FFI-RAPPORT

21/00069

Service decomposition using the NATO C3 Taxonomy

— case studies

Bjørn Jervell Hansen
Kate Foster
Trude Hafsøe Bloebaum
Ketil Lund
Frank Trethan Johnsen

Service decomposition using the NATO C3 Taxonomy
– case studies

Bjørn Jervell Hansen
Kate Foster
Trude Hafsøe Bloebaum
Ketil Lund
Frank Trethan Johnsen

Norwegian Defence Research Establishment (FFI) 29 January 2021

Keywords

Tjenesteorientert arkitektur
Kjernetjenester
Web Services

FFI report
21/00069

Project number
1431

ISBN
978-82-464-3224-3

Approved by
Trude H. Bloebaum, *Research Manager*
Jan Erik Voldhaug, *Director of Research*

Summary

NATO introduced the Connected Forces Initiative at the 2012 Chicago summit with the aim to enhance allied interoperability and readiness in order to strengthen the combat power of the alliance. One of the aspects highlighted by this initiative is the importance of providing an ICT infrastructure to make the forces connected, enabling them to communicate and share information.

A prevalent method for building such infrastructures in the civilian domain is following the principles of service-oriented architecture (SOA). These principles state that complex software functionality should be broken down into a number of smaller, less complex and autonomous software components known as services. One of the goals of doing such service decomposition is that it allows for the re-use of implementations as well as reducing complexity.

Both the Norwegian Defence Research Establishment (FFI) and Australia's Defence Science and Technology (DST) Group are planning experiments in order to provide advice to their respective armed forces regarding these adaptions. A part of the preparations for such experiments is to identify what elements are essential to implement in the ICT infrastructures, and this reports documents a study in which a preliminary list of such elements have been compiled.

In order to arrive at this list, the study followed a use case driven approach. The use cases were chosen from four different military communities of interest in order to provide the analysis with sufficient variety without promising to be exhaustive:

- Establishing situational awareness and planning a tactical manoeuver in the land domain.
- Establishing situational awareness and performing targeting and dynamic re-planning of operational tasks in the air domain.
- Request for information (RFI) submission in Joint Intelligence Surveillance and Reconnaissance (JISR).
- Providing Modelling & Simulation as a service.

The analysis identified the following NATO C3 Taxonomy Core Services as candidates for a first inclusion in an ICT infrastructure due to their importance across the use cases:

- Infrastructure Storage Services.
- Message-Oriented Middleware Services.
- Geospatial Services.

In addition, there is a need to include security and service management and control services as well as to identify whether the Core Services listed here have important dependencies to other Core Services, in which case should also be considered for inclusion.

Sammendrag

NATO introduserte i 2012 sitt *Connected Forces Initiativ*, der målet er å forbedre alliert interoperablitet og beredskap slik at alliansens slagkraft kan styrkes. Et av initiativets viktigste budskap er hvor viktig det er med en IKT-infrastruktur som sørger for at de forskjellige styrkene er sammenkoblet slik at de kan kommunisere og dele informasjon.

En utbredt måte å bygge slike infrastrukturer på, er å følge prinsippene tilknyttet tjenesteorienterte arkitekturer. Disse prinsippene legger vekt på at kompleks programvarefunksjonalitet brytes ned i mindre og selvstendig komponenter. Et av målene med slik nedbrytning er at disse komponentene, som kalles tjenester, da kan gjenbrukes ved å sette dem sammen på ulike måter, og en viktig del av en slik nedbrytning er å identifisere hvilken funksjonalitet det er behov for, og hvordan denne bør deles opp i tjenester.

Både Forsvarets forskningsinstitutt (FFI) og Australias Defence Science and Technology (DST) Group planlegger å gjennomføre eksperimenter for å kunne gi råd til sine respektive militære styrker om hvordan de kan bygge IKT-infrastrukturer med nødvendige egenskaper. Siden slike infrastrukturer i hovedsak bygges i samsvar med tjenesteorienteringsprinsipper, er en del av forberedelsene til slike eksperimenter å identifisere hvilke tjenester som bør prioriteres implementert.

I denne rapporten har vi brukt konkrete eksempler for å identifisere disse tjenestene. Eksemplene er hentet fra fire forskjellige militære kontekster for å gi tilstrekkelig bredde i analysene:

- Etablere situasjonsbevissthet og planlegge en taktisk manøver i landdomenet
- Etablere situasjonsbevissthet og gjennomføre målutvelgelse og dynamisk planlegging i luftdomenet
- Etterspørre informasjon i Joint Intelligence Surveillance and Reconnaissance (JISR)
- Tilby modellering og simulering som en tjeneste

Gjennom analysen av disse eksemplene fant vi at visse kjernetjenester benyttes i mange ulike militære kontekster, og var dermed spesielt viktige. I en IKT-infrastruktur tilpasset militær bruk bør derfor de følgende kjernetjenestene implementeres først:

- Lagringstjenester
- Meldingsorientert mellomvare
- Geografiske tjenester

Det må også implementeres tjenester for sikkerhet og tjenestehåndtering, da disse representerer støttefunksjonalitet som kjernetjenestene identifisert over er avhengige av. Dersom videre analyser avdekker flere slike avhengigheter til andre kjernetjenester, må også disse tjenestene vurderes implementert.

Contents

Summary **3**

Sammendrag **4**

Contents **5**

Preface **7**

1 Introduction **9**

2 Methodology **11**
2.1 NATO's C3 Taxonomy 12
2.1.1 Core Services 15
2.1.2 COI-Specific and COI-Enabling Services 17
2.2 Service decomposition using the C3 Taxonomy 17

3 Land C2 service decomposition **20**
3.1 Establishing situational awareness 21
3.2 Planning a tactical manoeuver 24
3.3 Requirements 27

4 Air C2 service decomposition **28**
4.1 Establishing situational awareness 28
4.2 Targeting 31
4.3 Dynamic replanning 33
4.4 Requirements 35

5 JISR service decomposition **36**
5.1 Request for Information (RFI) 39
5.2 Requirements 43

6 Modeling and simulation service decomposition **45**
6.1 MSaaS use case 46

6.2 Service placement in the C3 Taxonomy 48
6.3 Service decomposition 49
6.4 Requirements 52

7 Additional considerations 54
7.1 Security and Service Management & Control 54
7.2 Dependencies between Core Services 54

8 Analysis Summary 55

9 Conclusion 57

References 58

Preface

The study conducted as a basis for this report was a cooperation between scientists from the Norwegian Defence Research Establishment and the Australian Defence Science and Technology Group. The authors would like to thank their respective employers for the opportunity to conduct this cooperative study.

Kjeller, Norway and Adelaide, Australia 7 January 2021

Bjørn Jervell Hansen
Kate Foster
Trude Hafsøe Bloebaum
Ketil Lund
Frank Trethan Johnsen

1 Introduction

NATO introduced the Connected Forces Initiative at the 2012 Chicago summit[1] with the aim to enhance allied interoperability and readiness in order to strengthen the combat power of the alliance. One of the aspects highlighted by this initiative is the importance of providing an infrastructure to make the forces connected, enabling them to communicate and share information. The establishment of the specifications needed by such an infrastructure, often named an *information infrastructure*, is in the NATO context led by the NATO Federated Mission Networking (FMN) initiative where the goal is to support command and control and decision-making in future operations through improved information-sharing.

Service-Oriented Architecture (SOA) is a concept that enables resources to be provided and consumed as services, allowing for dynamic information sharing between entities (Erl, 2004) (Erl, 2005). Because there is no agreed-upon, common definition of SOA, different people may have different understandings of the concept. We base our work on the "10 Principles of SOA" (Tilkov, 2007), which is a set of principles that we believe provide a good foundation for understanding the concept of SOA. These principles state, among other things, that complex software functionality supporting business processes should be broken down into a number of smaller, less complex and autonomous software components known as services. An important first step in this process is to analyze the business processes of the organization, and determine which such service are needed to ensure good coherence between the business processes and the functionality offered by the information infrastructure. One of the goals of doing such a service decomposition is that it, in addition to reducing software complexity, allows for the re-use of implementations. Common functionality, like for instance message handling, can then be implemented once and reused in a number of different contexts.

Core services is one category of services within the SOA paradigm. These services are normally shared components that represent functionality that is necessary for other types of services. So because they represent commonly needed functionality, they are implemented as separate services, rather than being repeatedly implemented as part of other services. Examples of core services include discovery of services, message routing and translation, and messaging security. In the NATO NEC Feasibility Study (Bartolomasi, et al., 2005), a concept of "layered" services was developed, and in this concept, the *Core Enterprise Services* layer consists of services *[providing] fundamental support […] both in the form of infrastructure and enabler services, and in the form of independent general-service building blocks.*

As can be gathered from the references above, SOA is considered an important concept when building infrastructures. Building an information infrastructure for military usage is, however, quite different from building one in the civilian domain. Military usage puts harder demands on the infrastructure, for example by requiring it to work on networks with limited bandwidth and high latency, especially at the tactical level, and civilian solutions can rarely be used out of the

[1] NATO Press release (2012): Summit Declaration on Defence Capabilities: Toward NATO Forces 2020

box in these circumstances (see e.g. (Sliwa & Amanowicz, 2011)). Thus, it has not yet been possible to take full advantage of SOA in military infrastructures.

