.

That the Swedish Armed Forces has IT systems that are not fully adapted to handle a domain in terms of data handling capabilities, is a fact from the data collection (21,24). To connect it with the issues, you thus need to handle data more efficiently, to increase the conditions. This is done by introducing and starting to share data with other domains, more easily accessible, while at the same time excessively starting to analyze data and increasing the supply of skills where the system thinking of the work is introduced. In the case of an MDO, it is required that there is increased collaboration and a common system view, which according to the study (7,33) must be coordinated between the three pillars, people, organization, and technology.

6.2 Frameworks and information systems

As for frameworks and information systems, there is a need for the Swedish and British Armed Forces to enable the frameworks such as FMN to become a part of the culture. To understand how the Swedish Armed Forces can use and to see what conceptual frameworks in the form of literature reviews exist that can be used to support MDO, there is a clear common denominator among the literature study that the process flow for information systems must first be understood. The process from data supply in the form of information, where the information is being valued and assessed to then be handled by transferring information to the right person. This process needs to be clarified in an independent domain.

Further, in a more in-depth analysis of what this thesis has conducted regarding the research questions and the results from concept notes, and doctrines, the focus is on the following aspects. That frameworks such as LISI and FMN as well as technical standards make it possible for the communication process, automation, and the ability to work agile to have a good flow. Which will lead to an opportunity to work coordinated between different domains. Furthermore, it is seen from the interview study that it is a challenge that different domains do things differently depending on needs and conditions (10). This does not make it any easier either, as digitalization is gaining increasing focus in the Swedish and British Armed Forces.

FMN is the framework that is most emphasized in the background literature. For the Swedish Armed Forces to be compatible and enable FMN to improve and measure its level of interoperability, it is also required that C2 is updated and configured in parallel so that it becomes compatible enough and adaptable.

To improve the development of operations and coordination of domains, FMN contributes to routines and processes that are mutual throughout the hierarchy, both horizontally and vertically. Which in the long run is a consequence of C2 agility where the striving to work according to competence and not hierarchy is complied with, this can also be seen in the interview study (10, 28). Having same standards and processes contributes to an increase in efficiency, because, in an MDO, the people in the organization must manage the resources faster and in a shorter time, as it places higher demands due to several events at the same time.

In the results from the literature and data collection, the framework FMN and the measurement model LISI is strongly linked to different C2 domains and various protocols as well as system-level constraints. In a closer analysis of the C2 domain that belongs to the information area, it is required that digital services are functional and correctly implemented within the organization. Aspects such as security, reliability, storage, availability, and documentation must exist, but it requires that the nation then has a software architecture and a service foundation that contributes to sustainable and dynamic digitization that can be used to support MDO and to improve and measure its domain control systems.

One of the papers that helped me highlight the importance of FMN is Bengtson [18], where his paper also is a comparative analysis, much like this thesis. There are many resemblances with that, with the focus on Swedish command and control systems being able to support the use of basic human-to-human communication services. One of the main aspects of Bengtsson's paper is how and what the implementation of FMN means for the Swedish Armed Forces C2 systems, this thesis will analyze a similar aspect but from a distinct perspective. While Bengtsson highlights how different specifications that provide an understanding of how FMN as a framework and how FMN can be compatible, this thesis wants to focus more on how the Swedish Armed Forces can use FMN to both improve and measure its C2 systems interoperability.

To enable the function and coordination of domains, that are conducted on several fronts of MDO, there must be an architecture, both organizationally and technically. This is to implement technical communication between different domains. This leads to, based on the data collection, each development step towards a fully compatible FMN must be examined to see where in the FMN spiral the country de facto is. What you see here is that the LISI model has been developed for a larger purpose and today acts as a way of measuring the interoperability. The information systems that exist today are characterized by the technical architecture and communication processes, which are not fully integrated with the standard for what is required in FMN. Measurements are needed to become more compatible, which is done by managing different protocols through the different layers and models. It is mentioned in the related work that the focus will not be on working and doing studies with various protocols in the thesis, but that Durresi et al. work [19] may be the building block for how this thesis reasons about multi-domain operations. It has been shown that this is not the full building block for my thesis, however, the demonstration of how the protocol works in military contexts has helped me understand the importance of rules, standards, and procedures for how communication in a common network is important for MDOs.

6.3 Requirements for interoperability

What applies to what conceptual frameworks and literature reviews can be used to support MDO and to understand the requirements of interoperability are many. The challenge, that all participants during the data collection said, is that warfare takes shape in situations that require several domains to work together at the same time. This then means that there is increased system support that can manage and harmonize different channels and networks simultaneously. Today, the information system that exists today does not seem to work, which affects interoperability less well, according to the literature study.

To coordinate all personnel and systems together with other domains, an increase in the interoperability that exists today is also required, in terms of jointly achieving coordinating operations. Upon closer analysis of what the data collection produced, individual systems may require very far-reaching interoperability. This means, for example, that today's radio systems in the Armed Forces that act as a boundary for which levels can work together must be upgraded, and then both the Swedish and British Armed Forces must also think about language barriers that may exist between different domains.

