Interoperability barriers for interorganizational data exchange: A case study in the military sector

Winkler , F

Award date:
2023

Link to publication

Interoperability barriers for interorganizational data exchange: A case study in the military sector

Degree programme:	Open University of the Netherlands, Faculty Science
	Master of Science Business Process Management & IT
Course:	IM1803 BPMIT Graduation Assignment Preparation IM9806 Business Process Management and IT Graduation Assignment
Student:	Ferdy Winkler
Date:	08 February 2023
Thesis supervisor	Dr. Samaneh Bagheri
Second reader	Prof. dr. Rob Kusters
Version number:	1.0
Status:	Final draft

Abstract

Interorganizational data exchange remains a challenge due to different interoperability barriers. Legal, organizational, semantic and syntactic, and technical interoperability standards vary between organizations. It is essential to have a proper insight and understanding of these barriers to be able to collaborate and exchange data between organizations in an effective way.

This case study attempts to provide a better understanding of the barriers which are impeding interorganizational data exchange. During the research the authors designed a theoretical framework which consists of four aspects and fourteen sub-aspects of interoperability barriers related to interorganizational data exchange.

The framework has been empirically tested by executing thirteen semi-structured interviews within the Ministry of Defence and two collaboration partners. This resulted in the validation of all fourteen sub-aspects.

The results show that this framework can provide organizations working with and within the military sector a better understanding of the barriers which are impeding data exchange. This on the other hand can contribute to deciding subjectively better which benefits interorganizational interoperability.

Key terms

Interoperability, data exchange, military sector, interorganizational, framework.

Summary

Achieving interorganizational data exchange between heterogeneous systems, platforms and technologies is essential for organizations, like the Ministry of Defence. However, many systems and platforms are designed independently for a specific task without sufficient awareness to connect or exchange data with other systems. This causes a multitude of heterogeneous solutions which are mainly uncoordinated and have limited coherence. At the same time, the diversity of partnerships is increasing and putting additional pressure on the consistency and interpretation of data. To be able to collaborate and exchange data between organizations in an effective way, interoperability is needed. The objective of the research is to gain insight into which interoperability challenges impede interorganizational information exchange. Therefore, the research question is defined as follows.

Which interoperability challenges impede data sharing between different information systems?

To answer the research question, the Systematic Literature Review (SLR) method has been used to identify relevant articles. This resulted in a total of fourteen articles which were analyzed by using the Thematic Analysis Grid to identify interoperability barriers. This resulted in four different aspects namely legal barriers, organizational barriers, semantic and syntactic barriers, and technical barriers. Within these four aspects the authors identified another fourteen sub-aspects from the theoretical research which have been integrated into the theoretical framework.

For the empirical part of the research we conducted an embedded test case within the Ministry of Defence (MoD), the Netherlands Organization for Applied Scientific Research (TNO) and the Ministry of Interior and Kingdom Relations (MoI). The authors executed a total of thirteen semi-structured interviews with each 35 questions. During these interviews questions were put forward regarding relevancy and reason behind each sub-aspect, the usability of the framework and the overall completeness. The respondents also ranked each of the sub-aspects on three different subjects.

During the empirical research the authors validated all fourteen sub-aspects. The sub-aspects collaboration, and data ownership (intellectual property) were validated as the most important. The sub-aspects language, and ontology were validated as least important. Suggestions were received for refinement, such as change the sub-aspect intellectual property into data ownership and add intellectual property to the description of this sub-aspect. Another suggestion was to add culture and ethics to the sub-aspect collaboration. The final suggestion was to subdivide the semantic and syntactical barriers into a human aspect and the technical aspect. The suggestions for refinements during the empirical research resulted in the final framework.

The overall impression of the interviewees is that the current level of interoperability is limited as it is a very complex topic.

The most interesting results are that the top three solely consist of organizational and legal barriers, whereas the bottom three consist of semantic and syntactic barriers and technical barriers. This result might relate to the fact that a couple of interviewees stated that the technical barriers are often not the problem, but more the legal, and organizational barriers.

The second result which is noteworthy is that it seems that each Operational Command (OPCO) has a good idea of their own organization, but not interorganizational. This is presumably caused by the fact that each OPCO has its own domain specific culture, policies, and systems. Therefore, language, and ontology is rated low, because within the own organization it is not considered an issue.

The third noticeable result is that when it comes to the classified domain, interoperability is complicated, as certain systems are physically unable to link.

Addressed last is the purchasing process within the MoD which results in a diversity of systems. As a result systems are often not interoperable.

The specific domain in which the MoD operates might have influenced the validation of the framework. A partial explanation is the differences in (inter)national laws and regulations to which the MoD must comply and the use of weapon systems.

Although this paper allows room for refinement, the present stance is that the paper contains aspects which should be taken in consideration when organizations, like the MoD, want to create a better understanding of the barriers which are impeding data exchange. In turn the paper could contribute to better decision-making that benefits interorganizational interoperability.

Abbreviations

ABDO	General Security Requirements for Defence Contracts
AI	Artificial Intelligence
AIF	ATHENA Interoperability Framework
BA	Security Authority
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CIO	Chief Information Office
CS	Central Staff
DAOG	Management of Operational Readiness Directorate
DBB	Defence Security Policy
DMO	Defence Material Organization
DPIA	Data Protection Impact Assessment
DS	Data Science
EIF	European Interoperability Framework
EU	European Union
GDPR	General Data Protection Regulation
GrIT	Ground-breaking IT
HGI	High Classified Information Domains
IGO	Information-driven action
I&S	Intelligence and Security
JIVC	Joint Information Provision Commando
LCIM	Levels of Conceptual Interoperability Model
LISI	Levels of Information Systems Interoperability
LGI	Low Classified Information Domains
MoD	Ministry of Defence
MoI	Ministry of Interior and Kingdom Relations
OIM	Organizational Interoperability Model
OSI	Open Systems Interconnection
OU	Open University
R&D	Research and Development
RNLA	Royal Netherlands Army
RNLAF	Royal Netherlands Air Force
RNLM	Royal Netherlands Marechaussee
RNLN	Royal Netherlands Navy
SLR	Systematic Literature Review
SOCOM	Special Operations Command
SOF	Special Operation Forces
SSI	Self Sovereign Identity
TNO	Netherlands Organization for Applied Scientific Research
VIR E&E	Regulations for Information Security of the Government Service, Efficient & Effective

Contents

1. Introduction

1.1. Background

In the information era, the importance of and need for data as a valuable asset is indispensable and this dependence will only increase (Panetto et al., 2016).

Achieving interorganizational data exchange between heterogeneous systems, platforms and technologies is essential for organizations, because data is increasingly being used to support, improve, and manage daily operations. At the same time, the diversity of partnerships is increasing and putting additional pressure on the consistency and interpretation of data (Chituc, 2017).

Collecting and processing these large amounts of data from disparate systems and platforms requires compatibility and a certain level of interoperability (Buchinger, Kuhn, Kalogeropoulos, & Balta, 2021). However, many systems and platforms are designed independently for a specific task without sufficient awareness to connect or exchange data with other systems (Buchinger et al., 2021; Jamoussi, Al-Khanjari, & Kraiem, 2017). Nowadays, a technical problem is related to organizational, conceptual, and legal aspects, which makes effective interoperability mandatory. (Daclin, Daclin, Vincent, & Vallespir, 2016).

The objective of the research is to gain insight into which interoperability challenges impede interorganizational data exchange.

1.2. Exploration of the topic

Interoperability refers to the capability of heterogeneous and different system components, organizations or information technology systems to communicate and collaborate, exchange knowledge and information, covering aspects ranging from the technical to the organizational level, to realize reciprocal beneficial and agreed common objectives (Buchinger et al., 2021).

Although new initiatives are improving the developments towards a seamless interoperability, there are still a lot of challenges that need to be investigated (Chituc, 2017). These challenges are related to different aspects of interoperability and include technical, organizational, legal, and semantics as well as syntax aspects (Buchinger et al., 2021; Chituc, 2017; Rantos et al., 2020).

The technical interoperability aspect deals with the infrastructures and the applications connecting the different services and systems. The organizational interoperability aspect is the alignment of business processes, expectations, and responsibilities between organizations in order to achieve reciprocally agreed and jointly valuable goals. The legal interoperability aspect ensures that organizations are able to cooperate despite policies, strategies, and legal frameworks. The semantic and syntactic interoperability aspects establish that data is understood and the context and format of the exchanged data is correct (European Commission, 2017).

Due to the continuous need to acquire more and more data, organizations across the world, using heterogeneous systems, need to collaborate to exchange this data. But many systems have been developed without the necessity to connect, exchange and reuse data. Besides this, different organizations use different processes, policies, strategies, communication, and standards. This causes a multitude of heterogeneous solutions which are mainly uncoordinated and have limited coherence. In combination with legal restrictions regarding information sharing, these aspects are causing barriers which limit interoperability among organizations. To be able to exchange and interpret data, interoperability continues to be a prerequisite (Chituc, 2017; Daclin et al., 2016; Jamoussi et al., 2017; Panetto et al., 2016; Rantos et al., 2020).

1.3. Problem statement

It is critical for todays' networked organizations to exchange real-time data between heterogeneous information systems, which requires seamless interoperability (Chituc, 2017). But because of the fact that many systems and platforms are designed independently for a specific task, there is insufficient awareness to connect or exchange data with other systems. Due to all these different systems, many barriers cause a limited capability of mutual data exchange and a lack of interoperability (Buchinger et al., 2021; Jamoussi et al., 2017).

Although various studies have identified challenges concerning interoperability barriers within an interorganizational setting, they are usually limited to the technical aspect (Chituc, 2017; Shehzad et al., 2021). Therefore, they provide insufficient coverage of the overall interoperability aspect challenges within interorganizational settings. A more comprehensive and systematic view is therefore needed, which provides organizations a better understanding of the barriers which are impeding data exchange. This in turn can contribute to a better decision-making process which benefits interorganizational interoperability. In addition, literature does not provide insight into these challenges in a real-life situation.

1.4. Research objective and questions

The objective of the research is to investigate which challenges impede interorganizational data exchange. The research consists of two parts. The theoretical part focusses on identifying and classifying interoperability issues, from previous research, regarding interorganizational information sharing and in the second part these challenges are integrated in a theoretical framework. The challenges identified during the literature research are validated, adjusted and, if necessary, refined during the empirical part of the research.

The aim is to provide a better understanding on how organizations can exchange relevant data within partnerships so this may contribute to the effectiveness and efficiency of the collaboration.

The main research question is: **Which interoperability challenges impede data sharing between different information systems**?

To answer the research question, the following sub-questions are identified:

Theoretical part:
Sub-question 1: *Which interoperability challenges impeding an effective interorganizational data exchange can be found in literature?*
Sub-question 2: How can these interoperability challenges be integrated in a theoretical framework?

Empirical part:
Sub-question 3: How can the identified interoperability challenges for interorganizational data exchange be validated with empirical information?
Sub-question 4: How can the identified interoperability challenges be refined with empirical information?

1.5. Motivation/relevance

The most valuable and vulnerable resource of today's world is data (Rantos et al., 2020). To be able to collaborate and exchange data between organizations in an effective way, interoperability is needed (Daclin et al., 2016).

This paper substantiates previous research regarding interoperability challenges within interorganizational settings and contributes to the body of knowledge by filling in a part of the scientific gap in the field of data exchange between different information systems among organizations. The obtained insights, which describe how information should be exchanged, can be used by practitioners within organizations which are experiencing similar problems regarding the distribution of data.

1.6. Main lines of approach

Chapter 2 describes how the existing literature is collated and examined to find interoperability challenges. The results are synthesized and used to identify a framework which helps to answer the research question. Chapter 3 delineates the research methodology for the empirical part of the research, followed by chapter 4 in which the results of the empirical study are presented. In the final chapter results are compared with the theoretical framework and conclusions are drawn. The chapter concludes with the limitations of the study, together with suggestions for further research.

2. Theoretical framework

2.1. Research approach

Chapter 2 provides the theoretical framework to identify which interoperability challenges are impeding data sharing between different information systems. The articles found during the literature research are defined using the Systematic Literature Review (SLR) method presented in Figure 1. The objective is to provide insight into the topic by identifying previous studies and combine and synthesize the results of these studies using a theoretical framework. The framework is then tested during the empirical part of the research.

To answer the main research question, the following sub-questions need to be answered:

Sub-question 1: Which interoperability challenges impeding an effective interorganizational data exchange can be found in literature?
Sub-question 2: How can these interoperability challenges be integrated in a theoretical framework?

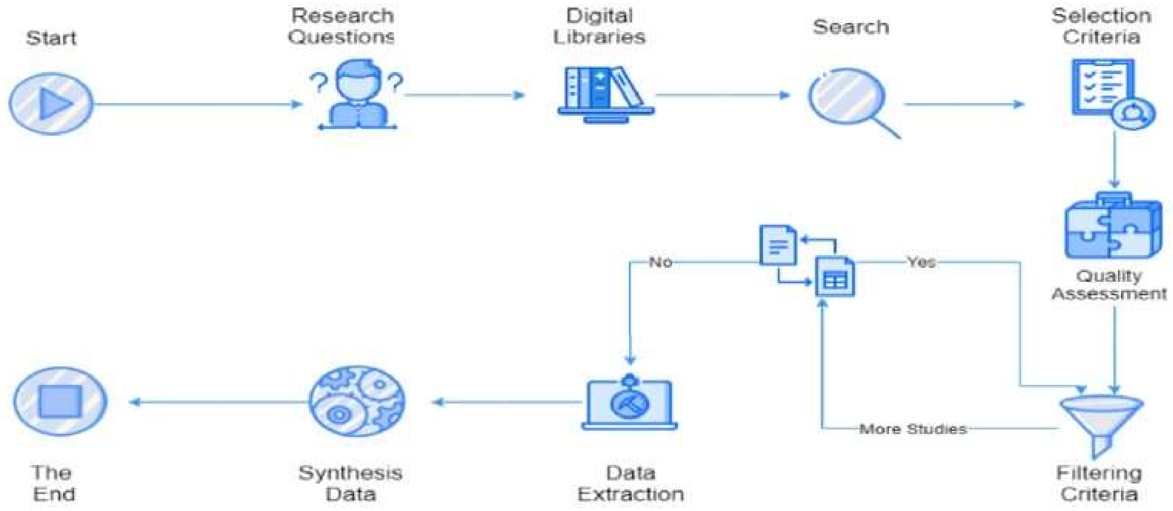


Figure 1: Systematic Literature Review steps (Aldhaheri, Alghazzawi, Cheng, Barnawi, & Alzahrani, 2020)

Keywords and search string

Relevant articles that contribute to the research are found by using the building block method, in which the combination of key terms from the sub-question and their synonyms are combined into one search string using Boolean Operators. The initial search consisted of the terms "interoperability", "interorganizational", "data-exchange", "challenges" and their synonyms. This resulted in less than 100 articles.

After some trial and error, and to get more articles from the search query, the decision was made to use "interoperability" and "interorganizational" and their synonyms. Some synonyms such as "interconcern", "interbusiness", "intercorporation" and "interinstitution" were not included in this particular case, because these synonyms did not add to the results.

In order to further improve the search string and to enhance relevance, the literature search was conducted on the title and abstract of the articles. The following query is used:

((SubjectTerms:(Interoperability)) OR (Abstract:(Interoperability))) AND ((Abstract:(interorganizational)) OR (Abstract:(interorganisational)) OR (Abstract:(inter-organizational)) OR (Abstract:(interenterprise)) OR (Abstract:(inter-enterprise)) OR (Abstract:(interagency)) OR (Abstract:(inter-agency)) OR (Abstract:(inter-firm)) OR (Abstract:(intercompany)))

Inclusion and exclusion criteria

By using the SLR method, it is possible to distinguish relevant articles from irrelevant articles. To do so inclusion and exclusion criteria were drafted (Aldhaheri et al., 2020). Below in Table 1 are the criteria which the SLR results must meet.

Table 1: Search criteria

Parameter	Criteria	Explanation
Search Engine	OU Library (https://bibliotheek.ou.nl/)	The OU library contains around 70 databases which can be searched at the same time
Language	English	Most common language, which results in the largest availabilty of articles, which contributes to transparancy
Publication date	No limitation	The research focuses on a specific area. For this reason there is no limitation in the publication date
Peer reviewed	Only peer reviewed publications	Contributes to the reliability of a paper
Title	Should contain keyterms from the search string	The keyterms or a synonym should be present in the title or abstract to find relevant articles
Availability	Only articles which are directly accesible via the OU library	Documents which are not available without a subscription were omitted from this study
Fields	Search in SubjectTerms and Abstract	Only the fields SubjectTerms and Abstract are searched for keyterms and/or synonyms
Citations	There is no specific number of citations which the paper should meet	Provides an indication of the quality of the paper

The exclusion criteria include all articles that:
1. Contain specific technical solutions, such as blockchain or cloud-based solutions;
2. Offer interoperability solutions for a single organization;
3. Are not mainly focused on interoperability.

Data selection

The search criteria in Table 1 are used for the selection of all relevant data. After using the inclusion criteria, the selection of articles is performed by assessing the articles by title. If the title corresponded to the research subject, the abstract and conclusion have been read and if the paper was not excluded at this time, based on the exclusion criteria, the rest of the paper was studied and summarized for further use (Saunders, Lewis, Thornhill, & Bristow, 2019).

Data extraction and synthesis

After assessing all articles against the inclusion and exclusion criteria, a final overview was available. To identify all relevant articles for the research, a data extraction form (Appendix A1) was used. Analysis and extraction of relevant information from the articles was executed by using the *Atlas.ti* program. The results were selected based on the barriers mentioned in the articles regarding which interoperability challenges impede data sharing.

The synthesis has been performed by using the Thematic Analysis Grid (Saunders et al., 2019). This grid consists of five steps which help to structure the articles in specific themes. In this case the step of the used methodology of the research was omitted, because the outcome did not contribute to the results and was therefore assessed as irrelevant. The remaining four steps are:

1. Identify potential themes;
2. Re-read each article and make brief notes;
3. Add new themes or remove them if no longer relevant;
4. Look for patterns across themes, is there consensus, are there contradictions and is this the most convincing literature?

In this way all relevant themes are included in a grid and later integrated and synthesized into a conceptual theoretical framework. These steps complete the SLR. The theoretical framework is then tested and adjusted during the empirical part of the research, if needed.

To classify and structure all aspects extracted from the articles in Appendix A2, the four aspects mentioned in the the European Interoperability Framework (EIF) are used. First the selected articles from Appendix A3 were checked and duplicates removed. Then similar aspects were identified and combined. Furtheron, the aspects are described and finally the barriers are classified using the aspects identified in the EIF framework which is further introduced in §2.3.

Reliability and validity

The data selection, data extraction and synthesis process is described in detail, enhancing reliability. All steps taken during the research are described, which makes it possible to replicate the particular research, which should lead to similar key findings. This ensures the reliability of the research.

By using a broad search string, relevant articles were identified and included in the research. To identify the most relevant articles, inclusion and exclusion criteria were used. Furthermore, all articles were evaluated in a structured way, using the Thematic Analysis Grid. This contributes to the construct validity of the research.

Despite the specific area of the qualitative research, it is expected that the outcomes can be generalized and applied to other organizations. Simply because interorganizational interoperability challenges, which are impeding data exchange between different systems, affect many organizations.

Using certain criteria such as only selecting English language articles from the OU Library, could create a certain kind of bias. However, the use of different search strings has revealed that there are not many articles available in other languages than the English language. Therefore, it is estimated that the research is not affected. To further minimize the researcher's bias, systematic literature research has been performed with the use of the Thematic Analyis Grid, so that the results and conclusions can be reproduced.

2.2. Implementation

Based on the above-mentioned criteria, the OU library was searched using the search string. During the initial search of the OU library, 207 articles were found (Appendix A2). Based on the inclusion criteria review, 127 results have been obtained which were further assessed on usability and relevance. Thirty articles have a relevant title. Further research, such as reading the abstract and conclusion of these articles, resulted in ten articles containing relevant information which could contribute to answering the sub-question. Of these ten articles, two were duplicates, so eight articles proved to be relevant for the research. The selected articles can be found in Appendix A3.

Due to the limited amount of articles found, the snowball method was used to find additional relevant articles. Therefore, the eight unique articles were analyzed, and their references and citations rated for usability. Such method is known as backward and forward snowballing (Wohlin, 2014). To find additional articles, the inclusion and exclusion criteria from §2.1 in combination with the keyword "interoperability" were used.

The backward snowballing method resulted in 402 articles, which are presented in Appendix A4. Based on the search criteria (Table 1), 82 results were acquired. Further assessment based on usability and relevance resulted in five unique articles. The selected articles can be found in Appendix A5.

The forward snowballing method resulted in five articles, which are presented in Appendix A6. Based on the search criteria (Table 1), only one result was acquired. Further assessment based on usability and relevance resulted in one article, see Appendix A7.

A total of fourteen relevant articles were identified during the literature research and are used for further research and the design of the initial framework.

2.3. Results and conclusions

Interoperability is a crucial subject for many organizations, but it remains a nebulous concept, considering there are diverse definitions and no real overarching vision. Several studies focus on interoperability problems, but sometimes there is no specific description of the content of these problems nor proof that these problems really exist. Some of the interoperability barriers are common aspects such as technological, organizational, and conceptual barriers (Chen, Doumeingts, & Vernadat, 2008; Chen, Vallespir, & Daclin, 2008; Mallek, Daclin, & Chapurlat, 2012). The identified articles mention four interoperability aspects: technical, organizational, legal, and semantic and syntactic interoperability (Chituc, 2017; Shehzad et al., 2021). The technical aspect is the most common and the legal aspect is only mentioned in six out of fourteen articles.

The EIF is mentioned in six of the identified articles because of its holistic approach. Other identified frameworks, such as LISI, LCIM, OIM, INTEROP and ATHENA, are more limited because none of these frameworks emphasize the legal aspect. This is also the main reason to use the aspects of the EIF (Figure 2), because this framework covers all identified aspects including the legal aspect, which is important to be able to exchange data between organizations. In addition, the framework is developed by the European Union (EU) and used by several public administration organizations to collaborate more efficiently between services and to improve interoperability governance within the EU. By using the aspects of the EIF, an attempt is made to identify and address the challenges which could impede interoperability.

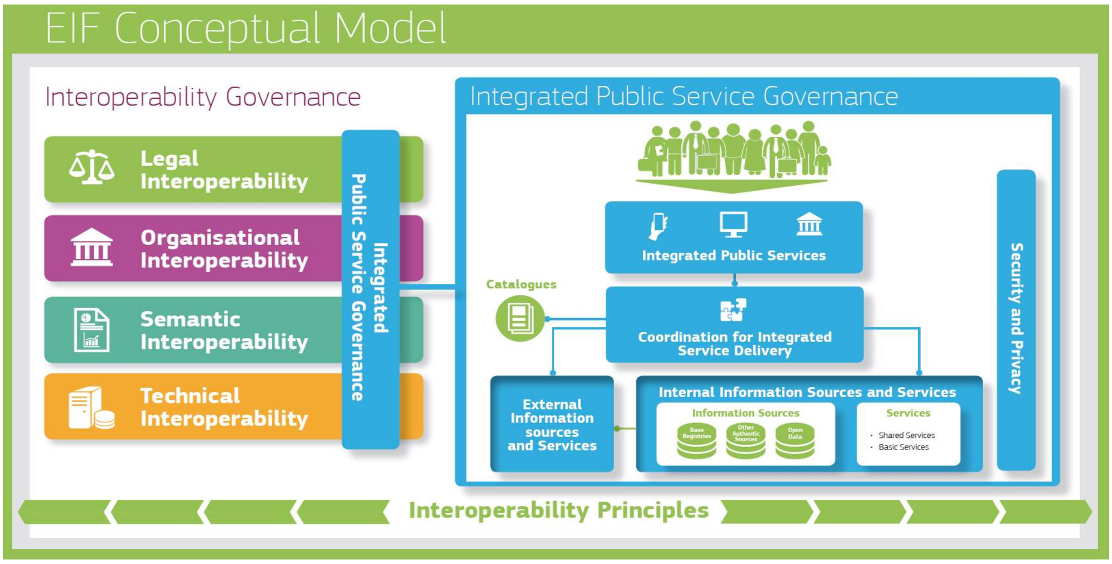

EIF Conceptual Model
Interoperability Governance
Legal Interoperability
Organisational Interoperability
Semantic Interoperability
Technical Interoperability
Integrated Public Service Governance
Integrated Public Service Governance
Integrated Public Services
Catalogues
Coordination for Integrated Service Delivery
External Information sources and Services
Internal Information Sources and Services
Information Sources
Base Registries
Other Authentic Sources
Open Data
Services
Shared Services
Basic Services
Security and Privacy
Interoperability Principles

Figure 2: European Interoperability Framework (EIF).

Synthesis

Sub-aspects such as time, quality and costs are mentioned in several articles, but are not considered during the research, due to the generality and the difficulty to measure these sub-aspects.

In some of the selected articles synonyms are used such as the conceptual aspect instead of semantic and syntactic, and the strategic aspect or business aspect instead of the organizational aspect. All these synonyms are incorporated in the four aspects.

By reading all relevant articles, analysing the content, and interpreting the possible challenges that impede interoperability, the following EIF aspects have been identified.

Legal interoperability

According to several of the identified documents, interoperability between organizations and with foreign countries continues to be one of the biggest problems because of legislation. Interorganizational data exchange remains a challenge due to (inter)national restrictions regarding privacy and the sharing of sensitive, confidential, and regulated information. In addition, there is a lack of formal mechanisms and knowledge about legal regulations. Which data can be shared, how will the data be used by the other organization, and does copyright apply? Although it is necessary to have laws concerning data exchange, these can obstruct the interorganizational interoperability, which in turn can lead to an undesirable situation.

Organizational interoperability

Literature shows that if enterprises want to collaborate by connecting and exchanging data with each other, processes, policies, and procedures need to be coordinated. Rules and norms, cultural differences, politics, and language need to be understood. Resistance to change among staff must be overcome. When these topics are not properly attuned to each other, this can have a negative impact on organizational readiness, mutual understanding, and trust between organizations and thus these barriers may impede interoperability. It is essential to create social networks, have a proper understanding of the objectives, the hierarchy, and roles and responsibilities within an organization. Communication and standards are key factors to the exchange of data in order to develop integrated solutions.

Semantic & syntactic interoperability

Each company is free to create its own concept for addressing semantic and syntactic interoperability. The aim is to understand and interpret the exchanged data. Due to a lack of common standards and protocols, there are many tools, systems, vocabularies, and ontologies. It creates challenges with respect to a common understanding of heterogeneous data and language. This is illustrated by problems regarding terminologies, context, definitions, representation, meaning and characteristics of information. Challenges regarding incomplete, inconsistent, conflicting, inaccurate, and unreliable data can be caused and create misinterpretation. Such challenges can cause serious problems for organizations and thereby impede interorganizational interoperability.

Technical interoperability

The technical aspect is the most elaborated aspect with regards to interoperability. As interorganizational collaboration is very important there is a need to achieve interoperability among heterogeneous information systems. In some cases, the technology may allow data to be exchanged but the organizational norms and rules prevent this. In other situations, there is a lack of coordination concerning outsourcing and the adoption of IT platforms within the organizations. This results in multiple different information systems using several types of soft- and hardware. Absence of technical support and knowledge create serious challenges with respect to the integration of these heterogeneous information systems and their networks. Resources are not always user-friendly and available when needed. To establish technical interoperability, it is essential to have technical support, protocols and a proper understanding of the infrastructure, available resources and used (modelling) languages.

All these interoperability barriers can impede the systems from exchanging data and services, and prevent proper data integration.

Conclusion

This SLR is concluded by the conceptual framework, which is presented below in Table 2. There are several interoperability barriers which need to be taken into account before organizations are ready to properly exchange data. All the articles covered the technical, organizational, and semantic and syntactic aspects, but only six out of fourteen articles mentioned the legal aspect. Validation of the conceptual framework is executed in the empirical part, which is presented in chapter 4.

Below in Table 2, the different interoperability aspects and sub-aspects are presented based on the four interoperability aspects. This overview can contribute to the development of interorganizational data exchange.

Table 2: Conceptual framework for interoperability barriers

Aspect	Sub-aspect	Description	References
Legal barriers	Intellectual property	Uncertainty regarding data ownership, return on investment and privacy barriers limits interoperability	(Chituc, 2017; Panetto et al., 2016; Shehzad et al., 2021; Yang & Maxwell, 2011)
	Accessibility	Although the data must be well secured, there is still a lack of formal mechanisms to exchange data in order to create interoperability	(Allen et al., 2013; Panetto et al., 2016; Yang & Maxwell, 2011)
	Knowledge	To create interoperability it is mandatory to know which data can be legally shared, how is it classified and what will happen with the data	(Allen et al., 2013; Vernadat, 2010; Yang & Maxwell, 2011)
Organizational barriers	Collaboration	A limited understanding of mutual objectives makes it difficult to build relationships, gain trust and realize interoperability	(Abdeen et al., 2021; Allen et al., 2013; Camara et al., 2014; Vargas et al., 2011; Yang & Maxwell, 2011; Zacharewicz, et al., 2017)
	Processes, policies, and procedures	Distinct organizations have their own internal processes, policies, and procedures. Although it is not realistic to merge all standards, it is necessary to align these sub-aspects in order to achieve interoperability	(Abdeen et al., 2021; Allen et al., 2013; Chituc, 2017; Grilo & Jardim-Goncalves, 2010; Rezaei et al., 2014 ; Vernadat, 2010; Zacharewicz, et al., 2017)
	Communication	Poor communication frustrates interoperability, hinders collaboration, and may cause undesirable situations	(Abdeen et al., 2021; Allen et al., 2013; Panetto et al., 2016; Zacharewicz, et al., 2017)
Semantic and Syntactic barriers	Data standards	Without common data standards, collaboration between organizations is impossible. Although it is very important to have data standards, there is almost no research with regards to achieving interoperability by using data standards	(Folmer et al., 2014; Shehzad et al., 2021; Zacharewicz, et al., 2017)
	Dictionary	To be able to use the exchanged data, dictionaries are needed to interpret and understand these data	Chituc, 2017; Shehzad et al., 2021; Zacharewicz, et al., 2017)
	Language	Different (modelling) languages and terminologies impede the exchange of data. Without a common language it is very complicated to communicate and interoperate	(Allen et al., 2013; Shehzad et al., 2021; Vargas et al., 2011; Zacharewicz, et al., 2017)
	Ontology	Due to an overload in data, many ontologies are created without standards or commonly agreed representations. For this reason, ontologies remain	(Camara et al., 2014; Panetto et al., 2016, Vernadat, 2010;

		uncorrelated and fragmented. Which limits the exchange of data interoperability	Zacharewicz, et al., 2017)
Technical barriers	Infrastructure	One of the main issues is to establish interoperability among platforms. This is created by the use of multiple different information systems. The data and technology evolution is still ongoing. This asks for an advanced technological infrastructure and software	(Abdeen et al., 2021; Camara et al., 2014; Rezaei et al., 2014; Shehzad et al., 2021; Yang & Maxwell, 2011; Zacharewicz, et al., 2017)
	Resources	There has to be a proper insight into the resources which are being used by an organization. The resources should be user-friendly and available when needed	(Abdeen et al., 2021; Mallek et al., 2012)
	Data integration	Old and new systems have to be interconnected with each other, which also contain several types of soft- and hardware. It is a serious challenge to integrate heterogeneous data which is originating from different information systems and networks	(Abdeen et al., 2021; Panetto et al., 2016; Yang & Maxwell, 2011; Shehzad et al., 2021; Zacharewicz, et al., 2017)
	Technical communication	A lack of communication guidelines between heterogeneous platforms hinders the sharing of data among agencies. Achieving seamless interoperability among heterogeneous communication systems is crucial	(Abdeen et al., 2021; Chituc, 2017; Zacharewicz, et al., 2017)

2.4. Objective of the follow-up research

The aim of the literature research was to provide insight, using the EIF, in which interoperability barriers are impeding an effective data exchange between organizations. This insight can help stakeholders to improve interoperability while taking the barriers into account. The objective of the follow-up research is to validate the framework in a real-life environment, to test the relevance of the framework for stakeholders and to discover their reasoning. This is executed empirically and can contribute to the adjustment of the suggested framework, so that the EIF can be complemented with results from practice.

3. Methodology

3.1. Conceptual design: select the research method(s)

For the research, the philosophy pragmatism, which is based on the fact that research starts with a problem is used. This type of research should lead to a practical solution that contributes to future practice. It does not consider theories, ideas, research findings, concepts and hypotheses in a theoretical way, but in terms of their practical consequences in a specific area (Saunders et al., 2019). As the aim of the empirical research is to validate the theoretical framework developed in §2.3 in a real-life situation, to create an in-depth understanding of the relevance of the interoperability barriers, and to adjust if refinement is needed, an exploratory and deductive research approach is used. This approach is to test the theory by using the collated data from the exploratory part of the research and helps to gain further insight into the topic (Saunders et al., 2019). For this reason, we answer the following questions:

Sub-question 3: How can the identified interoperability challenges for interorganizational data exchange be validated with empirical information?

Sub-question 4: How can the identified interoperability challenges be refined with empirical information?

Three research methods, namely a survey, an experiment and a case study, have been investigated to find the most suitable solution for this particular research.

According to Saunders et al. (2019) a survey is often related to a deductive approach and answers questions that begin with ‘who’, ‘what’, ‘where’, ‘how many’ and ‘how much’, and is therefore usually used for descriptive or exploratory research. A frequently used method to collect data from multiple respondents is a questionnaire. This can be beneficial because it enables the researchers to compare standardized data in an easy and quantitative way. The limitations of a survey include the fact that the process can be time-consuming, that multiple respondents with knowledge about the subject are needed, that the number of questions is limited, and questions and/or answers are subject to interpretation.

An experiment is often used as a quantitative method in natural sciences and answers questions that begin with ‘how’, ‘what’, ‘why’ and is therefore usually used for explanatory and exploratory research. The aim of an experiment is to examine the chance that a dependent variable changes due to a change in the independent variable. To study these changes, hypotheses are used to confirm or refute that a causal relationship exists between the dependent and independent variable (Saunders et al., 2019). Because of the qualitative nature of the research that does not focus on investigating causal relationships, this method is not suitable.

A case study is a qualitative method for extensive research into a phenomenon or topic within a real-life situation. This may include a group, process, person, organization or event. Case studies can be used by interpretivist and positivist researchers, inductively as well as deductively and for explanatory, exploratory and descriptive research. Often a combination of documentation and archival records, observations, interviews, questionnaires, reflections and research diaries are used.

According to Saunders et al. (2019) a case study is an excellent way to investigate an existing theory and the most-used method to evaluate a theoretical framework. Because of the aforementioned reasons, this method was used for the research.

In the embedded case study semi-structured interviews within multiple organizations have been used, because it will provide an in-depth insight into the study. The validation process, which involves the use of more than one data source, is known as triangulation (Saunders et al., 2019).

The main concerns regarding an embedded case study and the approach on how to manage the possible limitations are explained in §3.4.

3.2. Technical design: elaboration of the method

Case organization

The aim of the case study is focused on empirically validating the initial framework with regard to interorganizational data exchange. For this reason, selection criteria were composed. This may put special requirements to the interoperability evaluation and thus may influence the validation of the general framework organizations must meet. The selection criteria are:

- Knowledge of and experience with interoperability;
- Working with a great amount of data;
- Large contributor on the topic of interorganizational collaboration.

Based on the abovementioned criteria the Netherlands Ministry of Defence (MoD) is selected. The consideration is that the MoD strongly depends on a growing amount of data from modern systems, with different classification levels, which must be securely stored. To realize the ambitions in the field of interoperability, an infrastructure is needed that makes it possible to quickly and securely share data with other units or (external) partners when necessary. The MoD must be able to transfer data quickly and safely between different systems and partners, as well as efficiently process data it receives from multiple sources. Due to the unique case, the qualitative nature of the subject and time limitations, an embedded case study research was conducted within the MoD and two of its collaboration partners, namely Netherlands Organization for Applied Scientific Research (TNO) and the Ministry of Interior and Kingdom Relations (MoI).

Semi-structured interviews

The data was collected by performing semi-structured interviews. This allowed for the opportunity to use theoretically-deduced themes, which structure the interviews and produce comparable data. The use of semi-structured interviews also allows for opening up the discussion and ask follow-up questions to create a more in-depth understanding (Saunders et al., 2019). The collected data is used to validate the initial framework and test the relevance of the framework.

Participants

To collect empirical data, the authors performed semi-structured interviews within several departments of the MoD and two collaboration partners, TNO and MoI.

The participants of the interviews met the following requirements:

1. Work within the MoD or an organization which is directly related to the MoD;
2. Directly involved with interoperability challenges;
3. Knowledge and experience (expert) regarding interoperability;
4. The respondent should have a Bachelor’s or Master’s degree as the expectation was that it would create a better in-depth reasoning, and knowledge on the execution of this type of research.