The Norwegian Defence Research Establishment (FFI) is conducting experiments in order to support the Norwegian Defence in developing a service-oriented information infrastructure suited to the military domain. In order to focus these experiments and arrive at informed recommendations, there is a need to identify the most important core services needed in this military information infrastructure.

The Australian Department of Defence is currently also designing their future information infrastructure. The aim is to ensure interoperability with a scope from joint and combined operational level headquarters down to the deployed tactical level. A coherent design informs and supports capability experimentation, integration, and test and evaluation. A key aspect of designing the future network is defining the architecture and identifying services. Therefore, the Australian Defence Science and Technology (DST) Group is investigating service decompositions and identification of important services in order to inform these activities and support the development of the network. (Australian DoD, 2016).

In this study, the goal has been to identify candidates for these core services in order for both parties to move ahead with their experimentations. In order to do this we chose a use case driven approach: Four different communities of interest (COIs) were chosen as basis for the use cases to provide sufficient breadth to the analysis.

NATO's Consultation, Command, and Control (C3) Taxonomy (ACT, 2016) was used as the main tool in the analysis, giving us a chance to gain experience in using it as well as an opportunity to judge its suitability when used across several domains.

This report is structured as follows: The methodology is presented in section 2, and the use cases analyzed are detailed in sections 3, 4, 5, and 6. Additional considerations are summarized in section 7, while the analysis is summarized in section 8. The report is concluded in section 9.

2 Methodology

When performing a service decomposition, the goal is to ensure coherence between business processes and the functionality offered by the information infrastructure. The business processes of a military organization are complex, so instead of doing a full analysis we opted for a use case based approach. When choosing the use cases for the analysis, we focused on the following communities of interest (COIs):

- Land Command and Control (C2)
- Air C2
- Joint Intelligence Surveillance and Reconnaissance (JISR)
- Modelling and Simulation (M&S)

Since a use case driven approach was chosen for the analysis, it was important to strike a balance between a sufficient coverage of the different military COIs and a sufficient depth of analysis in each case. We sought to achieve this by choosing well-established military COIs, while also choosing COIs in which the different authors had sufficient knowledge to be able to perform the analysis. As the infrastructure in question is supposed to support more than just military operations, such as training, administration, and logistics, it was important to not only choose operational COIs. Hence the inclusion of M&S, as this COI was expected to highlight different, but still important, parts of the infrastructure.

When choosing a set of use cases that supports the analysis to a satisfactory degree, we looked for use cases that included a fairly high degree of infrastructure support. That way we were aiming at identifying the most important core services.

We used slightly different approaches for the different COIs to identify these use cases. With regards to the Land and Air C2 COI, this was done by looking for tasks typically performed within the COI. For the JISR COI, we chose a different approach as there already had been performed some work connecting tasks to services. In that case, we used these identified services as a starting point. Finally, for M&S we built on work performed in the NATO Science and Technology Organization (STO) Modeling and Simulation Group on *M&S as a Service*, adopting a use case already defined in that group.

This process resulted in the following use cases that form the core in our analysis:

- Land C2
    - Establishing situational awareness.
    - Planning a tactical manoeuvre.

- Air C2
    - Establishing situational awareness.
    - Targeting.
    - Dynamic replanning.
- JISR
    - Request for information
- M&S
    - M&S as a service (MSaaS)

The analysis consisted of the following steps:

1. Study the different use cases in light of NATO's Consultation, Command, and Control (C3) Taxonomy. A brief introduction to the C3 Taxonomy and an overview and explanation of the different symbols and colors used in the figures of this report is provided in Section 2.1.

2. Identify the services considered to be necessary to perform the different use cases.

3. Perform a service decomposition of these services. The service decomposition process is described in Section 2.2.

2.1 NATO's C3 Taxonomy

The purpose of NATO's C3 Taxonomy is to capture information about the different concepts, terms, capabilities, standards and systems that all contribute to NATO's capability to perform C3, and map these out in a structured and reusable way (ACT, 2016). This includes gathering information from a number of different COIs for classification, integration and harmonization purposes. Having a common taxonomy across communities is a way to help synchronize activities between those communities, while also improving the linkage between technical capabilities and the operational concepts the capabilities support.

The classification given in the C3 Taxonomy covers the entire C3 landscape, including both the Operational Context and the logical components of the capabilities required to meet NATO's information system and communication needs in support of Missions and Operations (Communications and Information Systems (CIS) capabilities). In the C3 Taxonomy, the term "taxonomy" is defined as "a particular classification arranged in a hierarchical structure organized by supertype-subtype relationships". As the definition states, the C3 Taxonomy has a hierarchical structure, where each category is gradually broken down into more and more

detailed services. The granularity of the service breakdown varies somewhat throughout the C3 Taxonomy, but a depth of 4-5 levels within each major category is common.

Note that in the C3 Taxonomy poster in Figure 2.1, this supertype-subtype relationship is illustrated with boxes inside boxes. For instance, the category “Technical Services” consists of three sub-categories: “COI Services”, “Core Services”, and “Communication Services”. Each of these sub-categories in turn contains several sub-categories (the figure shows only one level of sub-categories), and so on. An example of this is given in Figure 2.2, where the one of the sub-categories of the category “Core Services” is further broken down into two levels of sub-categories.

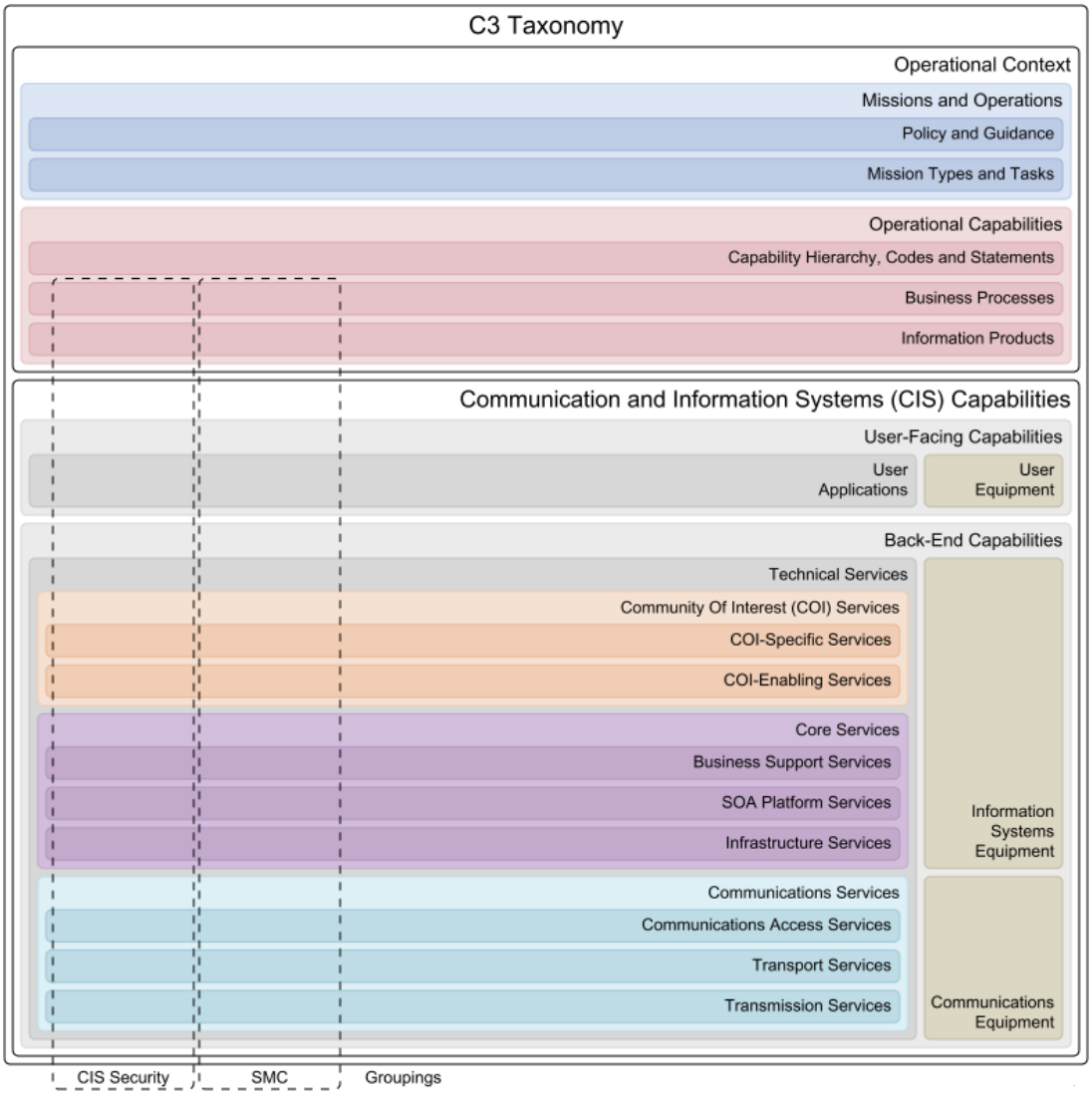


Figure 2.1 High level view of the C3 Taxonomy, Baseline 2.0, a.k.a. the C3 Taxonomy poster, from (NATO ACT, 2018).