What is recurring within what conceptual frameworks can be used to support MDO, the organization interoperability maturity model is an important aspect. For such a model, which is emphasized by Clark and Jones, among others [6], there is a clear guideline for how Swedish Armed Forces can process its interoperability by continuously measuring and implementing it and thus influence an operational level in the Swedish and British Armed Forces. Through various information systems. Here, Sweden and the UK must focus on how to use this interoperability to build a joint force to meet the challenges that arise when conducting joint operations.

Further, the requirements of interoperability can be measured through the standard and model found in Figure 5.1.3, which can demonstrate and act as a basis for how the Swedish and British Armed Forces can handle challenges to be able to cooperate through information systems. From the data collection and the participants' perspective, it is from the conditions the best possible and most ideal expectation to reach a level where all domains are unified. Judging from the data collection, the Swedish Armed Forces' interoperability is at the collaborative level, where attributes such as the existence of general doctrines and certain foreign experiences exist. While in the British Armed Forces, it is more of a mix of combined and collaborative organization, as they have a central role in NATO and more significant experience from foreign missions as a contribution to them having an increased chain of command with the home organization.

A model that has contributed to a framework that gives the Swedish and British Armed Forces a standard that can act as a basis for how to handle the challenges of cooperating through an information system is LCIM. From the concept notes and background literature, three layers (technical, syntactic, and semantic) should be met and understood to achieve interoperability that can be simulated and implemented with the help of information systems.

There are shortcomings, according to the answers from my interview study, in how the exchange of data works, which becomes more difficult at MDO. This requires interoperability that is based on a deeper technical foundation where information and software can be handled for exchange between domains. Furthermore, data should also be shared through different networks and at the same time via interfaces where intermediate programs can be used. Based on the data collection, this is something that is lacking today. What was characteristic of the result is how semantic interoperability can contribute to an increased potential for coordinated operations, both nationally and internationally. From the study, it can be discerned that semantic interoperability has been clearly described as an important part of achieving communication for the exchange of information and data.

6.4 Sweden and the UK

To understand how Sweden interprets MDO compared to the UK, in its approach to MDO, it must first be clarified that the countries have different prerequisites for conducting coordinated operations. This is because the UK has a greater focus on expeditionary operations than Sweden. In recent decades, the UK has been involved and played a central role in many missions abroad. This suggests that the British Armed Forces are more FMN-compliant, which has also led to them having greater opportunities for MDOs. Relative to the results from the data collection (8,11,15,18), feasibility increases when a country acts operationally and tactically in other countries together with other countries, which the UK has experienced several times. This has then led to them having to act in joint forces in several domains at the same time.

With the experiences the UK de facto has, they have managed and configured FMN spirals 1 and 2, where the UK has developed a network through NSoIT. This network, which provides solutions for communication through network systems and communication, has contributed to the UK having come further than Sweden as the UK has built up a more solid base regarding what their simplification of federated networks looks like. With such a C2 system, the possibilities for interpreting how to best carry out coordinated operations increase, as it becomes easier to handle text-based collaboration services and information directory data synchronization, regardless of which domain it is.

Based on the data collection, the countries are close to each other, both culturally and in how one looks at the need to conduct MDO. This is also seen from the participants' background, whereas two of the participants in the data collection have been at both the UK headquarters and the Swedish equivalent. The difference in how these countries interpret the domain is not large, both countries have an interpretation that today there are five operational domains. With the difference, the UK has decided to merge the electromagnetic spectrum and cyber into one domain. As for the response to the question of how the two nations interpret MDO, these five domains exist today to plan and see where the organization can be most effective to work in a coordinated manner to respond to new and complex threats.

Furthermore, it is interesting based on the background literature to see how the Swedish Armed Forces compared to the British counterpart handles its management and staff and what differences are that affect the ability to conduct MDO. It is more difficult for the British Armed Forces compared to the Swedish counterpart because their management structures, according to the British interview participants, are much more adaptable as the UK mostly leads operations abroad.

As previously mentioned, the UK has a greater international experience, and thus a greater tendency to have a staff that has experience in conducting MDO together with other nations. The UK has over the years worked in many exercises with NATO, so they have certain systems that are compatible with FMN, as FMN is an initiative from NATO. However, there is a clear perception from the data collection that the systems that exist in each country are not only about what technology is used but are mainly about methodological thinking and how the employees can act with the technology to work transversely. If you take a closer look at the need for technology in Sweden's case, there is an approach to automating functions so that domains can easily talk to each other, primarily for defense purposes.

6.5 Cloud solutions

In order for the Swedish Armed Forces to act in a coordinated way in different domains, certain technical aids are required, one of the technical solutions to facilitate MDO and increase and improve communication is to use cloud services. How the military can use cloud capabilities to see and enable cloud-based communication through different domains does not solve the challenge alone with MDO, but from the results, it will be helpful. Cloud solutions will help both the Swedish and British Armed Forces to become more digitalized, as cloud services in the military will help soldiers and officers to handle and store raw data on a large scale for a low cost. At the same time, cloud services would mean that countries such as Sweden and the UK can have data that have performed transformations and that they can then have many different types of data in the same repository.