Based on the abovementioned criteria, the following participants were interviewed (Table 3):

Table 3: Interview participants

Job description	Organization
Supervisor and policy maker	Central staff
Enterprise architect	Central staff
Policy advisor data governance	Central Staff
Representative I&S network	Central staff
Innovation manager	Defence Material Organization
Security architect	Defence Material Organization
Interoperability Manager	Defence Material Organization
Senior consultant	Defence Material Organization
IT security advisor	Ministry of Interior and Kingdom Relations
Senior consultant	Organization for Applied Scientific Research
Strategic advisor	Organization for Applied Scientific Research
Information security officer	Royal Netherlands Air Force
C4ISR developer	Royal Netherland Army
Senior staff advisor	Royal Netherlands Marechaussee
Plans officer	Royal Netherlands Navy

Interview protocol

An interview protocol was used to structure the semi-structured interviews. With this protocol, themes and questions were prepared that allowed for more in-depth questions. According to Kallio, Pietilä, Johnson, and Kangasniemi (2016) an interview protocol contributes to the reliability and the results of the study. In addition, questions are known and can be used and assessed by other researchers for future research.

Before the interviews were held, a pilot interview was held with an expert, with the goal to receive feedback on the interview protocol and interview style. The aim had been to raise the quality of the interviews and improve the collected data. The interview had been preceded by an explanation of the purpose of the interview, the ethical principles of those who take part and the duration of the interview. An explicit consent will be acquired prior to the use of the data (Saunders et al., 2019).

The interviews consisted of four parts. The first part contained the introduction. In the second part the aim was to get a comprehension about the knowledge of the interviewee with regard to the topic. During this part of the interview open questions regarding barriers were put forward, so that the interviewee could introduce (new) aspects. In the third part, the framework was introduced and validation questions about the content, the practical use and the reasoning of the interviewee were addressed. The interviewee could also indicate which of the elements were the most recognizable and impactful in practice and if they were complete and correct. By summarizing the answers and asking control questions, an in-depth understanding of the topic was acquired. This in turn contributes to the validity and reliability of the research. In the fourth and final part of the interview, an overall summary of the answers was provided and furthermore it was discussed if certain elements were missing. Depending on the answers of the interviewees, the framework could be refined.

The interviews were recorded for further analysis and complemented by taking brief notes. The interviewer could then concentrate during the interview and the results could be fully transcribed afterwards. The interviews were held in person and one-on-one in order to avoid interference from others. The interview protocol is available in Appendix B1 and the letter of consent in Appendix B2.

3.3. Data analysis

Each interview has been transcribed, including any non-verbal communication if applicable, and analysed. Transcriptions will be returned to the interviewees for fact checking the content and updated, if so required. All data will then be analysed using the Thematic Analysis Grid, which is suitable for qualitative research because of the accessible and flexible application, according to Saunders et al. (2019).

The objective of the research is to unveil patterns within the data and to recognize relations between themes. Each transcription will be analysed and coded, as done during the theoretical research. All barriers can then be identified according to the (sub)aspects of the theoretical framework or will be classified as new elements. The outcome of the analysis will be an empirical framework, which can be compared with the theoretical framework to find similarities and dissimilarities. Then the framework can be validated and adjusted. New aspects can be added and irrelevant aspects can be removed.

3.4. Reflection on validity, reliability, and ethical aspects

Construct validity

Construct validity is the extent to which the defined concepts measure what they are intended to measure. Within an embedded case study, it is possible to compare the results, because there are multiple independent sources of data (Saunders et al., 2019). By interviewing several experts within different organizations, with various roles and backgrounds, it is possible to compare and validate the results. The transcriptions will be send to the interviewees for fact checking.

Internal validity

Internal validity is the extent to which the findings can be attributed to the interventions rather than influenced by other factors. Firstly, a pilot interview has been held to validate the interview and analyse the answers and if necessary adjust the interview protocol (Saunders et al., 2019). The interviewees have remained anonymous, so that the interviewees are not restricted and can answer freely, which contributes to the quality of the results.

External validity

Although external validity is the extent to which the findings of the research can be generalized for other organizations, the main issue of using a case study is the lack of generalizable results. Due to the small samples, the ability to generalize is limited. Generalizability is applicable to research in which the characteristics of the research setting are similar (Saunders et al., 2019). Due to the unique case, domain specific elements such as (inter)national laws and regulations, and the use of weapon systems, could influence the validation of the general framework.

Bias

Bias is the extent to which a research process is comprehensive and does not contain false assumptions (Saunders et al., 2019). Due to the fact that the research has been performed by one researcher, who is an employee of the MoD, the chance exists that a bias has occurred within the data collection due to a false assumption or logical leap. The researcher is not familiar with interoperability within the MoD. By asking the same questions to all the interviewees and by explaining the steps that have been taken during the research, the researcher's bias has been minimized.

Reliability

Reliability is the extent to which an earlier research design can be replicated and produces the same results. Normally, the aspect will pay attention to the replication of a research. However, qualitative research is not necessarily intended to be replicated producing the same outcomes, because of the socially constructed interpretations within a specific setting and within a certain time frame. But a detailed description of the research design, the particular context and the methods used may help others to initiate comparable research (Saunders et al., 2019).

Ethical

The ethical aspect refers to the integrity and objectivity of the researcher, the respect for others, and the privacy of those who are taking part (Saunders et al., 2019). In the introduction, the purpose of the research was explained, together with matters such as privacy and the way how the data is used. If possible and allowed by the interviewees, the interview was recorded. The recordings will be deleted after the interviews have been processed. No references will be made which could lead to traceability.

4. Results

4.1. Research implementation

To validate and refine the theoretical framework, thirteen semi-structured interviews were held within three different organizations, namely the MoD, TNO and the MoI. Therefore experts were selected on the basis of their knowledge and experience with respect to the topic of interoperability with regard to interorganizational data exchange. The general information of the interviewees is presented in Table 4. The MoD contains seven separate departments of which five are included in the research. An overview of the organizations is available in Appendix C.

The information is based on the first five questions (Q1-Q5) of the interview related to the organization, current position, educational level, years within the organization and experience with the topic.

Table 4: General information interviewees

#	Organization	Position	Education	Within Org	Experience
1	RNLAF	Information security officer	Academic	17 years	3 years
2	DMO	Senior consultant	Academic	17 years	30+ years
3	DMO	Innovation manager	Academic	35 years	30 years
4	DMO	Security architect	Bachelor	3 years	16 years
5	TNO	Senior consultant	Academic	20 years	31 years
6	CS	Enterprise architect	Academic	2 years	20 years
7	TNO	Strategic advisor	Academic	17 years	22 years
8	CS	Representative I&S network	Academic	20 years	20 years
9	CS	Supervisor and policy maker	Academic	28 years	20 years
10	RNLA	C4ISR developer	Academic	18 years	5 years
11	CS	Policy advisor data governance	Academic	3 years	1.5 years
12	RNMP	Senior staff advisor	Academic	15 years	15 years
13	MoI	IT security advisor	Academic	6 years	6 years

4.2. Data analysis

4.2.1. Knowledge of and experience with the topic

In the second part of the interview, six question (Q6-Q11) were presented (Appendix D1), in order to obtain an understanding of the knowledge and experience of the interviewees with regards to interoperability, the organizational level of interoperability and the most common barriers.

The first question (Q6) concerned the definition of interoperability and how the interviewee would describe interoperability. The most mentioned phrases were the ability to collaborate (10) to exchange (8) and understand (5) relevant (2) and time sensitive (2) information, within (2) or between (2) organizations without unpleasant surprises (2).

ICT is an enabler to make it possible, not the starting point (according to interviewee #2). You can realize interoperability at all kinds of levels, organizational, policy, technical (#7).

During question 7 the interviewees answered in which way they are involved with the topic. Most of them spent their time on how to enhance interoperability within the MoD and/or with other organizations. It included legal aspects such as privacy issues, organizational aspects such as policies and procedures, among others related to security. Also, semantic aspects like the same vocabulary, same definitions, the same terms, and technical aspects: how do different systems fit together using for instance a generic interface or architecture.

Enabling information exchange between different classification levels (#3). We need to be interoperable with each other and this includes being operationally effective with our partners and our environment (#10). How could we share data between two organizations, in a technical way, but also find out which legal regulations would apply and what might be further required (#13).

When the interviewees were asked what their experiences were concerning this topic (Q8), the most common answer was that collaboration is always difficult (3). The reasons for this differ from the fact that systems are always developed for one function which often means different working methods and other standards, which often do not fit together. But also because of the fact MoD has no central procurement process, so there are no provisions for interoperability, and as a result, one can find fairly random configurations. Another interoperability issue is that differences between the interpretation of the term exist.

Different networks ask for different network specialists and at the end one needs to make everything work together and that is not sustainable (#1). Everyone focuses on the technology, and everyone seems to skip the organizational and semantic aspect (#5). Because we simply do not have the right equipment for it yet (#9).

In question 9 the interviewees were asked about the current level of interorganizational interoperability. According to six respondents the current level of interoperability is limited (#2), laborious (#5), fragmented (#6). They are islands and not multidomain operations (#8). We are not yet at the level we would like to reach (#9). Low to very low (#10). Four other respondents stated that when it comes to very specific processes, it is a bit more difficult (#3). I think it is fine in many domains (#7). Within the LGI it is reasonably in order (#12). We are well on our way, but we're still a long way from where we should be and we're not nearly mature enough on the collaboration (#13).

Barriers which are impeding effective data exchange (Q10) are the human factor (2), technological opportunities (3), purchasing process, lack of agreements (2), decision-making (2) implementation, overview, standards, and trust. Unnecessary compartmentalization and information security.

My idea is that it's never actually a technical problem (#7). I think there is not enough central control, someone has to make the decision and then it has to be implemented (#8). There are no Defence-wide reference lists (#11). Information security is very much focussed on control and mitigating risks (#12).

The most common interoperability barriers (Q11) are the diversity of systems (3), exchangeability (2), trust (2), proprietary of systems, lack of agreements and too many standards, differences in interpretation, hidden interests, willingness, bureaucracy, lack of manpower and knowledge.

Proprietary products. You can't make it operable because you don't know how it works (#4). There are too many standards, there is too much room for interpretation (#6).

4.2.2. Validation, refining and ranking theoretical framework

To be able to validate the theoretical framework each of the interviewees were asked fourteen open questions (Q12-Q25). Here four of the fourteen validated sub-aspects are presented that are the most notable. Some of the interviewees already made some suggestions for refinement. These suggestions have been taken into account. Because the sub-aspect ontology scored lower on the overall ranking than the sub-aspect technological communication, the sub-aspect ontology is presented. A complete overview of all validated aspects is found in Appendix D2.

Legal barrier - Intellectual property: Most of the interviewees (12) validated this sub-aspect, it had the highest overall average on recognizability, impact and relevance (4.36) and all the interviewees had major or minor suggestions for refinement. Most of the interviewees recognized that **data ownership** is a major problem, and that it is not properly arranged within the MoD, often because data is not (correctly) labelled. **Intellectual property** was also recognized by two interviewees as a problem, so the suggestion was to include **intellectual property** in the description. The problem within the MoD is created because a lot of products are purchased, without having control over the purchasing policies, which lead to inaccessible products. The term **return on investment** was also acknowledged by two of the interviewees and they translated it into "*quid pro quo*". Regarding the **privacy barriers**, two interviewees stated that there are issues regarding the unfamiliarity with the General Data Protection Regulation (GDPR), so it was admitted that it is an important part of this sub-aspect. Another suggestion was to add a sub-aspect "law and regulations", because if legally permitted to exchange information does not relate to the ability to exchange information. A sub-aspect law and regulations can determine what the boundaries are. Data ownership is an important sub-aspect of the framework.

Ownership also implies responsibility. If the ownership is unknown, we run into problems that hinder interoperability (#1). Return on investment must be translated into, what do I gain if I share my information (#3). Companies make products and make them inaccessible (#4). I also actually think that intellectual property also plays a role in operability, because we also have no management or control over our purchasing policy. So, it means that we get all kinds of packages and products from all kinds of manufacturers and we don't think about interoperability or only afterwards (#10).

Organizational barrier – Collaboration: Nearly all the interviewees (12) validated this sub-aspect, as it had the second highest overall average (4.26) and there were eight suggestions for refinement. Most of the interviewees within the MoD and TNO certainly recognized this barrier. The most frequently given reason was the difference in culture between the Operational Commands (OPCOs). Because of the old, ingrained patterns, a lot is still locked up in silos. Therefore, these organizations can be seen as separated islands with their own objectives, often building fences around information, and focussing on own organization first. This is also caused because regularly it involves a lack of trust. Another mentioned issue are the differences between civilians and serviceman. Civilians are more concerned with policies and serviceman more with operations, apart from the fact that a serviceman changes jobs every three to five years. One of the interviewees mentioned that the MoD is the only ministry whose implementation is also within the ministry and is not an organization on its own, this makes it not only a civilian and military matter, but also a political one.

100 percent. This is very recognizable, also at the MoD, also at the OPCOs with their own strategy and culture, their own requirements and laws. A common goal is missing in 99 out of 100 cases (#6). So it is important that you have shared objectives and if they have not yet been defined, it will also be very difficult to work together. Trust is also linked to culture, if you feel that a certain culture is less *reliable than your own culture, then it is also more difficult to exchange information with each other, because there is less confidence that the other party will handle the information with due care (#9). This is going reasonably well between our organizations. There is a rather different culture between the MoD and the rest of the government (#13).*

Semantic and Syntactic barrier – Language: This sub-aspect has been validated seven times, it has the lowest overall average (2.72) and there was solely one suggestion for refinement. According to four interviewees this sub-aspect is not very applicable, it is something to keep in mind, but we will make it work. According to four others it is important to stay focused, because in multidomain operations each OPCO uses its own specific abbreviations, with other meanings. This can be very challenging. Also internationally, when one thinks one speaks the same language, things can get dangerous. Within IT there is a lot to be gained regarding the sub-aspect. The suggestion was to separate the semantic and syntactical barriers into the human aspect and the technical aspect because semantics, syntax and technical barriers are now mixed up.

The explanation we give can be different. In our organization we have abbreviations, we sometimes have the same name for two very different things. Even some systems, with a different classification level, have the same name. This can be very challenging (#1). This is certainly a barrier, especially if you want to exchange information internationally (#2). Sometimes there is still room for improvement, especially when we look at the multi-domain performance. Within IT there is a lot to be gained from an unambiguous architecture, many architects all have a different language and therefore very easily talk past each other (#3). If you think you speak the same language, but your dictionaries are different, things can get complicated. The situation where you think you are using the same language is much more dangerous and difficult (#5).

Semantic and Syntactic barrier – Ontology*:* Eight interviewees validated this sub-aspect, it had the second lowest overall average (2.90) and there were no suggestions for refinement. Three interviewees indicated that the sub-aspect ontology was new or that they were not familiar with the sub-aspect. Four interviewees indicated that it is important to have standards and uniformity within data, one of them added that it is especially important for retrievability, and lineage and one interviewee said only in time of critical communication. One respondent stated that there is no ontology possible for interoperability itself, but does believe that within a certain context, like the MoD one should be able to define an ontology. Another interviewee stated that one must be careful with ontologies, that they do not become more important than the overarching principles.

If you want to transfer data and then large amounts of data between different units, this is a recipe for failure. Interpretation and context are of great importance here (#2). You have to be careful not to make your ontologies more important than the overarching principles that those ontologies should be under. The point is that you create joint solutions and that you can store your data in them. It's nice if you have everything the same, but it shouldn't become a kind of religion to coordinate those ontologies exactly, because then you will never come to cooperation (#12). Uniformity in data is very important, especially for your retrievability and your lineage on your data(#13).

Finally the interviewees were asked three questions (Q26-28) to rank the different sub-aspects from the theoretical framework. How much did they **recognize** (Q26, Table 5) the specific sub-aspect to be a current barrier, what was the **impact** (Q27, Table 6) and how **relevant** (Q28, Table 7) was the sub-aspect with regard to data exchange (Appendix D2). The ranking is based on the Likert-scale 1-5.

For *example, in Table 5 thirteen scores per sub-aspect are presented and the total score is based on the sum of all rankings together: (4 x 3=) 12 + (2 x 4 =) 8 + (7 x 5 =) 35 = a total of 55.*

Table 5: Recognition of sub-aspect (Q26)

Aspect	**Sub-aspect Score:**	**1**	**2**	**3**	**4**	**5**	**Total**	**Average**
Legal barriers	Intellectual property			4	2	7	55	4.23
	Accessibility	1	1	4	2	5	48	3.69
	Knowledge		3	2	3	5	49	3.77
Organizational barriers	Collaboration	1	1	3	2	6	50	3.85
	Processes, policies, and procedures			3	2	8	57	4.38
	Communication	1	2	2	3	5	48	3.69
Semantic and Syntactic barriers	Data standards	1	2	7		3	41	3.15
	Dictionary	1	2	6	2	2	41	3.15
	Language	1	5	4	2	1	36	2.77
	Ontology	4	2	3	1	3	36	2.77
Technical barriers	Infrastructure		2	3	2	6	51	3.92
	Resources		2	3	3	5	50	3.85
	Data integration		1	4	3	5	51	3.92
	Technical communication	2	3	4	2	2	38	2.92

Table 6: Impact of sub-aspect (Q27)

Aspect	**Sub-aspect Score:**	**1**	**2**	**3**	**4**	**5**	**Total**	**Average**
Legal barriers	Intellectual property		1	1	2	9	58	4.46
	Accessibility	1	3	3	1	5	45	3.46
	Knowledge		1	3	4	5	52	4.00
Organizational barriers	Collaboration			1	4	8	59	4.54
	Processes, policies, and procedures		2	2	3	6	52	4.00
	Communication		1	3	4	5	52	4.00
Semantic and Syntactic barriers	Data standards		2	4	3	4	48	3.69
	Dictionary	1	3	2	5	2	43	3.31
	Language	2	4	4	2	1	35	2.69
	Ontology	2	3	5		3	38	2.92
Technical barriers	Infrastructure		3	2	2	6	50	3.85
	Resources		2	5	1	5	48	3.69
	Data integration		1	5	4	3	48	3.69
	Technical communication	1	4	2	2	4	43	3.31

Table 7: Relevance of sub-aspect (Q28)

Aspect	**Sub-aspect Score:**	**1**	**2**	**3**	**4**	**5**	**Total**	**Average**
Legal barriers	Intellectual property			3	2	8	57	4.38
	Accessibility		4	2	2	5	47	3.62
	Knowledge		1	3	5	4	51	3.92
Organizational barriers	Collaboration			2	4	7	57	4.38
	Processes, policies, and procedures		2	2	4	5	51	3.92
	Communication		2	4	3	4	48	3.69
Semantic and Syntactic barriers	Data standards	1	2	2	3	5	48	3.69
	Dictionary	1	4	3	3	2	40	3.08
	Language	1	6	3	2	1	35	2.69
	Ontology	1	4	5		3	39	3.00
Technical barriers	Infrastructure		3	3	2	5	48	3.69
	Resources		1	7	1	4	47	3.62
	Data integration		3	4	3	3	45	3.46
	Technical communication	2	3	4	2	2	38	2.92

The interviewees ranked the fourteen sub-aspects within the three different subjects. Intellectual property and collaboration scored the highest and language and ontology the lowest. For a total overview of the averages see Appendix D3. What stands out is that the top three only consist of organizational and legal barriers, whereas the bottom three consist of semantic and syntactic barriers, and technical barriers.

4.2.3. Overall impression of framework

The interview was concluded by asking questions (Q29-Q35) about the overall impression and completeness of the framework and suggestions for refinement (Appendix D4). First, question 29 and 30 are presented in Figure 3. In total there were two remarks and four suggestions for refinement.

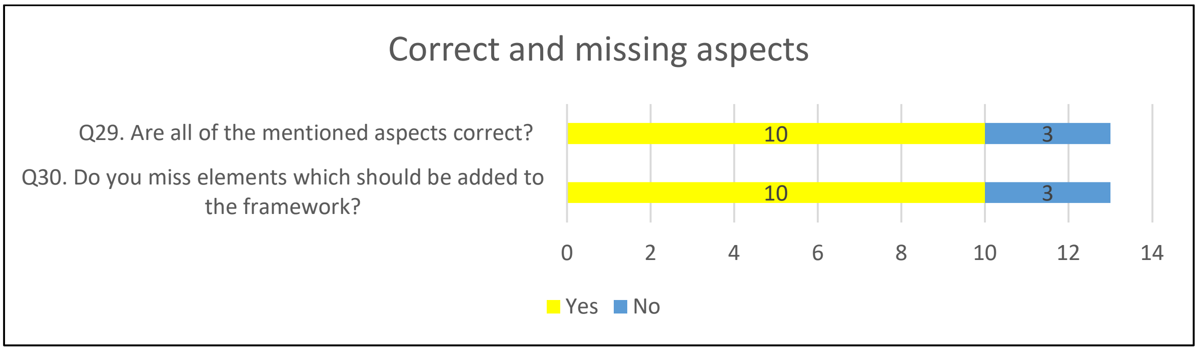


Figure 3: Correct and missing aspects

When asking question 31, six of the interviewees stated that it is a combination of all of these sub-aspects, which are impeding a proper interoperability implementation. One cannot pinpoint a sub-aspect as an showstopper according to one respondent, and the extent to which they affect interoperability depends on the process, according to two of them. Things happen in sub-areas, but there is no overall coherence. The real barriers are often caused by old thinking and culture, but there is a need to invest in the preconditions and benefits will be attained by thinking differently. One suggestion for refinement is to put the organization at the top of the framework.

Question 32 was if these sub-aspect could influence decision-making if they are not properly implemented. One interviewee stated that it would become a bigger web of disconnected systems. The effect is that one will fall behind potential opponents according to three interviewees and that may cause operational risks. Two interviewees replied “business as usual”, because if one does not settle somebody else does it. Then one will have to just go along with it, but it will be smarter to keep control. Two others said it would diminish your right to exist.

Question 33, 34 and 35 are combined in Figure 4.

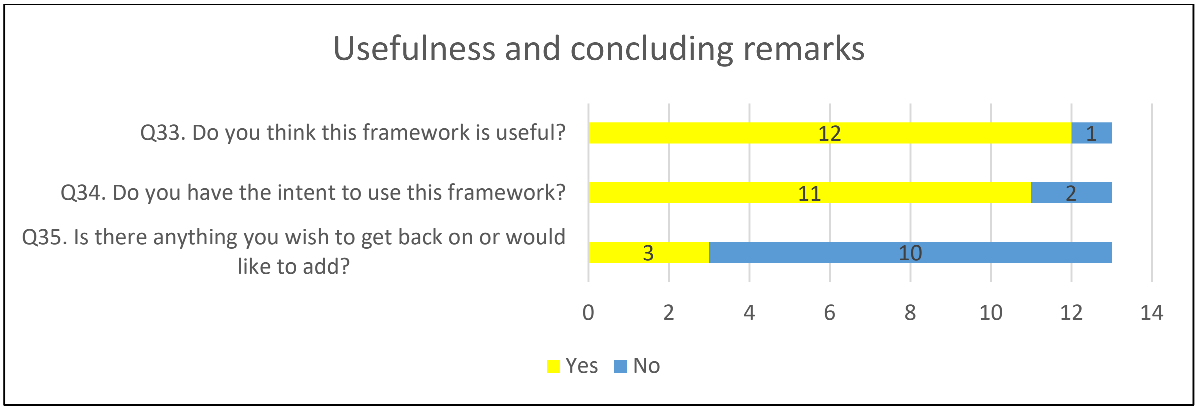


Figure 4: Usefulness and concluding remarks

Twelve interviewees answered that the framework is certainly useful for them. It provides guidance, insight to the upper management, and allows one to prioritize what is important, because it described all the layers that are required. If a timeline could be added with dependencies, it could be used to get an understanding of certain aspects and reporting purposes, because all sub-aspects are interdependent. And if it could be linked to advice or policies, it could be used as an operating model, but the question remains how it could be used or implemented as a steering instrument.

The overall impression of the interviewees is that the current level of interoperability is limited, since it is a very complex topic. Within the MoD there is a lack of collaboration between the different OPCOs. This is due to differences in systems, culture, standards, and policies. The framework could provide insight into the strengths and weaknesses and as such clarity on resolving the interoperability barriers. Additional research could provide insight and clarity.

4.3. Final version framework

In this paragraph the final version of the framework is presented after comparing the theoretical framework with the empirical research. The validation is based on the answers given in the interviews. In chapter 5 the results are interpreted and compared with previous research. This sequence was chosen for the framework because two respondents felt it had to start with the organizations interest. Firstly, the organizational willingness for the exchange of data needs to be present. Secondly, it must be legally allowed. Thirdly, it has to be technically possible to exchange the data. The suggestions for refinement and the added sub-aspects are found below in Table 8. Bold and underline assist in the recognition.

Table 8: Final framework

Aspect	Sub-aspect	Description	Comment
Organizational barriers	• Collaboration	A limited understanding of **cultural differences**, mutual objectives **and ethics** makes it difficult to build relationships, gain trust and realize interoperability	Validated, additions need to be validated in a second cycle
	• Processes, policies, and procedures	Distinct organizations have their own internal processes, policies, and procedures. Although it is not realistic to merge all standards, it is necessary to align **and coordinate** these sub-aspects in order to achieve interoperability	Validated, addition need to be validated in a second cycle
	• **Interpersonal** Communication	Poor communication, **due to social differences and a lack of insight in stakeholders**, frustrates interoperability,	Validated, additions need to be validated in a second cycle

		hinders collaboration and may cause undesirable situations	
Legal barriers	• **Data ownership**	Uncertainty regarding **intellectual property,** return on investment and privacy barriers, **such as GDPR**, limits interoperability	Validated, additions need to be validated in a second cycle
	• Accessibility	Although the data must be well secured, there is still a lack of formal mechanisms to exchange data in order to create interoperability	Validated
	• Knowledge	To create interoperability, it is mandatory to know which data can be legally shared**, how it can be shared**, how is it classified and what will happen with the data. **This asks for a less risk averse attitude**	Validated, additions need to be validated in a second cycle
Semantic and Syntactic barriers	• Data standards	Without common data standards **and knowing the context (and concept)**, collaboration between organizations is **difficult**	Validated, additions need to be validated in a second cycle
	• Dictionary	To be able to use the exchanged data, dictionaries are needed to interpret and understand these data	Validated
	• Language	Different (modelling) languages and terminologies impede the exchange of data. Without a common language it is very complicated to communicate and interoperate	Validated, additional research is needed. Closely related with collaboration and communication.
	• Ontology	Due to an overload in data, many ontologies are created without standards or commonly agreed representations. For this reason, ontologies remain uncorrelated and fragmented. Which limits the exchange of data interoperability	Validated, additional research is needed due to the unfamiliarity and big differences in scoring this sub-aspect is retained.
Technical barriers	• Infrastructure	One of the main issues is to establish interoperability among platforms. This is created by the use of multiple different information systems. This asks for advanced technological **hardware** and software which can use **common data models**	Validated, additions need to be validated in a second cycle
	• Resources	There has to be a proper insight into the resources which are being used by an organization. The resources should be user-friendly and available when needed	Validated
	• Data integration	Old and new systems have to be interconnected with each other, which also contain several types of soft- and hardware. It is a serious challenge to integrate **qualitative** heterogeneous data which is originating from different information systems and networks	Validated, addition need to be validated in a second cycle
	• Technical communication	A lack of communication guidelines between heterogeneous platforms hinders the sharing of data among agencies. Achieving seamless interoperability among heterogeneous communication systems is crucial	Validated, additional research is needed. Overlap with other three technical sub-aspects and communication.
Organizational barriers	• **Costs**	Costs were not taken into account in the research, because it is a part of every sub-aspect and difficult to measure	**Suggested as sub-aspect**
Legal barriers	• **Legal and regulatory**	This sub-aspect check if it is legally permitted to exchange data	**Suggested as sub-aspect**

5. Discussion, conclusion, and recommendations

5.1. Discussion – Reflection

5.1.1. Reflection on the literature review and framework development

The initial focus was on barriers which are impeding sensitive and exclusive data exchange between organizations. Due to the limited results which could be found regarding this subject during the literature review, the research was broadened to barriers which impede data exchange in general. To answer the research question, the formulation of a specific search query was started. The search query resulted in 207 articles from the OU-library of which eight articles proved to be relevant. Due to the limited amount of relevant articles, the snowball method was used. This resulted in an additional six articles, bringing the total to fourteen relevant articles which have been used for the research. The snowballing method is a limitation for the research because it resulted in articles which were used as a reference in the initial articles or which used the initial articles as a citation.

The fourteen articles were analysed to develop an initial theoretical framework. In six of the fourteen articles the European Interoperability Framework (EIF) is mentioned. Hereby the aspects of the EIF were used to provide a structure for the development of the own framework. It resulted in a theoretical framework that consists of four aspects which were further elaborated by adding fourteen relevant sub-aspects derived from the relevant articles.

5.1.2. Reflection on case study

An embedded test case was conducted within the MoD and two of its collaboration partners, as described in Chapter 3. A total of thirteen semi-structured interviews were held of which ten interviews with MoD employees, two interviews with TNO employees and one interview with a MoI employee. Although some of the MoD interviewees stated that the current level of interoperability at the MoD is still limited, they all were able to answer nearly all questions due to their expertise.

One limitation is that almost all interviews were conducted within the MoD and TNO. Because TNO is closely related to the MoD, it could be a limiting factor for the interorganizational aspect. On the other hand the influence could be negligible because the research has shown that despite the fact that the MoD is one organization, there are major differences between the seven departments, as they differ so much that they can actually be seen as separate organizations.

5.1.3. Reflection on interviews

Initially the plan was to hold fifteen interviews, but due to circumstances two interviewees were unable to participate. All of the respondents signed the letter of consent before the interview was held and every interview was held in a live setting. A total of 35 questions were put forward in which every aspect and sub-aspect was introduced. During the interviews most of the interviewees rated the current level of interoperability as limited. Due to their expertise on the topic and the limited level of interoperability supporting documentation was not demanded.

All interviews were recorded. After the transcription of the recordings, they were deleted and the results returned in Dutch and English to the interviewees for fact checking. Due to the holidays the deadline for feedback, if any, was set on three weeks. Six responded, one responded the week after and six did not respond at all.

All interviewees were keen on participating and happy to contribute to the research. The interviewees seemed to be comfortable and open about their knowledge and their views on the level of interoperability within the organization. Any non-verbal communication was not noted and the interviewees explained all as best they could. There was enough room for discussion, verification and follow-up questions, so an in-depth understanding of the topic was gained. Each sub-aspect of the initial framework was discussed and ranked on three subjects (recognizable, impact and relevance). The suggestions for refinement, made by the interviewees, are incorporated in the final framework.

5.1.4. Interpretation of the results

The results from the theoretical study (Chapter 2) and the findings of the empirical study (Chapter 4) are compared. Validation of the consistency of the results with the literature is provided and if it deviates, what the possible reasons for these deviations could be. The aspects are discussed in the final framework. The average score was based on all scores given for the subject recognizability, impact and relevance (see Appendix D3).

Organizational barriers

Collaboration has been validated by twelve interviewees with an average score of 4.26. According to the interviewees collaboration is a challenge because of a lack of trust, different cultures, personal objectives and distinct levels of understanding, as corresponding to the views of Abdeen, Fernando, Kulatunga, Hettige, and Ranasinghe (2021) and Grilo and Jardim-Goncalves (2010). Although the fact that the culture and ethics were not a part of this sub-aspect, it was mentioned by respectively five and three interviewees as an essential part for collaboration.

According to the views of Allen, Karanasios, and Norman (2013) and Zacharewicz et al. (2017) every organization has its own **processes, policies and procedures** which are not by definition consistent with other organizations. Although processes, policies and procedures are essential, they can also create bureaucracy and barriers with regards to data sharing, which makes a common operational picture complicated. This sub-aspect has been validated by twelve interviewees with an average score of 4.10. The interviewees stated that there is no shortage of processes, policies, and procedures. But they are so strict and developed from a risk perspective that they often result in bureaucracy. Each OPCO has its own standards, but these should be coordinated for the same operational problems. Chituc (2017) vision is that it is not realistic to merge all standards, but it is necessary to create a certain degree of compliance.

The sub-aspect **interpersonal communication** has been validated by ten interviewees with an average score of 3.79. The respondents confirmed that this sub-aspect is essential for the collaboration between multiple organizations. But often the organizational interest is put above the broader social effect. One might think to be on the same page, but often it is not the case and frequently has to do with culture. This is in line with Allen et al. (2013) who state that large public organizations fail to communicate due to cultural differences, which result in a lack of understanding.

Legal barriers

According to Shehzad et al. (2021) intellectual property has to do with the right of maintaining data ownership and privacy. Here the interviewees deviate from this view regarding intellectual property. They connect it to the purchasing processes, because it is not always clear who has control over a certain system and thus the authority over certain data. For this reason the sub-aspect was changed from intellectual property to data ownership. **Data ownership** has been validated by twelve interviewees with an average score of 4.36. For most of the interviewees it was recognizable that data ownership is not properly arranged and that is it essential for interorganizational interoperability. Two respondents stated that return on investment meant that data exchange should give something in return. Two respondents stated that there are issues regarding the unfamiliarity with the GDPR, which impedes data exchange. This is in line with Yang and Maxwell (2011) who indicate that privacy concerns limit data sharing behaviour.

Although data needs to be protected in accordance with law and regulations, it still needs to be accessible (Panetto et al., 2016). Limited access to data results in a lower level of data exchange which impede solutions for common problems (Yang & Maxwell, 2011). The sub-aspect **accessibility** was validated by twelve interviewees with an average score of 3.59. There is a lack of formal mechanisms that focus on accessing and exchanging data in a legally permitted way. Especially when it comes to the classified domain, it remains very complicated. Information is needed, but there is no access or possibility to exchange it. The need-to-know is usually arranged, but the need-to-use is more difficult.

Within the MoD the sub-aspect **knowledge** is recognized as a barrier and is validated by eleven interviewees with an average score of 3.90. People often do not know if information is for instance GDPR, how it is classified and how it can be distributed correctly. According to three interviewees there is a lack of knowledge within the legal affairs office, especially when it concerns the technical aspect. This is in line with Vernadat (2010). One answer which deviates from the theory is that this is caused by risk averse behaviour within the MoD, people do not answer because of the potential risks.

Semantic and Syntactical barriers

Data standards have been validated by twelve respondents with an average score of 3.51. Data from an organization often contains errors and characteristics, therefore it is needed to design data standards which promote interorganizational coordination and communication (Folmer, Wu, & Bekkum, 2014). Although there were differences in opinion on which or how many standards are needed, most of the interviewees agreed to the fact that it is important to know which concept and context has been attached to be able to interpret the data in a correct way.

Organizations use different definitions which result in various meanings and interpretations of the exchanged data, and it leads to confusion between parties. Successful collaboration requires consensus on standard definitions (Shehzad et al., 2021). The sub-aspect **dictionary** has been validated by eight respondents, with an average score of 3.18. Four interviewees stated that this sub-aspect was not really interesting, because one learned in practice. Others mentioned that dictionaries are often not available, so interpretation could be an issue, because not everything meant the same thing within the OPCOs. Meanings differ, although the same words and definitions are used.

Language has been validated by seven respondents, with an average score of 2.72. According to four interviewees this sub-aspect is not very applicable. It is something to keep in mind, but making it work is what it is about. So here the literature deviates. Allen et al. (2013) indicate that it is impossible to communicate if the language and terminology are unknown, Vargas, Boza, and Cuenca (2011) state that it is more difficult to realize interoperability.The sub-aspect scored the lowest on all subjects. Additional research is needed because of the variety of answers of the interviewees.

Ontology was the least known sub-aspect under the interviewees. It has been validated by eight respondents, with an average score of 2.90. Three interviewees indicated that the sub-aspect ontology was new to them. Four interviewees indicated that it is important to have standards and uniformity within data, according to Rezaei, Chiew, and Lee (2014) it is necessary that organizations share ontologies. Because of the unfamiliarity with this sub-aspect and the big differences in rankings, additional research is needed.

__Technical barriers__

The information systems which are being used by organizations contain various types of hardware and software, which challenges the integration of these heterogenous systems (Camara, Ducq, & Dupas, 2014; Yang & Maxwell, 2011). **Infrastructure** has been validated by eleven respondents, with an average score of 3.82. Four of the interviewees said that the technology itself is often not the problem. The infrastructure in general is interoperable. Faults occur in the non-alignment of policies, software, networks and a lack of common data models. Allen et al. (2013) agree on this and state that the technology is often not the problem, but the processes are.

Mallek et al. (2012) vision on **resources** is that they should be available when needed and should give a good understanding of the exchanged data. This is in line with the answers of the respondents. Twelve respondents validated this sub-aspect, with an average score of 3.72. Six of the interviewees recognized this sub-aspect and stated that it is often an issue due to a lack of availability, findability, or existence of (well-qualified) data. Four interviewees stated this is due to the fact that there is no integral idea, no central overview and no catalogue available.

As reported by several studies low data integration causes inadequate Interoperability. Often this is the result of software and the existing applications (Shehzad et al., 2021). This is consistent with four of the interviewees who stated that the problem within the MoD often has to do with old-new integrations, because centralization is cheaper, only it does not help to overcome the technical barriers. The sub-aspect **data integration** has been validated nine respondents, with an average score of 3.69. Three other respondents indicated that this should not have to be a technological problem. Because technology is not the solution, it is only a precondition and enabler.