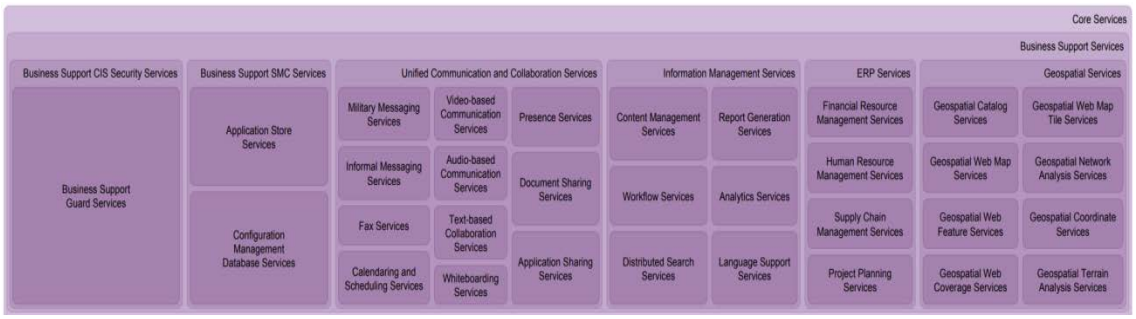


Figure 2.2 Example of a service category, with 3 levels of sub-categories (NATO ACT, 2018).

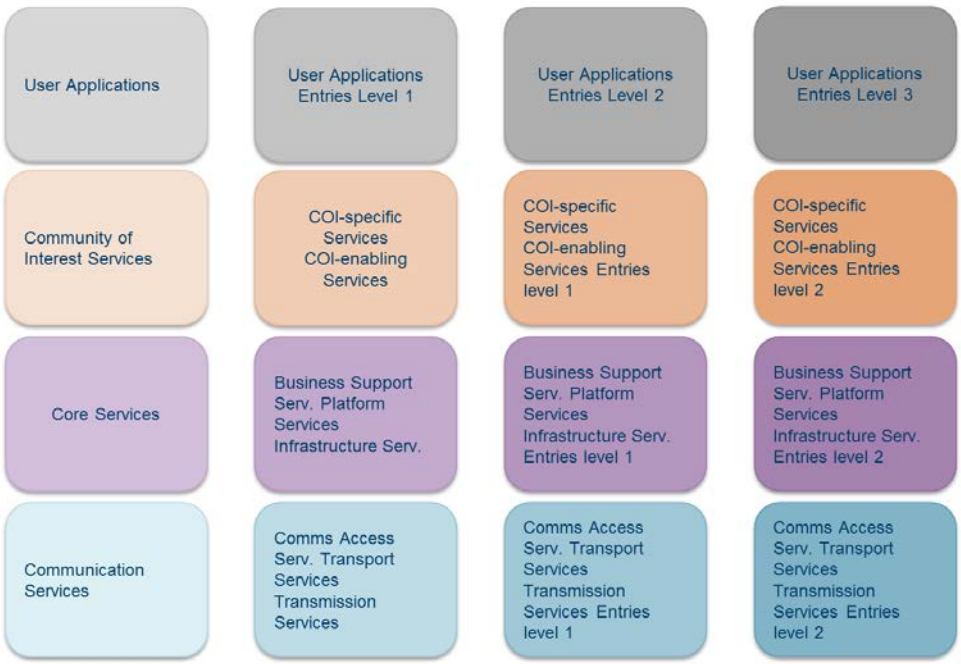


Figure 2.3 Color chart for CIS capabilities, from (NATO ACT, 2018).

In order to help present the categories and relationships in the C3 Taxonomy in a coherent and easily understandable way, the C3 Taxonomy comes with its own color scheme. This scheme, which can be seen in Figure 2.1, shows that each capability and top-level service category has its own color. Within each top-level service category, the different levels of sub-categories have darker shades of the top-level category color, as shown in Figure 2.2. The color chart for the CIS capabilities is shown in Figure 2.3, while the full color chart can be found in the Enterprise Mapping wiki (NATO ACT, 2018), which is also where the NATO C3 Taxonomy is maintained.

In addition to information about the lower levels in the taxonomy, the wiki also contains descriptions, functional and non-functional requirements, and even links to specific standards and technologies that may be used to realize the various concepts in the C3 Taxonomy.

Developing the C3 Taxonomy is an ongoing process. As new insight is gained, the C3 Taxonomy is updated to reflect these insights through changes to the Enterprise Mapping wiki. This means that the C3 Taxonomy undergoes frequent changes to ensure that it is as accurate and useful as possible. While these frequent changes are essential to ensure that the C3 Taxonomy remains relevant, these changes pose a challenge when using the C3 Taxonomy as a common reference as we do in this work. Because of this, we have chosen to base our work on the 2.0 Baseline version of the C3 Taxonomy. This version, which is described in (NATO ACT, 2015), was finalized on November 10th 2015 and was endorsed by the NATO C3 Board on February 11th 2016. Version 3.0 is currently being baselined, but was not yet available at the time of writing.

2.1.1 Core Services

The Core Services can been seen as shared components that should be available throughout the enterprise, as they provide a uniform means of access to central functionality such as discovery of services, message routing and translation, and messaging security.

At the top level, Core Services can be divided into the following three categories (see Figure 2.1):

1. Infrastructure Services
2. SOA Platform Services
3. Business Support Services

Of these three, the Infrastructure Services sub-category provides the most foundational capabilities and can be further subdivided into the following three sub-categories:

1. Infrastructure Processing Services
2. Infrastructure Storage Services
3. Infrastructure Networking Services

Here, the Infrastructure Networking Services will be employed by anyone wanting to communicate over a network, as this category includes all basic networking functionality (e.g., network transfer and Domain Name Service (DNS)). Further, the Infrastructure Storage Services will provide basic storage (e.g., on a file system). Infrastructure Processing Services contain operating system services (as needed by software systems and other services) as well as virtualized processing services (e.g., an enabler for virtual machines and cloud deployment). As such, every COI will need to leverage (a subset of) infrastructure services in order to support processing, storage, and networking needs of their systems.

SOA Platform Services provide services that enable SOA-based systems. Given NATO's adoption of SOA and related technologies as infrastructural building blocks (Bartolomasi, et al., 2005), the SOA Platform Services become increasingly important in future iterations of FMN as federated networking transitions more and more from interconnecting stovepipe systems to interconnecting middleware services. The SOA Platform Services encompass the following six sub-categories:

1. Message-Oriented Middleware Services
2. Web Platform Services
3. Database Services
4. Information Platform Services
5. Composition Services
6. Mediation Services

Here, the Message-Oriented Middleware Services encompass such communication paradigms as request/response and publish/subscribe middleware message exchange and services supporting these. Web Platform Services provide the necessary foundation for using and deploying Web services (the technology behind the middleware). Database Services provide database functionality (includes both classic relational databases as well as the recently popular non-relational databases). Information Platform Services include services that provide information about the SOA platform, including such aspects as metadata repository services and information discovery services to name a few. Composition Services provide the means to combine several services into an execution chain, and can also provide service-level transaction handling. Finally, Mediation Services encompass both protocol and data transformation services. Given the variety of basic functionality provided here, we can anticipate that any COI that leverages a SOA-approach in its COI-specific systems will use a subset (if not all) of the SOA Platform Services. Common for all the services at this level is that they define middleware behavior, i.e., they are intended for machine-to-machine communication.