As for what the prerequisites are in terms of how and when to use cloud-based solutions for MDO, there are several aspects to consider relative to the results from the literature and data collection. Cloud services would make it easier to share information more quickly, which is beneficial if the military is to work with the MDO. However, despite the abilities that cloud solutions add, there are also difficulties. These difficulties include the importance of data security and how to keep the information and data relevant and flowing throughout the organization regardless of the domain. Furthermore, there should be a strong emphasis on the fact that cloud services are already established in the civil and commercial spheres, and that it is only a matter of time before it becomes established in the military sphere as well. What the majority wants through cloud services is to increase consistency, which entails automation of the information flow. Instead of sending information from one domain to another, which may become out of date before a response is received, everything is directly accessible in the cloud.

An interesting aspect that is addressed by participants from the data collection is the concept of a “data lake”, in the British Armed Forces they have come a long way in how the data should be handled in aspects of how the information is stored. They want to move away from traditional data storage centers and use a so-called data lake. This data lake then functions as a center for all data that comes in and that comes out and contributes to an increased situational awareness that cannot be physically corrupted or damaged. This will also be cheaper in operation as the is little to no physical maintenance required, and at the same time, a transfer of data lake in war becomes virtual if it were needed in war. Also, another reason for the data lake initiative may be that the British Armed Forces do not want it to be associated with the common term (cloud services) used in civilian life, but in practice it means exactly the same thing.

Cloud services are also making it easier for collaborative operations. If the military is to achieve adequate C2 agility in their work processes, according to both the literature and the interviews’, increased efficiency is needed where soldiers and officers can find information more quickly. They also need access to shared information so that domains do not become dependent on other domains' access to information. Smart connectivity between the domains that can be produced through cloud services is also important. This goes hand in hand with how C2 agility should be developed where the focus is on having an organization that is easily accessible and where the information can flow both horizontally and vertically.

Relative to the research questions, a lot of focus is placed on the human-technology interaction in the military, with an emphasis on cloud solutions and how they can affect MDO. According to background literature and in particular, Powell [10], the view of cloud services as a service only for commercial and civilians is disappearing and is now becoming increasingly relevant for the military as well. But as in many other technical means, there are also challenges to this. Because in a scenario where an officer in a crucial situation loses contact with the cloud service, there must be backup in the form of traditional means. Several of the participants (30, 33) believe that it is a matter of time before Sweden and the UK use cloud services. But it must be able to function without the wide information connectivity where the risk of information inferiority is eliminated, and this is done through the right training and a compatible C2 system.

The result of the study shows that several military contexts want to enable communication between different domains but also within a single domain and between different soldiers and officers. Because if there is a clear barrier between two different domains, it will be a challenge to be able to quickly take in and process orders before it becomes obsolete or incorrect. In aspects of technology, most solutions have been presented to facilitate MDO, one of which is how to use artificial intelligence and machine learning to promote coordinated operations. This is important to do, for, imagine a scenario where the air force, for example, sends data to the army, and then the army sends back the data. Nonetheless, when the air force has received back the message, the situation has already been updated or changed, and if the data has changed while the army sent it back, the air force will get data that is conflicting. Thus, it is important to use share data storage space and have a data lake. There is also a common ground for this thesis and in Dinesh and Gregory's paper [16], one of the major factors in their research is that the military is approaching a new standard in terms of moving away from traditional warfighting methods to more digital ones. This is also a basis for why this thesis is done, where an understanding of how and why one can use multi-domain operations (MDO), which is a current and efficient way to both manage and integrate into the military.

How and when to use cloud-based solutions for MDO is not easy to know in military contexts, which is seen among the answers from the participants. Managing how the organization's interoperability in a C2 perspective can promote cloud solutions seems to be a key concept as a more agile organization contributes to the organization being able to adopt cloud solutions more easily. There are situations where the military and soldiers are in difficult terrain or deep forests where the connection can be less good, then it becomes a challenge to conduct coordinated operations if part of the information sharing takes place via the cloud. This is where you can use smart systems such as AI or ML, which is presented in Dinesh and Gregory’s paper [16], that can understand and publish information based on the situation and then the nation in question becomes less dependent on an individual technical solution.

A reasoning point with cloud solutions that were recurring during the interviews (7, 33) was the view of possible synergy effects regarding what happens if we start sharing data storage space. From the UK's perspective, a lot of restructuring of their ability to store and process data will be needed. In such a scenario, the data information should be able to be used both vertically and horizontally, which means that the information available becomes less controlled by hierarchy and more adapted to domain knowledge. What will be important here to consider, according to both the British and the Swedish participants in the interview study, is that the actual implementation of cloud services is not difficult, given today's technical standards. The challenge will be to develop and coordinate automated integrations and customizable information displays for both the Swedish and the British Armed Forces.

As for the problems that cloud services cause in situations where there is a poorer connection, there are solutions to it. In such cases, one possibility is to produce a closed cloud service in a closed network. The consequent question will be how to deal with the assurance of information security. Here, it thus becomes extremely important to see and understand how the process from the information in a device is handled, sent through a gateway, and handled by a transmission that then ends up in the cloud. If it can be ensured that the number of messages sent and handled by the transmissions is both encrypted and secure, then the military has come a long way. However, one should understand how cloud services can improve the interoperability, because the basis for data exchange between systems managed by cloud services is integrated, which goes hand in hand with what interoperability stands for. In the case of large-scale development of cloud services in the military, questions about trust capacity must also be answered where questions such as "who owns the cloud" were recurring in the interview study. Should it be owned commercially by a private company, or should the military build its systems from scratch?