Technical communication was validated by ten respondents, with an average score of 3.05. Three interviewees stated that it should not be a problem, especially when the three aforementioned sub-aspects are arranged. So, overlap exists with other sub-aspects. Technical communication does not stand in isolation. Networks need to be integrated and sometimes self-imposed barriers are introduced. Although it is crucial to achieve seamless interoperability between heterogenous communication systems (Chituc, 2017), the technology itself is often not the problem but the organizational rules and norms (Allen et al., 2013). Additional research into this sub-aspect is needed.

Remarkably, the top three barriers only consist of organizational and legal barriers, whereas the bottom three consist of semantic and syntactic barriers and technical barriers. This can be related to some of the interviewees who stated that the technical barriers are often not the problem, but the legal and organizational barriers. Obviously, the second thing is that each OPCO has a good idea of their own organization, but not interorganizational. This is presumably caused by the fact that each OPCO has its own domain specific culture, policies, and systems. it could also explain why language, ontology and technical communication is rated low, because within the own organization this is not an issue. The third result which is noticeable is that when it comes to the classified domain, interoperability is much more complicated, because certain systems cannot be physically linked to each other. The last aspect which needs to be addressed is the purchasing process within the MoD that results in a diversity of systems. As a result, systems are often not interoperable. The specific domain in which the MoD operates might have influenced the validation of the framework. A partial explanation can be the differences in (inter)national laws and regulations to which the MoD must comply and the use of weapon systems.

5.1.5. Reflection on validity, reliability, and ethical aspects

Construct validity

To validate the results the transcriptions were send to the interviewees for fact checking, if any. Six of the interviewees responded and confirmed that their transcription was correct. As the other respondents did not reply to the fact checking, the assumption needs to be made that they agreed to the transcription. Further analysis is needed for these results.

Internal validity

Before the interviews were held, a pilot interview was conducted in which the interview protocol and the letter of consent were validated. The recorded interviews were translated into the English language. The interviews were held in the Dutch language so as not to create a language barrier and to reduce the risk of misinterpretation. The letter of consent was sent prior to the interview in order to bar insight into the questions before the interview and gain more reliable answers during the interview. The responses were recorded in Dutch, translated into English and both versions were sent to the interviewees for fact checking.

To get a better understanding of the sub-aspects the interviewees were asked to rank all sub-aspects on three subjects. How much did they **recognize** the specific sub-aspect to be a current barrier, what was the **impact** and how **relevant** was the sub-aspect with regard to data exchange. Because the interviewees remained anonymous, there were fewer restrictions and they were able to answer more freely. It probably contributed to the quality of the results.

External validity

Although using an embedded case study, ten interviews were held with MoD employees and two interviews with TNO employees, which are closely related to the MoD. Only one interview was held with a person from another organization, namely the MoI. The generalizability of the results could be limited due to the small sample and the fact that the military sector concerns a specific setting. The framework could be useful for other public organizations such as the police, NATO and other military organizations that have problems with interorganizational data exchange.

Reliability

To increase the reliability of the research, all steps are described that were taken during the research. The articles and the results of the interviews can all be found in the appendixes. The researcher is an employee of the MoD, but was not familiar with interoperability within the MoD prior to the research, as such limiting the researcher’s bias. By asking the same questions to all interviewees, and transcribing the interviews within 48 hours, the researcher’s bias was further reduced.

Ethical

Before the start of the interview, a letter of consent was discussed and signed by all interviewees. All interviewees agreed on the recording of the interview, after the explanation that the interview recording would be deleted after the transcription. Their rights were explained that they were free to answer the questions and could always terminate the interview. The data was anonymized within the thesis and no relation to the interviewees can be made.

5.2. Conclusions

Achieving interorganizational data exchange between heterogeneous systems, platforms and technologies is essential for organizations, such as the MoD. At the same time, the diversity of partnerships is increasing and putting additional pressure on the consistency and interpretation of data (Chituc, 2017). To be able to collaborate and exchange data between organizations in an effective manner, interoperability is needed (Daclin et al., 2016). The objective of the research is to gain insight into which interoperability challenges impede interorganizational information exchange. The research question was defined as follows.

Which interoperability challenges impede data sharing between different information systems?

Four sub-questions were identified to answer the main question:

Which interoperability challenges impeding an effective interorganizational data exchange can be found in literature?

As described in Chapter 2, the Systematic Literature Review (SLR) method was used to identify relevant articles. In total fourteen articles were the result which were used for further analysis to identify the challenges by using the Thematic Analysis Grid. The result was four distinct aspects, namely legal barriers, organizational barriers, technical barriers, and semantic and syntactical barriers. Within these four aspects another fourteen aspects were identified which were later integrated in the theoretical framework.

How can these interoperability challenges be integrated in a theoretical framework?

Six out of fourteen articles mentioned the European Interoperability Framework, which also covered all four aspects mentioned in theory. Hereby the aspects of the EIF were used to provide a structure for the development of the own framework. A theoretical framework is the result which consists of four aspects that were further elaborated by adding fourteen relevant sub-aspects identified from the relevant articles.

How can the identified interoperability challenges for interorganizational data exchange be validated with empirical information?

To validate the theoretical framework, an embedded case study was conducted within three organizations. During the empirical research, thirteen semi-structured interviews were held, each consisting of 35 questions. During these interviews, questions were put forward about each sub-aspect to gain an in-depth understanding of the topic and the reasoning behind it. The respondents also ranked each sub-aspect on three different subjects. As a result, most sub-aspects were validated.

How can the identified interoperability challenges be refined with empirical information?

During the empirical research all fourteen sub-aspects were validated. The sub-aspect language and the sub-aspect ontology were seen as least important. Suggestions for refinement were also received, such as changing the sub-aspect intellectual property into data ownership, and adding intellectual property to the description of this sub-aspect. Another suggestion was to add culture and ethics to the sub-aspect collaboration. The last suggestion was to subdivide the semantic and syntactical barriers into a new human aspect and the technical aspect.

Additional sub-aspects have been suggested such as a sub-aspect for costs and a sub-aspect for legal and regulatory barriers. The suggestions for refinements during the empirical research resulted in the final framework (Table 8). The refinements and additional sub-aspects need to be further investigated. For this reason, additional necessary research is discussed in §5.4.

5.3. Recommendations for practice

Twelve participants agreed on the question if the framework is useful. The reasons that were given are that the framework provides guidance, insight for the upper management, and allows one to prioritize what is important, because it describes the layers that are required.

The framework can be used by other public organizations such as the police, NATO and other military organizations which might experience similar problems with regards to interorganizational data exchange.

Although there is still room for refinements, the framework contains aspects which could be taken under consideration when organizations, like the MoD, want to have a better understanding of the barriers which are impeding data exchange. It ensures that all are on the same page, discuss identical aspects and speak the same language. This in turn can contribute to making better decisions which benefit interorganizational interoperability.

5.4. Recommendations for further research

The results and limitations of the case study require further research. Due to time limitations and the specific query, the snowballing method was used to enlarge the amount of articles. This resulted in articles which were used as a reference in the initial articles or which used the initial articles as a citation. Therefore, the advice is to expand the literature review to identify other relevant articles that can contribute to the research.

Although the research was performed within three different organizations, the majority of the interviews were held within the MoD and TNO, an organization which is closely related to the MoD. Broader validation of the framework is required within the MoI, other partnerships like NATO, or the EU. This will also improve the generalizability of the framework.

Because of the divergent opinions regarding the sub-aspects ontology and language further research is required. This also applies to the validation of the refinements and additional sub-aspects, such as costs and the legal and regulatory aspect, which are included in the final version of the framework.

Further research is also needed to investigate if the semantic and syntactic sub-aspects can be subdivided into a human aspect and within the technical aspect. Another suggestion is to examine how the framework can be implemented within the MoD and collaboration partners.

References

Abdeen, F. N., Fernando, T., Kulatunga, U., Hettige, S., & Ranasinghe, K. D. A. (2021). Challenges in multi-agency collaboration in disaster management: A Sri Lankan perspective. *International Journal of Disaster Risk Reduction, 62*, 102399. doi:https://doi.org/10.1016/j.ijdrr.2021.102399

Aldhaheri, S., Alghazzawi, D., Cheng, L., Barnawi, A., & Alzahrani, B. A. (2020). Artificial Immune Systems approaches to secure the internet of things: A systematic review of the literature and recommendations for future research. *Journal of Network and Computer Applications, 157*, 102537. doi:https://doi.org/10.1016/j.jnca.2020.102537

Allen, D., Karanasios, S., & Norman, A. (2013). Information Sharing and Interoperability: The Case of Major Incident Management. *European Journal of Information Systems, 23*. doi:10.1057/ejis.2013.8

Buchinger, M., Kuhn, P., Kalogeropoulos, A., & Balta, D. (2021). *Towards Interoperability of Smart City Data Platforms.* Paper presented at the Proceedings of the 54th Hawaii International Conference on System Sciences.

Camara, M., Ducq, Y., & Dupas, R. (2014). A methodology for the evaluation of interoperability improvements in inter-enterprises collaboration based on causal performance measurement models. *International Journal of Computer Integrated Manufacturing, 27*, 103-119. doi:10.1080/0951192X.2013.800235

Chen, D., Doumeingts, G., & Vernadat, F. (2008). Architectures for enterprise integration and interoperability: Past, present and future. *Computers in Industry, 59*(7), 647-659. doi:https://doi.org/10.1016/j.compind.2007.12.016

Chen, D., Vallespir, B., & Daclin, N. (2008). *An Approach for Enterprise Interoperability Measurement*.

Chituc, C.-M. (2017). *Interoperability Standards for Seamless Communication: An Analysis of Domain-Specific Initiatives*.

Daclin, N., Daclin, S., Vincent, C., & Vallespir, B. (2016). Writing and verifying interoperability requirements: Application to collaborative processes. *Computers in Industry, 82*, 1-18. doi:10.1016/j.compind.2016.04.001

European Commission. (2017). New European Interoperability Framework: Promoting seamless services and data flows for European public administrations. Retrieved from https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf

Folmer, E., Wu, H., & Bekkum, M. (2014). Data standards quality measured for achieving enterprise interoperability: the case of the SETU standard for flexible staffing. *Information Systems and e-Business Management, 12*, 517-541. doi:10.1007/s10257-014-0236-5

Grilo, A., & Jardim-Goncalves, R. (2010). Value proposition on interoperability of BIM and collaborative working environments. *Automation in Construction, 19*(5), 522-530. doi:https://doi.org/10.1016/j.autcon.2009.11.003

Jamoussi, Y., Al-Khanjari, Z., & Kraiem, N. (2017). A Guidance Based Approach for Enhancing the e-Government Interoperability. *Journal of Information and Organizational Sciences, 41*, 35-56. doi:10.31341/jios.41.1.3

Kallio, H., Pietilä, A.-M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing, 72*(12), 2954-2965. doi:https://doi.org/10.1111/jan.13031

Mallek, S., Daclin, N., & Chapurlat, V. (2012). The application of interoperability requirement specification and verification to collaborative processes in industry. *Computers in Industry, 63*(7), 643-658. doi:https://doi.org/10.1016/j.compind.2012.03.002

Panetto, H., Zdravković, M., Jardim-Goncalves, R., Romero, D., Cecil, J., & Mezgár, I. (2016). New Perspectives for the Future Interoperable Enterprise Systems. *Computers in Industry, 79*, 47-63. doi:10.1016/j.compind.2015.08.001

Rantos, K., Spyros, A., Papanikolaou, A., Kritsas, A., Ilioudis, C., & Katos, V. (2020). Interoperability Challenges in the Cybersecurity Information Sharing Ecosystem. *Computers, 9*(1). doi:10.3390/computers9010018

Rezaei, R., Chiew, T. K., & Lee, S. P. (2014). A review on E-business Interoperability Frameworks. *Journal of Systems and Software, 93*, 199-216. doi:https://doi.org/10.1016/j.jss.2014.02.004

Saunders, M., Lewis, P., Thornhill, A., & Bristow, A. (2019). Research Methods for Business Students. In (8 ed.).

Shehzad, H. M. F., Ibrahim, R. B., Yusof, A. F., Khaidzir, K. A. M., Iqbal, M., & Razzaq, S. (2021). The role of interoperability dimensions in building information modelling. *Computers in Industry, 129*, 103444. doi:https://doi.org/10.1016/j.compind.2021.103444

Vargas, A., Boza, A., & Cuenca, L. (2011). *Towards Interoperability Through Inter-Enterprise Collaboration Architectures* (Vol. 7046).

Vernadat, F. B. (2010). Technical, Semantic and Organizational Issues of Enterprise Interoperability and Networking. *IFAC Proceedings Volumes, 42*(4), 728-733. doi:https://doi.org/10.3182/20090603-3-RU-2001.0579

Wohlin, C. (2014). Guidelines for snowballing in systematic literature studies and a replication in software engineering. *ACM International Conference Proceeding Series*. doi:10.1145/2601248.2601268

Yang, T.-M., & Maxwell, T. A. (2011). Information-sharing in public organizations: A literature review of interpersonal, intra-organizational and inter-organizational success factors. *Government Information Quarterly, 28*(2), 164-175. doi:https://doi.org/10.1016/j.giq.2010.06.008

Zacharewicz, G., Diallo, S., Ducq, Y., Agostinho, C., Jardim-Goncalves, R., Bazoun, H., . . . Doumeingts, G. (2017). Model-based approaches for interoperability of next generation enterprise information systems: state of the art and future challenges. *Information Systems and e-Business Management, 15*(2), 229-256. doi:10.1007/s10257-016-0317-8

Appendix A1 Data extraction form

General information

Title of the article	
Author(s)	
Year of publication	

Relevance and review questions

Subject	**Answer (Yes/ No)**	**Argumentation**
Are the research objectives close to our own?		
Is the context like our own?		
Is this article used as a reference in other articles?		
Does the article provide guidance for future research?		
Does the article contain challenges regarding interoperability?		
Does the article refer to data exchange between organizations?		
Is the study sufficient generic?		
Is the study’s methodology sufficient?		

Appendix A2 Articles

Number	Title	Year	Cited by	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
1	Business process interoperability and collaborative performance measurement	2009	9	Yes	No			No
2	The role of interoperability dimensions in building information modelling	2021	-	Yes	Yes			Yes
3	Coordinating for Flexibility in e-Business Supply Chains	2004	44	No				No
4	The application of interoperability requirement specification and verification to collaborative processes in industry	2012	-	Yes	Yes			Yes
5	The Business Interoperability Decomposition Framework to analyse buyer-supplier dyads	2019	-	Yes	No			No
6	An agent-based service-oriented integration architecture for collaborative intelligent manufacturing	2007	14	No				No
7	Ontological modeling of electronic health information exchange	2015	-	No				No
8	A conceptual model of an interorganizational intelligent meeting-scheduler (IIMS)	2003	-	No				No
9	Design observations for interagency collaboration	2014	-	No				No
10	Defining collaborative business rules management solutions: framework and method	2014	-	Yes	No			No
11	The formation of inter-organizational information sharing networks in public	2009	-	Yes	No			No

Number	Title	Year	Cited by	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
	safety: Cartographic insights on rational choice and institutional explanations							
12	The adoption stages (Evaluation, Adoption, and Routinisation) of ERP systems with business analytics functionality in the context of farms	2009	-	No				No
13	Data standards quality measured for achieving enterprise interoperability: the case of the SETU standard for flexible staffing	2014	-	Yes	Yes			Yes
14	Collaborative Knowledge Framework for Mediation Information System Engineering	2017	-	No				No
15	Do semantic standards lack quality?: A survey among 34 semantic standards	2011	-	No				No
16	Platform-based collaboration in digital ecosystems	2019	-	Yes	No			No
17	Ambient Assisted Living Healthcare Frameworks, Platforms, Standards, and Quality Attributes	2014	30	No				No
18	Adoption of blockchain in supply chain: an analysis of influencing factors	2020	-	No				No
19	Ontology based integration of XBRL filings for financial decision making	2014	2	No				No
20	Deriving and Formalizing Requirements of Decentralized Applications for Inter-Organizational Collaborations on Blockchain	2021	-	No				No

Number	Title	Year	Cited by	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
21	On research information and classification governance in an inter-organizational context: the Flanders Research Information Space	2016	-	No				No
22	Cross-lingual thesaurus for multilingual knowledge management	2008	-	No				No
23	Explaining organizational susceptibility to coercive pressure: results from a field experiment on e-invoicing IOIS adoption	2016	-	No				No
24	Going Concerns: The Governance of Interorganizational Coordination Hubs	2012	3	Yes	No			No
25	A Network Model for Human Interoperability	2014	-	No				No
26	Interoperability of Information Systems Managed and Used by the Local Health Departments	2016	3	Yes	No			No
27	Towards the development of the framework for inter sensing enterprise architecture	2014	7	No				No
28	Interoperability Standards for Seamless Communication: An Analysis of Domain-Specific Initiatives	2016	-	Yes	Yes			Yes
29	A Workflow Interoperability Approach Based on Blockchain	2020	-	No				No
30	An ontology-based collaborative business service selection: contributing to automatic building of collaborative business process	2018	-	Yes	No			No

Number	Title	Year	Cited by	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
31	Exploring Information Security Issues in Public Sector Inter-organizational Collaboration	2011		No				No
32	Cracking the humanitarian logistic coordination challenge: lessons from the urban search and rescue community	2016	1	No				No
33	Understanding Municipal Service Integration: An Exploratory Study of 311 Contact Centers	2014	-	No				No
34	Electronic Health Record Use in an Affluent Region in India: Findings from a Survey of Chandigarh Hospitals	2017	4	No				No
35	ODP RM reflections on open service ecosystems	2013	-	No				No
36	From traditional interorganizational systems to cloud-based solutions: The impact on supply chain flexibility	2018		No				No
37	Information sharing and interoperability: the case of major incident management	2014	3	Yes	Yes			Yes
38	Why corporate groups care about company standards	2020	-	No				No
39	Developing patient portals in a fragmented healthcare system	2015	-	No				No
40	Step-Based Data Sharing and Exchange in One-of-a-Kind Product Collaborative Design for Cloud Manufacturing	2013	-	No				No
41	Progress in data interoperability to support computational toxicology and chemical safety evaluation	2019	-	Yes	No			No

Number	Title	Year	Cited by	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
42	U.S. public safety networks: Architectural patterns and performance	2013	-	No				No
43	Analysis and Comparison of Role-Based Interorganizational Workflows for a Construction Project	2019	-	No				No
44	An Evaluation of Inter-Organizational Workflow Modelling Formalisms	2004	5	No				No
45	Forming Interoperability Through Interorganizational Systems Standards	2014	1	Yes	No			No
46	Getting the Sergeants on your side: the importance of interpersonal relationships and cultural interoperability for generating interagency collaboration between nurses and the police in custody suites	2020		No				No
47	A multi-criteria approach for managing inter-enterprise collaborative relationships	2012	9	Yes	No			No
48	What motivates small businesses for collective action in smart living industry?	2015	-	No				No
49	CARTOGRAPHY ENABLING COMMUNICATION AND DECISIONMAKING IN SUSTAINABILITY ISSUES (ECONOMIC, SOCIAL, ENVIRONMENTAL) OF TRANSNATIONAL DECLARATIONS, CONVENTIONS, TREATIES, FRAMEWORKS AND DIRECTIVES	2017	-	No				No
50	Effects of interorganizational information technology networks on patient safety: a realist synthesis	2020	-	No				No

Number	Title	Year	Cited by	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
51	Through a Glass Clearly: Standards, Architecture, and Process Transparency in Global Supply Chains	2011	-	No				No
52	A framework for sharing product information across enterprises	2006	11	No				No
53	A methodology for the evaluation of interoperability improvements in inter-enterprises collaboration based on causal performance measurement models	2014	2	Yes	Yes			Yes
54	Assessment of model-based data exchange between architectural design and structural analysis	2020	-	No				No
55	An integrated chemical environment with tools for chemical safety testing	2020	-	No				No
56	Simulation of the Long-Term Effects of Decentralized and Adaptive Investments in Cross-Agency Interoperable and Standard IT Systems	2010	1	No				No
57	Creating Smart Governance: The key to radical ICT overhaul at the City of Munich	2016	-	No				No
58	Towards Interoperability through Inter-enterprise Collaboration Architectures	2011	-	Yes	Yes			Yes
59	Requirements-Driven Design of Service-Oriented Interactions	2010	-	No				No
60	Collaborative process cartography deduction based on collaborative ontology and model transformation	2016	-	No				No

Number	Title	Year	Cited by	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
61	Collaborative emergency management and national emergency management network	2010	22	No				No
62	From trading to eCommunity management: Responding to social and contractual challenges	2007	-	No				No
63	Patterns and technologies for enabling supply chain traceability through collaborative e-business	2008	15	No				No
64	On the Move to Meaningful Internet Systems 2004: OTM 2004 Workshops: OTM Confederated International Workshops and Posters, GADA, JTRES, MIOS, WORM, WOSE, PhDS, and INTEROP 2004, Agia Napa, Cyprus, October 25-29, 2004. Proceedings	2004	-	No				No
65	On the Data Interoperability Issues in SCOR-Based Supply Chains	2012	-	Yes	No			No
66	Virtual enterprise — Information system and networking solution	1999	-	No				No
67	Interoperability standards for seamless communication : an analysis of domain-specific initiatives	2016	-	Dupl.				Dupl.
68	OSABIDE IN RESIDENCES: Continuity of care, through the Integration of Systems	2016	-	No				No
69	A case study of an inter-enterprise workflow-supported supply chain management system	2005	21	No				No

Number	Title	Year	Cited by	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
70	Designing electronic health records versus total digital health systems: A systemic analysis	2009	1	No				No
71	Inter-enterprise Collaboration Management in Dynamic Business Networks	2005	-	Yes	No			No
72	A Web services and process-view combined approach for process management of collaborative product development	2009	1	No				No
73	Towards a Reference Architecture for Collaborative Work Environments	2010	-	Yes	No			No
74	InDiA: a framework for workflow interoperability support by means of multi-agent systems	2004	-	Yes	No			No
75	Inter-organizational communication networks in healthcare: centralised versus decentralised approaches	2007	-	No				No
76	Interoperability Middleware for Federated Business Services in Web-Pilarcos	2007	-	Yes	No			No
77	Distributed systems security	2018	-	No				No
78	The Evolution of Worker Connect: A Case Study of a System of Systems	2013	-	No				No
79	Improving communication resilience for effective disaster relief operations	2018	-	No				No
80	A Context-Aware Inter-organizational Collaboration Model Applied to International Trade	2011	0	Yes	No			No

Number	Title	Year	Cited by	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
81	Factors Influencing the Adoption of Health Information Standards in Health Care Organizations: A Systematic Review Based on Best Fit Framework Synthesis	2020	-	Yes	No			No
82	Next Generation Information Technologies and Systems: 5th International Workshop, NGITS 2002, Caesarea, Israel, June 24-25, 2002. Proceedings	2002	-	No				No
83	Ontology Engineering for Simulation Component Reuse	2008	-	No				No
84	A SMART groundwater portal: An OGC web services orchestration framework for hydrology to improve data access and visualisation in New Zealand	2014	8	No				No
85	Paradigm Trajectories of Building Information Modeling Practice in Project Networks	2009	25	No				No
86	Trust factors influencing the adoption of internet-based interorganizational systems	2011	-	No				No
87	Computerized Information Standards Enabling Innovation in Public Procurement of Buildings	2014	-	No				No
88	Development of collaborative transportation management framework with Web Services for TFT-LCD supply chains	2010	7	No				No
89	Bridging organizational divides in health care: an ecological view of health information exchange	2013	5	Yes	No			No

Number	Title	Year	Cited by	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
90	Interorganizational GIS: Issues and prospects	1999	-	No				No
91	Context Model for Business Context Sensitive Business Documents	2013	-	No				No
92	XML-Based Schema Definition for Support of Interorganizational Workflow	2003	7	No				No
93	A brief history of nursing informatics in the United States of America	2008	6	No				No
94	CSP-Based Verification for Web Service Orchestration and Choreography	2007	1	No				No
95	Preservation-awareness in collaborative engineering	2014	-	No				No
96	Web Services, e-Business, and the Semantic Web: CAiSE 2002 International Workshop, WES 2002, Toronto, Canada, May 27-28, 2002, Revised Papers	2002	-	No				No
97	Web Service Based Architecture for Workflow Management Systems	2004	-	No				No
98	Component Framework for Strategic Supply Network Development	2004	-	No				No
99	A quantitative analysis of product categorization standards: content, coverage, and maintenance of eCl@ss, UNSPSC, eOTD, and the RosettaNet Technical Dictionary	2007	-	No				No
100	Realizing Model Driven Security for Inter-organizational Workflows with WS-CDL and UML 2.0: Bringing Web Services, Security and UML	2005	-	No				No

Number	Title	Year	Cited by	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
101	Introduction of shared electronic records : multi-site case study using diffusion of innovation theory	2008	40	No				No
102	Inter-organizational communication networks in healthcare: centralised versus decentralised approaches	2007	-	Yes	No			No
103	Integrated Digital Health Systems Design: A Service-Oriented Soft Systems Methodology	2009	-	No				No
104	Using BPEL Process Descriptions for Building Up Strategic Models of Inter-organizational Networks	2004	-	No				No
105	Decision inertia: Deciding between least worst outcomes in emergency responses to disasters	2015	6	No				No
106	The role of trust in the governance of business process outsourcing relationships: A transaction cost economics approach	2008	-	No				No
107	Profiles for conveying the secure communication requirements of Web services	2009	-	No				No
108	Affordances in e-government	2003	-	No				No
109	Recommendations toward a human pathway-based approach to disease research	2018	3	No				No
110	From Community to Public Safety Governance in Policing and Child Protection	2008	4	No				No

Number	Title	Year	Cited by	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
111	Challenges in multi-agency collaboration in disaster management: A Sri Lankan perspective	2021	-	Yes	Yes			Yes
112	Implementation of the health and social care assessment tool: resident assessment instrument - contact assessment (interrai-ca)	2016	-	No				No
113	Web Services Won't Match the Hype	2002		No				No
114	InDiA: a framework for workflow interoperability support by means of multi-agent systems	2004	-	Dupl.				Dupl.
115	A methodology for the evaluation of interoperability improvements in inter-enterprises collaboration based on causal performance measurement models	2014	2	Dupl.				Dupl.
116	eJustice, Security and Biometrics: the EU's Proximity Paradox	2005	2	No				No
117	E-GOVERNMENT SERVICE INNOVATION IN THE SCOTTISH CRIMINAL JUSTICE INFORMATION SYSTEM	2010	2	No				No
118	From EDI to XML	2008	4	No				No
119	nD modelling: industry uptake considerations	2007	-	No				No
120	MAGIC: a geoportal for the English countryside	2005	-	No				No
121	Sicurezza Territoriale e gestione delle emergenze: soluzioni ed architetture per sistemi collaborativi	2010	-	No				No

Number	Title	Year	Cited by	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
122	Whose Border Is It, Anyway? Rethinking North America's Defenses, from Smart Borders to Smart Missiles	2003	-	No				No
123	From Community to Public Safety Governance in Policing and Child Protection	2008	4	No				No
124	Sicurezza Territoriale e gestione delle emergenze: soluzioni ed architetture per sistemi collaborativi	2010	-	No				Dupl.
125	Towards Semantic Performance Measurement Systems for Supply Chain Management	2010	-	No				No
126	H2O Metacomputing – Jini Lookup and Discovery	2005	-	No				No
127	Workflow Requirements Modelling Using XML	2002	-	No				No

Appendix A3 Selected articles

General information

Title of the article	The role of interoperability dimensions in building information modelling
Author(s)	Shehzad, H. M. F., Ibrahim, R. B., Yusof, A. F., Khaidzir, K. A. M., Iqbal, M., & Razzaq, S.
Year of publication	2021

Relevance and review questions

Subject	**Answer (Yes/ No)**	**Argumentation**
Are the research objectives close to our own?	Yes	Interoperability is assessed via the EIF framework to collaborate more effectively between different stakeholders
Is the context like our own?	Yes	
Is this article used as a reference in other articles?	Yes	
Does the article provide guidance for future research?	Yes	
Does the article contain challenges regarding interoperability?	Yes	
Does the article refer to data exchange between organizations?	Yes	
Is the study sufficient generic?	Yes	
Is the study's methodology sufficient?	Yes	

Themes	**Challenges**	**Main findings**
Legal	Regulatory support Contractual environments Insurance framework Intellectual property	Construction stakeholders are reluctant in BIM investment due to the prevailing uncertainty about return on investment and lack of data ownership. There is a need for copyright and legal laws. Existing standard contracts have limited technological support for effective collaboration, and this causes distrust and insecurity among contractors. Interoperability is about ensuring that organizations operating under different legal frameworks, policies, and strategies can work together. Legal Interoperability is concerned with the legal framework for data ownership. Intellectual property is the privilege to hold for data ownership, privacy, and copyright, and it's the primary distress among construction stakeholders, particularly for design organizations. Designers need the protection of their model and its embedded

		features while exchanging models with other stakeholders. Studies show the lack of intellectual property as a barrier to a seamless exchange of models and data to achieve Interoperability. Construction players hesitate to share their design documents with other users due to the insecurity of their rights. There is a need to ensure the intellectual property rights of all industry players' to achieve interoperability
Organizational	Personnel Organizational readiness Role of top management support Financial constraints Uncertainty	Technical persons to manage applications, staff training is required, leading to the high cost of implementations. Also, coordination among peer companies is necessary. Lack of technical support for the implementation of technology. Need for additional staff, such as interoperability managers, to manage complexity. Organizational readiness is the most critical factor to achieve organizational interoperability. Uncertainty in data and risk of an investment, security, and privacy issues.
Semantic and Syntactic	Data standards Dictionary Defining ontologies Integration of data Exchange standards Workflow mapping	Actual meaning and interpretation of the exchanged data remained unrepresented; this leads to confusion among parties. It is getting challenging to standardize all discipline's definitions. Most standards suggest using the common definition and creating data dictionaries to avoid misunderstanding problems during data transmission. Combining data from multiple sources and analyzing in a single unit and its interpretation is a time and resources consuming process that results in delays and labor costs. There is a low tendency to adopt such technologies that do not provide data integration and processing capabilities. Organizations are following different definitions of terms and concepts. It creates problems in understanding the actual meanings of the transferred data and information. For successful collaboration, consensus on standard definitions is required. Issues arising due to misunderstanding of definitions should be addressed to achieve interoperability.
Technical	Data integration Interoperability between systems Data validation Data security	Using open file formats of data communications and exchange and the use of common language to make sure effective collaboration among stakeholders. Data and information are wasted due to a lack of interoperability. Data security is discussed in studies as a major issue in the construction industry. This causes low or limited communication of data among stakeholders, leading to low Interoperability.

General information

Title of the article	The application of interoperability requirement specification and verification to collaborative processes in industry
Author(s)	Mallek, S., Daclin, N., & Chapurlat, V.
Year of publication	2012

Relevance and review questions

Subject	**Answer (Yes/ No)**	**Argumentation**
Are the research objectives close to our own?	Yes	Interoperability is becoming a crucial issue for industry, and a lack of interoperability can be seen as an important barrier to collaborative work, in both public (inter-enterprise) and private (intra-enterprise) collaborative processes.
Is the context like our own?	Yes	
Is this article used as a reference in other articles?	Yes	
Does the article provide guidance for future research?	Yes	
Does the article contain challenges regarding interoperability?	Yes	
Does the article refer to data exchange between organizations?	Yes	
Is the study sufficient generic?	Yes	
Is the study's methodology sufficient?	Yes	

Themes	**Challenge**	**Main findings**
Legal		None
Organizational	Collaboration Roles and responsibilities Governance Costs, quality, and time	A lack of interoperability can be seen as an important barrier to collaborative work, in both public (inter-enterprise) and private (intra-enterprise) collaborative processes. Prior to any effective collaboration, it is necessary to inform enterprises, which aim to work together, whether or not they would be able to interoperate. Needs: Recognized frameworks are in place to support interoperability and shared goals are recognized and roles and responsibilities are allocated as part of on-going responsibilities, however, the organizations are still distinct.

		The governance of the procurement process explicitly links the business requirements to technical architecture through project financing. Keep the performance as good as possible in terms of cost, quality (product and service) and time spent, after the partnership is over, as before it was started.
Semantic and Syntactic	Communication protocol Data exchange	A communication protocol should exist for exchanging data between participating systems. Homogenize communication independent of the form, then have a semantic understood and shared by both partners. Repetition, ambiguity, imprecision, and incoherence must be removed. Problems mainly related to the expressiveness of natural language.
Technical	Identification of connected systems Availability of resources Exploitable data	The connection systems are identified by their ability to provide an understanding of the data exchanged. A resource must be available when it is needed. Send and receive exploitable data, and be sure that they are received by the other partner during the activity.

General information

Title of the article	Data standards quality measured for achieving enterprise interoperability: the case of the SETU standard for flexible staffing
Author(s)	Folmer, E., Wu, H., & Bekkum, M.
Year of publication	2014

Relevance and review questions

Subject	Answer (Yes/ No)	Argumentation
Are the research objectives close to our own?	Yes	SETU develops and maintains standards for the exchange of electronic data
Is the context like our own?	Yes	
Is this article used as a reference in other articles?	Yes	
Does the article provide guidance for future research?	No	
Does the article contain challenges regarding interoperability?	Yes	
Does the article refer to data exchange between organizations?	Yes	
Is the study sufficient generic?	Yes	
Is the study's methodology sufficient?		

Themes	Challenge	Main findings
Legal		None
Organizational	Common standards	Inter-organizational collaboration requires systems interoperability which is not possible in the absence of common standards.
Semantic and Syntactic	Data standards Data processing	Data standards are designed to promote communication and coordination among organizations. There is hardly any research on the achievements of data standards in achieving interoperability. Data standards organizations shows that the vast majority believe that their standards can be improved, and that improvements will lead to more interoperable systems. It is remarkable to notice that there are no data standardization organizations that use aforementioned measures to improve their standards, or any other quality measurement approaches for that matter. Data standards should play an important role in achieving inter-organizational interoperability. The data gathered from an organization often contain the same characteristics and errors. This research shows that having a data standard does not necessarily mean that (technical) interoperability will be achieved.

Technical	Standards	It turns out to be difficult for implementers to fully comprehend the technics and semantics of the standard if the implementer has not participated in the development process in the SETU workgroup. There may be a mismatch between the technology used in the SETU standard and the technical knowledge and means available to the implementers.

General information

Title of the article	Interoperability Standards for Seamless Communication: An Analysis of Domain-Specific Initiatives
Author(s)	Chituc, C.-M.
Year of publication	2017

Relevance and review questions

Subject	**Answer (Yes/ No)**	**Argumentation**
Are the research objectives close to our own?	Yes	It presents a review of current domain-specific standardization initiatives towards seamless communication and discusses challenges regarding these initiatives.
Is the context like our own?	Yes	
Is this article used as a reference in other articles?	Yes	
Does the article provide guidance for future research?	Yes	
Does the article contain challenges regarding interoperability?	Yes	
Does the article refer to data exchange between organizations?	Yes	
Is the study sufficient generic?	Yes	
Is the study's methodology sufficient?	Yes	

Themes	**Challenge**	**Main findings**
Legal		None
Organizational	Focus Standards	Economic performance assessment, goals, and strategy alignment. None of the initiatives tackles business interoperability. This emphasizes the extensive focus on technical aspects. Domain-specific standardization initiatives receive little attention, although numerous advances were made.

Semantic and Syntactic	Maturity Heterogenous communication Dictionary	While several industry-specific frameworks bring promising solutions towards achieving seamless interoperability, many initiatives did not mature, requiring further developments. As collaborations are more intense in today's networked economy, achieving seamless interoperability among heterogeneous communication systems is crucial. Information exchanged by heterogeneous distributed systems is meaningful and all the communicating parts interpret it in the same way. Semantic interoperability is ensured by a domain-specific dictionary/ vocabulary, and all the initiatives analyzed address it.
Technical	Security standards Interoperability between communication systems	The technical interoperability concerns issues related to e-communication, e.g., interfaces, ICT platforms, security standards, messaging service. The big challenge is cross-industry seamless interoperability. As it is not realistic to consider possible the merge of all standards and general acceptance, it is important to ensure a certain level of compliance between different standardization initiatives towards attaining seamless interoperability between communication systems built following the specifications of these standards.