Business Support Services may be in support of either machine-to-machine or human-to-human communication, and most of them focus on the latter. There are four sub-categories of Business Support Services:

1. Unified Communication and Collaboration Services
2. Information Management Services
3. Enterprise Resource Planning Services
4. Geospatial Services

Here, the Unified Collaboration and Communication Services support human-to-human communications, such as e-mail, audio and video-based conferencing and instant messaging. The two sub-categories Information Management Services and Enterprise Resource Planning Services provide supportive tools for management (e.g., analytics services) and planning tasks (e.g., human resource management and project planning services). Finally, Geospatial Services provides functionality for maps, navigation and positioning. Geospatial Services typically enable machine-to-machine support for specific services pertaining to geo (e.g., Web map services, terrain analysis services). Tools that include maps, positions, route planning and so on will rely on Geospatial Services to help implement this functionality.

2.1.2 COI-Specific and COI-Enabling Services

The COI Services category can be found just above the Core Services category in Figure 2.1, and consists of services that support one or more groups of users that share, for instance, interests, missions or business processes. The category consists of two sub-categories: COI-Specific Services and COI-Enabling Services.

COI-Specific Services are services required by individual user communities, and as such, the different sub-categories reflect the different communities typically found in military operations, exercises and routine activities.

COI-Enabling Services are services that deliver COI-specific functionality which is needed by more than one COI. They are similar to Business Support Services (Core Service) in that the services constitute building blocks for domain-specific services, but the COI-Enabling Services are less generic, and as such not relevant for the entire enterprise. In addition, these services are usually more oriented towards a military (in particular NATO) context.

One example that illustrates the difference between COI-Specific and COI-Enabling Services is the relationship between the different services used when building and distributing various recognized pictures, such as the Recognized Maritime Picture (RMP) and the Recognized Air Picture (RAP). These services have some functionality in common, but they also have functional differences. The common functionality, such as the ability to handle track information, combine track information from different sources, and handle symbol mappings, is found under the COI-Enabling Service category Situational Awareness Services. Situational Awareness Services are then used by the COI-specific RMP and RAP services, which add the COI-specific functionality needed for each specific recognized picture.

2.2 Service decomposition using the C3 Taxonomy

In our use of the C3 Taxonomy we have limited ourselves to using a subset of the categories. The tasks identified within each COI are first decomposed into functional services from the COI Services category. This decomposition is then used to identify which Core Services each task relies on, including which requirements the COI has to these services. By performing this decomposition for multiple COIs, we are then able to identify which services at the Core

Services level that these tasks have in common. Note that a use case based approach such as the one taken in this document will not provide an exhaustive list of all services needed but rather give an indication of central Core Services and the requirements put on those services by the COIs.

As we are describing the technical capabilities needed to support the given tasks, we have limited our descriptions to the Technical Services category of the CIS capabilities, and within this category we utilize two sub-categories, namely COI Services and Core Services (see Figure 2.1). We have chosen to omit the Communications Services sub-group from our study, as the main focus of the work is to identify central Core Services and the requirements the COIs have to those services.

The first step in our service decomposition use cases was to identify one or more specific tasks within each COI, identify what services are at play in this task, and then decompose those services. In the figures later in this report, we use the “box within box” notation from the C3 Taxonomy to highlight which service we are decomposing, and which COI-Specific Service category the chosen services belongs to. Figure 2.3 shows an example of this notation, highlighting that the Recognized Ground Picture (RGP) Service from the Land Services category is the subject of a decomposition.

Figure 2.4 The “box in box" notation used to highlight which service is being decomposed.

Once we have identified a service to decompose, we then show that service’s relationships to other services and service categories. There are two types of relationships in the figures throughout this report, namely “subtype of” and “depends on”.

The “subtype of” relationship shows that a service is a further specialization of a more generic service category. The “box in box” notation shown above is one way of showing this relationship, and this is also the method used to illustrate this relationship in the NATO C3 Taxonomy Poster. The “box in box” notation is compact, but using it makes it hard to illustrate other relationships clearly. Because of this, we primarily use the alternate notation shown in Figure 2.4 to show the “subtype of” relationship.

The second type of relationship between services is the “depends on” relationship. This relationship shows that one service uses the functionality represented by another service. The “depends on” relationship is, in the figures throughout this report, illustrated with a dotted arrow, as shown in Figure 2.5. The figure shows that the RGP Service, which is a “subtype of” Land Services, depends on both the COI-Enabling Service “Battlespace Information Services”

and the Core Service “Geospatial Services” (note that the decomposition shown here is not complete, the RGP Service has further dependencies, as discussed later in Chapter 4).

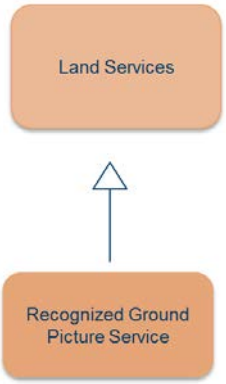


Figure 2.5 Alternative notation for the "subtype of" relationship. Here Recognized Ground Picture Service is a subtype of Land Services.

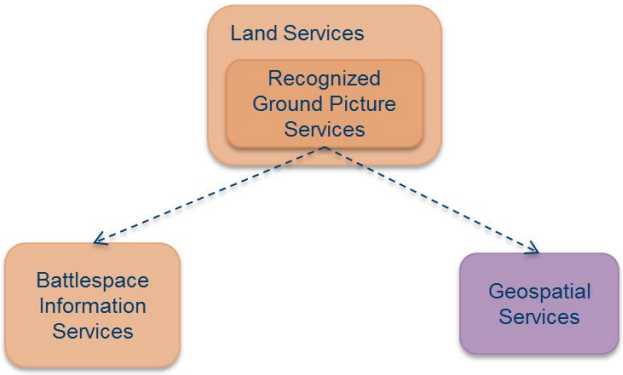


Figure 2.6 Notation illustrating the "depends on" relationship.

Also note the difference in color between the services in Figure 2.5. As explained in Section 2.1, the NATO C3 Taxonomy defines a color scheme for the different categories and sub-categories. In our work, we have used the same color scheme, and the parts of the color scheme relevant for this report are shown in Figure 2.3.

3 Land C2 service decomposition

A key component in all military operations is C2, which can be defined as "The exercise of authority by a properly designated commander over assigned and attached forces, performed through an arrangement of personnel, equipment, communications, facilities and procedures in the accomplishment of the mission."[2] The requirement for effective C2 applies equally to all warfighting domains, and performing C2 for one domain often includes collaboration and information exchange with partners working in other domains. In land C2, the primary concern is to perform C2 of land based forces, but collaboration with both air and naval forces is in many cases a part of the land C2 process.

Land forces are involved in most of the mission types defined by NATO policy and guidance, from collective defense operations, through counter-insurgency to disaster relief missions. This means that the land C2 processes, and the tools used to support these processes, must be flexible enough to handle all the possible tasks that are needed for this varied set of missions.

The C3 Taxonomy, as part of the Operational Context category, defines a number of business processes that are performed by NATO forces. One of those process categories is C2 processes, which in turn can be broken down into more specific C2 processes for the different domains. Figure 3.1 shows an excerpt from the C3 Taxonomy wiki, which highlights that the most central processes in land C2 are operation planning, operation execution and operation assessment.

Execution of all of these processes relies on technical support tools which assist the decision makers in their task for performing C2. These technical tools include both standard business collaboration tools such as phones and email, and land specific user applications. This last category of technical tools encompasses generic information management applications and applications that are developed specifically to support land operations. It is the latter of these application categories that supports the three land processes shown in Figure 3.1 directly.

In this chapter we are looking at two common land C2 tasks, and what type of functionality, represented as services from the C3 Taxonomy, that is needed in order to support those tasks. The purpose of this breakdown into services is to identify what Core Services land user applications typically rely on.

When determining which tasks to decompose, we were aiming to select tasks that are very common, that represent different C2 processes, and that have fairly high demands for infrastructure support. By selecting tasks in this manner, we are hoping to identify the majority of the functionality that is needed on the Core Services level. For our decomposition of land C2, we have chosen one operation planning task, namely planning a tactical manoeuver, and one operation execution task, namely establishing situational awareness.