7. Discussion

In this part of the thesis, I will discuss how and if I managed to answer my research questions. Furthermore, this part of the discussion will be different from the analysis in aspects that the following chapters will revolve around my thoughts on the results. The focus will consist of an overview of the literature study and the interviews, which here is called data collection. Furthermore, the method will also be discussed, where weaknesses and strengths are highlighted.

7.1 Results: Overview

The very concept of MDO has proved to be rather difficult to find a common interpretation of what it means at all because even though both the data collection and the literature study had roughly the same description, there is no trivial definition. To decipher from the general picture that I got through the data collection and literature study, the concept of MDO itself is new, but the way of thinking in coordinating different branches of defense has been relevant much longer than that. However, it has become relevant in a different way today, as technology and digitalization have contributed to changing how the military works and defends itself.

In this thesis, many of the research questions have been quite broad, which has been a conscious choice to not limit me and thus try to give the literature study and data collection greater breadth to influence where the actual challenges lie. However, managing operations that are multi-domain and at the same time comparing with another nation that has many similarities with Sweden, for example culturally, has proved to be a challenge as an answer has led to several questions.

It is clear from the interviews that the participants have many opinions about what it means to follow an MDO and what the interpretation looks like. But a common denominator was that they all emphasized that the combination between man and technology is of great importance if two or more domains are to be able to act as multi-domains.

People and Technology
A major aspect that is emphasized is how individuals from soldiers to officers should be able to collaborate and integrate into the technology that is required if MDO is to be possible on a large-scale level. It is interesting to see the result highlighted by the study in aspects of how people and technology have a collaborative role that should not be underestimated. The technology for conducting a thorough MDO is there, where the focus is on various means of communication to be able to collaborate better. The difficulties here will be the issue of data access and ownership. The results of this case study show great motivation and willingness to introduce a structure and basis for a coordinated military. However, an important approach, relative to the outcome, is that the military must establish a thorough data governance process that can handle, modify, and share data shared between different domains.

Furthermore, this structure must take place in an agreement between different domains, in order to have control over who has access to what. From the interviews, I see that there is a great deal of uncertainty among the individuals in the military about who should have access to what. I envision the following scenario where all the domains will coordinate a defense, how far in will an officer in the army have access to current air force information? Not only that, there is a great risk that there may be third-party stakeholders, looking at what the prerequisites look like from an organizational and technical perspective, so a current question should also be what technology to take in and use? An interesting aspect, however, was how to formulate the access point. In an organization with very sensitive material such as a military one tends to have, the question is who decides over the centralized or distributed data elements, which is highlighted as a key factor relative to my research questions.

Furthermore, an important part of the results is the synergy effects that are added to the collaboration between data and humans, where two keywords are redundancy and robustness in how we build and integrate our systems so that people can easily use them that the exchange of information becomes domain wide. This is important if you are to work in a coordinated manner. Training will also be an important part of this, that the military can teach its employees the importance of security with information because if all domains are to work in a coordinated manner, information will be even more sensitive. This leads to it becoming essential to work with encryption and how to store the information. Furthermore, both Sweden and the UK need to continue to process protocols and facilitate and plan for how the technical equipment will be promoted so that it can be easily moved.

C2 Agility and Interoperability

There are many conceptual frameworks in the form of literature reviews that can be used to support MDO and to understand the requirements of interoperability, which are described in more detail in chapter 6, analysis. In this text, a more detailed answer will be given on how these frameworks, which are based on literature reviews, can contribute to increased C2 agility and interoperability. What makes interoperability a challenge for the military, no matter what country it is, is that the military is hierarchical and remains to its traditional organizational methods. The result is then that the data exchange between domains becomes more difficult, because, in the case of an MDO, all data, organizationally, should be used both vertically and horizontally.

What I see from the data collection and literature study is that there is a weakness in both the Swedish and the British Armed Forces in how confidentiality works to handle the interoperability that comes with a multi-domain operation. The study shows that possible C2 operations with a combination of air, army, navy, space, and cyber capabilities entail a complexity in how to enable communication as different domains have different prerequisites depending on needs and capacity, it will be important to try from the leaders and those in charge to introduce an agile mentality, which is independent regardless of which domain you belong to. There will be situations that require easier decisions and sometimes there will be situations that require more complex decisions, thus both the Swedish and the British Armed Forces must decide where the line for their interoperable thinking goes.

An important factor in how successful interoperability is depended to a large extent on how the military can handle the sharing of information between different domains. If information sharing can be streamlined and made more accessible within the organizational structure of military organizations, which is both hierarchical and traditional, there is a greater chance that MDOs will be more successful. The study shows that the British Armed Forces have shown more commitment to introducing agile thinking within its military organizations where decisions and ideas are not divided by rank but by skills and needs, but this will take time as it is not something that happens overnight.