General information

Title of the article	Information sharing and interoperability: the case of major incident management
Author(s)	Allen, D., Karanasios, S., & Norman, A.
Year of publication	2013

Relevance and review questions

Subject	Answer (Yes/ No)	Argumentation
Are the research objectives close to our own?	Yes	This paper illuminates the technological and organizational issues organizations face concerning information sharing and interoperability
Is the context like our own?	Yes	
Is this article used as a reference in other articles?	Yes	
Does the article provide guidance for future research?	No	
Does the article contain challenges regarding interoperability?	Yes	
Does the article refer to data exchange between organizations?	Yes	
Is the study sufficient generic?	Yes	
Is the study’s methodology sufficient?	Yes	

Themes	Challenge	Main findings
Legal	Information sharing Accessibility Privacy Knowledge	Interoperability and information sharing across agencies (and borders) remain problematic and should be framed by a range of non-technical issues including legal, political and cultural aspects. Organizational issues around privacy and security and about what could be legally shared. Even the most sophisticated interoperability solution cannot overcome privacy barriers.
Organizational	Information sharing Costs Culture/ environment/ command structures Collaboration Training	For many private and public sector organizations information sharing has emerged as a major concern. Even though interoperability might be in the common interest of all public safety organizations, individually they have little incentive to absorb the costs of achieving it; and as no one in the group will react if no other agency makes a contribution, there is little action ‘it’s not a technology issue, it’s a process issue, people are not doing what they should, rather they are doing what they can’. Concentrate on ‘their’ sources of information and ‘their’ priorities, rather

	Processes/ procedures/ policies Norms/ rules Priorities Communication Irreversibility	than the overarching shared object. Services had a common object (management of the incident) they typically operate in an insular manner. Most challenging issues were not in the technical domain, but people issues. Interoperability is about what processes are people using and establishing the use of these processes through training and culture change. While strong norms and rules are essential to management of the bureaucratic form, they create a barrier to interaction and information exchange and make the creation of a common operational picture difficult. One organizational factor emphasized was interoperability surrounding classified data. Again, this is not a technical barrier but one of establishing processes and procedures for efficiently achieving the shared object. Challenges are things like policy and procedures about what information we can and should share, and an absence of a policy that defines that we need to share this information, about how do we go about doing. For responders in-situ often there is uncertainty concerning what information can be shared and what types of information is useful to others and vice-versa. Allowing different norms, rules, and approaches. Individual processes and rules and norms, bound each agency and were not necessarily congruent with other agencies. Each agency has different ways of working, doing their particular role without thinking about other emergency services. Individual agencies also have different priorities and absorb/react to different environmental cues, suggesting a bias in adopting a shared objective approach. Failure to communicate and share information led to loss of life, suffering and damage to property. Irreversibility-problem, resources are committed in a particular direction because of previous investments, which are problematic to reverse. The lack of communication between organizations at the start of an incident can also be a part of the genesis of a more holistic problem as it leads to a lack of a comprehensive understanding of the nature of the incident. This further illuminates the narrow frames that the individual agencies work within, and the lack of consideration given to the information and communication that may be of use between agencies. Where interoperability was referred to, it was mentioned in relation to communication between the strategic levels of the services to share information gathered from their respective organizations and coordinate activities. One thing you tend to notice about large public organizations is that processes become embedded in the organization culture and it is very difficult to change that.
Semantic and Syntactic	Language Terminology Information sharing Tools	A further issue raised was the use of language and terminologies (for instance, in Europe there are 23 official languages); that is if emergency workers do not know the common language, then it is impossible to communicate with one another as each is using different tools to achieve the object. While the tools used are similar, information sharing remains problematic; the key issue here is how

		and when the tools are used. Different services use different non-material tools leading to problems with semantic interoperability.
Technical	Silo's Technical standards Security Legacy systems ICT	The technology structures deployed often reinforce this silo approach. The difficulty of allocating different frequency/ transmission standards to individual public safety agencies; information-sharing security concerns; the dependence on legacy systems; the complication of managing systems across borders; the tailoring of systems to the specific requirement of the organization with little consideration for vertical and horizontal integration across organizations. Technical issues and challenges surrounding the development of ICT systems.

General information

Title of the article	A methodology for the evaluation of interoperability improvements in inter-enterprises collaboration based on causal performance measurement models
Author(s)	Camara, M., Ducq, Y., & Dupas, R.
Year of publication	2014

Relevance and review questions

Subject	**Answer (Yes/ No)**	**Argumentation**
Are the research objectives close to our own?	Yes	The article proposes a framework and methodology to evaluate and improve the interoperability for partners of an inter-enterprises collaboration
Is the context like our own?	Yes	
Is this article used as a reference in other articles?	Yes	
Does the article provide guidance for future research?	Yes	
Does the article contain challenges regarding interoperability?	Yes	
Does the article refer to data exchange between organizations?	Yes	
Is the study sufficient generic?	Yes	
Is the study's methodology sufficient?	Yes	

Themes	**Challenge**	**Main findings**
Legal		None
Organizational	Collaboration Social	Difficulties in using approaches in the literature to assess the contribution of interoperability to the strategy of the collaborating companies are present because these approaches do not take into account the relationships between the enterprise objectives and interoperability.
Semantic and Syntactic	Ontologies	Ontologies to address semantic challenges in the field of supply chain interoperability.

Technical	Information sharing	Interoperability barriers obstruct the sharing of information between systems and prevent the systems from exchanging services. Interoperability solutions remove these barriers at a specific enterprise level (concerns) through a specific interoperability approach.

General information

Title of the article	Towards Interoperability through Inter-enterprise Collaboration Architectures
Author(s)	Vargas, A., Boza, A., & Cuenca, L.
Year of publication	2011

Relevance and review questions

Subject	**Answer (Yes/ No)**	**Argumentation**
Are the research objectives close to our own?	Yes	This article seeks to analyze, link and synthesize the researches that has addressed the disciplines of enterprise architecture and business collaboration
Is the context like our own?	Yes	
Is this article used as a reference in other articles?	Yes	
Does the article provide guidance for future research?	Yes	
Does the article contain challenges regarding interoperability?	Yes	
Does the article refer to data exchange between organizations?	Yes	Information exchange
Is the study sufficient generic?	Yes	
Is the study's methodology sufficient?	Yes	

Themes	**Challenge**	**Main findings**
Legal		None
Organizational	Collaboration Standards Tools	Methodological proposals are mostly directed and oriented to individual enterprises. Researches are not taking into account the growing and rapidly evolving business collaboration environments where two or more companies involved in one or more supply chains make collaborative supply networks.

	Synchronization of processes Integration of key elements	Necessary to use tools that allow the visualization of the collaborative process and ensure a common understanding of collaborative processes between all companies and individuals involved in the process of joint business. The operation and organization of these collaborative networks should be structured and modeled through collaboration architectures designed with the purpose of supporting collaborative processes and their integration with information systems of partners involved in the collaboration. Interoperability between the companies that establish collaborative agreements is possible through the use of enterprise architectures that allow standardization and synchronization of joint processes and the integration of the key elements of global business.
Semantic and Syntactic	Language	Different modeling languages, makes it difficult to realize interoperability between different network architectures. The existence of such different modeling languages makes it much more complicated to implement the interoperability of the various enterprise networks.
Technical	Infrastructure	Interstate/international organizations relying on different infrastructure and thus technical details may become the stumbling block if not given sufficient prior attention. This may relate to both software and hardware aspects.

General information

Title of the article	Challenges in multi-agency collaboration in disaster management: A Sri Lankan perspective
Author(s)	Abdeen, F. N., Fernando, T., Kulatunga, U., Hettige, S., & Arjuna Ranasinghe, K. D.
Year of publication	2021

Relevance and review questions

Subject	**Answer (Yes/ No)**	**Argumentation**
Are the research objectives close to our own?	Yes	This study investigates the current challenges prevailing in relation to multi-agency collaboration during disaster management and at the strategies that should be implemented in order to overcome such challenges.
Is the context like our own?	Yes	
Is this article used as a reference in other articles?	Yes	
Does the article provide guidance for future research?	Yes	
Does the article contain challenges regarding interoperability?	Yes	
Does the article refer to data exchange between organizations?	Yes	
Is the study sufficient generic?	Yes	
Is the study's methodology sufficient?	Yes	

Themes	**Challenge**	**Main findings**
Legal		None
Organizational	Collaboration Communication Competition Coordination Culture Environmental Human capital	These reasons result in poor collaboration among agencies, leading to unnecessary casualties and damage to the environment and economies. No agreed policies and platforms for sharing their information with other agencies to develop a common understanding of risks and to prepare and respond better to disasters in a collaborative manner. Poor communication can hinder the overall effectiveness of the collaboration process. Lack of well-defined guidelines for sharing data among the agencies to establish a common view. Collaboration between authorities is often challenging due to various reasons, namely difference of cultures, processes and systems, different motivations, incentives and competition for limited resources, and a lack of coordination

	Information sharing Guidelines Social Standards Political Policies/ Procedures Training	between the agencies involved. Challenges emerging due to inefficiencies in communication can stall the collaboration process. A lack of communication between all the agencies, has been identified as a reason for ineffective response to disasters. Despite the critical importance of communication across agencies, the issue of interoperability in communication continues to persist between agencies. Political rivalries between jurisdictions have been identified as a fact that hinders inter-governmental cooperation. Problems due to incompatible procedures, processes, policies and a lack of understanding of concepts. Non-existence of a well-defined guidelines on data sharing and lack of a collaboration platform for sharing data were identified as information related challenges. Lack of formal and systematic coordination procedures; a lack of interorganizational interdependencies and collaboration procedures and no long-term plans or policies for their incorporation; a lack of policies on data transformation and a lack of international collaboration that can bring innovation and support. Lack of human capital and training. Lack of government guidelines or standards for relief-assistance;
Semantic and Syntactic	Inconsistent Misinterpretation Conflicting Inaccurate Incomplete Unreliable Data sharing protocol	Available inter-organizational information is inconsistent, implying that agencies have a low level of appreciation of the value of inter-organizational information sharing. Misinterpretation of information was identified, conflicting, inaccurate, unreliable, or incomplete information. a lack of data sharing protocols and platforms; data and information gaps
Technical	Lack of technology Low connectivity Resources Infrastructure	Communication was considered as the dominant challenge due to the lack of technology. Lack of a collaboration platform, low connectivity Platform for multi-agency collaboration for seamless exchange of information Data sharing across entities to overcome the challenges relating to poor communication. Lack of advanced technological infrastructure. Unavailability of a proper coordinated system for providing updated information during emergency situations.

Appendix A4 Articles backward snowballing

Additional articles found by using backward snowballing method

References from “The role of interoperability dimensions in building information modelling”.

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
1	Barriers to implementation of building information modeling (BIM) to the construction industry: a review	2018	No				No
2	A comprehensive identification and categorisation of drivers, factors, and determinants for BIM adoption: a systematic literature review	2017	No				No
3	Driving lean and green project outcomes using BIM: a qualitative comparative analysis	2017	No				No
4	Building information modelling in Denmark and Iceland	2013	No				No
5	Digital technologies in Facility Management – the state of practice and research challenges	2017	No				No
6	Interoperability specification development for integrated BIM use in performance based design	2018	Yes	No			No
7	New York District US Army Corp. Of Engineers Official Manual for Building Information Modeling Projects	2009	No				No

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
8	Building information modeling (BIM): trends, benefits, risks, and challenges for the AEC industry	2011	No				No
9	Information systems theory	2012	No				No
10	Barriers and facilitators for BIM use among Swedish medium-sized contractors -' we wait until someone tells us to use it	2017	No				No
11	Understanding BIM adoption in the AEC industry: the case of Jordan	2017	No				No
12	LACCD Building Information Modeling Standards	2017	No				No
13	BIM Particular Conditions	2015	No				No
14	Technical Vision - buildingSMART	2016	No				No
15	BIM Guide Project, BuildingSmart	2015	No				No
16	NBIMS-US-3: 5.2 minimum BIM	2015	No				No
17	University of Southern California building Information Modeling (BIM) Guidelines Version 1.6 for Design Bid Build Contracts	20121	No				No
18	AEC (CAN) BIM Protocol	2014	No				No
19	Practices and effectiveness of building information modelling in construction projects in China	2015	No				No
20	Enterprise interoperability framework	2006	Yes	No			No
21	Bridging BIM and Building: from literature review to an integrated conceptual framework	2015	No				No

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
22	The outlook of building information modeling for sustainable development heap-yih Chong1 and Xiangyu Wang2,3 1School	2015	No				No
23	Dimensions of interoperability in the AEC industry	2014	Yes	No			No
24	Data interoperability assessment though IFC for BIM in structural design – a five-year gap analysis	2017	Yes	No			No
25	BIM implementation throughout the UK construction project lifecycle: an analysis	2013	No				No
26	A survey of current status of and perceived changes required for BIM adoption in the UK	2015	No				No
27	Confirmatory strategic information technology implementation for building information modelling adoption model	2016	No				No
28	Current Legal Problems and Risks With BIM in the Swedish AEC Industry	2018	No				No
29	BIM awareness and acceptance by architecture students in Asia	2016	No				No
30	New European interoperability framework	2017	Yes	No			Background
31	An Interoperability Framework for Pan-European E-Government Services (PEGS)	2004	Yes	No			No

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
32	A critical review of legal issues and solutions associated with building information modelling	2018	No				No
33	Organizational Adoption Models for Early ASP Technology Stages	2005	No				No
34	Georgia Tech BIM Requirements & Guidelines for Architects, Engineers and Contractors	2016	No				No
35	Value proposition on interoperability of BIM and collaborative working environments	2010	Yes	Yes	Yes	Yes	Yes
36	A conceptual framework to support solar PV simulation using an open-BIM data exchange standard	2014	No				No
37	BIM Legal and Insurance Issues Brian’ S’ Laws’ of Risk Allocation	2015	No				No
38	BIM adoption across the Chinese AEC industries: an extended BIM adoption model	2018	No				No
39	Three approaches to qualitative content analysis	2005	No				No
40	Improving interoperability between architectural and structural design models: an industry foundation classes-based approach with web-based tools	2016	Yes	No			No
41	Pseudo-genetic model optimization for rehabilitation of urban storm-water drainage networks	2017	No				No

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
42	Indiana University Building Information Modeling (BIM) Guidelines and Standards for Architects	2012	No				No
43	Building Information Models – Information Delivery Manual – Part 1: Methodology and Format	2016	No				No
44	BIM investment, returns, and risks in China's AEC industries	2017	No				No
45	Energy modeling system using building information modeling open standards	2013	No				No
46	Integration of ifc objects and facility management work information using Semantic Web	2018	No				No
47	Validations for ensuring the interoperability of data exchange of a building information model	2015	Yes	No			No
48	The building information modeling and its use for data transformation in the structural design stage	2016	No				No
49	Building information modelling and standardised construction contracts: a content analysis of the GC21 contract.	2015	No				No
50	The integration of BIM in later project life cycle phases in unprepared environment from FM perspective	2016	No				No

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
51	Qualitative content analysis	2000	No				No
52	BIM technology acceptance among reinforcement workers - the case of Oslo airport's terminal 2	2016	No				No
53	The levels of conceptual interoperability model	2003	Yes	No			No
54	Interoperability assessment for building information modelling	2015	Yes	No			No
55	Data interoperability assessment though IFC for BIM in structural design–a five year gap analysis	2017	Yes	No			No
56	National BIM Standard - United States TM Version 2	2012	No				No
57	NATSPEC National BIM Guide	2016	No				No
58	A shared ontology approach to semantic representation of BIM data	2017	No				No
59	GSA Building Information Modeling Guide Series 01 – Overview	2007	No				No
60	Barriers to the integration of BIM and sustainability practices in construction projects: a delphi survey of international experts	2018	No				No
61	Where the gaps lie: ten years of research into collaboration on BIM-Enabled construction projects	2017	No				No
62	An updated and streamlined technology readiness index: TRI 2.0	2015	No				No
63	Semantic web technologies in AEC industry: a literature overview	2017	No				No

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
64	Planning and developing facility management-enabled building information model (FM-enabled BIM)	2018	No				No
65	Proposal for an open data model Schema for precinct-scale information management	2017	No				No
66	Building Information Modeling (BIM) partnering framework for public construction projects	2013	No				No
67	Which industries are the most digital and why	2016	No				No
68	Exploring how information exchanges can be enhanced through Cloud BIM	2012	No				No
69	A governance approach for bim management across lifecycle and supply chains using mixed-modes of information delivery	2013	No				No
70	Diffusion of Innovations, fifth	2003	No				No
71	Diffusion of Innovations, 4th ed	1995	No				No
72	A review of building information modeling protocols, guides and standards for large construction clients	2016	No				No
73	The Dynamics of BIM Adoption : A Mixed Methods Study of BIM as an Innovation within the United Kingdom Construction Industry	2015	No				No
74	Common BIM Requirements	2012	No				No

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
75	Building information modeling: factors affecting the adoption in the AEC industry	2019	No				No
76	Recent developments of BIM adoption based on categorization, identification and factors: a systematic literature review	2020	No				No
77	The adoption of building information modeling in the design organization: an empirical study of architects in Korean design firms	2014	No				No
78	What drives the adoption of building information modeling in design organizations? An empirical investigation of the antecedents affecting architects' behavioral intentions	2015	No				No
79	STATSBYGG BIM-MANUAL 2.0	2019	No				No
80	BIM Maturity Matrix - Organizational Discovery	2015	No				No
81	Building Information Modeling (BIM) Project Delivery Standards	2019	No				No
82	Interoperability matter: levels of data sharing, starting from a 3D information modelling. International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences	2017	Yes	No			No
83	BIM Manual V 2.2	2017	No				No

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
84	The information systems interoperability maturity model (ISIMM): towards standardizing technical interoperability and assessment within government	2012	Yes	No			No
85	An ontology-based analysis of the industry foundation class schema for building information model exchanges	2015	No				No
86	Analysis of the adoption rate of building information modeling [BIM] and its return on investment[ROI]	2017	No				No
87	Digitisation in facilities management: a literature review and future research directions	2018	No				No
88	Users-orientated evaluation of building information model in the Chinese construction industry	2014	No				No
89	BIM and sustainability education: incorporating instructional needs into curriculum planning in CEM programs accredited by ACCE	2016	No				No
90	A multi-server information-sharing environment for cross-party collaboration on a private cloud	2017	No				No

References from “The application of interoperability requirement specification and verification to collaborative processes in industry”.

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
1	Aide a` la conception de Syste`me d'Information Collaboratif: support de l'interope´ rabilite´ des entreprises	2007	No				No
2	Dussart, Syste`me d'Information Inter-Organizationnel, Rapport Bourgogne, Groupe CIRANO	2002	No				No
3	Inte´gration des approches SOA et oriente´e objet pour mode´liser une orchestration cohe´ rente de services	20100	No				No
4	Advanced automation technologies and their applications, Part 1: Framework for enterprise interoperability	2009	Yes				No access
5	IDEAS Project Deliverables, «WP1-WP7»	2003	No				No
6	INTEROP: Enterprise Interoperability-Framework and knowledge corpus – Final report, INTEROP NoE, FP6	2007	Yes				No access
7	Guidelines and best practices for applying the ATHENA interoperability framework to support SME participation in digital ecosystems	2007	Yes				No access
8	C4ISR Architecture Working Group Levels of Information Systems Interoperability (LISI)	1998	Yes				No access
9	The Levels of Conceptual Interoperability Model	2003	Dupl.				Dupl.
10	Organizational Interoperability Maturity Model for C2, Proc. of Command and Control Research & Techn. Symposium	1999	Yes	No			No

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
11	Methodology for enterprise interoperability, in: 17th IFAC World Congress (IFAC'08)	2008	Yes	No			No
12	Interoperability measurement, PhD Thesis, Department of the Air Force Air University, Air Force Institute of Technology	2008	Yes	No			No
13	Business Process Modeling Notation, V1.2	2009	No				No
14	Interoperability maturity model	2007	Yes	No			No
15	System Engineering (SE) Handbook Working Group, System Engineering Handbook	2007	No				No
16	IEEE Standards 15288.2008 – Systems engineering – System life cycle processes (2nd edition)	2008	No				No
17	A day in the life of a verification requirement, in: U.S. Air Force T&E Days	2008	No				No
18	Measuring systems interoperability: challenges and opportunities	2004	Yes	No			No
19	Expanding our horizons in verification, validation and accreditation research and practice	2002	No				No
20	Model Checking	1999	No				No
21	Systems and Software verification: Model Checking Techniques and Tools	2001	No				No
22	A Tutorial on Uppaal, Department of Computer Science	2004	No				No

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
23	Enterprise model verification and validation: an approach	2003	No				No
24	Conceptual graphs, IBM Journal of Research and Development	1976	No				No
25	Interoperability in collaborative processes: requirements characterisation and proof approach	2009	Yes	No			No
26	Version 5.2.0, Reference Manual	2009	No				No
27	Specification of the ATL Virtual Machine	2005	No				No
28	Model-checking in dense real-time, Information and Computation	1993	No				No
29	Using timed model checking for verifying workflows	2005	No				No
30	System interoperability analysis by mixing system modeling and MAS: an approach, agent-based, technologies and applications for enterprise interoperability (ATOP)	2009	Yes	No			No

References from “Data standards quality measured for achieving enterprise interoperability: the case of the SETU standard for flexible staffing”.

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
1	Pragmatic interoperability: a systematic review of published definitions	2010	Yes	No			No
2	Semantic technologies and e-business. In: Kajan E (ed) Electronic business interoperability: concepts, opportunities and challenges	2011	Yes	No			No
3	Standards development and diffusion: a case study of RosettaNet	2007	No				No
4	Interoperability costs in the US automotive supply chain	2002	No				No
5	Use profile management for standard conformant customisation	2010	No				No
6	Standard for eBusiness in SMEs networks: the increasing role of customization rules and conformance testing tools to achieve interoperability	2011	Yes	No			No
7	Demystifying integration	2004	No				No
8	Fundamentals of standards and standardization	2007	No				No
9	The specification, engineering, and measurement of information systems quality	1992	No				No
10	Collaborative business process support in eHealth: integrating IHE	2008	No				No

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
	profiles through ebXML business process specification language						
11	European interoperability framework for pan-european eGovernment services	2004	Yes	No			Background
12	Data quality requirements of collaborative business processes	2012	No				No
13	Quality of semantic standards	2012	No				No
14	Top IS research on quality of transaction standards, a structured literature review to identify a research gap	2009	No				No
15	Do semantic standards lack quality? A survey among 34 semantic standards	2011	No				No
16	Economic impact assessment of the international standard for the exchange of product model data (STEP) in transportation equipment industries	2002	No				No
17	Social shaping and standardization: a case study from auto industry. In: Paper presented at the 38th Hawaii International Conference on System Sciences (HICSS)	2005	No				No
18	An empirical evaluation of the quality of interoperability specifications for the web Software Engineering and Advanced Applications (SEAA)	2010	No				No

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
19	Information quality benchmarks: product and service performance	2002	No				No
20	ISO standards for interoperability: a comparison	2006	Yes	No			No
21	Three dimensions of organizational interoperability	2009	Yes	No			No
22	Development life cycle for semantically coherent data exchange specification	2008	No				No
23	Preface to the focus theme section: 'business interoperability' business interoperability research: present achievements and upcoming challenges	2007	Yes	No			No
24	Industry-wide information systems standardization as collective action: the case of US residential mortgage industry	2006	No				No
25	Factors in software quality	1977	No				No
26	Analysis and metrics of XML schema	2004	No				No
27	Interorganizational system standards development in vertical industries	2005	No				No
28	A review of XML-based supply chain integration	2004	No				No
29	A characteristics framework for semantic information systems standards	2011	No				No
30	Standards: the language for success	1993	No				No

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
31	Business process requirements, modeling technique and standard: how to identify interoperability gaps on a process level	2006	Yes	No			No
32	Cooperative advantage and vertical information system standards: an automotive supply chain case Study	2011	No				No
33	Promoting e-business through vertical IS standards: lessons from the US home mortgage industry	2007	No				No
34	A case study of the adoption and implementation of STEP	2008	No				No
35	Achieving technical interoperability—the ETSI approach	2006	Yes	No			No
36	Luhmann ontmoet ''The Matrix''	2009	No				No
37	Anchoring data quality dimensions in ontological foundations	1996	No				No
38	Towards Quality of Data Standards: Empirical Findings from XBRL	2009	No				No
39	Quality of XBRL US GAAP Taxonomy: empirical evaluation using SEC filings	2010	No				No
40	Quality of data standards: framework and illustration using XBRL taxonomy and instances	2011	No				No

References from “Interoperability Standards for Seamless Communication: An Analysis of Domain-Specific Initiatives”.

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
1	A Compilation of IEEE Standard Computer Glossaries	1990	No				No
2	Interoperability in collaborative networks: independent and industry-specific initiatives - the case of the footwear industry	2008	Yes	No			No
3	North Atlantic Treaty Organization Standardization Agreement	n.d.	No				No
4	The biggest issue: interoperability vs. integration	2001	Yes				No access
5	New perspectives for the future interoperable systems	2016	Yes	Yes	Yes	Yes	Yes
6	XML and industrial standards for electronic commerce	2000	No				No
7	A review of XML-based supply-chain integration	2004	No				No
8	XML-based e-business frameworks and standardization	2006	No				No
9	A review of e-business interoperability frameworks	2014	Yes	Yes	Yes	Yes	Yes
10	An empirical framework for evaluating interoperability of data exchange standards based on their actual usage	2015	Yes	No			No
11	Lessons learned from the implementation of remote control for the interoperability standard ISO/IEEE 11073-20601 in a standard weighing scale	2016	Yes	No			No

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
12	Integrating HL7 RIM and ontology for unified knowledge and data representation in clinical decision support systems	2016	No				No
13	The Authoritative Dictionary of IEEE Standards Terms	2000	No				No
14	Backgrounder interoperability for joint operations	2006	Yes	Yes	Yes	No	No
15	Systematisation of interoperability body of knowledge: the foundation for Enterprise Interoperability as a science	2013	Yes	No			No
16	An approach for testing interoperability and robustness of real-time embedded software	2012	Yes	No			No
17	Enterprise interoperability framework	2006	Yes	No			Background
18	An analysis of basic interoperability related terms, system of interoperability types	2002	Yes	Yes	Yes	No	No
19	A standardized language for specifying and exchanging information	2005	No				No
20	Unmanned aerial vehicle domain: areas of research	2015	No				No
21	CoNSIS: demonstration of SOA interoperability in heterogeneous tactical networks	2012	Yes	Yes	Yes	No	No
22	Implementing healthcare interoperability utilizing SOA and data interchange agent	2015	Yes	No			No

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
23	Levels of Information Systems Interoperability	1998	Yes	No			No

References from “Information sharing and interoperability: the case of major incident management”.

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
1	Critical factors and patterns in the innovation process	2011	No				No
2	Working with activity theory: context, technology, and information behavior.	2011	No				No
3	How should technology-mediated organizational change be explained? A comparison of the contributions of critical realism and activity theory	2013	No				No
4	Trust, power and interorganizational information systems: the case of the electronic trading community translease	2000	No				No
5	Action, interaction and the role of ambiguity in the introduction of mobile information systems in a UK police force	2004	No				No
6	Information systems as technological innovation	2000	No				No
7	Report of the workshop on ‘interoperable communications for safety and security	2010	Yes	No			No

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
8	Inter-organisational information sharing systems	1982	No				No
9	Challenges and obstacles in sharing and coordinating information during multi-agency disaster response: propositions from field exercises	2010	No				No
10	The incident command system: high reliability organizing for complex and volatile task environments	2001	No				No
11	Organizing emergent safety organizations. The travelling of the concept 'netcentric work' in the Dutch safety sector	2010	No				No
12	Sending out an S.O.S.: public safety communications interoperability as a collective action problem	2007	Yes	No			No
13	Emergency response information system interoperability: development of chemical incident response data model	2008	Yes	No			No
14	Case study in disaster relief: a descriptive analysis of agency partnerships in the aftermath of the January 12th, 2010 Haitian earthquake	2012	No				No
15	Information technology implementation research: a technological diffusion approach	1990	No				No
16	Perceived usefulness, perceived ease of use, and user acceptance of information technology	1989	No				No

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
17	IOS resources, electronic cooperation and performance: a conceptual model	2011	No				No
18	European Interoperability Framework (EIF) for European public services: Annex 2	2010a	Yes	No			No
19	The European eGovernment Action Plan 2011–2015: Harnessing ICT to promote smart, sustainable & innovative Government	2010b	No				No
20	European interoperability framework for pan-European e-government services	2004	Dupl.				Dupl.
21	When the center does not hold: the importance of knotworking	1999a	No				No
22	Perspectives on Activity Theory	1999b	No				No
23	Information sharing and trust during major incidents: findings from the oil industry	2012	No				No
24	More than meets the eye? Intuition and analysis revisited	2009	No				No
25	When is an information infrastructure? Investigating the emergence of public sector information infrastructures	2010	No				No
26	Dialectical Logic: Essays on its Theory and History	1977	No				No
27	Applications of global information technology: key issues for management	1991	No				No
28	New and emergent ICTs and climate change in developing countries	2011	No				No

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
29	ICT and development in the context of Chernobyl nuclear power plant closure	2013	No				No
30	In Advances in Man-machine Systems Research	1989	No				No
31	An overview of naturalistic decision making applications	1997	No				No
32	Naturalistic decision making. Human Factors: The Journal of the Human Factors and Ergonomics Society	2008	No				No
33	Group value and intention to use: a study of multi-agency disaster management information systems for public safety	2011	No				No
34	Major incident: procedure manual. Report-London Emergency Services Liaison Panel	2007	No				No
35	Communication and information sharing at VA facilities during the 2009 novel h1n1 influenza pandemic	2012	No				No
36	Report of the 7 July review committee	2006	No				No
37	Inter-organizational information systems adoption – a configuration analysis approach	2011	No				No
38	Digital cross-organizational collaboration: a metatriangulation review	2010	No				No
39	Communication challenges in emergency response	2007	No				No

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
40	The politics of public safety communication interoperability regulation	2005	Yes	No			No
41	Multi-agency operations: cooperation during flooding	2012	No				No
42	Information sharing during multi-agency major incidents	2011	No				No
43	9/11 commission report. The National Commission on Terrorist Attacks upon the United States	2004	No				No
44	Decision-making in high-velocity environments: the importance of guiding principles	2005	No				No
45	The Logic of Collective Action: Public Goods and the Theory of Groups	1965	No				No
46	Interorganizational information integration: a key enabler for digital government	2007	No				No
47	Information systems interoperability: what lies beneath?	2004	Yes	No			No
48	Cognitive radio emergency networks – requirements and design	2005	No				No
49	Learning Lessons from the 2007 Floods	2008	No				No
50	Interorganisational communication in civil–military cooperation during complex emergencies: a case study in Afghanistan	2009	No				No
51	Diffusion of Innovations	2003	No				No

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
52	A motivational model for technology-supported cross-organizational and cross-border collaboration	2010	No				No
53	Safecom: the road to interoperability	2006	Yes	No			No
54	A scenario-based study on information flow and collaboration patterns in disaster management	2009	No				No
55	Process integration, information sharing, and system interoperation in government: a comparative case analysis	2012	Yes	No			No
56	Network: Theorizing Knowledge Work in Telecommunications	2008	No				No
57	Interoperability: stop blaming the radio	2007	Yes	No			No
58	A study of the interaction between information technology and society: an illustration of combined qualitative research methods	1991	No				No
59	User acceptance of information technology: toward a unified view	2003	No				No
60	A multi-criteria approach for managing inter-enterprise collaborative relationships	2012	No				No
61	Mind in Society: The Development of Higher Psychological Processes	1978	No				No
62	A review of sociotechnical systems theory: a classic concept for new command and control paradigms	2008	No				No
63	Basic Content Analysis	1985	No				No

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
64	The collapse of sense-making in organizations: the Mann Gulch disaster	1993	No				No
65	Information-sharing in public organizations: a literature review of interpersonal, intra-organizational and inter-organizational success factors	2011	Yes	Yes	Yes	Yes	Yes

References from “A methodology for the evaluation of interoperability improvements in inter-enterprises collaboration based on causal performance measurement models”.

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
1	Description and Access Task Force on Metadata	2010	No				No
2	The ATHENA interoperability framework	2007	Yes	No			No
3	Contribution a la caracterisation et a l‘evaluation de l‘interoperabilite pour les entreprises collaboratives	2006	No				No
4	Business Process Management with ADONIS	2011	No				No
5	Deal: A Package for Learning Bayesian Networks	2003	No				No
6	Graphical Means for Inspecting Qualitative Models of System Behaviour	2010	No				No
7	Towards a Structured Approach to Building Qualitative Reasoning Models and Simulations	2008	No				No

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
8	Dealing with Dilemmas: Where Business Analytics Fall Short	2010	No				No
9	Using Organizational Analysis and IDEFO for Enterprise Modelling in SMEs	1998	No				No
10	Performance Measurement Systems for Virtual Enterprise Integration	2004	No				No
11	Architectures for Enterprise Integration and Interoperability: Past, Present and Future	2008	Yes	No			No
12	An Approach for Enterprise Interoperability Measurement	2008	Yes	No			No
13	Applied Multiple Regression/Correlation Analysis for the Behavioral Sciences	2003	No				No
14	System Engineering Fundamentals	2001	No				No
15	Production Management and Enterprise Modelling	2000	No				No
16	GEM: GRAI Evolution Method: A Case Study	2001	No				No
17	New Definition of Performance Indicators for Interop NoE Deliverable	2004	No				No
18	How to Measure Interoperability: Concept and Approach	2008	Yes	No			No
19	Asymptotics of Cross-Validated Risk Estimation in Estimator Selection and Performance Assessment	2005	No				No
20	Linking Actions to Profits in Strategic Decision Making	2001	No				No
21	A Survey on Interoperability Measurement	2007a	Yes	Yes	Yes	No	No

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
22	The Interoperability Score	2007b	Yes	No			No
23	Using IIAM to Assess Interoperability Investments: A Case Study	2007	Yes				No access
24	Reengineering the Corporation: A Manifesto for Business Revolution	1993	No				No
25	Qualitative Reasoning in Business, Finance, and Economics: Introduction	1995	No				No
26	Data Mining: Concepts and Techniques	2001	No				No
27	Learning Bayesian Networks: The Combination of Knowledge and Statistical Data	1995	No				No
28	Simulation in Financial Services with the Business Process Management System ADONIS	1997	No				No
29	A Set Theoretic Foundation of Qualitative Reasoning and Its Application to the Modeling of Economics and Business Management Problems	2003	No				No
30	A Model for Assessing the Performance of Interoperable, Complex Systems	2006	Yes				No access
31	Rapports D'analyse Dynamique	2011	No				No
32	European Interoperability Framework for pan-European eGovernment Services	2004	Dupl.				Dupl.
33	The Balanced Scorecard: Translating Strategy Into Action	1996	No				No
34	The Strategy-Focused Organization	2001	No				No
35	Strategy Maps: Converting Intangible Assets into Tangible Outcomes	2004	No				No

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
36	Measuring Systems Interoperability: Challenges and Opportunities	2004	Dupl.				Dupl.
37	An Organizational Interoperability Agility Model	2005	Yes	No			No
38	Qualitative Reasoning: Modeling and Simulation with Incomplete Knowledge	1994	No				No
39	Qualitative Simulation	2004	No				No
40	Interoperability Impact Assessment Model: An Overview	2007	Yes				No access
41	Collaborative Networks for a Sustainable World: IFIP Advances in Information and Communication Technology	2010	No				No
42	A Petri-Net-Based Simulation and Optimization Approach for IEM and EI	2009	No				No
43	The Application of Interoperability Requirement Specification and Verification to Collaborative Processes in Industry	2012	One of eight initial articles				Dupl.
44	SCOR-Based Enterprise Architecture Methodology	2012	No				No
45	Demystifying Supply Chain Management	1998	No				No
46	System of Systems Interoperability (SOSI): Final Report	2004	Yes	No			No
47	Towards a Systemic Formalisation of Interoperability	2010	Yes	No			No
48	The Performance Prism: The Scorecard for Measuring and Managing Business Success	2002	No				No
49	Getting the Measure of Your Business	2002	No				No

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
50	Balanced Scorecard Step by Step	2002	No				No
51	Business Process Model and Notation (BPMN)	2009	No				No
52	Prediction in Multiple Regression	2000	No				No
53	Towards a Classification Framework for Interoperability of Enterprise Applications	2007	Yes				No
54	An Ontological Approach for Strategic Alignment: A Supply Chain Operations Reference Case Study	2011	No				No
55	Formulating Measures of Effectiveness	2002	No				No
56	A Language for Interoperability Modeling and Prediction	2012	Yes	No			No
57	Towards a Pivotal-Based Approach for Business Process Alignment	2011	No				No
58	Technical, Semantic and Organizational Issues of Enterprise Interoperability and Networking	2010	Yes	Yes	Yes	Yes	Yes
59	Formal Measures for Semantic Interoperability Assessment in Cooperative Enterprise Information Systems	2012	Yes	No			No
60	BPM Exception Monitoring Based on Process Knowledge	2010	No				No

References from “Towards Interoperability through Inter-enterprise Collaboration Architectures”.