[2] This is the definition coined by the NATO Command and Control Centre of Excellence (C2COE) as their working definition, due to the lack of an official NATO definition of C2. From https://c2coe.org/organisation/c2coe-mission-and-vision-2/

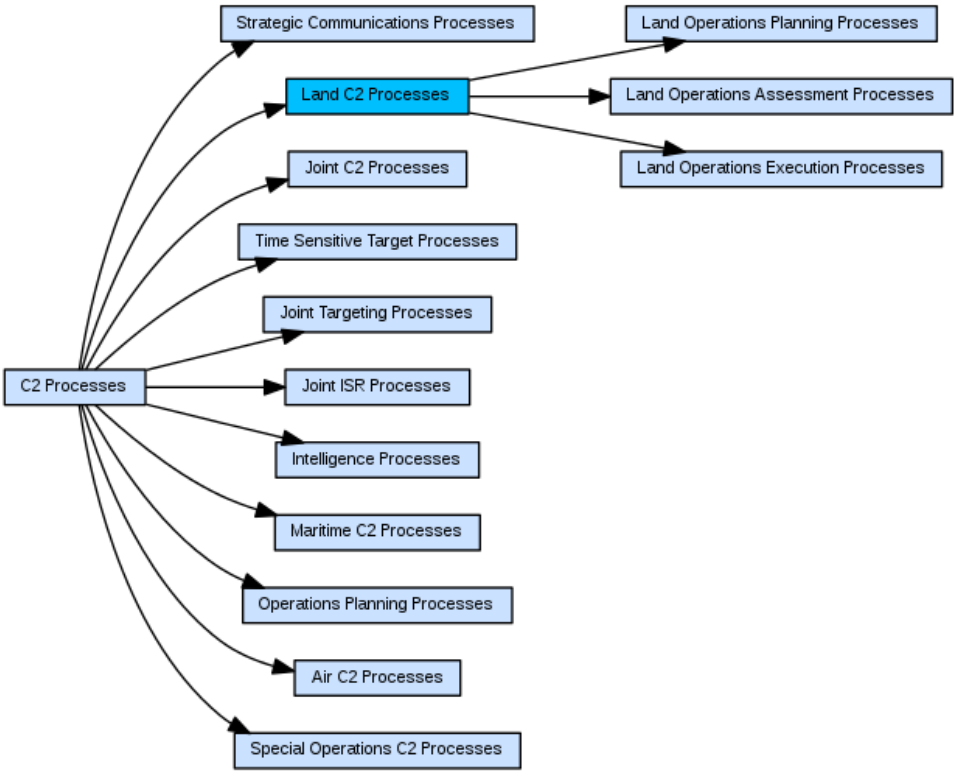


Figure 3.1 C2 processes breakdown focused on C2 for the land domain (NATO ACT, 2018).

3.1 Establishing situational awareness

Establishing situational awareness is a complex task, as it involves collecting, distributing and processing information, which must then be presented to a user in such a way that the user gets a correct understanding of the situation at hand. The user relies on information from a large number of different sources, such as the JISR processes, C2 systems and platform specific weapons systems, but also information gathered through the direct interaction with other people.

In this service decomposition we are looking at one sub-process of establishing situational awareness, namely the building and distribution of the Recognized Ground Picture (RGP). Looking at the C3 Taxonomy, this functionality can be found within the COI-Specific Land Services, where RGP Services are located. Note that this service will often rely on other services from other COIs, such as the corresponding picture services for the other domains (air, maritime, logistics etc.) and other information services such as the JISR Analysis and Production Services from the JISR COI.

Building and distributing the RGP depends on Battlespace Information Services, Situational Awareness Services and Operational Planning Services, all COI-Enabling Services. In addition, the RGP Service directly relies on services from other COIs and the Unified Communication

and Collaboration Services (from the Business Support Services within Core Services). These relationships are illustrated in Figure 3.2.

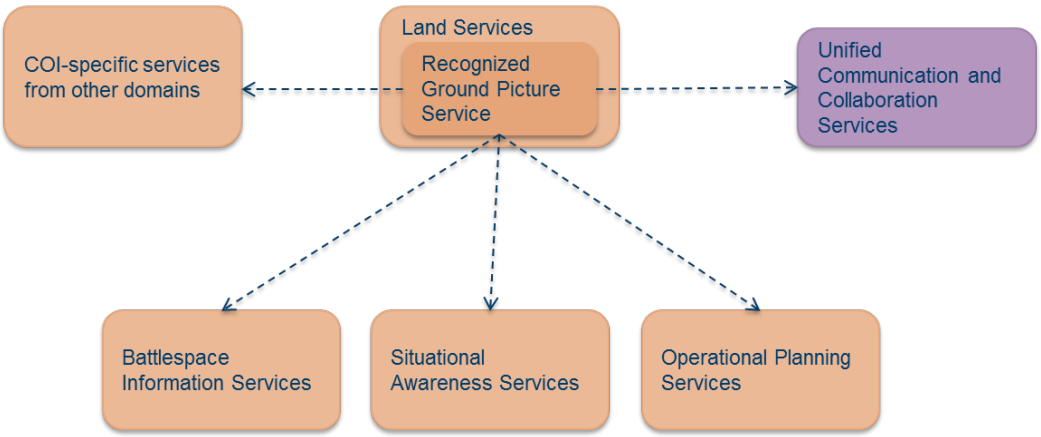


Figure 3.2 COI Services for the Establishing situational awareness task.

In order to be able to identify which Core Services the RGP Services rely on, we first need to better understand RGP. The RGP Services themselves, as described in the C3 Taxonomy, "… provide the means to produce, manage and disseminate the RGP. The RGP is the compilation of validated data relating to a defined ground area that is disseminated to enable situational awareness and support decision making at all levels. The RGP Services will support the development of the RGP through the collection, aggregation, correlation and fusion of information from multiple sources". Much of this is not specific to the land domain, and can thus be found among the COI-Enabling Services in the C3 Taxonomy.

As illustrated in Figure 3.3, the RGP Services relies on Battlespace Information Services, Situational Awareness Services, and Operational Planning Services. Each of these service categories can be further divided into sub-services, and it varies how many of those services are required. From the Battlespace Information Services and the Situational Awareness Services the full set of services is needed. Depending on implementation, this can be realized either as a part of a C2 system that implements the RGP, or as a different or standalone system.

In addition to the required functionality from these two categories, the RGP Service might also use information from services in the Operational Planning Services. This category includes services such as Order of Battle (ORBAT) Services, Deployment Plan Services, Courses of Action Services and Targeting Services. The RGP Services do not require the ability to produce and manage these information types, but access to the information can, depending on the level of ambition, be used to further enrich the RGP.

Based on the RGP Service decomposition in Figure 3.3, we can then map out which Core Services are required in order to support RGP Services.

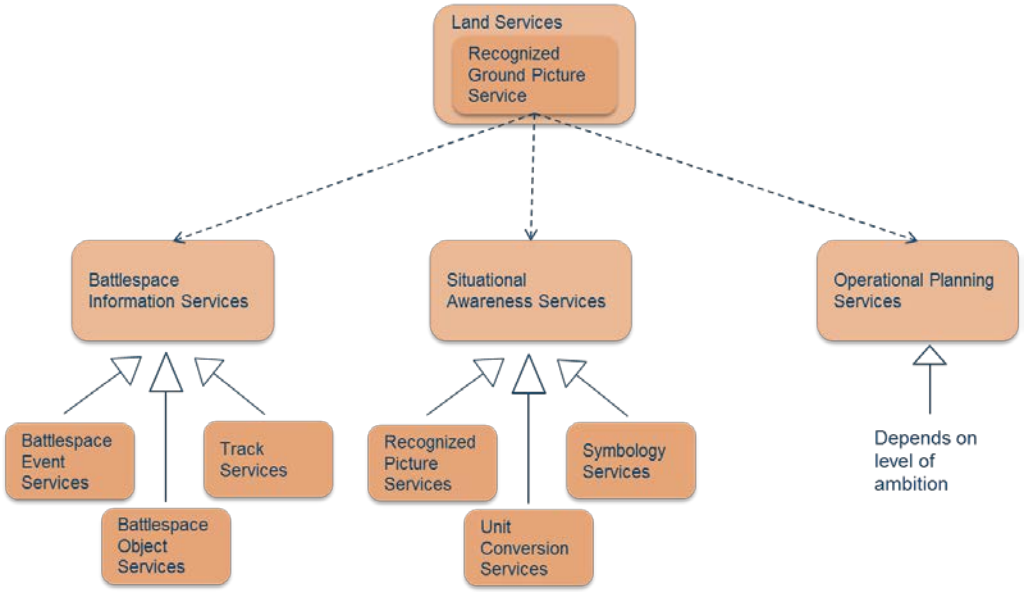


Figure 3.3 RGP Services mapped to the COI-Enabling Services the RGP encompasses.