Information sharing should be smooth, regardless of which staff or unit you belong to. A possible solution and starting point that is derived from the data collection for how the process is when planning and changing information is from Figure 5.1.1. It is a good example of how to adapt models from the commercial standards and adapt it to a possible military structure that has its basis from the tactical, operational, military strategic, and strategic aspects. To be able to collaborate, you can then build the C2 agility by following the six phases and working iteratively to promote the flow and increase the continued communication to improve strategic assessments.

Technical Solutions and Digitalization

Implementing an MDO, whilst maintaining defense capabilities requires that countries such as Sweden and the UK have systems that are both reliable and user-friendly. The military is approaching a new standard when it comes to moving away from traditional warfare methods to more digital ones. A system that is highlighted by the literature study is a method for using and understanding AI and machine learning. This is to identify when and how to use MDO so that the coordinated operation can be fulfilled in terms of when and where they are to cooperate, to influence and simplify communication. The possibilities with AI/ML are great, but I think, considering what the participants said during the interview regarding the technology, it is too immense of a step to implement on a large scale. Hence it is better to look at less complex solutions such as how different domains can from a technical perspective use cloud solutions. And how they can be combined with multi-domains in both peace and war time scenarios

Cloud solutions are a good start for promoting MDO, as a major challenge in coordinating operations has proven to be the information exchange and data governance process, which can be solved with cloud services. An essential question of whether to build your solutions or buy from the business community, then it becomes a question regarding the price of those services and weighing it against the security aspect. If you compare Sweden with the UK, you can still see that the UK has come a long way in its interoperable ability to work agile, not necessarily because they are directly better suited to conduct MDO, but it may be because they have been a part of NATO and its standards for a long time, and has thus had greater demands and expectations of having a military that is better suited to information sharing can be streamlined and made more accessible.

Another aspect is to look at how the military uses protocols. As I mentioned earlier, communication is important to be able to conduct MDO and there is a need for a standard and regulations on how the transmission of data and information should look like in data communication. Where an important aspect is a so-called HMD protocol such as Durresi et al. [19] have produced. Such a protocol can, in addition to contributing to synergies to potential cloud services as they contribute to a strengthened communication capability that paves the way for a common data lake and promotes based routing.

7.2 Method: Weaknesses and Strengths

In this chapter, it will be discussed how the method was conducted and what the possible strengths and weaknesses are.

Comparative Case Study

There are many benefits to choosing a comparative case study as a method, but there are arguably shortcomings to it as well. In my case where I had the focus on how a military can conduct MDO, it has been required that I have had to go both wide and deep because there is not much research on the subject and the concept of MDO itself is quite discussed today. In my comparative case study, I have had a clear case to work against, but I have actively chosen to compare it with another country to first do a general background analysis and then compare it against two different countries. In this way, I have then investigated and later understood why and how certain things happen in this context, and through the comparison between the Swedish Armed Forces with the British Armed Forces see what can be done to achieve a certain scenario that can improve its interoperability.

Furthermore, it has been shown that a strength of this type of method is that it could be used in both data collections that may be qualitative or quantitative, which is an advantage if one is to collect data from both structured interviews and various literature. A comparative case study has been very useful, as it helped me to understand and compare the broad context of both the technology and organizational reasons for how to accomplish MDO and thus answering my research questions**.**

Interviews

The interviews that laid a great foundation for the data collection were held in both English and Swedish, depending on which language the participants mastered. A potential advantage here would be to hold all interviews in the same language, to make the prerequisites the same, regardless of language. This could lead to other answers as a possibly insufficient vocabulary in how to translate and express oneself, can differ. However, I do not think it has affected the result, but it is still worth considering that it is preferable to hold the interviews in the same language. Furthermore, it was an advantage that all the participants had different experiences, but they all had a domain expertise.

I have chosen to use semi-structured interviews, which is because the questions were to some extent prepared. An advantage of these is that they gave me and the participants opportunities to speak freely, which usually contributed to dialogue instead of a monologue, which according to Hove and Anda [25] is a useful way to conduct interviews as it becomes a more nuanced discussion because you allow the other participant to speak more openly so that it becomes an interactive communication. The challenge here was to build up questions that allow the participants to highlight their perspectives, but it turned out to be difficult as the participants were not completely anonymous, which may have affected the answers as you may not want to say as it is or that you say the expected answer. An area for improvement here would have been to either increase the number of participants or to carry out a questionnaire study, but because of time and resource limits, it was not possible.

The strength of conducting data collection in the form of interviews was that I could partly get different perspectives, as all my participants have different backgrounds. Furthermore, a strength of the interview is that they were held on different occasions, which allowed me to test the questions and possibly revise them so that they are better adapted to the next interview. In this way, it becomes iterative when you go back and the interview can thus be improved, which has been done according to Kallio et al. [26].

Literature Review

My literature study consisted of many different sources, including peer-reviewed journal articles and documents as well as publications from FOI. However, I have used many sources that have not been peer-reviewed or sources from various organizations such as NATO. This has been positive as my work required that I had a thorough understanding of MDO, as there is not much material on the subject. But at the same time, this has contributed to me having to be much more source-critical and carefully review all sources, which has taken extra time and resources.

8. Conclusion

What is Needed to Conduct MDO?