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
1	A Collaboration Framework for Cross-enterprise Business Process Management	2005	No				No
2	ARDIN extension for virtual enterprise integration	2003	No				No
3	An enterprise architecture framework for collaboration of virtual enterprise chains	2008	No				No
4	Extended Enterprise Architecture Framework Essentials Guide	2006	No				No
5	Industrial automation systems - Requirements for enterprise-reference architectures and methodologies.: International Organization for Standardization	2000	No				No
6	CIMOSA: Enterprise engineering and integration	1999	No				No
7	Marco arquitectónico para la propuesta IE-GIP. Extensión de la arquitectura CIMOSA	2009	No				No
8	Enterprise Integration and Networking: challenges and trends	2007	No				No
9	Enterprise Integration—Business Processes Integrated Management: a proposal for a methodology to develop Enterprise Integration Programs	1999	No				No
10	References architectures for enterprise integration	2001	No				No

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
11	Enterprise modeling and integration (EMI): Current status and research perspectives	2002	No				No
12	PERA and GERAM enterprise reference architectures in enterprise integration	1998	No				No
13	Enterprise Architecture at Work: Modelling, Communication and Analysis	2009	No				No
14	Arquitectura empresarial- Una visión general	2010	No				No
15	An introduction to enterprise architecture	2005	No				No
16	Arquitectura de Empresa. Visión General	2005	No				No
17	Arquitectura empresarial: un nuevo reto para las empresas de hoy	2010	No				No
18	ARCHIMATE, The Power of Enterprise Architecture	2009	No				No
19	Enterprise Architecture Principles: Literature Review and Research Directions	2010	No				No
20	Enterprise architecture validation	2004	No				No
21	CIMOSA Primer on key concepts, purpose and business value	1996	No				No
22	GRAI integrated methodology and its mapping onto generic enterprise reference architecture and methodology	1997	No				No
23	PERA Enterprise Integration Web Site	2005	No				No
24	A handbook on master planning and implementation for enterprise integration programs	2001	No				No

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
25	GERAM: Generalised Enterprise Reference Architecture and Methodology	1999	No				No
26	Propuesta para el Desarrollo de Programas de Integración Empresarial en Empresas Industriales	1998	No				No
27	Architecting business and IS/IT strategic alignment for extend enterprises	2011	No				No
28	The Open Group	2011	No				No
29	Propuesta para el Modelado del Conocimiento Empresarial	2007	No				No
30	ARIS – Architecture of Integrated Information	2006	No				No
31	Enterprise integration - Framework for enterprise modelling	2006	No				No
32	Supply Chain Management and advance planning	2002	No				No
33	Planificación Colaborativa en un contexto de varias Cadenas de Suministro: ventajas y desventajas	2004	No				No
34	Desarrollo de una Arquitectura para la definición del proceso de Comprometer Pedidos en contextos de Redes de Suministro Colaborativas	2005	No				No
35	An Examination of Collaborative Planning Effectiveness and Supply Chain Performance	2005	No				No

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
36	Estado del arte de la planificación colaborativa en la cadena de suministro: Contexto determinista e incierto	2007	No				No
37	Modelos para la planificación colaborativa en la cadena de suministro: contexto determinista e incierto	2006	No				No
38	Collaborative Planning in Supply Chains	2009	No				No
39	A framework for collaborative planning and state-of-the-art	2009	No				No
40	Collaborative Planning	2008	No				No
41	A framework for an efficient implementation of logistics collaborations	2010	No				No
42	A Framework for Information Systems Architecture	1987	No				No

References from "Challenges in multi-agency collaboration in disaster management: A Sri Lankan perspective".

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
1	Does rising income increase or decrease damage risk from natural disasters	2008	No				No
2	Opportunities for improving disaster management in Chile: a case study	2007	No				No
3	Coordinating multi-organisational responses to disaster: lessons from the March 28, 2000, Fort Worth tornado	2002	No				No
4	An integrative approach to disaster management and planning	2004	No				No
5	Coordination in emergency response management	2008	No				No
6	Advances in multi-agency disaster management: key elements in disaster research	2010	No				No
7	Coordination during multi-agency emergency response: issues and solutions	2011	No				No
8	Emergency logistics in a large-scale disaster context: achievements and challenges	2019	No				No
9	A case study of co-ordinative decision-making in disaster management	2000	No				No
10	Challenges and obstacles in sharing and coordinating information during multi-agency disaster response: propositions from field exercises	2010	No				No

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
11	Humanitarian aid logistics: supply chain management in high gear	2006	No				No
12	Report on Koslanda Landslide: Aerial, Field Survey and after Action Review	2014	No				No
13	Sri Lanka rapid post disaster needs assessment floods and landslides	2017	No				No
14	Disaster Risk Reduction in Sri Lanka Overview: Status Report 2019	2019	No				No
15	Guidebook for Multi-Agency Collaboration for Sustainability and Resilience	2020	No				No
16	Getting Agencies to Work Together: the Practice and Theory of Managerial Craftsmanship	1998	No				No
17	The effect of problem severity, managerial and organizational capacity, and agency structure on intergovernmental collaboration: evidence from local emergency management	2010	No				No
18	Incrementalism before the storm: network performance for the evacuation of new orleans	2006	No				No
19	The “big questions” of Katrina and the 2005 great flood of New Orleans	2007	No				No
20	Managing boundaries in American administration: the collaboration imperative	2006	No				No

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
21	The concept of assisted management of large-scale disasters by horizontal organizations	2001	No				No
22	Linking emergency management networks to disaster resilience: bonding and bridging strategy in hierarchical or horizontal collaboration networks	2015	No				No
23	Collaborative Public Management: New Strategies for Local Governments	2003	No				No
24	Decentralization and collaborative disaster governance: evidence from South Korea	2016	No				No
25	Study on Disaster Risk Reduction, Decentralization and Political Economy, Global Assessment Report on Disaster Risk Reduction	2011	No				No
26	Improvising Disaster in the City of Jazz: Organizational Response to Hurricane Katrina	2005	No				No
27	Interlocal emergency management collaboration: vertical and horizontal roadblocks	2012	No				No
28	The National Incident Management System: A Multi-Agency Approach to Emergency Response in the United States of America	2006	No				No
29	Emergency incident management: an evolving incident control system framework	2009	No				No

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
30	A Strategic Approach to Emergency Preparedness in the UAE	2015	No				No
31	Joint emergency services interoperability Programme: working together saving lives	2014	Yes	No			No
32	Harnessing the power of metaphor: uncovering a hidden language of interoperability within the natural speech of emergency managers	2019	Yes	No			No
33	Local interoperability in UK emergency management: a research report	2017	Yes	No			No
34	Ministry of Disaster Management, Sri Lanka National Disaster Management Plan	2014	No				No
35	Key Challenges in Multiagency Collaboration during Large-Scale Emergency Management	2012	No				No
36	Role of information in collective action in dynamic disaster environments	2010	No				No
37	Crisis management in hindsight: cognition, communication, coordination, and control	2007	No				No
38	Multi-agency operations: cooperation during flooding	2012	No				No
39	Complex systems in crisis: anticipation and resilience in dynamic environments	2001	No				No
40	Planning the resilient city: concepts and strategies for coping with climate change and environmental risk	2013	No				No

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
41	Building Community Disaster Resilience through Private-Public Collaboration	2011	No				No
42	Interoperability of e-government information systems: issues of identification and data sharing	2007	Yes	No			No
43	Governance struggles and policy processes in disaster risk reduction: a case study from Nepal	2014	No				No
44	The role of GIS-enabled mobile applications in disaster management: a case analysis of cyclone Gaja in India	2020	No				No
45	The research design maze: Understanding paradigms, cases, methods and methodologies	2012	No				No
46	Culture's Consequences: Comparing Values, Behaviours, Institutions, and Organizations across Nations	2001	No				No
47	Boundary work among groups, occupations, and organizations: from cartography to process	2019	No				No
48	Adaptive governance as a catalyst for transforming the relationship between development and disaster risk through the Sendai Framework	2018	No				No
49	Adaptive governance and managing resilience to natural hazards	2011	No				No
50	Toward a Sustainable and Resilient Future	2012	No				No
51	Resilience and transformation	2012	No				No

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
52	Transforming development and disaster risk	2018	No				No

Appendix A5 Selected articles backward snowballing

General information

Title of the article	Value proposition on interoperability of BIM and collaborative working environments
Author(s)	Grilo, A., & Jardim-Goncalves, R.
Year of publication	2010

Relevance and review questions

Subject	**Answer (Yes/ No)**	**Argumentation**
Are the research objectives close to our own?	Yes	AEC organizations are being pressured by new business relationships, that is, driven by new contractual challenges and the exchange of information and documents with new partners.
Is the context like our own?	Yes	
Is this article used as a reference in other articles?	Yes	
Does the article provide guidance for future research?	No	
Does the article contain challenges regarding interoperability?	Yes	
Does the article refer to data exchange between organizations?	Yes	
Is the study sufficient generic?	Yes	
Is the study's methodology sufficient?	Yes	

Themes	**Challenges**	**Main findings**
Legal		None
Organizational	Collaboration Culture Processes/ policies/ procedures Communication Coordination	It must address business processes, culture and values between the interacting parties. The main purpose of interoperability is to exchange information. There is an engagement to achieve results that the participants would be unable to accomplish alone, as interoperability is a backbone for the collaboration. This implies joint goals, joint responsibilities, and working together for the creation of innovative solutions. The informational interaction type has evolved. Currently, beyond simple Web pages with descriptions, organizations make available databases with sophisticated data

		about products, services, and the exchange. The goal is to align activities for mutual benefit, avoiding gaps and overlaps, and thus achieve results efficiently. Interoperability is used for obtaining mutual benefits by sharing or partitioning work. This will not only allow greater efficiency, but also the possibility to obtain some differentiation through time and cost savings.
Semantic and Syntactic	Language Data formats Standards	Translatable into a file format, so that all of the object's information can be transferred correctly. In most cases it is a challenge for such a translation to retain all the information that the model contained in its original native file format
Technical	ICT systems Software tools Location Compatibility	The actual perspective of interoperability advocates that this problem is not just an ICT issue, which is to say that it is not just about connecting information systems. Different software tools and often geographically dispersed, it must be compatible with models created by other software tools.

General information

Title of the article	New perspectives for the future interoperable systems
Author(s)	Panetto, H., Zdravkovic, M., Jardim-Goncalves, R., Romero, D., Cecil, J., & Mezgár, I.
Year of publication	2016

Relevance and review questions

Subject	Answer (Yes/ No)	Argumentation
Are the research objectives close to our own?	Yes	The constant pressure of requirements for more data, more collaboration and more flexibility motivates us to discuss about the concept of Next Generation EIS (NG EIS) which is federated, omnipresent, model driven, open, reconfigurable and aware. All these properties imply that the future enterprise system is inherently interoperable.
Is the context like our own?	Yes	
Is this article used as a reference in other articles?	Yes	
Does the article provide guidance for future research?	No	
Does the article contain challenges regarding interoperability?	Yes	
Does the article refer to data exchange between organizations?	Yes	
Is the study sufficient generic?	Yes	
Is the study's methodology sufficient?	Yes	

Themes	Challenges	Main findings
Legal	Usability Ownership Accessibility	Sensitive data or protected applications are critical for outsourcing issues. Whilst the data should be protected in a form that addresses legislative issues with respect to data location, it should at the same still be manageable by the system.
Organizational	Collaboration Standards Communication Coordination	Challenges for standards, transparency of control, user simplicity, rights management, IT and business working in a cooperative environment. Research challenges include interoperability and system behavior and adaptability; communication, collaboration and coordination facilities. Research challenges in this domain include Enterprise Interoperability and the adaptability, management and

	Social networks Culture Objectives Lack of formal maturity models	efficiency of networks. However, enterprises, such as humans, have their own identity and their own objectives.
Semantic and Syntactic	Fragmented and uncorrelated Ontologies Data exchange Heterogeneity Standards Definitions Characteristics Meaning Common understanding	Despite the data explosion and rising use of semantic technologies for its representation (open linked data), the underlying semantic structures (ontologies) are still fragmented and uncorrelated. The number of ontologies, addressing different domains, realities, applications and problems, produced by the scientific community today is growing extensively. It is common that 60–80% of the resources in data sharing projects are spent on addressing the issues of semantic heterogeneities. The lack of unified interoperability theory is considered as a significant obstacle for innovation in the semantic interoperability research arena. Semantic aspects of interoperability, in particular definition of the basic properties and characteristics of information; the meaning and ''common understanding'' of information objects; the construction, use and dissemination of information objects; comparison between information objects; measurement of information objects.
Technical	Security Rights management Communication Infrastructure Data storage Networks Cloud interoperability Data portability	Challenges for achieving secure openness and capability to interoperate of and with all entities. Challenges for interfaces and communication platforms as well as service-oriented architectures. The greatest challenge facing longer-term adoption of cloud computing services is not security, but rather cloud interoperability and data portability. The lack of integration between these networks makes it difficult for organizations to consolidate their IT systems in the cloud and realize productivity gains and cost savings.

General information

Title of the article	A review of e-business interoperability frameworks
Author(s)	Rezaei, R., Chiew, T. K., & Lee, S. P.
Year of publication	2014

Relevance and review questions

Subject	**Answer (Yes/ No)**	**Argumentation**
Are the research objectives close to our own?	Yes	An E-business Interoperability Framework contains standards and concepts that should be followed to ensure success with interoperability issues. It provides assumptions, values, and practices to practitioners in terms of enabling seamless interaction within their enterprises as well as with other enterprises.
Is the context like our own?	Yes	
Is this article used as a reference in other articles?	Yes	
Does the article provide guidance for future research?	Yes	
Does the article contain challenges regarding interoperability?	Yes	
Does the article refer to data exchange between organizations?	Yes	
Is the study sufficient generic?	Yes	
Is the study's methodology sufficient?	Yes	

Themes	**Challenges**	**Main findings**
Legal	Legal heterogeneities	Digital signatures interoperability is the mutual recognition of electronic signatures among countries, that involves overcoming of the current legal (legislation, management authorities) as well as technical heterogeneities in terms of attributes, validation, format and algorithms
Organizational	Costs Rules/ norms Culture Social networks	Lack of interoperability could cost the industry a huge amount of money. Interoperability issues should be further supported by gaining a more concrete understanding of rules, objects, software systems, cultural, social networks, electronic identity, cloud, and ecosystems interoperability issues. Standards and concepts that should

	Standards Concepts Processes Knowledge	be followed to ensure success with interoperability issues. It provides assumptions, values, and practices to practitioners in terms of enabling seamless interaction within their enterprises as well as with other enterprises.
Semantic and Syntactic	Common understanding	By addressing the lack of common understanding caused by the use of different representations, different purposes, different contexts, and different syntax-dependent approaches.
Technical	Software systems Social networks Electronic identity Cloud Ecosystems	Major challenges lie ahead in the scientific area of software systems interoperability in view of new technological and computer science's advances that indicate the need of a ubiquitous approach that guarantees a high degree of maintainability against the rapid software technology evolution.

General information

Title of the article	Information-sharing in public organizations: a literature review of interpersonal, intra-organizational and inter-organizational success factors
Author(s)	Yang, T.-M. & Maxwell, T. A.
Year of publication	2011

Relevance and review questions

Subject	**Answer (Yes/ No)**	**Argumentation**
Are the research objectives close to our own?	Yes	Information sharing is considered an important approach to increasing organizational efficiency and performance. With advances in information and communication technology, sharing information across organizations has become more feasible. However, information sharing can be a complex task. Identifying factors that influence information sharing is critical.
Is the context like our own?	Yes	
Is this article used as a reference in other articles?	Yes	
Does the article provide guidance for future research?	Yes	
Does the article contain challenges regarding interoperability?	Yes	
Does the article refer to data exchange between organizations?	Yes	
Is the study sufficient generic?	Yes	
Is the study’s methodology sufficient?	Yes	

Themes	**Challenges**	**Main findings**
Legal	Privacy Knowledge Information sharing Legislation Accessibility Policies	Concern about information privacy has been identified as a main concern for people who may otherwise exhibit information-sharing behavior. With limited access to and sharing of information and knowledge, organizational members lack the capability to develop integrated solutions to problems. The lack of legislative support to assure the privacy and confidentiality of shared information can impede cross boundary information sharing in the public sector. However, laws and regulations also create barriers to obstruct cross-boundary information sharing in government agencies. Cross boundary information sharing can be hindered because of policies that

		prohibit government agencies from sharing sensitive and regulated information in domains such as public safety and national security.
Organizational	Objectives Hierarchy Culture Rules/ norms Reward/ incentive Power games Social identity Social network Trust Collaboration Information exchange Knowledge Processes Autonomy Resistance to change Resources	Information is power, more worrying is that information can be hoarded as an asset to protect one's place and enhance individual status and identity. Organizational structure and organizational culture, ritual, and norm are the factors that have a broad impact on all activities of an organization. Reward and incentive, power games, social identity, social network, and trust are factors that can be formed and influenced by organizational structure and organizational culture. Reciprocity is an important positive factor influencing organizational members' attitudes towards the sharing of information and knowledge. Centralization has a significant negative impact on knowledge sharing in a multiunit organization it can hinder initiatives of inter-group information exchange and collaboration. It takes time and energy for organizational members to learn to use IT systems to contribute to information sharing. Concerns of autonomy loss and information misuse by other organizations that would incur liabilities for the sharing organization. Lack of resources such as staff shortages can also hamper initiatives of cross-boundary information sharing.
Semantic and Syntactic	Definitions Data standards	Bridge information systems and heterogeneous databases that have inconsistent data structures and definitions. It is a challenge to integrate heterogeneous information systems of different platforms.
Technical	Data sharing Infrastructure Standards Security Outsourcing	If the implemented information technology is not easy and efficient to use, organizational member's IT usage will be lower, and information and knowledge sharing activities could be negatively influenced. Different organizations have various types of hardware and software in their information systems. Security and confidentiality, it is critical to design a system that can handle access authorization and authentication for shared information. The IT adoption of government agencies in information-sharing systems can also be a challenge. Information system outsourcing also raises the difficulty in cross boundary information sharing, because of system design and specification details may not be well-written and preserved.

General information

Title of the article	Technical, Semantic and Organizational Issues of Enterprise Interoperability and Networking
Author(s)	Vernadat, F.B.
Year of publication	2010

Relevance and review questions

Subject	Answer (Yes/ No)	Argumentation
Are the research objectives close to our own?		Enterprise networking refers to any kind of organization structures in which two or more geographically dispersed business entities need to work in interaction. This can happen within a single distributed enterprise or among several enterprises. The paper uses the European Interoperability Framework (EIF).
Is the context like our own?	Yes	
Is this article used as a reference in other articles?	Yes	
Does the article provide guidance for future research?	Yes	
Does the article contain challenges regarding interoperability?	Yes	
Does the article refer to data exchange between organizations?	Yes	
Is the study sufficient generic?	Yes	
Is the study's methodology sufficient?	Yes	

Themes	Challenges	Main findings
Legal	Legal bases and legislation Knowledge Confidentiality	In a global economy, enterprise networking usually means working with partners in other member states or in foreign countries. Legislations are not the same. Data protection regulations may be different. Intellectual property rights (IPR) differ. What can be shared and what cannot? Which confidentiality levels are necessary and what protection levels are associated? What happens to the data that I share with other partners?
Organizational	Collaboration Culture	Different human and organizational behaviors, different organizational structures, different business process organizations and management approaches, different senses of value creation networks,

	Processes/ policies/ procedures Rules/ norms Hierarchy Trust Political Standards	different business goals, cultures or methods of work and different decision-making approaches. Trust management linguistic aspects, especially in the case of international contexts. Multinational firms, international organizations or cooperation between member states obviously have a political dimension.
Semantic and Syntactic	Heterogeneity of information Interpretation Terminology Inconsistencies Ontology Data formats	Data/information integration and consistency issues to support cooperation and collaboration, and especially knowledge and information sharing. Semantic barriers include heterogeneity of information, different interpretations of the same concepts, database schema integration with naming problems (e.g., homonyms and synonyms), structural logical inconsistencies, etc. There are simply too many ontologies around and no commonly agreed or standard representation of these ontologies.
Technical	System incompatibility Legacy systems ICT systems	The technological challenges to be solved concern system incompatibility due to high system heterogeneity, the existence of legacy systems and the heterogeneity of ICT solutions from different vendors.

Appendix A6 Articles forward snowballing

Additional articles found by using forward snowballing method

References from “The role of interoperability dimensions in building information modelling”.

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
1	No cited by in OU library						No

Additional articles found by using forward snowballing method

References from “The application of interoperability requirement specification and verification to collaborative processes in industry”.

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
1	No cited by in OU library						No

Additional articles found by using forward snowballing method

References from “Data standards quality measured for achieving enterprise interoperability: the case of the SETU standard for flexible staffing”.

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
1	No cited by in OU library						No

Additional articles found by using forward snowballing method

References from “Interoperability Standards for Seamless Communication: An Analysis of Domain-Specific Initiatives”.

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
1	No cited by in OU library						No

Additional articles found by using forward snowballing method

References from “Information sharing and interoperability: the case of major incident management”.

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
1	Toward a unified view of technology and activity The contribution of activity theory to information systems research	2018	No				No
2	Developing SCM framework associated with IT-enabled SC network capabilities	2017	No				No
3	An advanced decision support system for European disaster management: the feature of the skills taxonomy	2018	No				No

Additional articles found by using forward snowballing method

References from “A methodology for the evaluation of interoperability improvements in inter-enterprises collaboration based on causal performance measurement models”.

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
1	Model-based approaches for interoperability of next generation enterprise information systems: state of the art and future challenges	2017	Yes	Yes	Yes	Yes	Yes
2	An axiomatic design framework to design interoperable buyer-supplier dyads	2019	No				No

Additional articles found by using forward snowballing method

References from “Towards Interoperability through Inter-enterprise Collaboration Architectures”.

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
1	No cited by in OU library						No

Additional articles found by using forward snowballing method

References from “Challenges in multi-agency collaboration in disaster management: A Sri Lankan perspective”.

Number	Title	Year	Relevant title	Relevant abstract & conclusion	Interorganizational	Interoperability challenge	Relevant
1	No cited by in OU library						No

Appendix A7 Selected articles forward snowballing

General information

Title of the article	Model-based approaches for interoperability of next generation enterprise information systems: state of the art and future challenges
Author(s)	Zacharewicz, G., Diallo, S., Ducq, Y., Agostinho, C., Jardim-Goncalves, R., Bazoun, H., Wang, Z., & Doumeingts, G.
Year of publication	2017

Relevance and review questions

Subject	**Answer (Yes/ No)**	**Argumentation**
Are the research objectives close to our own?	Yes	This paper relates existing work, and it examines barriers that, at the moment, are preventing further improvements due to current methodological and technological limits
Is the context like our own?	Yes	
Is this article used as a reference in other articles?	Yes	
Does the article provide guidance for future research?	Yes	
Does the article contain challenges regarding interoperability?	Yes	
Does the article refer to data exchange between organizations?	Yes	
Is the study sufficient generic?	Yes	
Is the study's methodology sufficient?	Yes	

Themes	**Challenge**	**Main findings**
Legal		None
Organizational	Social Communication Hierarchy Standards Processes	Future EIS will depend on its sociability skills. A major problem frequently identified in the EIS definition is the gap between different people visions (models) that describe and use the information process. Existing EIS frequently lacks to propose innovative information exchange between humans and are not being completely adapted with users' current practices. Human unformal and direct communication is not sufficiently considered even as it remains a critical communication vector to transmit information. The different visions of the

	Culture Maturity Collaboration	business process between the enterprise leaders and the developers are still a gap. Most of the EIS project failures are coming from a lack of appropriation from the users. Another main challenge is to deploy coherently the models according to different users' (business people, customers') values and needs at each modelling level. Lack of maturity of the domain. However, the use of EISs reaches a limit in collaborative environments because enterprises management methods diverge and EISs are mainly inflexible resource packages that are not built with an interoperability objective. One problem is that partners use different processes, organizations and different enterprise information systems which leads to horizontal barriers of interoperability. Business, Process, Service and Data and Enterprise collaboration. These different abstraction and viewpoint levels require different models that involve different categories of information and do not match instinctively.
Semantic and Syntactic	Data standards Ontology Vocabulary Language	Remaining work includes: (1) the rules and formalisms of information exchange, and (2) the way of exchanging information between the two sides using ontology alignment. Currently most of the defined rules are either designed to general purpose and are less efficient for specific work domain vocabulary and vice versa. Bridging language between the harmonizing visions of the EIS, it is not addressed yet, and it has to be discovered for joining divergent visions with interoperability. for both ontology, model transformation, language and models there is still a need to compare, align and rank results. In effect, even if research works and standardization initiatives have recently emerged, there are no common metrics (or indicators) that can be fully admitted and used to compare if the level of interoperability obtained in the operational solution is coherent with the interoperability prescribed in the strategic model. Also, the choice and the quantification of the indicators are still challenging. Enable better understanding and matching of data exchanged between partners' heterogeneous EIS. For conceptual and technical consideration, semantic heterogeneity is becoming a major barrier that obstructs achievement of EIS interoperability. The difficulties are caused by the diversity and ambiguity of natural languages, which are used to represent the entities in ontology. Problem is that algorithms from off-the-shelf products are designed for typical use cases and for particular model types such as class diagrams or similar model types only. Do not propose and support specific modelling languages.
Technical	Integration Reusability Transformability Standards Communication	Future EIS will depend on its integration, reusability, and transformability. One future EIS challenge can be to standardize in between the systems rather than inside in order to facilitate the connections. A general problem is to deal with hybrid situation where existing EIS components have to communicate with non-existing or unavailable yet services in the enterprise. Existing software and hardware components. It means that most of the models are starting from legacy systems; another challenge is in consequence the reusability aspect. The challenge is to reuse as much as possible the valid data structure, functions and behavior from existing system to be sooner ready to use and, above all, flexible enough to be rapidly modified according to modifications in the enterprise strategy.

Appendix B1 Interview protocol

Introduction

During the preface we will briefly introduce the objective of the research and the aim of the interview. When this is clear, the interview will be started.

General information

1. Which company do you present?

2. What position do you hold within this company?

3. What is your highest level of education?

4. How long have you worked for this organization?

5. How many years of experience do you currently have in this area?

Second part

During this part we will ask open questions to get a better understanding of the experience of the interviewee with the subject. And gives the interviewee the possibility to introduce (new) aspects.

6. How would you define interoperability?

7. In which way are you involved with this topic?

8. What is your experience regarding this topic?

9. How would you judge the level of interorganizational interoperability with regard to data exchange? Why?

10. Based on your own experience, which interoperability barrier are impeding interorganizational data exchange? Why these aspects?

11. What are the most common interoperability barriers?

Third part

In this third part we will introduce our framework for validation purposes. In this way we will be able to validate the aspects and refine the framework if needed and get an in-depth understanding of the extent to which these barriers are relevant for the MoD.

12. To what extent do you estimate that the legal interoperability barrier **intellectual property** impedes effective interorganizational data exchange? Please motivate, possible solution.

13. To what extent do you estimate that the legal interoperability barrier **accessibility** impedes effective interorganizational data exchange? Please motivate.

14. To what extent do you estimate that the legal interoperability barrier **knowledge** impedes effective interorganizational data exchange? Please motivate.

15. To what extent do you estimate that the organizational interoperability barrier **collaboration** impedes effective interorganizational data exchange? Please motivate.

16. To what extent do you estimate that the organizational interoperability barrier **processes, policies, and procedures** impedes effective interorganizational data exchange? Please motivate.

17. To what extent do you estimate that the organizational interoperability barrier **communication** impedes effective interorganizational data exchange? Please motivate.

18. To what extent do you estimate that the organizational interoperability barrier **data standards** impedes effective interorganizational data exchange? Please motivate.

19. To what extent do you estimate that the semantical and syntactical interoperability barrier **dictionary** impedes effective interorganizational data exchange? Please motivate.

20. To what extent do you estimate that the semantical and syntactical interoperability barrier **language** impedes effective interorganizational data exchange? Please motivate.

21. To what extent do you estimate that the semantical and syntactical interoperability barrier **ontology** impedes effective interorganizational data exchange? Please motivate.

22. To what extent do you estimate that the technical interoperability barrier **infrastructure** impedes effective interorganizational data exchange? Please motivate.

23. To what extent do you estimate that the technical interoperability barrier **resources** impedes effective interorganizational data exchange? Please motivate.

24. To what extent do you estimate that the technical interoperability barrier **data integration** impedes effective interorganizational data exchange? Please motivate.

25. To what extent do you estimate that the technical interoperability barrier **technical communication** impedes effective interorganizational data exchange? Please motivate.

26. Which of the interoperability barriers on a scale of 1 to 5 are the most recognizable (1 least recognizable, 5 most recognizable)? Why these interoperability barriers?

27. Which of the interoperability barriers on a scale of 1 to 5 are the most impactful in practice (with regards to data exchange)? Can you give an example?

28. Which of the interoperability barriers on a scale of 1 to 5 are the most relevant in practice (with regards to data exchange)? Can you give an example?

Closing

In the closing part of the interview an overall summary of the answers is given and discussed if certain elements are missing. Depending on the answers of the interviews the framework can be further refined.

29. Are all the mentioned aspects, correct? If not, please motivate.

30. Do you miss elements which should be added to the framework?

31. In which way are the interoperability barriers impeding a proper interoperability implementation?

32. To what degree is this influencing decision-making?

33. Do you think this framework is useful?

34. Do you have the intent to use this framework?

35. Is there anything you wish to get back on or are there any concluding remarks you would like to add?

Appendix B2 Letter of consent

The purpose of this interview is to collect information to evaluate and refine the theoretical framework aimed at interorganizational data exchange. This provides relevant insights which should be considered by the MoD when implementing interoperability concerning interorganizational data exchange.

Information will be collected by interviewing several actors with different perspectives. This data will be used to validate the framework in practice.

Interviews will take about 90 minutes and will be held one-on-one preferably face-to-face, but if necessary online. The interview will be recorded after consent of the interviewee and the data will be used to further complete the research. After processing the data, recordings will be deleted. Results will be shared with the interviewee, so that adjustments can be made. No references will be made which could lead to traceability, so that interviewee remains anonymous. The interviewee may refuse to answer the question without further explanation and can terminate the interview at any time.

On the next page the consent form can be found in which permission is asked to use and analyse the collected data to complete the research.

Research project: Interoperability barriers for interorganizational data exchange: A case study in the military sector

Researcher: Ferdy Winkler

- I have been informed about the research. I have read written the information letter.

- I have been given the opportunity to ask questions about the study.

- I have been able to think about my participation in the study.

- I understand that I can withdraw from the study at any time, and I do not need to give a reason for doing so.

- I consent to the use of the data collected during this study for the purposes of this scientific research and I can withdraw this consent at any time.

- I understand that any information I provide in connection with the research will be collected anonymously and will not trace back to me or my organization.

- I understand that the data collected (anonymized) will be kept in a secure manner by the Open University for 10 years.

If you have read the above points and agree to participate in the study, please sign this consent form below.

Signature:

Name:

Date:

Appendix C Case description

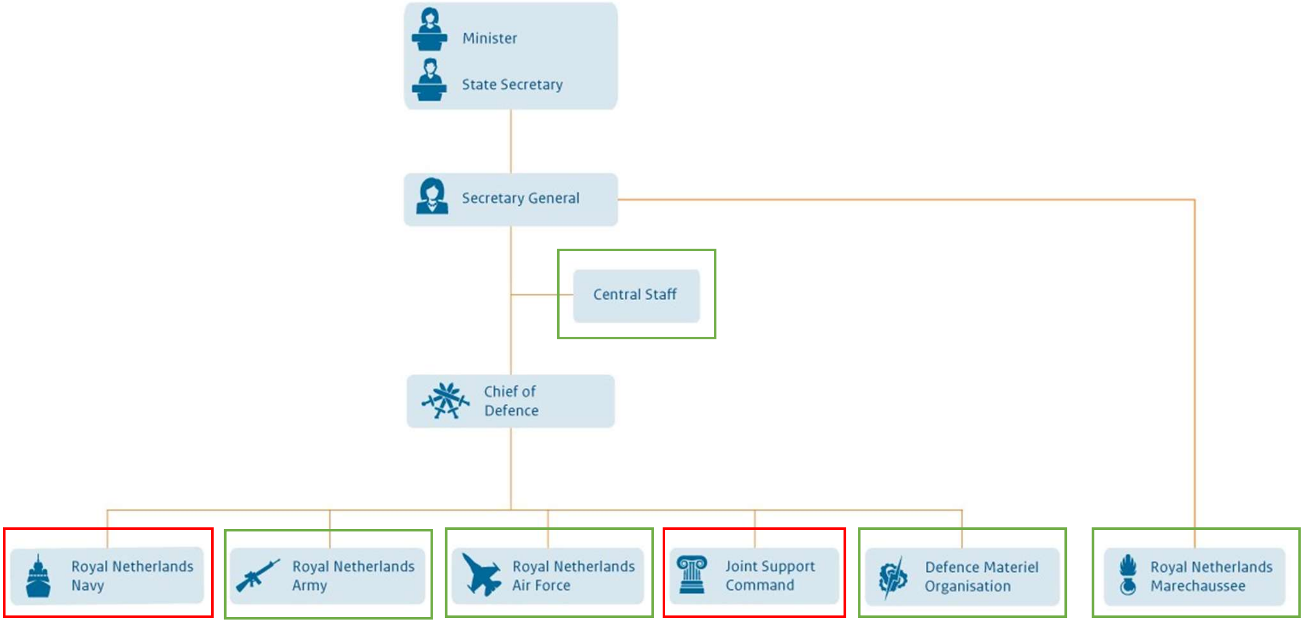
During this embedded case-study we conducted a research within the Ministry of Defence and two of its collaboration partners namely Netherlands Organization for Applied Scientific Research (TNO) and the Ministry of Interior and Kingdom Relations (MoI) which are collaboration partners of the Ministry of Defence.

The **Ministry of Defence** has approximately 68.000 employees of which 41.000 active serviceman, 20.500 civilians and 6.500 national reserve. These employees are divided among seven suborganizations. These seven suborganizations are:

- The **Central Staff** with approximately 3.200 employees;
- The **Royal Netherlands Army** with approximately 23.500 employees;
- The **Royal Netherlands Navy** with approximately 11.300 employees;
- The **Royal Netherlands Air Force** with approximately 8.100 employees;
- The **Royal Netherlands Marechaussee** with approximately 7.700 employees;
- The **Defence Material Organization** with approximately 5.100 employees;
- The **Defence Support Command** with approximately 9.300 employees.

The **Netherlands Organization for Applied Scientific Research** has approximately 3.700 employees.
The **Ministry of Interior and Kingdom Relations** has approximately 5.000 employees.

The MoD-departments with a green box are included in the research, the ones with a red box aren't.



Ministry of the Interior and Kingdom Relations

TNO innovation for life

Appendix D Data analysis synthesis

D1 Knowledge of subject

Interview #	Question 6 Definition of interoperability
#1	Getting the right information, to the right people in the right way at the right time. Without creating a risk for the deployment and without exaggerating safety measures, which could lead to losing sight of the operational gain.
#2	Business processes should be able to work together between different organizations, ICT is an enabler to make it possible (not the starting point). From the information point of view I reason, what exactly do you need and what do you want to achieve.
#3	Being able to collaborate with people with whom you want to share information. Being able to exchange information in a good way between sender and receiver in the broadest sense of the word. You are interoperable if the information you wish to send also has been received by the other.
#4	The ability of organizations to process information from each other without unpleasant surprises.
#5	The ease with which you can work with someone. This is a combination of exchanging data, the technical component, but also understanding each other, speaking the same language.
#6	The ability to exchange information in an understandable way.
#7	That if you want to work with parties that it is made possible. You can realize interoperability at all kinds of levels, organizational, policy, technical. But it is basically everything you need to work together.
#8	The information must be relevant, timely and it must end up in the right place where it can be used.
#9	This is about cooperation between organizations and the question how we can exchange information with each other.
#10	The possibility to work together within organizations, in a broad sense.
#11	Interoperability is an ability, so something you can do to a weak or strong degree, and then the ability to exchange data or not. It's not, you can, or you can't, there is a certain degree to which it is facilitated or made difficult.
#12	The extent to which you can work together analogue and digital in an efficient manner in an ecosystem.
#13	The way in which two organizations or departments can work together undisturbed and unhindered, in the broadest sense of the word.

Interview #	Question 7 Involved in subject
#1	I am often being questioned regarding, this is the policy we must comply with, but this is what we want to achieve, how can we achieve this and what changes should be made to the current policies and procedures?
#2	Extensive experience. Jurist who understands technology and business processes.
#3	Enabling information exchange between different classification levels.
#4	Involved with GrIT, new crypto possibilities, and data diodes.
#5	Research and consultancy projects for the MoD for Command & Control and I&S and the connection between those two subjects.
#6	On different levels, from the semantical level to the technical level. From the semantical point of view, do you have the same vocabulary, do you have the same definitions, do you use the same terminology, towards the increasingly detailed, conceptually logical and technical level.
#7	Various projects in which we look at how we now get information from one side to the other. What are the security requirements and how do I offer a good solution for this, both organizationally and technically.

#8	From the user side, the information must end up in the right place and people must be able to do something with it. And also how this is arranged throughout Defence, in particular within the OPCOs, that they can do what they need to do with the correct and timely information.
#9	Whether it is technically possible and allowed.
#10	What our next steps will be towards the IGO development. Because we must be interoperable with each other and this also means to be operationally effective with our partners and our environment.
#11	In the context of data governance, it is part of the tasks, responsibilities and authorities, and interoperability is something that touches all three aspects.
#12	Our office is in a partnership, setting up an innovative project to support people in a smarter way. You see that all organizations that aim for the same effect are digitally compartmentalized in such a way that it is very difficult to work together.
#13	How we could share data between the two organizations, in a technical way, but also finding out which legal regulations would apply and what might be further required. In addition, in terms of architecture, it is of course also part of developing different systems and how they could fit together technically one-on-one.