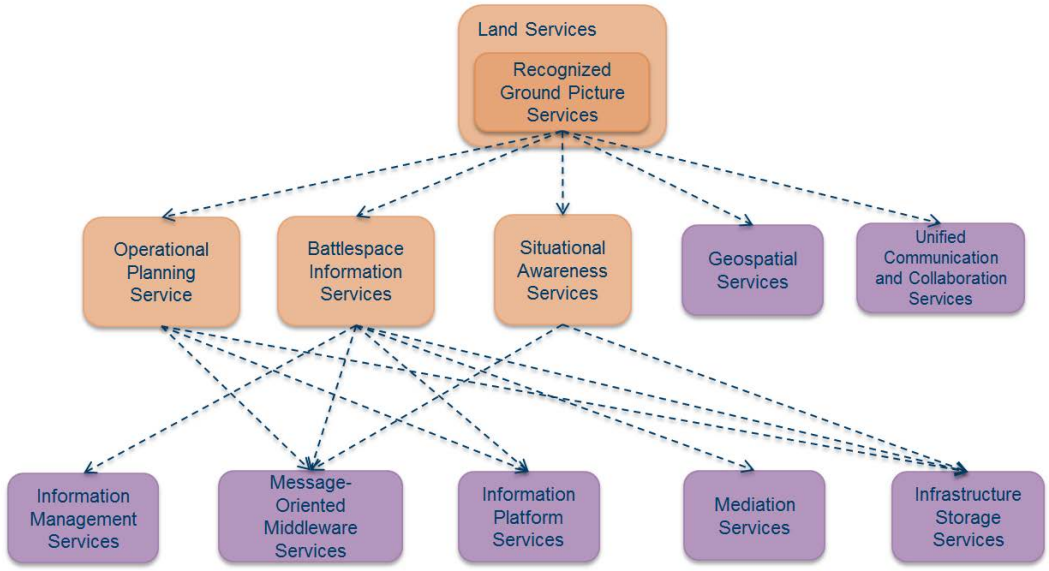


Figure 3.4 Core Services for the Establishing situational awareness task.

Figure 3.4 shows the mapping between the RGP Services and the high-level Core Services that are needed to build and distribute the RGP. Two of the Core Services, Geospatial Services and Unified Communication and Collaboration (UCC) Services are from the Business Support Services and are used directly by the RGP Service to provide maps and to coordinate between people when building the RGP.

As for the COI-Enabling Services used by RGP Services, all of them require the use of Message-Oriented Middleware Services to distribute their information objects, and Infrastructure Storage Services to store the information objects. In our experience, current systems often implement this as part of the C2 systems rather than as shared services, but the functionality is required. In addition, Information Management Services, Information Platform Services and Mediation Services are needed by a subset of RGP Services:

- From the Information Management Services, the Analytics Services are used to help verify incoming information flows.
- The Message-Oriented Middleware Services can be used to disseminate information from all the COI Services. Exactly which services will be used depends on implementation choices.
- The Information Platform Services provides annotation, aggregation and discovery of information.
- From the Mediation Services, both Data Format Transformation Services and Protocol Transformation Services are used to combine information from multiple services.
- Infrastructure Storage Services provide generic services for storing information objects. Depending on implementation, systems will require one or more services from this category.

3.2 Planning a tactical manoeuver

The planning of a land-based operation, independent of the operation type, requires a number of services from other COIs, in addition to services from the Land Services. The most important service when planning a tactical manoeuver is the Manoeuver Planning Services (MPS) (from Land Services), as shown in Figure 3.5. Which other services are required by the MPS, and which information is needed from those services, depends on the specific operation that is being planned. However, common services that are needed are the Recognized Picture Services (land, maritime, air etc.), but also Logistics Services, JISR Services and services that enable coordination with civilian partners (Civil-Military Cooperation (CIMIC) Services) and other government entities. These dependencies are illustrated with the “COI-specific services from other domains” element in Figure 3.5.

Having a rich set of UCC Services available is important when the planning process is done distributed, so that the planners can both talk to each other and work on information products in a distributed fashion. Examples of such services are Audio- and Video-based Collaboration Services, but more advanced collaboration services, like Application Sharing Services and Whiteboarding Services may be used as well.

Figure 3.5 COI Services for the Planning of a tactical manoeuver task.

MPS utilizes a number of different COI-Enabling Services. Information from the Battlespace Information Services and Situational Awareness Services are used, together with for instance JISR Services, to create knowledge about the current situation and the environment in which the planned operation will take place. The Operational Planning Services are used to perform the actual planning phase, before the Tasking and Order Services are used to task the units that will carry out the planned operation.

Figure 3.6 further details the decomposition of the MPS. From the Battlespace Information Services group, all services may be needed, but the Battlespace Object Services are the most central of these. From Situational Awareness, only Recognized Picture Services are used, as the other services in that category are used to *build* the recognized picture rather than just give access to it. From Operational Planning Services and the Orders and Tasking groups all services are needed.

In addition to these services, Figure 3.6 also shows that the MPS can use Modeling & Simulation Services to simulate how different plans can play out, enabling planners to take the expected outcome of a given course of action into account. If, and to which degree, such Modeling and Simulation Services are used depends on the level of ambition for the system implementing the MPS.

Figure 3.7 shows the mapping between the COI-level functionality encompassed by the MPS and the Core Services that are needed to support MPS. Geospatial Services, and to some degree Environmental Services (not shown in the figure, as it is optional), are used to provide information about the area the operation will take place in, while UCC are used to collaborate while preforming the planning.

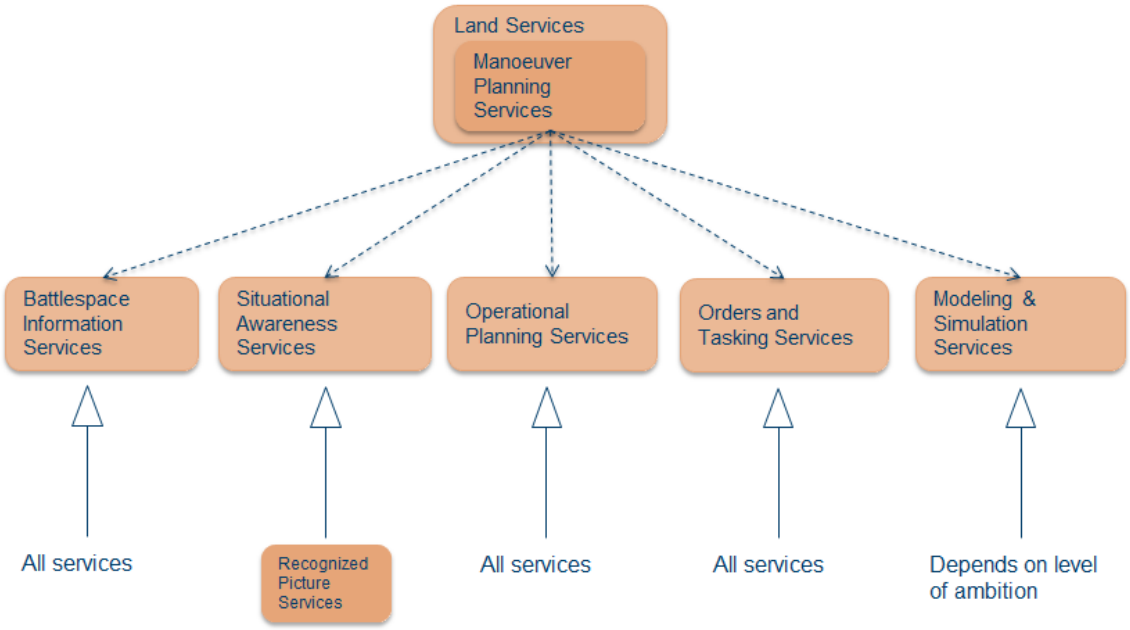


Figure 3.6 Decomposition of the Manoeuver Planning Services.

All of the COI-Enabling Services require access to functionality for retrieving and disseminating information, particularly in the case when the planning is done distributed. There is also a need for services for Information Management and Mediation, in addition to Infrastructure Services such as Networking and Storage.

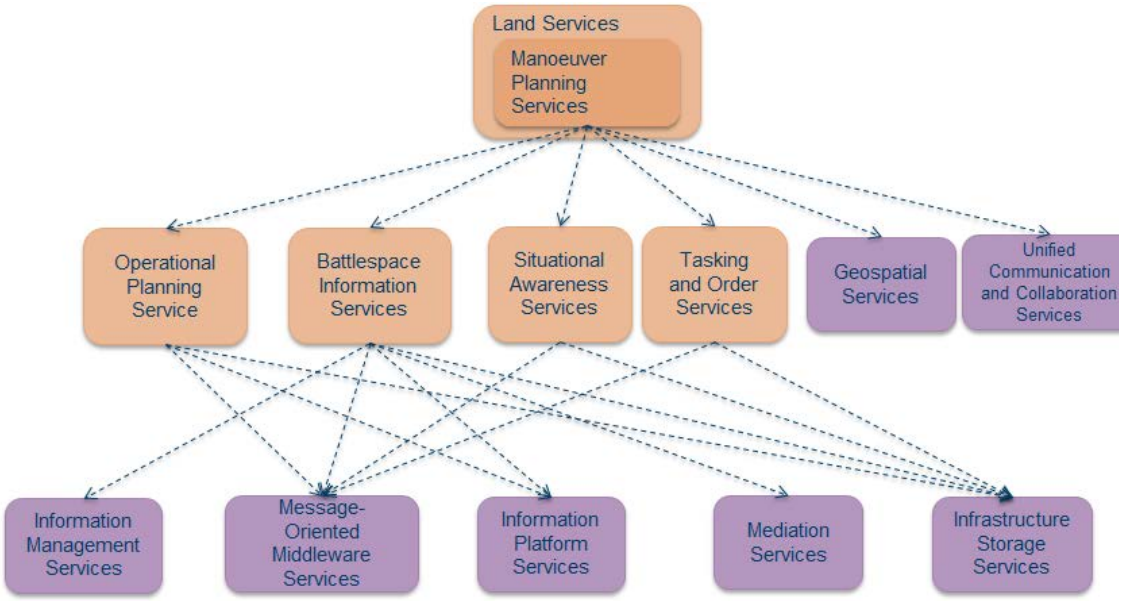


Figure 3.7 COI Services for the Planning of a tactical manoeuver task (M&S Services are optional and thus not included).