Based on this case study, I see that MDO is inevitable for both the Swedish and British Armed Forces, as they must begin to coordinate complex operations. Then what we call (MDO) is irrelevant. The important thing is to understand what they want to achieve. The main conclusion is that both the Swedish and British Armed Forces must be quick to take effect because they will live in a society with a faster flow of information and a higher risk of complex warfare. On the other hand, there is today a great challenge with how the military organization is structured, which is explained more in chapter 5.1.3, organizational interoperability. This makes an agile organization where MDO can be promoted more difficult, since in an agile organization the focus should be on working according to a competence-driven organization where you control the process both vertically and horizontally, instead of a strictly vertical organization where the most decision is controlled by rank.

The further down you get in the hierarchy, the greater the risk that the technology initiative will work less well, and then an important conclusion will be to draw the line for how the command language should work, independent of the domain. If you look at Sweden, we have both Swedish and English terms, here we must investigate and act in English sometimes to be able to make interoperability favorable. In other words, there is a potential technical solution in cloud services, but there are greater challenges such as the personal and how we communicate with each other.

Within the framework of a network that is shared by all domains, one can reflect that we have a unit that is in another nation and communicates with another unit. It requires that information from a low tactical unit can go all the way up to a high level, which then places demands on both the Swedish and the British Armed Forces regarding security and the flow of communication. Both the Swedish and the British Armed Forces have good prerequisites to implement MDO, what we have for difficulties with in the Swedish Armed Forces is that we do not have command and control systems that allow you to change the relevant data that you need.

Where does Sweden Stand Compared to the UK?

Sweden and the UK have a similar mindset. From Sweden, there are many concept developers located in the UK. Those in the UK talk about domain integration, it is about integrating forces and authorities, and that should be the case even in peacetime. One conclusion here is that integration is a good way of looking at it all, because in the UK a different conceptual framework has been adopted, where it is easier to understand how to collaborate on this. Furthermore, the British Armed Forces are conceptually more developed than the Swedish Armed Forces, which is an indirect result of the British Armed Forces being more internationally active.

What Factors are Relevant for the Both the Swedish and the British Armed Forces in Terms of Using Cloud Solutions and Frameworks?

Several factors play a role here, where the most important ones revolve around security, access, and transmission. From the data collection, a conclusion is to use a data lake, the military must build an infrastructure that focuses on security, who should have access to what, and how far down the ranking soldiers should have access to the data. Furthermore, the number of transmissions that will act as a data stream between different domains over the internet must increase with the introduction of cloud solutions in the military. This is due to increasing the handling of all data, which must be both accurate and reliable. What is important here is to determine who owns the cloud and what happens if a soldier or commander wants to put their information in the cloud, how does the person know that that information will not be used incorrectly?

From an FMN perspective, a conclusion is that it is quite relevant that we start using cloud services. The challenges here lie with access and ownership. Not all organizations are optimized to handle modern conflicts or even multi-domain operations. There are no preparation periods, which is an indirect warning that domains do not cooperate, the conclusion is that this problem is solved by having an information flow and an information division that is common, and independent of the domain.

It is a fact that frameworks and measurement models such as LISI and FMN as well as technical standards make it possible for the communication process, automation, and the ability to work agile to get a good flow. It will lead to opportunities to work in a coordinated manner between different domains. With that said, the study also shows that it is hard to know where to begin and precise the problems of why we do not begin using MDO on a greater scale.

8.1 Future work

In the future, it is interesting to carry out a prototype implementation of this caliber from an IT perspective of what an actual cloud service would look like. Furthermore, the focus in this thesis has been on Sweden's and United Kingdom's perspectives, but there are more nations and organizations such as NATO that this is relevant, but it requires more resources to do this case study for all of them, so that would be interesting as well.

Another future work is to start investing, now that the basis is presented, why the Swedish Armed Forces do not use MDO as a standard. Why has it taken so long to realize this. Is it because people, in general do not think the situation with MDO is urgent enough? My thesis has shown that it is hard to concretize the topic around MDO, which may also be the reason why the Armed Forces also have a hard time defining it. So, here it is interesting to see why we cannot define it and make it less abstract.

9. Bibliography

[1] W. Holt and S. Bratton, "The department of the air force role in joint all-domain operations.," 2021. [Online]. Available: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-99/AFDP%203-99%20DAF%20role%20in%20JADO.pdf.

[2] H. Grest and H. Heren, "Shaping NATO for Multi-Domain Operations of the Future, What is a Multi-Domain Operation?," in *Joint Air & Space Power Conference 2019*, Congess centre Essen-east, germany, 2019.

[3] SAS, "Agile Multi-Domain C2 of Socio-Technical Enterprises in Hybrid Operations," 02 05 2018. [Online]. Available: https://www.sto.nato.int/SitePages/newsitem.aspx?ID=3578.

[4] J. Watling and D. Roper, "European Allies in US Multi-Domain Operations," Royal United Services Institute for Defence and Security Studies, London SW1A 2ET United Kingdom, 2019.

[5] FM, "GEM192202S Huvudstudie Ledning – Delrapport 2020," Swedish Armed Forces, Stockholm, 2020.