Interview #	Question 8 Experience regarding topic
#1	Different networks ask for different network specialists and at the end you need to make everything work together and that is not sustainable.
#2	Tricky subject, systems are always developed from one function. They have other working methods and other standards, which often do not fit together.
#3	-
#4	That the procurement process does not have any provisions for interoperability, so you can find random configurations if you are unlucky. Many islets.
#5	Everyone focuses on the technology, and everyone seems to skip the organizational, the will, and semantic aspect. The four different OPCO’s are the biggest barrier and the technology is often not the problem.
#6	-
#7	Interoperability can always be better and certainly in terms of understanding each other and knowing what you are talking about. Part of the interoperability issues are simply because we are talking about different things, when we think that we are talking about the same thing (semantics).
#8	During missions, the different dynamics often made it possible to switch gears faster and exchange information. It is often also very person dependent. We often have no access to specific systems, or there is fear that certain units will switch to a new system, to which the OPCOs are not linked.
#9	Because we simply do not have the right equipment for it yet.
#10	That we have a big challenge to achieve interoperability, both internally and with our partners, and especially externally. Fragmentation between different OPCOs, often already challenges within the pillar, but especially in order to be effective, we have a field of tension with our own bureaucratic organization and a multitude of developments within the organization, in addition to the lack of guidance from above on how we want to realize interoperability or if we have the guidance, it is often too spacious.
#11	-
#12	We're not there yet and we can't do that yet.
#13	Collaboration is always difficult. The legal basis that exists for processing or acquiring data differs per organization and that this entails policy-technical challenges. The problems in collaboration are mainly because IT people are stubborn. At the moment the strategy or the tactical layer decides, we start working together, then the ideas that live in this collaboration do not always match with what is possible at the workplace.

Interview #	Question 9 Level of interorganizational interoperability
#1	The MoD has many legacy systems that are linked together. There is a lot of space for improvements, and I do not think that the problem is a technical problem, because there are technical solutions. Almost everything is technically possible, but it requires a different way of thinking. It also requires acceptance that we use a more generic approach and stick to this approach instead of switching every time.
#2	Specific systems are purchased for certain core functions and therefore it often does not fit in bigger picture. The MoD is managed like a multinational, but if you look closely at it, it are all small and medium-sized enterprises, which makes integration difficult. The interoperability is limited. This forces you to take measures, which may then weaken the security.
#3	When it comes to very specific processes, it is a bit more difficult.
#4	-
#5	Laborious, a lot of manual work, a lot of USB sticks, and also a kind of false security. If it is not linked then it is safe, but if you cannot access the information, it is of no use to you. But everyone is trying to work around safety.
#6	Fragmented, there are points where this has a high level of maturity and there are also points where it still goes completely wrong.
#7	It depends on what domain you're looking at. I think it is fine in many domains. I think that technically it is starting to come together reasonably well, but the fact that it is technically possible does not mean that the organization has the need to do it or that it is allowed at all.
#8	The Air Force can already do quite a lot with data, and they are also very busy with that. But in the multidomain we are not very far yet. There is no direction and no control. They are islands and not multidomain operations.
#9	We have devised options for how we can do it for many areas and very often it is automated, but very often it is also a USB stick. We are not yet at the level we would like to reach. The higher the classification, the more difficult the link becomes.
#10	Low to very low, because we lack standards and resources on both technical and data level to achieve interoperability, but interoperability also receives insufficient attention from an organizational perspective. It depends on many things, it certainly depends on many islands and systems that we have created, but we have never consciously created them, because everyone has fulfilled their own needs and the challenge is to eventually direct and to make one system of what we want.
#11	I think it's good to make a difference within domains and between domains. Within domains you encounter fewer problems with definitions and formats, and it is less of a problem if they deviate, because then we can work it out together. Between domains it becomes more interesting, because you can have a discussions about what is an operation.
#12	Within the LGI it is reasonably in order. We have made progress there, but we still have a long way to go to connect with our digitizing society. But there is sometimes no possibility to do this with partners in the LGI or HGI domain, except from using with USB sticks or via an external cloud solution. But this is not secure and often there are no agreements.
#13	We are well on our way. We're still a long way from where we should be and we're not nearly mature enough on the collaboration.

Interview #	Question 10 Barriers impeding interorganizational data exchange
#1	The human factor. A lot of people still think that they know what is best and everyone thinks that their data needs are special and that there should be unique systems for their specific needs instead of that those choices are being made by a group with specialists. It is not necessary that every need must have a special solution. Sacred houses, islands, it does not always match the bigger picture, which they do not see themselves.
#2	There are opportunities in IT, because there are more possibilities than what we are using it for. Information on paper or USB can generally be easily exchanged. The willingness to exchange information is there, even if there are sometimes legal restrictions, but these can often also be settled. When the information really needs to be exchanged, problems often arise again. We often pretend to be very safe, but meanwhile we stick a knife between our own ribs, which prevents you from functioning properly. It often necessitates measures that you do not want to take at all.

#3	On the security side, availability is always a challenge, we always have to think in terms of multiple solutions in order to communicate, which makes it very difficult because you always have to be able to act autonomously. Integrity, especially when you talk about classified information, you don't want to get everything in if it has not been properly checked, because that can corrupt your network or information provision. You want to be able to make decisions based on honest information, which is very important. The moment you have done an analysis and you want to send it within the organization, there is always an aspect of exclusivity. After all, you always want to be able to share information, but not everything, only specifically that which is important for the operator or for an intermediate organizational level.
#4	In the end the purchasing process. If you have to wait for a NATO standard, the NATO standard will lag behind the rest of the world's technology by the time it is finished. If there are more modern products, what can we do if NATO standards are (far) behind.
#5	The technical one, but I see that people often work around it. Not knowing that someone benefits from your information and that the other person also does not know that you have relevant information available. Being unfamiliar with, so actually the factor people and organization.
#6	-
#7	Barriers that when people want to exchange data, they find out that all kinds of other things are at play, we have a certain interest in not doing it, there are all kinds of legal restrictions on whether or not to do it. I don't trust certain parties to do it or not. And my idea is that it's never actually a technical problem.
#8	Unnecessary compartmentalization, scoring urge management tricks, often no decision is being made. And that is the part where we are still lacking within the MoD and certainly because we never implement, we often get stuck at the point that someone does not (entirely) agree with it, and then we do a little more research. I think there is not enough central control, or at least, someone has to make the decision and then it has to be implemented. The problem is, a lack of direction with perseverance. It must be clear and that is often not the case, you can go in any direction you want as an OPCO.
#9	I think that the technology is a difficult challenge to make certain things possible. The agreements between the organizations that do not exist yet, so that you would like to provide information and collaborate, but that also includes a certain agreement framework around it, so that they also understand each other, know what you want, know what to exchange and what to exchange. Because you don't want to send everything out into the free world, you also have to have a certain objective with the collaboration and then you eventually look for interoperability to make that possible Opportunities are in creating a common network. You just have to sit down together and do it (human factor).
#10	Lack of good interfaces at the network layer, lack of broader management, that means high-level IT design for good management of the IT portfolio, good management in the field of interoperability, because they want to go to IGO in 2035, do we want to get there, this must entail the right direction, priorities and the right resources. The bureaucratic organization as a whole ensures that we cannot anticipate on developments, which also makes it difficult. So, it is a multitude of developments, and we also miss a piece of standardization.
#11	At the moment there are no Defence-wide reference lists, for example we do not have a Defence-wide data catalogue in which we have an overview of exactly which references and definitions are used. So, the lack of overview is a barrier. Data quality is also a very big thing. Information management and its importance are fairly undervalued.
#12	The way in which we have set up our information security. This is very much focussed on control and mitigating risks. And less focused on risk acceptance. So what risk are we now willing to accept in order to facilitate information sharing? But it is often no. Bureaucracy and old thinking are in the way. This way of approaching projects no longer fits the present time. I think you have to work much more experimentally, that you have to involve the market much more in this kind of IT accelerators, which can bring about connections between organizations.
#13	-

Interview #	Question 11 Most common interoperability barriers
#1	The diversity of systems. In the same classification domains and classification levels, we have different systems and because it all has to be kept up and running, we do not have the capacity and the knowledge in terms of people to look at how you can do that uniformly in a better way. So, in my opinion it would be better to consolidate within classification levels, go back to one or maybe two networks within the same classification level.
#2	Freedom to provide someone with free information (file format) and to put information in systems or to remove it is often still very difficult. Text-driven information can all be exchanged, but more modern media is limited (exchange of data). Often you cannot get information from one platform on the other platform, in the file where you want it. If we want to collaborate with external companies, a schedule of requirements must be drawn up, but often the companies are not (yet) ABDO certified.
#3	Human trust. I think trusting and understanding each other's position is often the biggest barrier and I think people's ability to see what the potential risks are means they are more cautious than they really need to be. People are often unable to assess the risks in depth and cannot properly assess the impact of the choices they make. You can see that operationally the commander always takes responsibility, because he makes a good assessment of not having information available versus keeping the information safe. The greatest limitation is human rationality and awareness of the potential risks. We often make solutions that are so complex that they are almost impossible to use. We also have to get rid of that, we have to make sure that the technology is supportive and easy to use.
#4	Companies that make a beautiful and good product but keep it completely proprietary. You can't make it operable because you don't know how it works.
#5	The separate organizations, data which is not mutually linked, people often know, but it's too complicated. Technology does not always work, but it can be made workable.
#6	Lack of agreements in the broadest sense. There are 10 standards for something and that is seen as detrimental to interoperability, so a solution is created to solve this problem and that results in an 11th standard. Difference in interpretation, in the world of Defence, this can have somewhat more serious consequences, because it can be dangerous to use your own interpretation and assume that it is a certain system. There are too many standards, there is too much room for interpretation and in a sense an agreement on what makes a message interoperable. When people have to talk to each other, it is difficult. It is seen that eventually there must be some kind of overarching definition or standard, but that is very difficult and often results in an additional standard.
#7	Hidden interests. It often starts that we have a common interest in exchanging information with each other and then there are always limitations. And I think one of the biggest barriers is that it's very late in the information sharing and operability process that those barriers come up on the table.
#8	Willingness, there are reasons why things don't happen, also due to a lack of manpower. But my experience is that if something really has to be done, when push comes to shove, we fix it, then everything is possible, one has to feel it and in reality one often doesn't feel it.
#9	Do we trust each other. If you want something, you must have the confidence that the other party will handle your information with due care. Seeing the will to cooperate and the need to share things with each other, that is the main starting point.
#10	At the technical story, so the amount of networks then it concerns the lack of good interfaces between those networks. At the data layer, it is more the uniformity, the standardization in that area and the direction that is missing there. We need to have a broad picture of the process and the operation and how we want to achieve integrated interoperability.
#11	Bring the technical barriers of interoperability, a little closer to the policy challenges.
#12	Bureaucracy is one of the biggest problems. The old-fashioned step-by-step plan that we have to go through, before we finally arrive at the point of new technology. Legislation does not have to be a limiting factor at all. It is often also a jurist who has no affinity with ICT and is far removed from the subject, and is not specialized in the IT. The same goes for ethics, but people find it very exciting to take their responsibility in a certain area.
#13	Different signing authorities. On a technical level you are dealing with different shared services organizations that do not always work well together. We have different systems, other rules regarding recording, other ways of recording or different archival laws.

D2 Framework validation, refining and ranking

Interview #	Question 12 Legal barriers: Intellectual property
#1	Ownership is also responsibility, both at the data level and at the system level. At the MoD we are not yet good enough to do this at the data level. If the ownership is unknown, we run into problems which hinders interoperability. Within the MoD we do not deal much with intellectual property.
#2	When discussions arise regarding intellectual property, most of the time we look at who owns the information, but this is often very unclear, especially within the MoD. And that's often because we don't label the information or know what the original source is.
#3	Return on investment must be translated into, what do I gain if I share my information.
#4	Companies make products and make them inaccessible. Within a military organization I think privacy is less of a problem.
#5	It is very recognizable that it is not actually arranged. The basis of data ownership and what can I do with this data is not in order at all because it is not sexy.
#6	I think I wouldn't see it so much as a barrier to interoperability, but rather as a dimension that you would like to add to interoperability because whether or not legally permitting the exchange of information does not say anything about being able to exchange that information. Is there already a way to universally link data to what the provision restriction is, whether or not legally based? I think the answer to this is no, so that in turn leads to additional agreements to be made. Whether it is a barrier, I don't know if I completely agree on that, if one aspect is the legality of ownership, but I see it mainly as a potential additional condition or constraint that you would like to place on interoperability, and I think there are insufficient mechanisms and technology in the world to really guarantee that.
#7	I think the biggest problem is often keeping the control over your data. Within the MoD, it is more a quid pro quo, so when you work together you have all kinds of parties and you want to share, but you have to get something in return. But there are all kinds of parties that do not allow or limit what you are allowed to do with the system. The data is in the system, but someone else then determines what you can and cannot do with the system, especially when you want to extract it.
#8	We have legislation, and the problem here is that it applies to multiple organizations. So we have a law that places us under very heavy restrictions, while we often operate abroad, but we are (partly) bound by strict domestic legislation during foreign operations. The GDPR also applies to the MoD, while this is often not the case abroad. In today's world where readiness often spills over into commitment, you always need to be ready.
#9	I would include legal barriers and laws and regulations as separate bullets. These matters mean that it is not always possible to share information with each other. State secrets law, you may not share it with another party and that is certainly not on the intellectual property side, but intellectual property can play a role in the fact that you do not want to share certain information with a certain party because the information is so important to your company. Law and regulations determine what options you have. From a business objective or return on investment or data ownership, you could classify that as a part of intellectual property.
#10	If I look at who takes ownership, the need must come from the business and management. I also actually think that intellectual property also plays a role in operability, because we also have no management or control over our purchasing policy. So it means that we get all kinds of packages and products from all kinds of manufacturers and we don't think about interoperability or only afterwards. It is also possible that you realize a broader high-level IT governance board which can give direction and controls this.
#11	In some cases, privacy is a very big limitation and, in some cases, not at all. Return on investment doesn't mean very much to me in this case.
#12	We also generate a lot of intellectual property within Defence that we do nothing with. If we work together with chain partners, I would really like to use the sensors of other NLD organizations, but this is not possible. Data exchange cannot take place between parties who are all in the same domain.
#13	Certainly applicable, not so much your return on investment or the privacy barriers, but the ownership aspect. In the collaboration complex policy-technical questions appear like who the owner is if something has been labelled as property of the MoD, then not all of the MoI employees are allowed to access it. So if there is no clear policy on this, it will certainly get in the way of cooperation.

Legal barrier - Intellectual property: *Uncertainty regarding data ownership, return on investment and privacy barriers limits interoperability.* Most of the interviewees (12) validated this sub-aspect, it has the highest overall average on recognizability, impact and relevance (4,36) and all of the interviewees had bigger or smaller suggestions for refinement. Most of the interviewees recognized that data ownership is a large problem within the MoD, and that it is not properly arranged, often because data is not (properly) labelled. Intellectual property was also recognized by two interviewees as a problem, so the suggestion was to include intellectual property in the description. This problem within the MoD is created because a lot of products are bought, without having control over the purchasing policies, what leads to inaccessible products. The term return on investment, was also acknowledged by two of the interviewees and they translated it into "*quid pro quo*"*,* you have to get something in return. Regarding the privacy barriers, two interviewees stated that there are issues regarding the unfamiliarity with the GDPR, so it has been admitted to be an important part of this sub-aspect. Another suggestion was to add a sub-aspect "law and regulations", because whether or not legally permitting the exchange of information does not say anything about being able to exchange that information. A sub-aspect law and regulations would determine what the boundaries are. So for most of the interviewees this sub-aspect is a very important part of the framework, and it is essential for interoperability within and between organizations.

Ownership is also responsibility. If the ownership is unknown, we run into problems which hinders interoperability (#1). Return on investment must be translated into, what do I gain if I share my information (#3). Companies make products and make them inaccessible (#4). I also actually think that intellectual property also plays a role in operability, because we also have no management or control over our purchasing policy. So it means that we get all kinds of packages and products from all kinds of manufacturers and we don't think about interoperability or only afterwards (#10).

Interview #	Question 13 Legal barriers: Accessibility
#1	The possibilities are often there to exchange data, but the knowledge of the people about how is often lacking. And out of fear or ignorance the exchange is not made possible. There is a lack of awareness within the MoD about the value of data, this must be increased. We all need to become more aware of the value of certain data within the MoD. If that distinction is made, it will also become easier to share data with each other. Accessibility is possible but stands or falls with the knowledge about legal barriers.
#2	You have a system that forces you to do things in a certain way, but you also have your own responsibility. But certain things are not provided or are difficult to arrange.
#3	It is very difficult to give a general picture of this. Some things are very accessible and some things less, you can hardly weigh this. I personally think that there is still room for improvement for a number of critical processes, and I am really talking about the military operational level in particular. The rest is sometimes difficult but is somewhat less important. If I look purely at the value for the organization, so joint situational awareness and the information that we have to exchange for this, I think there is still a lot to gain.
#4	It is clear that we are going beyond those traditional boundaries and that we must and want to share information more.
#5	I very much agree with this. It explicitly says formal mechanisms. This is a major barrier, especially since there are many informal ways.
#6	I think I also see this sub-aspect more as a policy issue, what I see is that the Dutch government sets standards or even requirements about the accessibility of information, including privacy-sensitive information. In order to meet certain requirements or standards, we take measures that I think are too restrictive for what we would actually like in policy, namely that all data should in principle be available to everyone, provided that this is legally permitted or required. Now the measure is stricter than the intention.
#7	I don't think I see the formal mechanisms for data exchange very often. Need-to-know is usually arranged, but the need-to-use is usually a consideration that becomes a bit more difficult. But how do you decide not on the basis of need-to-know, but on the basis of need-to-use. I need information, but I'm not actually allowed to access it, but the advantage is greater to share it now instead of not. And that trade-off, especially in defence terms, and when it comes to the classified domain, it's very complicated. There is someone who has determined that something must be classified, but then someone else has to determine on what grounds he may or may not share this. But he just doesn't know why it's classified. The system properties determine whether it is classified in the first place. That is a very big issue and we have no standards for that.
#8	We don't have a common network. That's one of the biggest problems.
#9	General Security Agreement or Memorandum Of Understanding (MOU), this is an agreement with the other party that it will handle our information with due care, these are more country-country or government-government constructions. When it comes to companies, this often concerns the contract which is drawn up with each other in which you make agreements about what information you will exchange with each other and for what purpose. When you talk about contracts that the MoD draws up with companies, they often also come with sanctions.
#10	Very recognizable. We often use a recognized network, which is very safe, but it does not help with accessibility. So there we miss the toolbox to arrange that properly.
#11	We don't have all the technology in order, because we still do a lot with USB sticks, but I think those are issues that are more nice to have than a need to have.
#12	This is also still a big problem, it has improved somewhat, but when I look at our partners it is very difficult to access each other's data. There was once an idea of a service bus within Defence, but that has still not been done. So, this is not well arranged. Luckily the sense of urgency is growing that we have to invest in that accessibility, but at the moment it is not yet arranged.
#13	Kind of, I think we're doing pretty good between the organizations. We have enough facilities to guarantee this, both technically and in terms of policy, as long as it is covered from the start. So, then this would apply more to need-to-know.

Legal barrier – Accessibility: *Although the data must be well secured, there is still a lack of formal mechanisms to exchange data in order to create interoperability.* The interviewees validated this sub-aspect twelve times and there are no suggestions for refinement. This sub-aspect is also seen as a necessary part of the framework, seven interviewees recognize the lack of formal mechanisms which are focussed on accessing and exchanging data in a legally permitted way. Especially when it comes to the classified domain, it remains very complicated. Information is needed, but there is no access or possibility to exchange it. According to another interviewee the possibilities are often there, but the knowledge how is often lacking. One stated it is possible, but it has to be arranged from the start. Another interviewee sees this sub-aspect more as a policy issue, and that it is too restrictive. But there are many informal ways, because the system forces you to do things in a certain way. The need-to-know is usually arranged, but the need-to-use is more difficult. We are beyond the traditional boundaries and often the advantage to exchange data is greater than not sharing it at all. So it is recognized that it is often hard to access data. So most of the interviewees agree that the sub-aspect accessibility is a necessary part of the framework.

The possibilities are often there to exchange data, but the knowledge of the people about how is often lacking (#1) You have a system that forces you to do things in a certain way, but you also have your own responsibility (#2). All data should in principle be available to everyone, provided that this is legally permitted or required. Now the measure is stricter than the intention (#6). There is someone who has determined that something must be classified, but then someone else has to determine on what grounds he may or may not share this (#7). It has improved somewhat, but when I look at our partners it is very difficult to access each other's data (#12). We have enough facilities to guarantee this, both technically and in terms of policy, as long as it is covered from the start. (#13).

Interview #	Question 14 Legal barriers: Knowledge
#1	What makes it difficult these days is the question when digital information is regarded as personal data and when not (GDPR) this makes it quite restrictive in what you are allowed. Still a lot of times the answer is no, unless it is specifically described. But this has never been the approach of the GDPR and is currently a real big issue.
#2	As MoD we are reasonably aware of this. Where it's sometimes lacking is when a question is asked, we do not dare to answer, because there may be risks involved (responsibility). Not so much the knowledge, but the courage and the decision to actually do it. The tricky thing is when you give something to someone, you have to trust that the trust will not be damaged. This is often a sensitive point, especially when there is a lot of pressure.
#3	The classification in particular is an issue and the limited degree of rationality of the people is the basis for this. Understand the impact of sharing or not sharing information.
#4	I don't really know enough about it.
#5	Great lack of knowledge and the knowledge that is there is so scarce. Jurists are often risk-averse, which means that they quickly say no instead of thinking along. I think this is what you want to achieve, it is not allowed this way, but it is allowed if you do it this way. You need a jurist with technical and organizational affinity. Now it often becomes a means to protect upper management from major mistakes. They think more often in limitations than in possibilities.
#6	Certainly recognizable, I always wonder to what extent this is deliberate or really ignorant. There are systems of laws that have rules going around them and I think it's human nature to try to find the loopholes, so I don't know if that really has to do with knowledge just to get creative accounting. I would say that usually the law and regulations are freely available, so anyone can inform themselves about that. This still requires interpretation and translation into policy. Then you are on the dividing line of legal affairs and policy departments that try to make a sport of trying to write it down as woolly or not specific as possible. There is a large gray area in between, but in theory I think it is quite possible to take that knowledge and make decisions based on the limitations that are captured in a law or regulation. I do notice and that is domain specific, if you leave a domain, specific laws and regulations sometimes apply per domain. If then interoperability is desired with an OPCO or organizational units that are not primarily active in the same domain, specific laws and rules sometimes apply per domain and then the knowledge of the partner party about the specific rules within the other domain can be restrictive. If anything is accessible, it is laws and rules. I can also imagine that if it is not your rules or laws, the knowledge may be lacking a bit, but well you are going to interact with a party whose work it is, so I don't think the knowledge should be a barrier.
#7	I think that this is not properly regulated. There are very good regulations on how to classify information, but there are virtually no rules on how to distribute information correctly. It is all well-organized at the place where it has to be classified, but at the workplace where the decision has to be made, it is not known when you can start sharing it. If you look at the policies, there is actually nothing in place, certainly not between all kinds of parties that now have to work together.
#8	It often goes wrong here. You often see that Legal Affairs is in the no mode. You see that thinking about what is and how is it possible is not always there, because it is easier to say no. It's about being able to do your job, and not about breaking rules, because nobody wants that. Decisions whether or not to do something are always political and the minister has to decide on this, and then there are often completely different factors than the effectiveness of defence or the armed forces.
#9	Certainly, from a security point of view, if people are familiar with it and act accordingly, you could perhaps classify that as compliance. Knowledge sounds more like, do you have the proper knowledge and are existing frameworks arranged, yes or no. That is why I say knowledge in the form of awareness, because in the end it is described in those laws and regulations, but being able to actually apply it is sometimes difficult for people because they do not exactly know how it works.
#10	Knowledge is lacking, the legal implications and the knowledge thereof are not always clear. What you see very often is risk-averse behaviour. Because very often it is now about mitigating risks and then we say no or probably not. And that also depends on knowledge, do the jurist have the right knowledge to provide good input on these types of complex subjects in IT files and security files.
#11	We struggle with these questions. Our workforce is not yet completely data minded and data driven, so these are important aspects. My image is that the knowledge about IGO is limited at the legal affairs office. They are taking less action than we would like them to take, because the knowledge is not there, but they are thinking along.
#12	Knowledge of the way in which you could share data is not really there. The very classic links are still being looked at when it comes to data sharing. While I think you should also have knowledge of more modern IT infrastructures to get a good picture of where we ultimately want to be in 5 years.
#13	Very appropriate, but we have managed this reasonably well. I think that if we do not have this in place, we will soon get a warning from the supervisory authorities.

Legal barrier – Knowledge: *To create interoperability it is mandatory to know which data can be legally shared, how is it classified and what will happen with the data.* The interviewees validated this sub-aspect ten times and there are six suggestions for refinement. Within the MoD this sub-aspect is recognized as a barrier, because often people don't know if information is for instance GDPR, how it is classified and how it can be distributed correctly. One of the reasons is, according to six interviewees, the risk averse behaviour within the MoD. Also, the legal department is responsible for this, because of a lack of knowledge, including ICT, which makes it is often easier to say no, then to think along. Although laws and rules are accessible, a lot of policies are written as woolly or not specific as possible, so often people don't know how to apply them. From another point of view one of the interviewees stated that this sub-aspect is arranged reasonably well.

We do not dare to answer, because there may be risks involved (#2). The classification in particular is an issue and the limited degree of rationality of the people is the basis for this. Understand the impact of sharing or not sharing information (#3). Great lack of knowledge and the knowledge that is there is so scarce. Jurists are often risk-averse, which means that they quickly say no instead of thinking along. They think more often in limitations than in possibilities (#5). You often see that Legal Affairs is in the no mode. You see that thinking about what is and how is it possible is not always there, because it is easier to say no (#8). Very appropriate, but we have managed this reasonably well (#13).

Interview #	Question 15 Organizational: Collaboration	
#1	Collaboration means trust in each other and means that you have to be on the same level of understanding, but sometimes we still speak different languages. Different cultures are starting to diminish, but the islands are still a problem. This is not only a Dutch problem, but also an issue within other armed forces. The way of operating and acting means that people are looking differently at things. As long as this remains, it will stay difficult to realize a complete exchange.	
#2	This is precisely in the field of cooperation that you have to find each other. This takes time and effort. You also have to clarify each other's goals and understand each other well. This is often forgotten, and it quickly goes over the mail and then it quickly stops. The parties think that they are talking about the same thing, but this is often not the case. We have to work together interdepartmentally and that doesn't always work, people don't trust each other, sometimes without a proper reason. It is a point that can be a major obstacle to interoperability, but we also spend too little time on it.	
#3	This is deeply embedded in our culture, especially when you talk about the Navy, Army, Air Force and the RNLM. We are very used to arranging maximum certainty in our own task, because we always work in a very uncertain environment. And this creates a culture to properly arrange your own affairs in which things are not automatically shared with each other by nature, because you first want to do your own job well. And you slowly see the culture and the mentality emerging that we can gain something by sharing information. That goes with small steps.	
#4	This plays a very big role, this is the purpose of it. Defence organizations work together and for this purpose knowledge must be exchanged, otherwise they cannot exchange their functions. All of the above gets in the way of this, applications that make it difficult for us, we're talking about a traditional view of putting fences around information so it doesn't leak. Those things make it difficult for us. People don't want to break the law, so in a priori they are careful on the one hand, and on the other hand sometimes they can't because the data doesn't always come out of the system, because the application builder has locked it up.	
#5	This is very relevant, in terms of culture the MoD has different OPCO's, and a soldier is different from a civilian. And then there is also a difference between the citizens in the political part of the ministry, who are much more concerned with the policies and therefore often do not know well enough what is going on operationally. What also makes it difficult is that the a serviceman changes jobs every 3-5 years. So when they understand how it works, they often leave again. Defence is the only ministry whose implementation is also within the ministry and is not an organization on its own. That's why you don't just have military and civilians, but also politics vs. implementation, this makes it very complicated.	
#6	100 percent. This is very recognizable, also at the MoD, also at the OPCOs with their own strategy and culture, their own requirements and laws. A common goal is missing in 99 out of 100 cases. It would be nice if they could unite, but then you quickly end up in your own politics. This is a real and big barrier.	5
#7	Just for fun, you should take a look at the major projects and programs to see what objectives are set. And they're usually goals that everyone involved can't disagree with. They are generic goals. And certainly in a military context I have to do that with parties that I just inherently do not trust. Collaboration, they actually all say we want to work together, but implicitly the opposite is often true. And especially that difference makes it a challenge.	
#8	We are in a permanent state of competition (cyber) we have meanwhile moved from wars of choice to wars of necessity, and the policymakers does not always agree with that.	
#9	So, it is important that you have shared objectives and if they have not yet been defined, it will also be very difficult to work together. Trust is also linked to culture, if you feel that a certain culture is less reliable than your own culture, then it is also more difficult to exchange information with each other, because there is less confidence that the other party will handle the information with due care. That certainly plays a part.	
#10	They are all islands that do not all talk to each other and have different objectives and that does not always work easily.	
#11	So I think it is mainly due to the fact that we have no agreements and that it partly has to do with knowledge and partly with the unfamiliarity about how the data can help the organization and how will it ultimately will help me.	
#12	Within the RNLM we were reorganized a few years ago, so we first had a number of districts (6) and now we have one National Tactical Command. And from there, our entire operation is controlled. So internally at the RNLM there is no organizational barrier to properly store data, the structure is the same throughout the country and the operation is managed from one central point. That should make it much easier to properly arrange that structure, and also how you want to share your information and data. You see that the IT projects, somehow do not lead to the result we want, because they are so cumbersome and traditional. And also because we always place that responsibility for the IT projects outside our own organization. You should cultivate knowledge and expertise in your own organization. Interorganizational cooperation and	

	within the OPCOs is still very difficult, because I do notice that at the Police, the RNLM, the Public Prosecution Service and the NCTV everyone has the same goal in mind, but IT is still viewed very differently within the organizations. There are still a lot of ingrained, old patterns that are still very much fixated on silos and on own organization first.
#13	I want to say no. I see that this is going reasonably well between our organizations. But what I do find interesting, is that there is a rather different culture between the MoD and the rest of the government. This tends to lead to friction, nothing insurmountable, but it's always interesting to see the interaction between those two cultures.

Organizational barrier – Collaboration: A limited understanding of mutual objectives makes it difficult to build relationships, gain trust and realize interoperability. Nearly all of the interviewees (12) validated this sub-aspect, it has the second highest overall average (4,26) and there were eight suggestions for refinement. Most of the interviewees within the MoD and TNO certainly recognize this barrier. The most frequently given reason for this is the difference in culture between the OPCO's. Because of the old ingrained patterns, a lot is still fixated in silos. Therefore these organizations can be seen as separated islands with their own objectives, often building fences around information, and focussing on own organization first. This is also caused because there is regularly a lack of trust. Another mentioned issue is the differences between citizens and serviceman. Citizens are much more concerned with policies and serviceman more operationally, apart from the fact that serviceman changes jobs every 3-5 years. One of the interviewees mentioned that the MoD is the only ministry whose implementation is also within the ministry and is not an organization on its own, this makes it not only a civilian and military matter, but also a political one. One of the interviewee stated that this sub-aspect is very relevant, but didn't recognize this as a barrier, because the collaboration is going reasonably well between the organizations.

100 percent. This is very recognizable, also at the MoD, also at the OPCOs with their own strategy and culture, their own requirements and laws. A common goal is missing in 99 out of 100 cases. It would be nice if they could unite, but then you quickly end up in your own politics. This is a real and big barrier (#6). So it is important that you have shared objectives and if they have not yet been defined, it will also be very difficult to work together. Trust is also linked to culture, if you feel that a certain culture is less reliable than your own culture, then it is also more difficult to exchange information with each other, because there is less confidence that the other party will handle the information with due care (#9). This is going reasonably well between our organizations. There is a rather different culture between the MoD and the rest of the government (#13).

Interview #	Question 16 Organizational: Processes, policies and procedures
#1	Most processes and procedures are in place to enable data exchange. If they are not there, it is often because they are outdated and have not yet been revised due to a lack of people's capacity and knowledge. What often goes wrong is the interpretation of the value of data. If this is interpreted differently the process associated with this is also interpreted differently and this is more often the problem than the process itself.
#2	We are pretty good at this within the MoD. But within Defence we are often so strict about this that these are not developed from a cooperation perspective, but are developed from a security or risk perspective, mitigating risks, so that at a certain point it is no longer workable. Comply or explain, this helps a lot, we explain why we do something. The policy or process is often drawn up as “one size fits all”, which means that it often does not fit and the risk is minimised. It is well set up, but not workable, so workarounds are often made up, it should have a more open structure. From a business point of view, the SME can be ran like a one-man multinational, but that is not possible. The Air Force operates completely differently than the Navy. An aircraft meets completely different requirements than a ship. You also have to look closely at the turnaround time of information. If it takes five days to exchange information with each other and it is only valid for one day, then it is not much use. We take refuge in processes, policies and procedures, but the effect is that it doesn't always help.
#3	If you talk about basic things, we've got it right. On the operational level, we have different solutions from the different defence departments for almost the same work. There is technically a lot of overlap between all these different projects. This is still not standardized across the board, so solve similar problems in one. Anyone can shoot at the implementing organization and if you're lucky someone will say, this all looks a bit alike, this is not going well yet. You should do more demand synchronization, but this is very difficult. Somewhere in the intermediate steps we don't come together, we have to look for that. Substantive direction. Ensure that there are fewer individual questions, but much more demand bundling, control over control. The relative slowness. We have departments that speak one-on-one with the operational commander, but we have joint, we have land, we have air, for a very large part we should also look at how we want to solve this. This is all going well at the infrastructure level, but somewhere there is an intermediate layer about where that interoperability arises and on the information itself, and we should make a more generic offer there. We often leave too much behind, often due to a lack of money. We are often forced by money. Unfortunately, within the Ministry of Defence, we do not work with business cases, but with a budget.
#4	Depends on the OPCO, this has historically grown this way. I don't know if that also makes handling information more difficult. They all have access to the different systems. But at the basic level, they all have the same needs. Procedures have to be coordinated in order to work together properly. It doesn't always go very well from a historical point of view, but this is where Defence shows that you can get a square pole in a round hole.
#5	Sometimes I get the idea that we think we can manage it all centrally. But actually when you talk about interoperability, and you realize that defence consists of 4 OPCOs that all operate in a different world, you see that the RNLAF who cooperates a lot with NATO and the US, they work with certain standards. The Navy also does a lot with NATO, but with slightly different standards. The Army often cooperates with Germany. So, then it is quite strange that they all have their own partners and their own world, but inwardly they all have to work together in the same way. Then you may have to accept that they are all different organizations and that we do not have to have the same standards. You just have to define a certain basis of cooperation standards. While I've been hearing people talk about a universal data model for as long as I've been working here, but it still doesn't work.
#6	I think this is also a very real problem. When it comes to processes, policies and procedures, the different organizations have a completely different interpretation of what it means. We also see with regard to security policies that the same standard can lead to a different assessment and risk assessment. For one, hardware must meet these requirements and for the other the same rules are interpreted differently. You then have the same standard and the same law, but different policies and procedures to achieve that. This barrier is perhaps as real as the previous one
#7	I recognize this very strongly. I continue to be amazed that they always talk about classification levels, but never say which policy applies. The procedures, policies and processes are often in place, but their application is sometimes lacking. The Security Authority (BA) provides the policy frameworks, but the commander makes the decisions. And interoperability is also about knowing what work people have to do and supporting that from a security policy, because the work has to be carried out anyway. And what are we saying, you have to do your job, but how you want to do it is not allowed. What happens then, people just do their job. What do you see in practice, that people are going to come up with all kinds of work arounds, which you don't want and then you get all sorts of things that you can no longer control at all. Aligning policies and techniques are always a problem.

#8	It could be a problem, but I believe that defence already spends so much capacity on this, that if this is still not in order, someone should make decisions and say now we are going to do it like this, but we don't. We need control and clarity as an armed force.
#9	That's right, this is absolutely a condition (benchmark). You will check everything and if both parties have comparable security policies and comply to these policies, you have in fact laid the foundation for trust. Of course, what we often do with countries is use the NATO umbrella as a steppingstone
#10	I still see it too limited and not emphatically present enough. This is both internal and external. It is up to the organization to weigh up how important I think the objectives are, if I want to achieve the objectives then they must also be given a certain weight and that is still too limited at the moment. It may also be that the knowledge of IT within the organization is too limited to make this an easy dossier. As far as NATO regulations are concerned, this could be a solution, that we align as much as possible towards NATO-wide standardization in a broad sense and also include these aspects, but I wonder whether that is always smart, but now there is no guidance at all. So we now say NATO unless, so we could take over all the standardization of a Federated Mission Networking, but that would leave a lot of blind spots or things that need more insight and you don't see them coming together well now.
#11	This is where we can improve and that also requires financial investments, in order to be able to set up those processes properly. But I think that this could be very helpful if we had clearer agreements for this in order to increase trust in this way, because then as an organization you can say it is written down here. The growth of capacity is to blame for this.
#12	Often the process is more important than the result. If you complete the process, it does not always lead to the desired result. I don't mind at all that there are processes and procedures, and I don't mind having to go through bureaucracy either. But it has to lead to something and work and that is not always the case.
#13	Very applicable, you see that despite the fact that we have to comply with the same laws and regulations, you see that the implementation between the different departments often differs. You can see that in this area, but also in the management area, span-of-control, who is in charge of what. You see that those two, if they diverge, cause difficult situations, so recognizable and certainly applicable.