3.3 Requirements

Land operations are characterized by the fact that there often is a large number of units involved in an operation, and that those units can be distributed over a large geographical area. Providing communication to land-based forces is often challenging, as external factors, such as topology and weather may easily interrupt communications. Because of this there is a particular need to ensure that the services that the land forces rely on are able to adapt to changing communications conditions and potential disruptions in information flow. There is a need to, as far as possible, maintain a stable minimum of services (audio-based collaboration and the ability to exchange positional information for own forces are central here). These services need to be provided with close to real-time support, so that the operations can be planned and executed without the risk of blue-on-blue situations.

The manner in which the land forces conduct a given operation greatly influences the requirements for the systems used by the forces to support the operation. If decision makers are geographically distributed the need for capacity in the communications services and richness in the set of services offered increases.

4 Air C2 service decomposition

Australia's military capability is enabled by air power. Together with land and sea power, air power makes a vital contribution to the security of Australia and its interests (Royal Australian Air Force, 2013). A key component of air power is C2, which is the "…process and means for the exercise of authority over, and lawful direction of, assigned forces" (ADF Warfare Centre, 2009). In the air domain, C2 is realized by the air power missions of air campaigning and battlespace management (Figure 4.1). The air campaigning mission incorporates the planning of the air campaign, its execution, and the targeting process. Battlespace management includes management of air and space operations, airspace and electronic warfare. An introduction on C2 in general can be found in Chapter 3.

Three tasks were chosen that support the air campaigning mission. These tasks are: establishing situational awareness, targeting, and dynamic replanning. The following sections discuss each of these tasks and decompose them into Core Services.

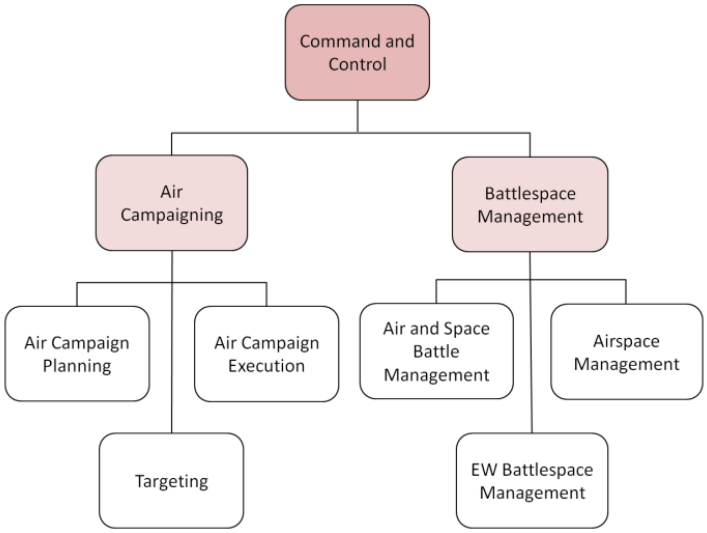


Figure 4.1 Air C2 missions (adapted from Figure 4-2 in (Royal Australian Air Force, 2013)).

4.1 Establishing situational awareness

Within this task, a situational picture is built in order to develop an understanding of the operational air environment. The COI Services that best represent this task are the Recognized Air Picture Services within Air Services. In the C3 Taxonomy, Recognized Air Picture Services are described as providing

"…the means to produce, manage and disseminate the Recognized Air Picture. These services will generate a de-conflicted and agreed picture of the air environment through the collection, aggregation, correlation and fusion of information from multiple sources."

Figure 4.2 shows that Recognized Air Picture Services rely on JISR within COI-Specific Services and Battlespace Information and Situational Awareness Services within COI-Enabling Services.

Recognized Air Picture Services have been broken down into Core Services in Figure 4.3. The Business Support Services they rely on are Geospatial Coordinate Services (within Geospatial Services) and Analytics Services (within Information Management Services). Recognized Air Picture Services rely on several services within SOA Platform Services: Direct Messaging Services (within Message-Oriented Middleware Services); Information Aggregation Services, Information Annotation Services and Metadata Repository Services (all within Information Platform Services); and Mediation Services. Finally, Infrastructure Storage Services (within Infrastructure Services) are also used.

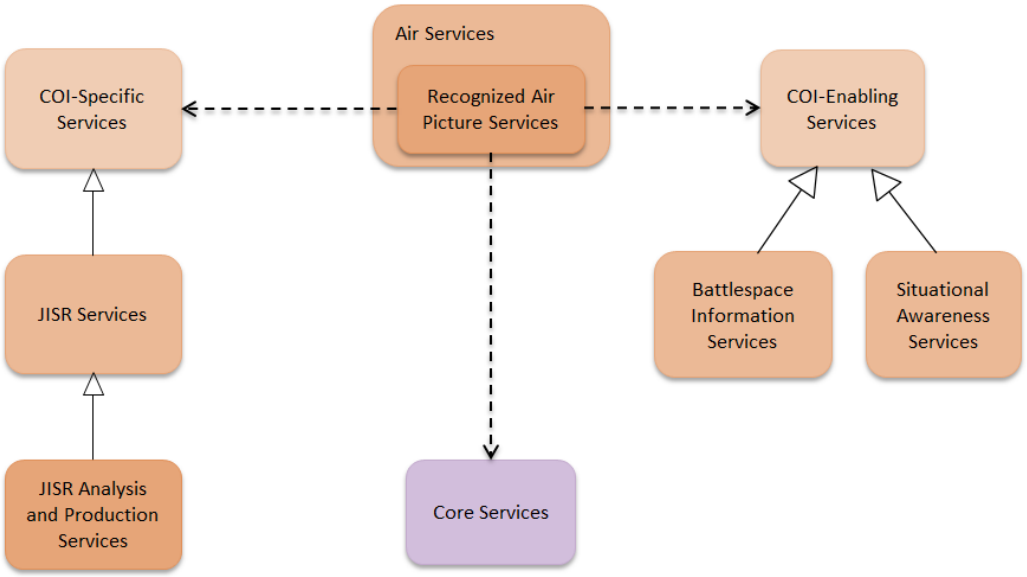


Figure 4.2 COI Services for the Establishing situational awareness task.

In Figure 4.4 a mapping of COI-Enabling and COI-Specific Services to Core Services is presented for Recognized Air Picture Services. JISR Services require Information Management Services, Message-Oriented Middleware Services, Mediation Services and Infrastructure Storage Services. Battlespace Information Services require all six Core Services and Situational Awareness Services require Message-Oriented Middleware Services and Infrastructure Storage Services.