[6] T. Clark and R. Jones, "Organisational Interoperability Maturity Model for C2," 2011.

[7] SAS, "Final Report on C2 Agility," NATO. SAS-085, 2014

[8] GOV.UK, "Guidance Multi-Domain Integration," Strategic Command and Ministry of Defence, London, 2022.

[9] S. Valaker, R. Stensrud, T. Haugen, A. Eikelboom and I. Bemmel, "The influence of harmonization levels on multi-domain operations effectiveness: The moderating roles of organizational environment and command and control variety," in *Conference: 25 International Command and Control Research and Technology Symposium*, Den Haag, Netherlands, 2020.

[10] D. Powell, "The Military Applications of Cloud Computing Technologies," Army command and general staff college fort leavenworth ks school of advanced military studies, 2013.

[11] V. Marius and A. A. J. R. David, C2 Re-envisioned The Future of the Enterprise, CRC Press, 2014.

[12] M. Granåsen, N. Hallberg, A. Josefsson, C. Ekenstierna and P. Barius, "Ledningskoncept 2035 - Resultat av 2018 års konceptutveckling," FOI, Stockholm, 2019.

[13] Z. Irani, P. Love, T. Elliman, S. Jones and M. Themistocleous, "Evaluating e-government: learning from the experiences of two UK local authorities," in *Information Systems Journal, 15: 61-82*, https://doi.org/10.1111/j.1365-2575.2005.00186.x.

[14] J. Runesson, "Från internationellt samarbete till ett nytt svenskt ledningssystem (Dissertation)," 2019. [Online]. Available: http://urn.kb.se/resolve?urn=urn:nbn:se:fhs:diva-8815.

[15] H. D. William and R. M. Ephraim, "The DeLone and McLean Model of Information Systems Success: A Ten-Year Update," in *Journal of Management Information Systems*, 2003, DOI: 10.1080/07421222.2003.11045748.

[16] G. Cirincione and D. Verma, "Federated machine learning for multi-domain operations at the tactical edge," in *Proceedings Volume 11006, Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications*, Baltimore, Maryland, United States, 2019.

[17] I. Mann, Hacking the Human: Social Engineering Techniques and Security Countermeasures, Taylor & Francis Group, 2008.

[18] I. Bengtsson, "Vad innebär införandet av FMN för Försvarsmaktens insatsledningssystem?," Försvarshögskolan, Stockholm, 2016.

[19] A. Durresi, M. Durresi and L. Barolli, "Heterogeneous Multi Domain Network Architecture for Military Communications," in *International Conference on Complex, Intelligent and Software Intensive Systems*, 2009, DOI:10.1109/CISIS.2009.155.

[20] F. K. James and R. Keith, Computer Networking: A Top-Down Approach, 7th Edition, Pearson Education, 2016.

[21] J. Rowley, "Using case studies in research," in *Management Research News*, pp. 16-27.

[22] B. Kitchenham, S. Pfleeger, L. Pickard, P. Jones, D. Hoaglin, K. E. Emam and J. Rosenberg, "Preliminary guidelines for empirical research in software engineering," in *In: IEEE Transactions on Software Engineering 28.8*, 2022, DOI: 10. 1109/TSE.2002.102779.

[23] P. Runeson and M. Höst, "Guidelines for conducting and reporting case study research in software engineering," Department of Computer ScienceSoftware Engineering Research Group, 2009, DOI: 10.1007/s10664-008-9102-8 .

[24] G. N. Ian, "A guide to systematic reviews," in *Journal of Clinical Periodontology,* 2003, https://doi.org/10.1034/j.1600-051X.29.s3.15.x.

[25] S. E. Hove and B. Anda, "Experiences from conducting semi-structured interviews in empirical software engineering research," in *11th IEEE International Software Metrics Symposium (METRICS'05)*, 2005, DOI: 10.1109/METRICS.2005.24..

[26] H. Kallio, A. Pietilä, M. Johnson and M. Kangasniemi, "Systematic methodological review: developing a framework for a qualitative semi-structured interview guide," in *Journal of Advanced Nursing,* 2016, https://doi.org/10.1111/jan.13031.

[27] L. Bartlett and F. Vavrus, "Comparative Case Studies: An Innovative Approach," in *Nordic Journal of Comparative and International Education (NJCIE)*, 2017, DOI:10.7577/njcie.1929.

[28] Försvarsmakten, "Svensk planerings- och ledningsmetod, SPL," in *Försvarsmakten,* Stockholm, 2017.

[29] B. Brehmer, "Insatsledning - Ledningsvetenskap hjälper dig att peka åt rätt håll," Försvarshögskolan, Stockholm, 2013.

[30] Försvarsmakten, "Networking, Affiliation Beslut - Försvarsmaktens svarsbrev om Federated Misson, FM2016-4935:2," Försvarsmakten, Stockholm, 2016.

[31] Försvarsmakten, "Doktrin för Gemensamma operationer (DGO)," Försvarsmaktens, Stockholm, 2020.

[32] C. C. Serena, I. R. P. III, J. B. Predd, J. Osburg and B. Lossing, "Lessons Learned from the Afghan Mission Network: Developing a Coalition Contingency Network," Santa Monica, CA, 2014,ISBN 978-0-8330-8511-5.