Organizational barrier – Processes, policies and procedures: *Distinct organizations have their own internal processes, policies and procedures. Although it is not realistic to merge all standards, it is necessary to align these sub-aspects in order to achieve interoperability.* The interviewees validated this sub-aspect twelve times and there is three suggestions for refinement. Most interviewees recognize this as a barrier. But according to most interviewees there is no shortage on processes, policies and procedures, but they think that within the MoD we are to strict. A lot of times we have to comply to the same laws and regulations. But often the law and regulations are not implemented and interpreted in the same way, which results in different processes, policies and procedures. According to one of the interviewees we often take refuge in processes, policies and procedures, which results in bureaucracy and processes which seems to be more important than the result. Next to this a lot of times processes, procedures and policies are outdated because of financial constraints and capacity, are composed as an one-size-fits-all solution and developed from a risk perspective, so are not workable. Because of this work-arounds are being created, which you can't control. According to three interviewees processes, policies and procedures have to be coordinated to work properly, so we only need standards for the same (operational) problems, on a basic level and with regards to cooperation. In other cases we maybe have to accept that we are all different organizations, so that we do not have to have the same standards.

Within Defence we are often so strict about this that these are not developed from a cooperation perspective, but are developed from a security or risk perspective, mitigating risks, so that at a certain point it is no longer workable. The policy or process is often drawn up as "one size fits all", which means that it often does not fit and the risk is minimised. It is well set up, but not workable, so workarounds are often made up (#3). Sometimes I get the idea that we think we can manage it all centrally, defence consists of 4 OPCOs that all operate in a different world, then you may also have to accept that they are all different organizations and that we do not have to have the same standards (#5). Very applicable, you see that despite the fact that we have to comply with the same laws and regulations, you see that the implementation between the different departments often differs (#13).

Interview #	Question 17 Organizational: Communication
#1	The lack of communication is annoying. Stakeholders are often not yet identified or are involved at the last minute. You should determine in advance who have an interest or share.
#2	Totally agree. I also often have to arrange this, to get things done again. I have a lot of experience in this field and I know a lot of people. You should realize that many people do not have these qualities and often only email each other. They don't call to listen to each other's points or objections. So I try to get the process going again and keep it going. Good communication promotes interoperability in a huge way, the effect of systems can often even be negated with this, but you have to have people who can and dare to do this. I know exactly who to call, who will call back and this is important because it allows you to start a process, get things done and trust each other. Soldiers are not trained for this and civilians are not always trained either. Other skills are often expected of you. There is a difference between operation driven communication and politics. When you communicate about goals, when you communicate with a foreign colleague you have to address them differently than a Dutch colleague, this just works differently. You have to respect each other and seek dialogue.
#3	Yes this is the case, but it's not the most relevant barrier for us. Interoperability may be there technically, but not in terms of targeting, I'm talking about information sharing here. If you look at the information orientation, the problem is maximal, because we talk past each other and do not have the same goal in mind.
#4	It's possible, it's very personal. It goes beyond professionalism, but it is incidental.
#5	That certainly applies. At the level where TNO and the MoD cooperate, there is a different picture of what the two organizations are and how they are related to each other, than at the level where it is decided to cooperate. All Defence Research and Development (R&D) has been outsourced to TNO and there is a kind of legal extension in it, we also often contribute to NATO panels on behalf of the MoD. However, some things are not arranged properly, which prevents interoperability. Poor coordination and communication between the organizations leads to frustration and undesirable situations within the collaboration. Everyone thinks that everything is well organized, but nobody really knows what the preconditions are.
#6	This is also interoperability, but on the (semantic) personal level. So that's kind of circular reasoning. There is no interoperability because you can't talk to each other and you don't talk to each other because there is no interoperability. In a broader context, but then I think you are on the finesse of it, within NATO you have different armed forces, each with their own doctrines. A doctrine is actually a representation of the combination of culture and environment. And then it is only logical to establish that the doctrine of one country is drawn up differently and has a different effect than the doctrine of another country, often a middle ground (false compromise) is chosen, joint doctrine. The middle is the best truth, to me that is a classic fallacy and not the intention. I think interoperability should also ensure that it is relevant and relevant within your cultural environmental context and not that you both have to compromise a little. So it has to fit into the world view and it has to fit into the other person's world view as well. And what do I have to arrange in our communication to get that done.
#7	Very recognizable, then they just say we have a Cross domain solution, and I say what's in it, because I have no idea. What exactly have you built, they often can't explain that and then you get the problem, how do I even get it accredited or with whoever has to make policy wise decisions. I think a very large part is due to security people who can't properly explain what they are doing. They often cannot make the translation of how it works functionally.
#8	Practice what you preach, the top layer often does not do it themselves, they are often no longer involved in managing staff, but more with himself. A little clarity and sobriety is allowed and tell it like it is, where a lot remains vague, you are just not clear and a lot is left open.
#9	Understanding each other is certainly an important aspect, otherwise you can talk past each other for a very long time. That happens every now and then. Communication is important to make things possible, but of course even if it is already working well, you also have to keep communicating with each other. Context of how you read and appreciate things is of great importance and this is also linked to culture.
#10	For me, this is related to collaboration, which includes communication. Everyone has their own political agenda, which we often see reflected in the boards that have to decide on certain projects and that does not always benefit interoperability. And that is where open communication or directing communication is desirable. Culture will certainly play a role. Within the military culture there is still relatively little attention at all for supporting the process and IT in particular. Culture is also a leadership culture where risk-avoiding behaviour is rewarded in my experience. Complex files often ask for some risk to be taken. And within the OPCOs the interservice rivalry, across all axes, is recognizable and problematic.
#11	I can't rate this one properly.

#12	This one certainly applies when you're talking about collaboration between multiple organizations. Often the organizational interest is put above the broader social effect and that is very understandable, but not good of course. I notice that within Defence you already have many different cultures. Subcultures even within Defence, they are already very different and it is difficult enough to connect them with each other. If you then look outside your own organization, it becomes even more complex. If you sit down with the experts, I notice that things get better pretty quickly, but getting it approved by the policymakers is another story. I get it too, because it's much more complex, but we have to find a mode for that.
#13	Certainly recognizable and important, but I think we are getting better and better at this. I think a group of people is emerging on both sides of the organization who really know how to find each other and that group of people is getting bigger and bigger. So that's going in the right direction

Organizational barrier – Communication: *Poor communication frustrates interoperability, hinders collaboration and may cause undesirable situations.*

The interviewees validated this sub-aspect eleven times as and there are four suggestions for refinement. This is not the most relevant barrier for us, but understanding each other is an important aspect, because we sometimes talk past each other according to two interviewees. A other interviewee mentioned that stakeholders are often not identified, which makes communication very difficult. One interviewee states that this is a kind of circular reasoning. There is no interoperability because you can't talk to each other and you don't talk to each other because there is no interoperability. Three interviewees stated that this barrier often has to do with culture within the organization, but if you look outside the organization it becomes even more complex. One of the interviewees says we are getting better and better at this and are going in the right direction.

Understanding each other is certainly an important aspect, otherwise you can talk past each other for a very long time. That happens every now and then. Communication is important to make things possible, but of course even if it is already working well, you also have to keep communicating with each other. Context of how you read and appreciate things is of great importance and this is also linked to culture (#9). This one certainly applies when you're talking about collaboration between multiple organizations. Often the organizational interest is put above the broader social effect and that is very understandable, but not good of course. I notice that within Defence you already have many different cultures. Subcultures even within Defence, they are already very different and it is difficult enough to connect them with each other. If you then look outside your own organization, it becomes even more complex. If you sit down with the experts, I notice that things get better pretty quickly, but getting it approved by the policymakers is another story (#12).

Interview #	Question 18 Semantic and Syntactic: Data standards
#1	The general defence architecture. This should not be left to the OPCOs themselves, but should be managed centrally. You have different data standards and data types. It doesn't matter which one you choose, but if you leave this open it will be very difficult to merge everything together. I think that the MoD should choose a number of standards for a number of aspects and also see whether these standards communicate with each other. If we choose something new within defence or within a particular OPCO, it must comply with the universal (data) standard. Data standards are important, but you also have to attach the same concepts and context to them. You can't do one without the other, they have to be on the same level.
#2	This certainly limits the data exchange. The question is always what you want to do with certain data, what is the context, or the date. Personal data may be normal data for the outside world, but for an investigative service such as the RNLM this data may have a completely different value or meaning. This distinction is often not made and if you look at standards it sometimes goes wrong on diaeresis, addresses with house numbers sometimes written together, sometimes a separate field. In many cases you would simply have to have the same systems for this, because with the systems that are now there, for example, there are already five different ways to display an address. A system forces you to fill in certain fields, but this is not always possible, for example if someone is homeless, and sometimes the selection lists are not complete.
#3	There is a lot, but there is also still profit to be made, but then I would emphasize the time-critical matters and high impact, that we all have a good overview of this. And if you look at information-driven action or multi-domain action, we're going to look closely at what are the most critical business processes and look primarily at the data standards. There is a lot to gain from data standards in business operations, but this mainly concerns efficiency gains.
#4	Quite a lot of research has been done. But the standards it produces lag behind technological developments and the procurement process does not put an end to that.
#5	If you don't have standards, then the data you exchange actually means nothing. Within the standards, the focus is often much more on syntax and less on semantics. Defence and TNO do not exchange much operational data, but mainly reports. But what you write differs semantically per OPCO, you use different terms and words. We often perform operational matters within the defence environment. What often is a limitation is the exchange of software. Data is sometimes shared from specific systems. Because TNO and the MoD have no formal link, data standards do not really play a role. Within the MoD standards do play a role, because the various OPCOs work together with other external parties, but this applies more to the standards of the external world than to the standards of the MoD itself.
#6	My name contains a special character and although there are plenty of standards, so that should be very easy, we still can't. Those standards still leave room for interpretation. So, I agree with the statement, I do know there are too many standards. Perhaps you should allow 1000 data standards, so that you can clearly indicate which standard in which variant and with which context you mean here. I think that will yield more than an all-encompassing data standard.
#7	This is taking off quite a bit, I know that from TNO, among others, that all kinds of departments are working on this. If you make a certain choice, don't close yourself off from a very large set.
#8	Please take the NATO standards,
#9	This is something we often try to do, because if we want to work together, you look for a common standard, and if you are going to work together for a very long time, you also look at whether you can record this standard, so that companies can use this protocol. You need standards to be able to exchange things properly and more easily and also available in the market, but companies often find this a bit more difficult, because they want to keep you inside and then they cannot be replaced by another company. I think we also strive for standards within defence, because if no agreements are made about what I receive from you, then it is very difficult to interpret, what to do with it and in which system can I process it. So standards, and that is of course also related to the technical barriers, are simply needed.
#10	What makes it difficult and that is often said, federated mission networking unless, NATO unless, which seems very logical for Defence, but if we look at the broader development, then we also have to look at standardization from a national perspective, and think about data standards. In both areas, there is a lack of proper guidance, or the dossier is incomplete, so in the end it is a development in which many steps still need to be taken. And fundamental choices have to be made. There is a need in how to deal with NATO where this does not meet national wishes. I want to become interoperable with NATO partners in a military context and the world is not just a military context, less and less I think, more and more hybrid. So I think the most important thing is to first think about what we want with data standardization in a broad sense.

#11	Move towards standardization more, so with a data catalogue, which we would like to have a protected data catalogue, it's either organized diffusely or it's not there, in that sense it would be useful. I think there is no shortage of data standards, but more with the cuts in many staff functions, a lot of knowledge has just been lost.
#12	It is useful if you all use the same data standards. But if you know which data you need, you can also convert it yourself within your own organization to a way that is interpretable for you. So then you can leave that translation to the user and also the responsibility for cleaning and data quality. Without common data standards collaboration is impossible, I don't think so. I think it's still possible, but it's more difficult.
#13	Hugely applicable. As organizations we process large amounts of data, there are of course standards within the government to model this data, there are architecture standards for this and this is very important. Otherwise you are only transferring and transforming data, instead of sharing it or using it together, so very important.

Semantic and Syntactic barrier – Data standards: *Without common data standards, collaboration between organizations is impossible. Although it is very important to have data standards, there is almost no research with regards to achieving interoperability by using data standards.* The interviewees validated this sub-aspect twelve times and there are four suggestions for refinement. Although there are different opinions regarding this sub-aspect, most of the interviewees agree on the fact that it is important to know which concept and context has been attached to the data to be able to interpret it in a correct way. Otherwise you are transferring and transforming data instead of sharing and using it. One of the interviewees states that a lot of times software is a limiting factor, because data is shared from specific systems. For this reason data standards within the MoD should be managed centrally, instead of within the OPCO's. In this way we can comply to certain standards when something new is being introduced. For the above mentioned reasons this sub-aspect is also recognized as an important part of the framework.

If we choose something new within defence or within a particular OPCO, it must comply with the universal (data) standard. Data standards are important, but you also have to attach the same concepts and context to them (#1). Perhaps you should allow 1000 data standards, so that you can clearly indicate which standard in which variant and with which context you mean here. I think that will yield more than an all-encompassing data standard (#6). Please take the NATO standards (#8). It is useful if you all use the same data standards. But if you know which data you need, you can also convert it yourself within your own organization to a way that is interpretable for you. Without common data standards collaboration is impossible, I don't think so. I think it's still possible, but it's more difficult. (#12).

Interview #	Question 19 Semantic and Syntactic: Dictionary
#1	Value, where we sometimes rate data at a higher value, sometimes perhaps too high, it is valued lower by others or vice versa. What we literally mean by it and how valuable we think it is, can be different due to interpretation.
#2	We often don't have this, we often don't know what something means.
#3	This is less relevant. You quickly find out things when you work together for a while. A dictionary is no longer of this time.
#4	I recognize it, but it's not a super interesting part.
#5	I don't think those dictionaries are there. I do notice that it plays a role and not everything means the same within the MoD. The word operational, for example, sometimes means the performance, sometimes the level of operational in relation with strategical, operational and tactical (SOT), and in the civilian world the latter two are even reversed (STO). You will learn all this in practice.
#6	There should also be formalized standards for this.
#7	We use the same word, we have exactly the same definition and yet we mean something different. The label often implies that we are talking about the same thing, but we check very little whether we use the label in the same context and within the same scope and therefore use the same criteria. And 9 times out of 10 we are just talking past each other. So dictionaries can certainly help with this, but especially for what does that actually mean and how do I apply it.
#8	Sure, we've done it before.
#9	Data standards is implicitly linked to the mutual exchange and dictionaries, if I get something from you am I reading it correctly or do you mean something else by it. We think we can speak English, but if you compare it with an Englishman you will notice that he has completely different nuances and uses every word in a slightly different context than we use English.
#10	In a broad sense, Defence is also very specific in its wording and the meaning of words can be different in different contexts, so yes it is important. This one, for me, is a bit related to ontology. This goes into a lot of detail, but I think it's an important facet in itself, because in order to understand the world I have to speak the same language first, otherwise we all have different interpretations, and that's why this is another important element. For me more on a micro level, first answering the parent question, but also recognizable and relevant.
#11	Nothing is standardized. The RNLM has now started with a reference list, which is very nice and it is now all starting to simmer a bit that it would be nice if we could also take up this defence-wide. We are still in its infancy here.
#12	This is true.
#13	Applicable, but I think this is primarily due to the manual and guideline that are available for the various departments and functions. To be honest, I expect to a certain extent that when you perform a similar function on both sides of the organization, your activities are so similar that you have comparable dictionaries. Appropriate, but less than the rest.

Semantic and Syntactic barrier – Dictionary: *To be able to use the exchanged data, dictionaries are needed to interpret and understand these data.* The interviewees validated this sub-aspect eight times and there are three suggestions for refinement. Five of the interviewees stated that this barrier is relevant, but much less than others. One interviewee stated that a dictionary is no longer needed. Others mentioned that dictionaries are often not available, so interpretation can be an issue, because not everything means the same within the OPCOs. But according to two others most of the time this is learned in practice.

This is less relevant. You quickly find out things when you work together for a while. A dictionary is no longer of this time (#3). We use the same word, we have exactly the same definition and yet we mean something different. The label often implies that we are talking about the same thing, but we check very little whether we use the label in the same context and within the same scope and therefore use the same criteria. And 9 times out of 10 we are just talking past each other. So dictionaries can certainly help with this, but especially for what does that actually mean and how do I apply it (#7). In a broad sense, Defence is also very specific in its wording and the meaning of words can be different in different contexts, so yes it is important. This one, for me, is a bit related to ontology. This goes into a lot of detail, but I think it's an important facet in itself, because in order to understand the world I have to speak the same language first, otherwise *we all have different interpretations, and that's why this is another important element. For me more on a micro level, first answering the parent question, but also recognizable and relevant (#10). Nothing is standardized (#11).*

Interview #	Question 20 Semantic and Syntactic: Language
#1	The explanation we give can be different. In our organization we have abbreviations, we sometimes have the same name for two very different things. Even some systems, with a different classification level, have the same name. This can be very challenging.
#2	This is also very different. This is certainly a barrier, especially if you want to exchange information internationally. Some systems are in Dutch, and then you have to translate everything, but this takes time, but also an understanding of the country where the information comes from. Military strategic, operational and tactical are in business strategic, tactical and operational, which is the other way around.
#3	Sometimes still room for improvement, especially when we look at the multi-domain performance. We can still put some energy into this for the important things. So that we can understand each other better. Within IT there is a lot to be gained with an unambiguous architecture, many architects all have a different language and therefore very easily talk past each other.
#4	This depends again on the OPCO and a bit the same as with the dictionaries, we make it work.
#5	It does apply, but at the same time one common language is not going to happen. You will have to accept that different languages are spoken in different domains. If someone speaks a different language, you know that you have to make an effort to understand the other person. But if you think you speak the same language, but your dictionaries are different, things can get complicated. The situation where you think you are using the same language is much more dangerous and difficult.
#6	This one can also be related to standards.
#7	This certainly applies. Even if you think you speak the same language, you have to stay focused and check if there are any deviations. This really takes some skills to do well.
#8	There are things to keep in mind.
#9	Perhaps you should try to separate this into the human aspect and the technical aspect, because I notice that semantics, syntax, and technical barriers are now a bit mixed up. I would perhaps make the blue part (Semantics and Syntax) a bit more human-human, and partly link it to the technical aspects. I don't know what it means for your model, but human-human exchange and technical exchange are necessary to make things happen. Because you now have legal, organization, people and technology. That would be the fourth division, maybe you have to transfer some things from the blue part to the yellow part. That makes the whole thing just a little sharper.
#10	I interpret it here a little more technically. You actually see that the direction is missing. What does our landscape look like, what do we want with that landscape and what ensures interoperability and now it is a very diverse landscape with little control. What I found most interesting with the introduction of GrIT was, here we are thinking about how we are going to introduce legacy applications to GrIT, it seems like a logical idea, but this is actually reasoning completely towards the error, because you actually have to look from the other side, reasoning from the guidance, which standards should my applications meet, which I want to have installed instead of the other way around. In a broad sense, this is also recognizable as a problem and relevant. This has been the opportunity to start with a greenfield, but we didn’t, so I think this is going to cause problems. But especially when I think interoperability is important, these are the points on which I can steer and think about. So, we also lack direction in a broad sense
#11	The entire NATO cloud hangs a bit above this.
#12	Yes, it is certainly true, that language is certainly important that you make agreements about it, but perhaps technology can bridge it or enable us to mitigate those language barriers (partly), so that we use it in a smarter way to deal with.
#13	Not very applicable.

Semantic and Syntactic barrier – Language: *Different (modelling) languages and terminologies impede the exchange of data. Without a common language it is very complicated to communicate and interoperate.* This sub-aspect has only been validated seven times, it has the lowest overall average (2,72) and there was one suggestion for refinement. According to four interviewees this sub-aspect is not very applicable, it is something to keep in mind, but we will make it work. According to four other it is important to stay focused, because everybody has its own specific abbreviations, with other meanings, this can be very challenging. Also internationally, when you think you speak the same language, but you use different dictionaries, things can get dangerous. Also, within the IT there is a lot to be gained on this sub-aspect. One of the interviewees suggested to separate the semantic and syntactical barriers into the human aspect and the technical aspect, because the semantics, syntax and technical barriers are now a bit mixed up.

The explanation we give can be different. In our organization we have abbreviations, we sometimes have the same name for two very different things. Even some systems, with a different classification level, have the same name. This can be very challenging (#1). This is certainly a barrier, especially if you want to exchange information internationally (#2). Sometimes still room for improvement, especially when we look at the multi-domain performance. Within IT there is a lot to be gained with an unambiguous architecture, many architects all have a different language and therefore very easily talk past each other (#3). if you think you speak the same language, but your dictionaries are different, things can get complicated. The situation where you think you are using the same language is much more dangerous and difficult (#5).

Interview #	Question 21 Semantic and Syntactic: Ontology
#1	The word itself is new to me. I don't think we're at this level yet. We must first have the data standards up to standard. It is important to be able to differentiate and to do this quickly, so you can distinguish this is interesting and relevant and this is not.
#2	Absolutely agree. If you want to transfer data and then large amounts of data between different units, this is a recipe for failure. Interpretation and context are of great importance here, what exactly are you looking at. You have to be very well-informed before you take action, know what you are talking about, if there is a lack of knowledge, you have a good chance of making a mistake.
#3	This also applies.
#4	This is kind of the story of the companies that are ahead of the standard, and in doing so, are actually creating a new world that goes beyond the standard. Standards lag behind developments. You can't really counter this either. So you are held to standards that are lagging behind.
#5	This is very applicable.
#6	Interesting, because that implies that an ontology is possible for interoperability. I would say that is I think a domain argument. As Defence or NATO, I think you could very well draw up an ontology for the concepts that are relevant within your domain. And you can agree on that ontology and what that ontology adds to a taxonomy is the relationship and the travers ability of those relationships, which is an extra aspect on data. So I don't believe there's any kind of canonical ontology possible, but I do believe that within your context, say the MoD, you should be able to define an ontology, where you get very explicit about how we see certain things and how it's connected and how you're going to get from one understanding to another as well.
#7	I have less experience with this and I actually have no insight into what happens with this.
#8	You just have to standardize this as much as possible, and where there is no other way, you have to do it differently. But you really have to choose a standard. We often don't start, we talk about it over and over again, but we don't build and don't start. Can't we just do learning by doing, implement something and go from there. But someone else often thinks differently about it, so it doesn't happen.
#9	I think in a time of critical communication then I completely agree with you, but if you have the time to fight it out among yourselves, you will work it out among yourselves. But in time-critical situations it is of course a drama to spend a day trying to find out exactly what the other person has said.
#10	I can think of anything, I can start using NATO ontologies, but these are often incomplete and then I will also commit myself to the English language. Then the question is, do we want this, I think we do, perhaps not. And then there is a lot missing in the ontologies. Then we will have to think for ourselves about how we want to solve that. And if there is a lack of direction, you will create a landscape that will become more difficult to interoperate.
#11	This is one step deeper than languages. I'm not familiar enough with this.
#12	I think you have to be careful not to make your ontologies more important than the overarching principles that those ontologies should be under. The point is that you create joint solutions and that you can store your data in them. It's nice if you have everything the same, but it shouldn't become a kind of religion to coordinate those ontologies exactly, because then you will never come to cooperation
#13	This very much depends on who you ask, but I think it's very important. Uniformity in data is very important, especially for your retrievability and your lineage on your data, this is very important.

Semantic and Syntactic barrier – Ontology: *Due to an overload in data, many ontologies are created without standards or commonly agreed representations. For this reason, ontologies remain uncorrelated and fragmented. Which limits the exchange of data interoperability. E*ight interviewees validated this sub-aspect, it has the second lowest overall average (2,90) and there were no suggestions for refinement. Three interviewees indicated that the sub-aspect ontology was new for them or that they were not familiar enough with this aspect. Four interviewees indicated that it is (very) important to have standards and uniformity within data, one of them added that it is especially important for retrievability and lineage and one interviewee said only in time of critical communication. One interviewee stated that there is no ontology possible for interoperability itself, but does believe that within a certain context, like the MoD you should be able to define an ontology. Another interviewee stated that you have to be careful with ontologies, that they don't become more important than the overarching principles. It should not become a kind of religion.

If you want to transfer data and then large amounts of data between different units, this is a recipe for failure. Interpretation and context are of great importance here (#2). I think you have to be careful not to make your ontologies more important than the overarching principles that those ontologies should be under. The point is that you create joint solutions and that you can store your data in them. It's nice if you have everything the same, but it shouldn't become a kind of religion to coordinate those ontologies exactly, because then you will never come to cooperation (#12). Uniformity in data is very important, especially for your retrievability and your lineage on your data(#13).

Interview #	Question 22: Technical: Infrastructure
#1	We have a lot of legacy systems, which technically shouldn't be a problem, because there is a solution for everything. But it requires a commitment from the organization that wants to change this and go back to the drawing board and to lay the foundation again. You have certain hardware and software within systems that don't talk to each other. But the biggest risk, due to years of cutbacks, is that systems are so outdated and not kept up to speed.
#2	It is not such a problem within a pillar, if the organization is not in the same pillar and works with a different system, then it often becomes difficult and people resort to USB and e-mail. If it becomes more specific than internal use only, it often becomes difficult.
#3	It applies, but not as shown here. It asks for common data models, that's what it's all about. They need to provide good integral insight and harmonize with each other within the organizational units, that is much more relevant, we do have architects who do things in general terms, but really the data models tuning to that level, that happens far too little.. But for this you need to have an integral insight into where a data object is created and where it is all used and how we can reuse it.
#4	If it doesn't work, you make it work. We often say that we can't do something because we think we can't do something. I'm much more optimistic.
#5	This is very much applicable, often, this is not due to the technology, but it is still not operational, because it has stalled because the various security managers do not agree (trust).
#6	There are measures in the area of the information domain that prescribe that they may not be physically linked to each other. That seems to me to be an obvious limitation for interoperability. So that must be separated with diodes, for example, which makes it more difficult to interoperate. And what it actually does is emphasize the whole specific interaction. So that means that we're going to have to talk more closely with each other, and that's a little contradictory to interoperability. So some of the agreements that we make, work against interoperability, but it doesn't make it impossible. The infrastructure shouldn't really matter, it's an enabler for communication, at the same time there are sometimes restrictions, infrastructure should in theory be able to enable just fine, but we are so afraid that we physically want to see that infrastructure separately from each other. Then I think it will be a disabler.
#7	I think from my perspective all these new technologies, it offers functionality, but the problem with interoperability and then more in the context of security, to what extent do we have the assurance that it works well. There are quite a few technologies that functionally do the same thing, but assurance wise I have no idea at all whether we will reach the same level. In addition, who actually makes that system, who is in control of that system. So I think when you talk about technical barriers that it's mainly in the context of interoperability and enabling things, do you have enough confidence in the technology. Often things are already in place before there is a policy.
#8	There are ideas to get a certain connectivity with CSD's that you take one main network, to which you can stick these CSDs. But often it has to do with money and other choices. We keep saying this should be possible and that should be possible, but if you never implement, it will be different again in about 5 years and then you will have nothing. You are always behind, but accept that and start somewhere. People who all think they are doing the right thing, but they don't, this has to do with management and clarity. You can always deviate and always choose your own path and sometimes is seems almost a hobby, but there is no management who acts on it.
#9	-
#10	The funny thing is actually that the infrastructure is quite interoperable in general. But if we look at the network level, then we all have different networks and then it is all suddenly no longer interoperable, so there is also a very big problem there. Success is now being made with HGI baseline GrIT networks, but we are still a long way from solving that problem.
#11	I think what limits this is not so much in the lack of platforms, but more in how that platform looks and to what extent it is influenced by other aspects, so such as legal aspects, privacy aspects and capabilities.
#12	This is a gigantic challenge. GrIT is based on requirements from 5 or 10 years ago. But in the last 5 or 10 years the whole world changed very quickly. I really see this as a big showstopper if we don't deal with this smartly in order to be able to take the steps towards a modern IT organization. GrIT's principles were good when they were created, but the world is changing. We have to deal with the way in which we approach these kinds of large projects. We try to eat the whole elephant at once, maybe you need to experiment a little bit more.

#13	Infrastructure is extremely important for cooperation. That has to fit together, that has to work together, that should preferably be uniform, but often the technology is not the problem. This requires a serious investment and then it becomes a consideration whether we are going to make that investment or not. That is often a multi-year plan, and you also often have to bring in other personnel or train and retrain your personnel, which is also an investment.

Technical barrier – Infrastructure: *One of the main issues is to establish interoperability among platforms. This is created by the use of multiple different information systems. The data and technology evolution is still ongoing. This asks for an advanced technological infrastructure and software.* Eleven interviewees validated this sub-aspect and there are two suggestions for refinement. Four of the interviewees say that the technology is often not the problem. The infrastructure in general is quite interoperable, especially within the own OPCO, but sometimes it is outdated. Where it often goes wrong is due to security policies, people who disagree with each other, software, different networks and/or a lack on investments. One of the interviewees indicates that is it is a problem, but not as shown here. It is due to a lack on common data models. This sub-aspect proofs to be a relevant aspect for the framework.

There are measures in the area of the information domain that prescribe that they may not be physically linked to each other. That seems to me to be an obvious limitation for interoperability. Some of the agreements that we make, work against interoperability, but it doesn't make it impossible. The infrastructure shouldn't really matter, it's an enabler for communication, at the same time there are sometimes restrictions, infrastructure should in theory be able to enable just fine, but we are so afraid that we physically want to see that infrastructure separately from each other. Then I think it will be a disabler (#6). The funny thing is actually that the infrastructure is quite interoperable in general. But if we look at the network level, then we all have different networks and then it is all suddenly no longer interoperable, so there is also a very big problem there (#10).

Interview #	Question 23 Technical: Resources
#1	It often involves the knowledge and skills to know how to get this data to the right place, which is a bigger problem, and knowing where the data is or is located. A solution can be a hit and no-hit database. In this way is it clear if certain data is available and in which direction it can be found, that would help a lot.
#2	People often know where to get information in general and from which systems. The availability is often reasonable, but then you have to find the right person who can get it out of the system. The question is also whether you can use the data for the purpose you are pursuing. The data is often separated between people who can extract the overview (metadata vs. case data).
#3	Few people have an integrated picture of all the information that is available and the way in which it can be made accessible. I think everyone has an idea of their own silo from their silo, but not integrally.
#4	This is something I recognize very much. This is happening on a continuous basis. The catalogue is missing, but if it were there, which is also limited by the search function on the intranet, then it is not consulted well enough. A Catalogue should just be there. What you would like is some sort of base layer of information services within all classification compartments. You have a kind of operational base layer. You should be able to make that definition and you should also be able to enrol the systems you buy into this base tier. So that everyone can be connected to this basic layer We also have to investigate the official solution, so that we know that it is allowed, but now we are not allowed and we do not dare.
#5	Yes, there is, but we have never reached this level of cooperation between Defence and TNO and if you do not first overcome a number of other barriers, this alone will not help.
#6	Making data streams findable and usable is definitely a barrier coupled with the human tendency to get on top of it and rake it together. I think that's the lack of insight or not having it user friendly that feeds the tendency to rake it to yourself.
#7	This is relevant, especially when I look at “it should be user friendly and available when needed”. This means that you know when you need what kind of information and that is demand-driven looking at data and technology. And what is happening now is very much supply driven. Whether I can automatically do something with it, that is not a given.
#8	I think everything is possible within the Central Staff, but outside of it is only possible if there is a certain advantage and this is not always the case. So at that point we often no longer think in terms of defence or the Armed Forces, but to what extent does it help the Central Staff. There is also too little insight into what is available within Defence, you should have a central overview. Back to basic.
#9	I think this certainly plays a role, user-friendly is ultimately how we deal with it as humans. But availability means the organization has the people, technology, and IT available to make this possible. You have to start with the organizational interest first and then you automatically get to the point where you actually make the resources, people and machines available to realize this.
#10	So on all sides I miss the data or I don't have reliable data or I don't even know that the data exists. And it is also important to distinguish between peace operations and a traditional military operation. Data availability is an issue on all sides. This is one mechanism, and we have a whole lot of mechanisms that hinder integration. Security and policy is also one in a broader sense, networks and infrastructure is a third
#11	Links are a big issue and I wonder whether data quality is also part of this or whether it is more of a different technical aspect. The availability is certain, we have also written in the Defence memorandum and the Defence vision that we have the risk of drowning in the large amounts of data we have. But the availability of well-qualified data is still an issue, and so is findability.
#12	If it is only applies to data, then it is quite difficult. But I notice that if you explain what you are doing, people understand that what you are doing is necessary.
#13	Availability (BIV, availability, integrity and confidentiality triangle) of information and information systems is perhaps the most important.

Technical barrier – Resources: *There has to be a proper insight into the resources which are being used by an organization. The resources should be user-friendly and available when needed.* Twelve interviewees validated this sub-aspect and there is one suggestions for refinement. Six of the interviewees recognize this sub-aspect and stated that this is often an issue due to a lack of availability, findability or existence of (well-qualified) data. Four interviewees stated this is due the fact that there is no integral idea and, central overview or catalogue available. Within each OPCO people generally know where to find the information, but often you have to find the right person to extract it. There is also a lack of a proper search function, a base layer of information services per classification or a hit/no-hit database.

There is also too little insight into what is available within Defence, you should have a central overview (#8). So on all sides I miss the data or I don't have reliable data or I don't even know that the data exists (#10). We have the risk of drowning in the large amounts of data we have. But the availability of well-qualified data is still an issue, and so is findability (#11).

Interview #	Question 24 Technical: Data integration
#1	Our problem is that we always want that old and new can work together, but sometimes we just need to migrate the old system to something new. Sometimes you shouldn’t want everything to work together, but choose for something new and then build on it.
#2	This is also a tricky aspect. A lot is integrated at the RNLM and it is also a data-intensive organization that practices little, but does things 24/7. The RNLM, for example, is almost a logistics company. Often when new systems are introduced, old systems are switched off and data migration is difficult, so this is often not done as this is very laborious, because the old system is no longer maintained. If the information is still available, it often has to be searched for in the old system. This is also difficult with the GDPR, because people often ask why we keep information for so long. But the old system does not have these thresholds, because it concerns historical data.
#3	We are now setting up new IT and that has to work together with the old IT, which makes it many times more complex than if you were to build Greenfields. You now often have an old-new integration problem. This is a major challenge for our organization.
#4	This is a bit like infrastructure, we will make it work. Don't think on forehand, we can't do this.
#5	It is very applicable, but not between TNO and Defence, because we are not connected. But what you actually see now, within the MoD, is that GrIT actually comes as a new environment and that the applications are converted to GrIT, but they are still the same separate applications, you don't get a greenfield, while some people thought that that would happen. Centralization is cheaper, but this does not help to overcome technical barriers. The experience of GrIT is that people think that we have a technical environment that we can access everywhere, but it is only technically one world, the data remains separate. If you think that technology is the solution, then every technical project ends in failure, it is only a precondition. I see this happening a bit at GrIT as well. The technical barriers are preconditions. You are in one world, but mutual cooperation is still difficult.
#6	This is a very real barrier in certain scenarios. I do have the idea that thinking and technology are now becoming available, which will help with this, but have not yet been widely introduced at the Ministry of Defence.
#7	Defence mainly suffers from the fact that it has to work together in very dynamic partnerships.
#8	This is all possible.
#9	Try to write down your policy in a relatively normative and somewhat abstract way so that you have room for implementation and therefore also give some room for interpretation, and not all of it is exactly described. You also try to write it down in a somewhat generic way that different types of techniques can make use of the same policies. What people find very difficult is how do I make the translation from the generic policy to my specific application. Sometimes something is black and white and for others there is room for interpretation, which sometimes makes it special, in what context do you read it, while you are in the same organization and yet you both read it differently. But not because you necessarily want to read it differently, but because it is apparently read differently by one person. I always find it a nice challenge, that if it is not allowed to go left, how can we make it possible, so think along a bit. One explains it very precisely and the other explains it from the spirit in which the law is written. Demonstrate that you have followed the procedure, that it has all been done in accordance with the law. The GDPR is a good example of this.
#10	This is a huge problem. This is actually quite easy to solve technically, but there is a lot around it. Security policy, standardization, but data integration I think is very important in the goal of reaching IGO by 2035, and the attention paid to this is relatively low I think. Technology is still a barrier for us, even though this should not be the case.
#11	There are other challenges, which are preconditions for this.
#12	This is a very big problem. We also have systems here that are about 25 years old. Because there is no innovation and the projects all take so long, you cannot integrate them into your chain in a modern way.
#13	Certainly important, but data integration always comes down to a choice. Of course you can always choose to continue using two systems side by side, in the end that comes down to a choice you have to make, yes or no. So yes important, but not very important.

Technical barrier – Data integration: *Old and new systems have to be interconnected with each other, which also contain several types of soft- and hardware. It is a serious challenge to integrate heterogeneous data which is originating from different information systems and networks.* Nine interviewees validated this sub-aspect and there is one suggestions for refinement. Three of the interviewees indicated that this should not have to be a technological problem. Because technology is not the solution, it is only a precondition. Four interviewees stated that the problem within the MoD often has to do with old-new integrations, which is more complex than setting up a new system and migrate the old one. There is a lack of innovation and projects are taking too long, so they cannot be integrated into your chain in a modern way. A other interviewee stated that Defence mainly suffers from the fact that it has to work together in very dynamic partnerships.

Our problem is that we always want that old and new can work together, but sometimes we just need to migrate the old system to something new. Sometimes you shouldn't want everything to work together, but choose for something new and then build on it (#1). We are now setting up new IT and that has to work together with the old IT, which makes it many times more complex than if you were to build Greenfields. You now often have an old-new integration problem. This is a major challenge for our organization (#3). This is a very big problem. We also have systems here that are about 25 years old. Because there is no innovation and the projects all take so long, you cannot integrate them into your chain in a modern way (#12).

Interview #	Question 25 Technical: Technical communication
#1	If we believe that the value of the data is so high, you don’t want to send it wirelessly over certain means of communication or make use of a public cloud. A other issue is that we are purchasing more and more services outside the MoD (outsourcing), these companies work with new standards that make exchange much easier, but do not always deliver the guarantees that we want. Those technical aspects make it difficult, because they look differently at security or how data should be handled. The systems and the technical aspects they use are intended for the environment and the setting in which their product has to operate, and the MoD still had until recent the idea of the "wars of choice", we choose when the moment is right and then we enter the operation. But nowadays with the digital domain, it is no longer a choice when you are in a conflict, because with digital systems you are always in conflict. Where the standards for a commercial application work well, we have to prepare for a different context. We have sometimes lost sight of that different context in the recent years, that is where the discrepancy lies.
#2	This isn’t a real problem, this usually goes well. If it is already at this level, then you have already had and settled the three previous sub-aspects. Technical communication does not often stand on its own.
#3	This is important and not on the static situation (IP) because it all works fine there. But we have interrupted communication and different technical forms of communication (radio, ip, satcom) and especially switching between these different options in an operational situation is very difficult. I think that this has been properly arranged for a number of defence units, including with regard to interoperability for their direct task. But for the joint task, there is still a challenge.
#4	Documenting is an eternal craft. Documenting is difficult and no fun. Documentation is therefore invariably incomplete. The standard for documentation is also terribly difficult to make and adhere to. That said, I've read very good documentation, so it's possible. There is still a whole bubble around it, from input, training, exploitation, all of which also have to be arranged. This is not necessarily an interoperability problem, but a communication problem, this concerns the organizational part, due to a limited understanding and because of internal processes.
#5	There are guidelines of what you are not allowed to do, but they are so strict that they are often ignored because it is not workable (work around). Because there is often no formal arrangement, information is exchanged more easily, but methods are used that are not safe (enough). Ignoring often has advantages, but the disadvantages are often not considered.
#6	I think sometimes we introduce self-imposed barriers, because of safety features or because of this is the standard here and this is the standard there. So I think when you talk about technical communication, with packets and networks, it runs smoothly. So, I don't really see a problem with that.
#7	You certainly see with the older systems that it is not always known how it has been implemented. So you have to coordinate things with the collaboration you are in at that moment. Also with the alignment of your doctrine, how do you actually do things.
#8	It is a matter of, if you have the platforms, which shouldn’t be too heterogeneous, it can be queried from a central network by means of CSDs. Say you take one main network that everyone can use, then you can query the network through CSD's if you are authorized to do so and you can compartmentalize it if you wish. This would give a lot of possibilities.
#9	For me, this is also a bit in data standards and how do I explain things, old and new systems. So, for me this overlaps with the other sub-aspects.
#10	This is related to the previous question. Ultimately, you need good data interfaces. One is the technical side, the network side and the other is the interface itself, the software side, we are missing this part and that hinders the possibility of integrating data at all. Because of this we can forget about everything else above it. So, this is also a big problem. What will help with this is integration of networks.
#11	That it is more important, from ethical and legal considerations, ensure that we make agreements about this. So, I don't see the biggest challenges here either. It also has to do with the level of ambition, because I think that super connectivity and operability is not something you should want to pursue.
#12	I think we don't know exactly where we stand as a Defence organization at the moment. Which data will be available on which platform and when? So it is very difficult to realize that technical communication properly. So much is unclear or is delayed in the development of the new IT environment. Some things are running, but based on old-fashioned ways and techniques and it must be replaced or renewed at some point.
#13	Very applicable, although I think we have this reasonably well in order, but very important. Because if you can't communicate, what are you going to do with collaboration.

Technical barrier – Technical communication: *A lack of communication guidelines between heterogeneous platforms hinders the sharing of data among agencies. Achieving seamless interoperability among heterogeneous communication systems is crucial.* Ten interviewees validated this sub-aspect and there were no suggestions for refinement. According to three interviewees this shouldn't be a real problem. Networks need to integrate and sometimes we just introduce self-imposed barriers. It is difficult to realize technical communication properly because we often don't know where we stand. Where the standards for a commercial application work well, the MoD has to prepare for a different context. One of the interviewees stated that because of interrupted and the different technical forms of communication it is difficult to switch between these different options in an operational environment. Three others stated that this sub-aspect overlaps with data standards, data integration, policies or organizational communication.

Where the standards for a commercial application work well, we have to prepare for a different context (#1). But we have interrupted communication and different technical forms of communication and especially switching between these different options in an operational situation is very difficult. For the joint task, there is still a challenge (#3). I think we don't know exactly where we stand as a Defence organization at the moment. Which data will be available on which platform and when? So it is very difficult to realize that technical communication properly. So much is unclear or is delayed in the development of the new IT environment. Some things are running, but based on old-fashioned ways and techniques and it must be replaced or renewed at some point (#12).

Question 26: Which of the interoperability barriers on a scale of 1 to 5 are the most recognizable (1 least recognizable, 5 most recognizable)? Why these interoperability barriers?

Aspect	Sub-aspect	1	2	3	4	5	Total	Std dev	Mean	Average
Legal barriers	• Intellectual property			4	2	7	55	0,9	5	4,23
	• Accessibility	1	1	4	2	5	48	1,3	4	3,69
	• Knowledge		3	2	3	5	49	1,2	4	3,77
Organizational barriers	• Collaboration	1	1	3	2	6	50	1,3	4	3,85
	• Processes, policies, and procedures			3	2	8	57	0,8	5	4,38
	• Communication	1	2	2	3	5	48	1,3	4	3,69
Semantic and Syntactic barriers	• Data standards	1	2	7		3	41	1,2	3	3,15
	• Dictionary	1	2	6	2	2	41	1,1	3	3,15
	• Language	1	5	4	2	1	36	1,0	3	2,77
	• Ontology	4	2	3	1	3	36	1,5	3	2,77
Technical barriers	• Infrastructure		2	3	2	6	51	1,1	4	3,92
	• Resources		2	3	3	5	50	1,1	4	3,85
	• Data integration		1	4	3	5	51	1,0	4	3,92
	• Technical communication	2	3	4	2	2	38	1,3	3	2,92

Likert scale	Validation	Answers	Percentage
1 = totally disagree	Negative	12	7%
2 = disagree	Negative	26	14%
3 = neutral	Neutral	52	28%
4= agree	Positive	29	16%
5= totally agree	Positive	63	35%
Total		182	100%

Sub-aspect (Recognizable)	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10	#11	#12	#13	Total	Std-dev	Mean	Average
Intellectual property	5	5	3	3	5	3	4	3	5	5	5	4	5	55	0,9	5	4,23
Accessibility	1	3	5	5	3	2	3	4	3	5	4	5	5	48	1,3	4	3,69
Knowledge	5	3	5	5	5	2	4	2	3	5	4	4	2	49	1,2	4	3,77
Collaboration	5	5	3	3	5	5	3	4	4	5	2	5	1	50	1,3	4	3,85
Processes, policies and procedures	3	5	3	5	5	5	4	3	4	5	5	5	5	57	0,8	5	4,38
Communication	4	5	3	1	5	4	5	5	3	5	2	4	2	48	1,3	4	3,69
Data standards	5	3	5	1	3	3	2	3	3	5	3	3	2	41	1,2	3	3,15
Dictionary	3	3	3	3	3	5	3	2	2	5	4	4	1	41	1,1	3	3,15
Language	3	3	3	2	2	2	3	2	1	5	2	4	4	36	1,0	3	2,77
Ontology	1	3	3	4	5	1	1	2	2	5	1	3	5	36	1,5	3	2,77
Infrastructure	5	5	3	4	5	2	3	4	2	5	5	5	3	51	1,1	4	3,92
Resources	4	2	5	4	5	4	2	3	5	5	3	5	3	50	1,1	4	3,85
Data integration	5	3	5	5	5	2	3	3	4	5	4	4	3	51	1,0	4	3,92
Technical Communication	4	3	5	4	2	3	2	3	2	5	1	3	1	38	1,3	3	2,92

Question 27: Which of the interoperability barriers on a scale of 1 to 5 are the most impactful in practice (with regards to data exchange)? Can you give an example?

Aspect	Sub-aspect	1	2	3	4	5	Total	Std dev	Mean	Average
Legal barriers	• Intellectual property		1	1	2	9	58	0,93	5	4,46
	• Accessibility	1	3	3	1	5	45	1,39	3	3,46
	• Knowledge		1	3	4	5	52	0,96	4	4,00
Organizational barriers	• Collaboration			1	4	8	59	0,63	5	4,54
	• Processes, policies, and procedures		2	2	3	6	52	1,11	4	4,00
	• Communication		1	3	4	5	52	0,96	4	4,00
Semantic and Syntactic barriers	• Data standards		2	4	3	4	48	1,07	4	3,69
	• Dictionary	1	3	2	5	2	43	1,20	4	3,31
	• Language	2	4	4	2	1	35	1,14	3	2,69
	• Ontology	2	3	5		3	38	1,33	3	2,92
Technical barriers	• Infrastructure		3	2	2	6	50	1,23	4	3,85
	• Resources		2	5	1	5	48	1,14	3	3,69
	• Data integration		1	5	4	3	48	0,91	4	3,69
	• Technical communication	1	4	2	2	4	43	1,38	3	3,31

Likert scale	Validation	Answers	Percentage
1 = totally disagree	Negative	7	4%
2 = disagree	Negative	30	17%
3 = neutral	Neutral	42	23%
4= agree	Positive	37	20%
5= totally agree	Positive	66	36%
Total		182	100%

Sub-aspect (Impact)	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10	#11	#12	#13	Total	Std-dev	Mean	Average
Intellectual property	5	3	5	5	5	2	5	4	5	5	4	5	5	58	0,93	5	4,46
Accessibility	1	2	5	5	5	2	3	4	3	5	5	3	2	45	1,39	3	3,46
Knowledge	5	4	5	5	3	2	5	4	3	5	4	3	4	52	0,96	4	4,00
Collaboration	5	5	5	5	5	5	5	4	4	5	4	4	3	59	0,63	5	4,54
Processes, policies and procedures	2	5	2	5	3	5	4	3	4	5	4	5	5	52	1,11	4	4,00
Communication	4	5	5	4	3	2	5	5	3	5	4	3	4	52	0,96	4	4,00
Data standards	5	5	4	5	3	3	3	4	3	5	4	2	2	48	1,07	4	3,69
Dictionary	3	5	1	4	4	4	4	2	2	5	4	2	3	43	1,20	4	3,31
Language	3	4	2	3	2	1	4	2	1	5	3	2	3	35	1,14	3	2,69
Ontology	3	3	2	5	3	1	1	2	2	5	3	3	5	38	1,33	3	2,92
Infrastructure	5	5	2	5	3	2	3	4	2	5	4	5	5	50	1,23	4	3,85
Resources	3	3	5	5	5	2	2	3	5	5	3	4	3	48	1,14	3	3,69
Data integration	3	4	5	4	5	3	4	3	4	5	3	3	2	48	0,91	4	3,69
Technical Communication	5	4	5	4	3	1	2	3	2	5	2	2	5	43	1,38	3	3,31

28. Which of the interoperability barriers on a scale of 1 to 5 are the most relevant in practice (with regards to data exchange)? Can you give an example?

Aspect	**Sub-aspect**	**1**	**2**	**3**	**4**	**5**	**Total**	**Std-dev**	**Mean**	**Average**
Legal barriers	• Intellectual property			3	2	8	57	0,84	5	4,38
	• Accessibility		4	2	2	5	47	1,27	4	3,62
	• Knowledge		1	3	5	4	51	0,92	4	3,92
Organizational barriers	• Collaboration			2	4	7	57	0,74	5	4,38
	• Processes, policies, and procedures		2	2	4	5	51	1,07	4	3,92
	• Communication		2	4	3	4	48	1,07	4	3,69
Semantic and Syntactic barriers	• Data standards	1	2	2	3	5	48	1,32	4	3,69
	• Dictionary	1	4	3	3	2	40	1,21	3	3,08
	• Language	1	6	3	2	1	35	1,07	2	**2,69**
	• Ontology	1	4	5		3	39	1,24	3	**3,00**
Technical barriers	• Infrastructure		3	3	2	5	48	1,20	4	3,69
	• Resources		1	7	1	4	47	1,00	3	3,62
	• Data integration		3	4	3	3	45	1,08	3	3,46
	• Technical communication	2	3	4	2	2	38	1,27	3	**2,92**

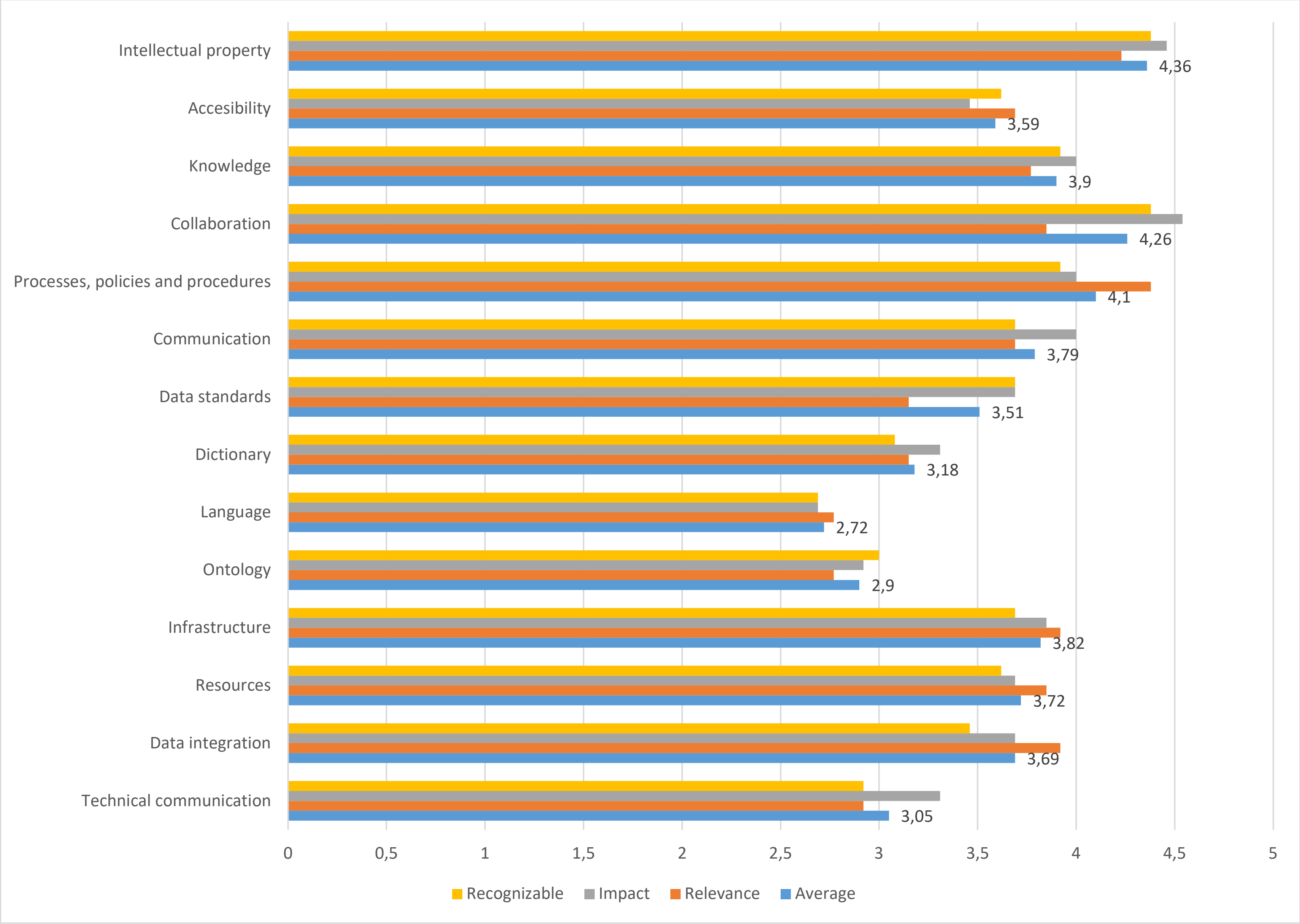
Likert scale	Validation	Answers	Percentage
1 = totally disagree	Negative	6	3%
2 = disagree	Negative	35	19%
3 = neutral	Neutral	47	26%
4= agree	Positive	36	20%
5= totally agree	Positive	58	32%
Total		182	100%

Sub-aspect (Relevance)	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10	#11	#12	#13	Total	Std-dev	Mean	Average
Intellectual property	5	3	5	5	5	3	5	4	5	5	4	5	3	57	0,84	5	4,38
Accessibility	2	2	5	5	5	2	3	4	3	5	5	4	2	47	1,27	4	3,62
Knowledge	4	3	5	5	4	2	5	4	3	5	4	3	4	51	0,92	4	3,92
Collaboration	4	5	3	5	5	5	5	5	4	5	3	4	4	57	0,74	5	4,38
Processes, policies and procedures	2	4	2	5	3	4	5	3	4	5	4	5	5	51	1,07	4	3,92
Communication	4	4	2	2	3	5	5	4	3	5	3	3	5	48	1,07	4	3,69
Data standards	5	4	4	5	3	1	4	5	3	5	5	2	2	48	1,32	4	3,69
Dictionary	2	3	1	2	4	4	5	3	2	5	4	3	2	40	1,21	3	3,08
Language	2	3	2	2	2	2	4	2	1	5	4	3	3	35	1,07	2	2,69
Ontology	2	3	3	5	3	2	1	2	2	5	3	3	5	39	1,24	3	3,00
Infrastructure	5	5	2	3	3	2	4	4	2	5	3	5	5	48	1,20	4	3,69
Resources	3	3	5	5	3	3	2	3	5	5	3	4	3	47	1,00	3	3,62
Data integration	4	3	5	2	5	2	4	3	4	5	3	3	2	45	1,08	3	3,46
Technical Communication	4	3	3	1	3	1	2	4	2	5	2	3	5	38	1,27	3	2,92

D3 Overall average

Below there is an overview of the overall average. This is the sum of all averages from Q-26 to Q-28 (Recognizable, Impact and Relevance). The scores are represented as top 14 of which the top 3 values and bottom 3 values are displayed separately.

Sub-aspect	Average Recognizable	Average Impact	Average Relevance	Sum of averages	Overall average	Top 14
Intellectual property	4,23	4,46	4,38	13,07	**4,36**	1
Collaboration	3,85	4,54	4,38	12,77	**4,26**	2
Processes, policies and procedures	4,38	4,00	3,92	12,30	**4,10**	3
Knowledge	3,77	4,00	3,92	11,69	**3,90**	4
Infrastructure	3,92	3,85	3,69	11,46	**3,82**	5
Communication	3,69	4,00	3,69	11,38	**3,79**	6
Resources	3,85	3,69	3,62	11,16	**3,72**	7
Data integration	3,92	3,69	3,46	11,07	**3,69**	8
Accessibility	3,69	3,46	3,62	10,77	**3,59**	9
Data standards	3,15	3,69	3,69	10,53	**3,51**	10
Dictionary	3,15	3,31	3,08	9,54	**3,18**	11
Technical Communication	2,92	3,31	2,92	9,15	**3,05**	12
Ontology	2,77	2,92	3,00	8,69	**2,90**	13
Language	2,77	2,69	2,69	8,15	**2,72**	14


Intellectual property
Accesibility
Knowledge
Collaboration
Processes, policies and procedures
Communication
Data standards
Dictionary
Language
Ontology
Infrastructure
Resources
Data integration
Technical communication
4,36
3,59
3,9
4,26
4,1
3,79
3,51
3,18
2,72
2,9
3,82
3,72
3,69
3,05
0
0,5
1
1,5
2
2,5
3
3,5
4
4,5
5
Recognizable
Impact
Relevance
Average

D4 Overall impression and completeness

Interview #	Question 29 Mentioned sub-aspects correct
#1	I haven't seen anything I can't agree with.
#2	Complete model, which touches all layers and good cohesion. The GDPR does not allow that, to which I indicate where it is written and then it often becomes silent
#3	Yes, where I found it difficult I passed.
#4	Yes, I agree with the explanation and think it's a complete framework.
#5	Yes.
#6	Maybe what I'm missing is how do you design this. What ways or methods do you have now to design full stack and identify bottlenecks.
#7	It could be a bit more specific, because I notice that the sub-aspects sometimes overlap or have a relationship. With the layers I have the idea that you are approaching the right aspects. I think is technically not a barrier at all. Where technology is still a barrier, I think it is so marginal that you rule 80/20, that you don't have to delve into it any further.
#8	Yes, I think there is a lot of overlap, because one cannot do without the other, it all has to do with each other. I've given a bit of a high opinion about everything, without getting too technical. But I do think this is complete.
#9	I would add law and regulations to legal barriers, the organization is indeed important and the other sub-aspects are about people and technology, so I would split it up and then I think you have it completely clear.
#10	Yes, I'm not going to go into the details, but they are all important themes within this discussion.
#11	Yes, as far as I can judge, I'm not familiar with ontology.
#12	Yes.
#13	There weren't things that I say I don't recognize, so that's a positive.

A total of ten interviewees stated that there were no sub-aspects they didn’t recognize and that the different sub-aspects, as far as they can assess, has been correctly described. One interviewee stated that it could be a little bit more specific, because some sub-aspects have a certain overlap or relation with each other. A other interviewee is very interested in how a framework like this can be designed to really identify the barriers. So which part do I need when, instead of another tool in the toolbox or a framework which can be used. Yet another suggested that he would add law and regulations to legal barriers, because this would make the framework more clear and distinct.

Interview #	Question 30 Missing aspects
#1	Maybe an aspect between the legal (ownership) and the organizational barrier (collaboration, communication) you need to have a clear vision from the organizational leadership, switching certain people at a low level every few years is fine, but that capriciousness doesn’t have a positive impact on interoperability. Constantly changing choices on the higher level does not contribute. You must have a long-term vision and stick to it. We must stick to the direction that has been chosen and bear this decision together, leadership commitment for the long term. No own stamps, not everyone has to have an own legacy, you shouldn’t be the limiting factor in terms of interoperability.
#2	Financial aspects, if you are going to use systems together you have to divide the costs, this often leads to a lot of discussion
#3	Culture gap within the OPCOs, but also TNO and strategic partners, understand each other better. Some specific branches (FAC) do understand each other at a certain point, but the big worlds are still separate, which makes it difficult to find a common interest and use a common language.
#4	The purchasing process and a proper catalogue.
#5	I find it difficult to estimate whether the framework is complete.

#6	You did indicate human somewhere, so I think there could be a social or cultural context aspect somewhere and data quality.
#7	Standardized methodology that also takes into account, what are the opposing forces.
#8	The main question, why don't we get it done. Just implement because there are always people who will disagree.
#9	Ethics, do we want to work together. We work in a different way than the English-speaking countries. Desirability, morality, ethical issues like that can also be the basis for this.
#10	Security policies, organizational barriers (policies), are of great importance within this organization, so perhaps more attention should be paid to this. Security does stand in the way of interoperability. Does the security policy still meet the goals we want to achieve and does our security policy not stand in the way of this too much?
#11	Data quality. A subject that we also deal with is ethics, so what is something like “meaningful human control” and “human machine teaming” what should that whole relationship looks like.
#12	Ethics should also be an sub-aspect within the legal aspect, but also in the collaboration sub-aspect. I think ethical IT development is still very much in its infancy. But soon you will be able to gain insights with AI and with all the new technology that you may have to rule out in advance, some things you just shouldn't want to know. And it's very good to include the ethical aspect from the very beginning of development, just as you have privacy-by-design and security-by-design, you also need to have ethics-by-design. So, it's good to focus on that. We really need to think about that as an organization and perhaps as a whole chain. With visions, how long can something be kept, but this is a very short cycle, how much money do you get, how much time do you get, what exactly is your objective as the MoD, what does the Defence memorandum say. There are so many aspects that influence that. You have to set your own course and stick to it.
#13	I think at the bottom of the line it's a combination of all these aspects. I think the most important in the collaboration are the organizational barriers and the human factor (cultural differences).

On the question if certain sub-aspects where missing in the framework one of the interviewees suggested there maybe should be a sub-aspect which is focuses on a longer commitment of the central management and a long term vision. Other suggestions for refinement were made by three interviewees with regards to an additional sub-aspect for culture, another three suggested ethics, furthermore suggestions were made for costs, the purchasing process, a proper catalogue, security, and data quality. So the most important suggestions focusses on the organizational aspects (collaboration → ethics and cultural differences).

Interview #	Question 31 In which way are the interoperability barriers impeding a proper interoperability implementation
#1	We still talk past each other and there is still a lack of agreements to which we comply/ obey. Standards are very important.
#2	You have to have all aspects in order otherwise things will go wrong. It's not an either-or, but an both-and story and that's the tricky part, because you actually have to have everything in order to get this done.
#3	Almost all of them are relevant and the extent to which they affect interoperability depends very much on the business process you are talking about.
#4	The procurement process is not sufficiently focused on interoperability, there must be a catalogue function. You can buy something based on a certain standard, but there are sometimes 20 standards for one specific area.
#5	Technical barriers ensure that many preconditions have not been met and syntactic barriers are closely related to the technical barriers. Semantics are closely related to the organizational barriers in terms of understanding. The preconditions must be met, but they do not immediately solve your problem. The real barriers are caused by old thinking and culture change, but this is often less sexy. IGO should contribute to changing the need-to-know principle into the duty to share. But I’m afraid that it will turn out to be I want to share but I can't. Maybe you would like to start in some kind of greenfield, but that's not going to happen, even though some think this is GrIT, but this is just for the infrastructure and not for the resources and data integration. The preconditions must be invested in, but you will only get the benefits if you start thinking differently.
#6	Obstructing as in complicating and also less willing to change.

#7	That the right things are addressed on all those things, but the coherence is missing. Things are happening well in sub-areas, but whether the right things are happening in conjunction, I only see that happening to a very limited extent.
#8	A large part concerns behaviour and people, perseverance and direction, culture, also because we are used to the fact that someone is allowed to have the last word. If you really want something and have the money for it and it is supported within the armed forces, then get to work. Let's do something, now a lot of people are frustrated.
#9	The topics we have discussed all play a role to a greater or lesser extent, depending on what one is doing. I don't think you can pinpoint one subject that is a showstopper. Maybe you should also put the organization at the top, this is why we do it, we have certain objectives and that includes certain partnerships and based on that you will organize certain things and what do you need, laws and regulations, frameworks of agreements , learning to understand each other, the human and the technical factor. I think that's a slightly more natural flow within these four topics.
#10	To a large extent, each individual ensures that interoperability does or does not get off the ground, and that also makes it very difficult, because I have to understand all these aspects in order to take steps and take all these aspects from within the organization to take these steps. and this can never start with the individual. So, this must always start with the organization, with good management and policy on this.
#11	I think this pretty much covers the way they limit interoperability.
#12	Interoperability is not a choice, we cannot choose to do it or not. Or we will soon be forced to work this way, then you get some big-bang scenario where we go to some kind of government cloud-like solution and over which we have no control or we just go with it strike now because we've actually already been overtaken by the industry. I think these kind of pointers can keep you well on track, that you have to take these into account in the steps we're going to take. I think it's very can be valuable.
#13	I think at the bottom of the line it's a combination of all these aspects. I think the most important in the collaboration are the organizational barriers and the human factor.

Six of the interviewees say that it is a combination of all of these sub-aspects, which are impeding a proper interoperability implementation. You can’t pinpoint one sub-aspect as an showstopper says one, and the extent to which they affect interoperability depends on the process, according to two of them. Things are happening well in sub-areas, but there is no overall coherence. The real barriers are often caused by old thinking and culture, but there need to be invested in the preconditions and you will only get the benefits when you start think differently. One suggestion is to put the organization at the top of the framework.

Interview #	Question 32 Influencing decision-making
#1	The OODA loop (Observe, Orient, Decide, and Act) is certainly not going to speed up, but rather slow down, as we get an even bigger web of disconnected systems, trying to get data from one end to the other, which will cost more time than that we are actually using the data. If we don't address this thoroughly, it will only negatively affect interoperability.
#2	You cut back on your right to exist, if we can no longer provide what is necessary for society, then you can ask yourself what your right to exist is at that moment and what it will be in the future.
#3	The effect is then certainly for your primary task that you will fall behind. It is about life and death, so on those key aspects we must always stay ahead or at least stay ahead, because otherwise it can cost lives and you cannot act operationally. Perception of safety determines your right to exist. We can't share information now with a short delay.
#4	Then we continue on the current road. That also works, but we have an IGO ambition. If you're serious about IGO you have to be serious about interoperability, so you have to get these things in place or you have to have a different path.
#5	If you look at the collaboration between TNO and the MoD, the consequences are delays and frustration. And delay also means that you could have achieved a higher / better result, but we live in a bureaucratic world, so things are slow and we are not going to change that anyway. The OPCOs as 4 different worlds, but everyone is

	starting to realize that we are constantly at war, so we have to cooperate and realize a better mutual understanding to create multi domain operations, and there is increasing awareness that if we fail it can cause a lot of economic damage.
#6	On the one hand I tend to say business as usual, more work for information people. I think it's mainly a matter of neighbour's locks. If we don't settle them and someone else does, then I think you're going to fall behind potential opponents or adversaries in a broad sense.
#7	You are left with the point solutions and you are inflexible, if you look at the Defence organization. You will soon have to be able to work with all kinds of parties in a very diverse composition. If you do not solve this, you will always be left with problems in the operation. That things don't work, that things can't and shouldn't. Work arounds have to be invented again. You will continue to have problems with this until the end of days.
#8	We can still manage decision-making, in my opinion we are even too focused on this. Ultimately whether or not the man in the field gets his information in time can be a danger if there is, for instance, an IED and the information is known, but cannot reach the person.
#9	Strongly depends on which showstopper this ultimately concerns, but it can of course harm the effectiveness of your organization if you can't work together.
#10	That we are ultimately no longer relevant in our actions, that we eventually have to enter a fight too late, based on insufficient information, and then you are no longer relevant.
#11	The ultimate goal is that we maintain an advantage over the opponent and we can do that best if we are technologically advanced. And that is a very big concept that is difficult to measure, but of which we do know that these kinds of aspects are very important. In that sense, being able to work together technically is very important. I think it only gets interesting in certain contexts, because then you know what you're missing and then you know what you don't have. The entire impact of technology, as long as we do not control it ourselves, the technology will do it, then it will be dictated more by the market and the potential that certain technology offers. We want to focus on multi-domain action and this is so incredibly important, because if defence departments cannot work well together, this is a barrier. We actually know that every conflict / fight will have an IT component. So in that sense, it will also mean that we are much less able to counter certain threats such as digital and hybrid threats, so it will have an effect on that.
#12	Delay, I don't think it will get out of hand. Whether you want to or not, you will just have to go along and eventually it will all work out, but it is smart to keep control yourself. Our bureaucratic processes and equipment can also can slow down young talented technical personnel to work for the Ministry of Defence.
#13	Then you only work together for 50%. So you have to work together completely or not at all.

When asked in which way these sub-aspect could influence decision making if they are not properly implemented, one interviewee stated that it would become a bigger web of disconnected systems. The effect is that you will fall behind potential opponents according to three interviewees and that causes operational risks. Two interviewees tend to say business as usual, because if you don't settle someone else does and then you will just have to go along, but it will be smarter to keep control. Two others say it will diminish your right to exist.

Interview #	Question 33 Is the framework useful
#1	The key features, challenges, that you have to tackle give you a direction in which to look. Attention should be paid to that. If we have that in order, then we can move towards better cooperation within the Ministry of Defence. It gives you guidance and direction, allowing you to prioritize what's important. With the limited capacity we have, you have to prioritize and you can do that with this framework.
#2	I have never seen it worked out so nicely, because it describes all the layers that are required. Collaboration, how are we doing financially and organizational?
#3	I see added value in the field of awareness within the organization. I think that a very solid story will come out of this, which can raise awareness among a very large group of people, the framework helps with this.
#4	I do see the added value myself.
#5	Yes, the framework has added value if people understand it and start using it. If you can somehow add a timeline to the sub-aspects, with dependencies, you can report the progress, because all things are interdependent. It is very complex, but it is also a complex subject.

#6	Yes, if it can be linked in a follow-up step/follow-up study with measures. If you have the model and you can then assign a score to it and that can be the result of, if you are extremely bothered by this barrier here, other than of course just the inverse of it, what are the facilities or measures that you could hit to put air in there. So I think it's a valuable start and I think it's very understandable but what I think would make it more powerful, is if you could link it to advice or policy so that you as an organization can use it as operating model.
#7	Sure, I also see some things that we're already using.
#8	Yes I see the value.
#9	I like the framework, we are often looking for how we want to arrange things. And if you can discuss it like this, you get some refinement in your model, it does indicate very clearly where it starts with and what you ultimately need to realize something and often we don't realize it, but this all comes into play and we often don't realize it
#10	Yes, most certainly. The way how is irrelevant to me, but putting the effect of all these facets on the agenda and doing something with it is very important. It's about the will to do something, then is it about being allowed to do it and finally, are you being able to do it.
#11	I think it's good to use this as a measurement tool.
#12	What I'm still struggling with a bit is how you would like to use it. I'm still trying to figure out how to put this into practice. It certainly contains pointers that I would like to take with me, but I'm still struggling a bit how I will be able to use it as a steering instrument.
#13	Certainly, I think it's helpful to provide insight to the upper management. In this way you can visualize what we're doing. But when we look at the things that could potentially be a barrier then you will see that we simply do not do enough about this or score much too low on it. You can make it quite visual quite easily. So, I'm definitely curious how this will develop further.

To the question if the framework is useful twelve interviewees answered that it is certainly useful for them. The answers that were given are that the framework can raise awareness, gives you guidance, direction, insight to the upper management, and allows you to prioritize what is important, because it describes all the layers that are required. If a timeline could be added with dependencies, it could be used for measurement and reporting purposes, because all sub-aspects are interdependent. And if it could link it to advice or policies, than it could be used as an operating model, but one of the interviewees is struggling with how it can be used or implemented as an steering instrument.

Interview #	Question 34 Intention to use the framework
#1	With this framework you could better articulate, substantiate and structure. Because this is based on theory, you can speak the same language more often. What I mean by the value of data can be explained to someone else in a different way. If you have the same dictionary, you can also have a discussion about how we interpret it instead of having a semantic discussion with each other (structure).
#2	I do think I can use the framework because I often act in these areas to get things done. So in this way you have insight into which things still need to be thought of. This is often done unconsciously, but on paper it is much more structured
#3	I think so, this framework can help to take steps towards a more integrated information provision. You have to be careful with a framework that you don't want to do everything, but bring focus.
#4	If I were to use it would be from the catalogue function or the really specific technical content.
#5	Yes, I think so.
#6	I think I would present it as a model, as a kind of SWOT, your strengths and weaknesses.
#7	I think in addition to the framework, I would be very interested in a methodology, of how do you apply it. The framework does offer structure, but I think that, especially within the Ministry of Defence, you should provide tools on how I am going to apply it.
#8	Yes, this framework is good for brainstorming.
#9	-

#10	I don't know if I am the right person to start using the framework. Ultimately, I see this more at the level of the CIO/CDO office, IT control groups and IT policy.
#11	Maybe as part of such a data maturity study.
#12	If it were to be published as a management tool, I would certainly look into it.
#13	I certainly think we can use this.

Eleven of the thirteen interviewees stated that they can use this framework to a greater or lesser extent. The framework is good for brainstorming, offers structure, it gives insight in the strengths and weaknesses, in this way it becomes clear what is needed. Two interviewees stated that they are very interested in a methodology, of how do you apply it and if it was published as a management tool they would certainly look into it.

Interview #	Question 35 Concluding remarks
#1	Diversity of systems leads to more Single Points of Failure, as where generic systems provide more people who can do the same thing.
#2	No
#3	No
#4	No
#5	No
#6	No, but one thing I would like to underline is the social or human aspect. Interoperability also depends on how a person experiences certain aspects. Within the MoD we use a lot of abbreviations and domain specific terms. This makes it nearly impossible for the MoD to interoperate with a financial company. For instance if we use the term operation, this has a different meaning and context within the MoD than within a civil organization or a healthcare institute.
#7	No
#8	We need guidance and persistence, because we are on this planet to support the armed forces so that they can operate and this essential part is sometimes forgotten within the MoD.
#9	No
#10	No
#11	No, but the specific domain in which the MoD operates, can make it more challenging to introduce a framework like this. We have the ability to use weapon systems and what does this mean for the framework.
#12	No
#13	No

Eleven out of the thirteen interviewees answered this question with no, four interviewees had additional remarks concerning the diversity of systems creates often a single point of failure and more generic systems contribute to more personnel with similar skills. One interviewee wanted to underline the social or human aspect. Interoperability also depends on how a person experiences certain aspects. Within the MoD we use a lot of abbreviations and domain specific terms. A other interviewee stated that we need guidance and persistence, because we are on this planet to support the armed forces so that they can operate and this essential part is sometimes forgotten within the MoD.