[33] D. A. Eisenberg, D. L. Alderson, M. Kitsak, A. Ganin and I. Linkov, "Network Foundation for Command and Control (C2) Systems: Literature Review," in *IEEE Access*, vol. 6 , DOI: 10.1109/ACCESS.2018.2873328.

[34] A. Tolk, S. Diallo and L. Bair, "Supporting Network Enabled Capability by extending the Levels of Conceptual Interoperability Model to an interoperability maturity model," in *The Journal of Defense Modeling & Simulation*, 2013, DOI: 10.1177/1548512911428457.

[35] NATO, " Semantic interoperability, RTO Technical Report, TR-IST- 075 Final Report," NATO, Brussels, Belgium, July 2010.

[36] M. Codner, Hanging Together: military interoperability in an era of technological innovation, London: Royal United Services Institute for Defence Studies, 2003.

[37] J. Andersson, J. Bennhult, E. Johannesson, M. Norsell, J. Nylund and J. Thörn, "Interoperabilitet," Försvarshögskolan, Stockholm, 2009.

[38] M. Kasunic and W. Anderson, "Measuring Systems Interoperability: Challenges and Opportunities," Software Engineering Measurement and Analysis Initiative, 2004.

[39] B. Johansson, Luotsinen, J. Herkevall, E. Axell, G. Tolt and M. Granåsen, "Future Command and Control and Command Posts – project report 2021," FOI, Linköping, 2021.

Appendix 1 - interview material

A: Interview guide (UK)

General layout

- Presentation of the interviewer
- Explanation of the thesis' background and aim
- Presentation of the interviewee's background
- Presentation of the agenda and structure for the interview
- Explanation of how the information and data will be handled

MDO and Background

- How do you define domain and multi-domain from an armed forces perspective?
- Which domains do you think the British Armed Forces operates in today?
- How do you define domain and multi-domain in a total defense perspective?
- Do you think the concept of multi-domain operations is important?
  - Why?
  - Why not?
- What is the difference between MDO and MDI (multi-domain integrations) from a British perspective?
- How does the UK think about its approach to multi-domain operations?

Prerequisites and Challenges

- What are the prerequisites for the UK to conduct multi-domain operations?
- What are the prerequisites for the UK to participate in multi-domain opera tones together with other nations?
- What are the challenges from an IT / organizational perspective by developing and creating composite capabilities for a multi-domain operating environment?
- What are the capabilities that affect multi-domain from an organizational and people perspective?
- What are the capabilities that affect multidomain from a technical and information systems perspective?

Needs and Requirement

- How to look at the relations between war and peace from a multi-domain perspective?
- At what levels does a unit need to collaborate/communicate to be able to coordinate different help/support from another unit
- The importance of cloud services to be able to participate in multi-domain operations
- From the multi-domain perspective, how do you see the need for interoperability in the British armed forces' command system?

The future

- What are the needs, today and in the future, related to infrastructures for management support systems to be able to operate in MDO contexts?
- What do you think the future holds for MDO?

B: Interview guide (Sweden)

Upplägg på introduktionen

- Presentation av den som håller i intervjun
- Förklaring av examensarbetes bakgrund och syfte
- Presentation av deltagarens bakgrund
- Presentation av agenda och struktur för intervjun
- Förklaring av hur informationen och uppgifterna från denna intervju kommer att hanteras

MDO och Bakgrund

- Hur definierar man domän och multidomän i ett försvarsmaktsperspektiv?
- Vilka domäner tror du att den brittiska Försvarsmakten verkar inom idag?
- Hur definierar man domän och multidomän i ett totalförsvarsperspektiv?
- Tycker du att konceptet med multidomänoperationer är viktigt?

    - Varför?
    - Varför inte?

- Hur tänker Sverige i sin ansats till multidomänoperationer

Förutsättningar och Utmaningar

- Vilka är förutsättningarna för att Sverige ska kunna bedriva verksamhet med flera domäner?

- Vilka är förutsättningarna för att Sverige ska delta i operationer med flera domäner tillsammans med andra nationer?

- Vad finns det för utmaningar sett ur ett IT/organisatoriskt-perspektiv genom att utveckla och skapa sammansatta förmågor för en multidomänsoperationsmiljö

- Vilka är de förmågor som påverkar flera domäner ur ett organisatoriskt och människors perspektiv

- Vilka är de förmågor som påverkar multidomän ur ett tekniskt och informationssystemperspektiv

Behov och Krav

- Hur man ser på relationerna mellan krig och fred ut ett multidomänsperspektiv

- På vilka nivåer behöver att förband samverka/kommunicera för att kunna samordna olika hjälp/understöd från ett annat förband

- Hur ser molntjänsters betydelse ut för att kunna delta i multidomänoperationer

- Ur multidomänperspektivet, hur ser du på behovet av interoperabiliten i den svenska Försvarsmaktens ledningssystem

Framtiden

- Vilka behov finns (idag och i framtiden) relaterade till infrastrukturer för ledningsstödsystem, för att kunna verka i MDO-sammanhang?

- Hur tror du att framtiden ser ut för MDO?