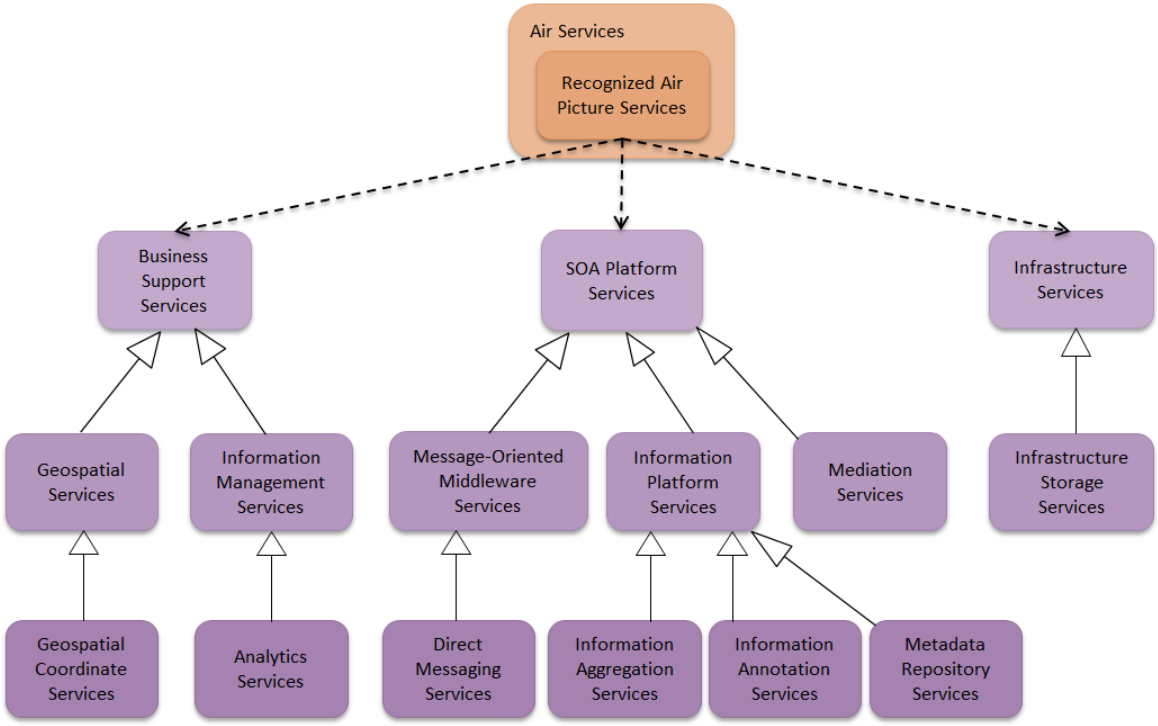


Figure 4.3 Core Services for the Establishing situational awareness task.

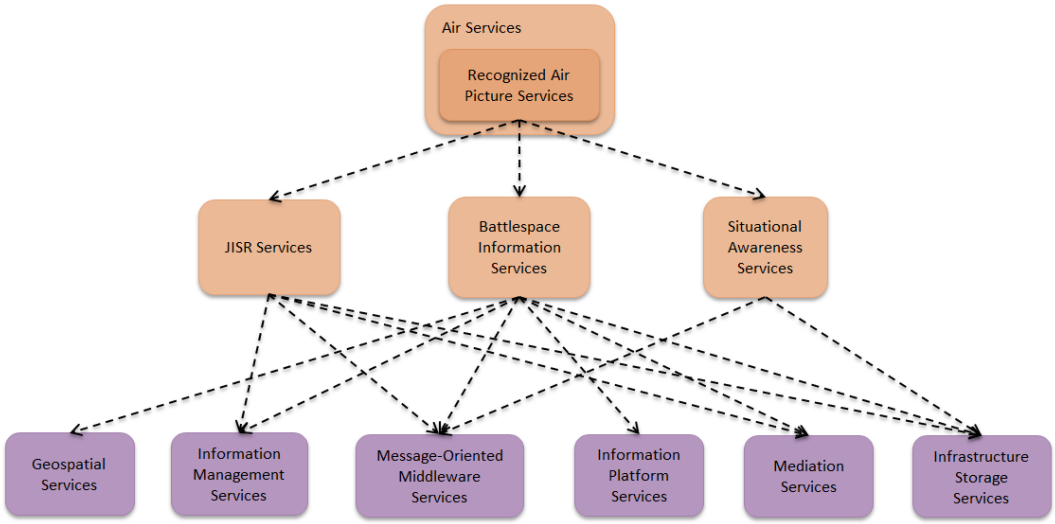


Figure 4.4 Mapping COI Services to Core Services for the Establishing situational awareness task.

4.2 Targeting

The Targeting task is concerned with selecting and prioritizing targets as well as matching appropriate actions to those targets to create the desired effect. The COI Services that best represent this task are the Targeting Services within Operations Planning Services. In the C3 Taxonomy, the Targeting Services are described as providing

> "…the means to select and prioritize targets, while matching the appropriate target response. A target is an entity or object considered for possible engagement or action. It may be an area, structure, object, person or group of people against which lethal or non-lethal capability can be employed to create specific psychological or physical effects to support the Commander's objectives, guidance, and intent."

The relationship between Targeting Services and COI-Enabling and COI-Specific Services is shown in Figure 4.5. Within the COI-Enabling Services, Targeting Services rely on Battlespace Information Services, Tasking and Order Services, Recognized Picture Services (within Situational Awareness Services) and Order of Battle Services (within Operations Planning Services). Within the COI-Specific Services, Targeting Services rely on NATO Crisis Response Measures Services (within Joint Services), and Air Weapon Matching Services and Air Threat Analysis Services (both within Air Services).

Targeting Services have been broken down into Core Services in Figure 4.6. The Business Support Services they rely on are Geospatial Network Analysis Services and Geospatial Terrain Analysis Services (within Geospatial Services), and Unified Communication and Collaboration Services. Targeting Services rely on several services within SOA Platform Services: Direct Messaging Services (within Message-Oriented Middleware Services); Information Discovery Services, Information Annotation Services and Metadata Repository Services (all within Information Platform Services); and Mediation Services. Finally, Infrastructure Storage Services (within Infrastructure Services) are also used.

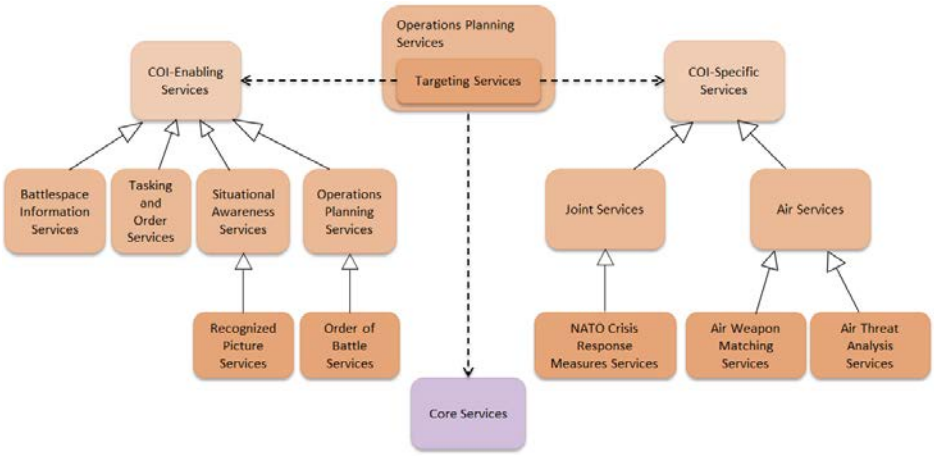


Figure 4.5 COI Services for the Targeting task.

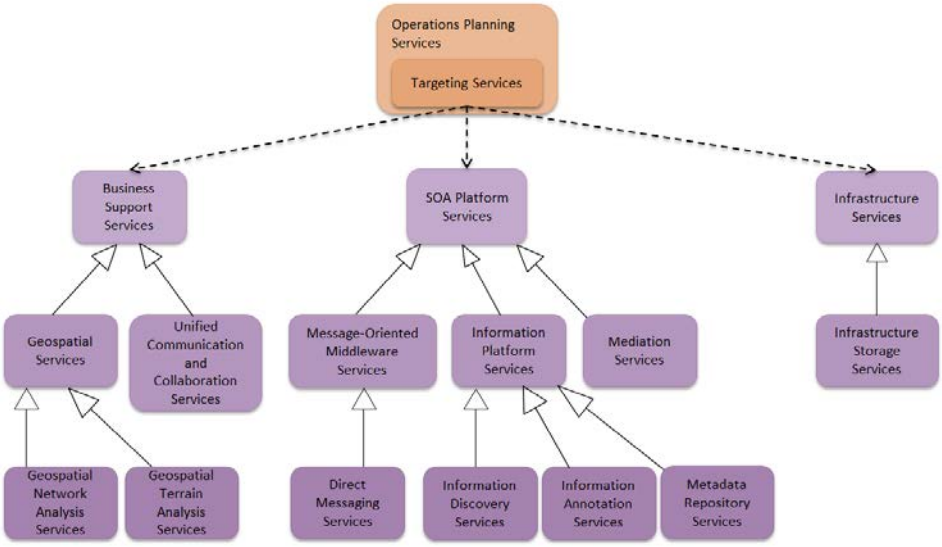


Figure 4.6 Core Services for the Targeting task.

In Figure 4.7 a mapping of COI-Enabling and COI-Specific Services to Core Services is presented for Targeting Services. Battlespace Information Services require all six Core Services. Tasking and Order Services require Unified Communication and Collaboration Services and Information Platform Services, and Situational Awareness Services require Message-Oriented Middleware Services and Infrastructure Storage Services. Joint Services require Unified Communication and Collaboration Services, Message-Oriented Middleware Services and Infrastructure Storage Services. Air Services require Unified Communication and Collaboration Services, Message-Oriented Middleware Services, Information Platform Services and Infrastructure Storage Services.

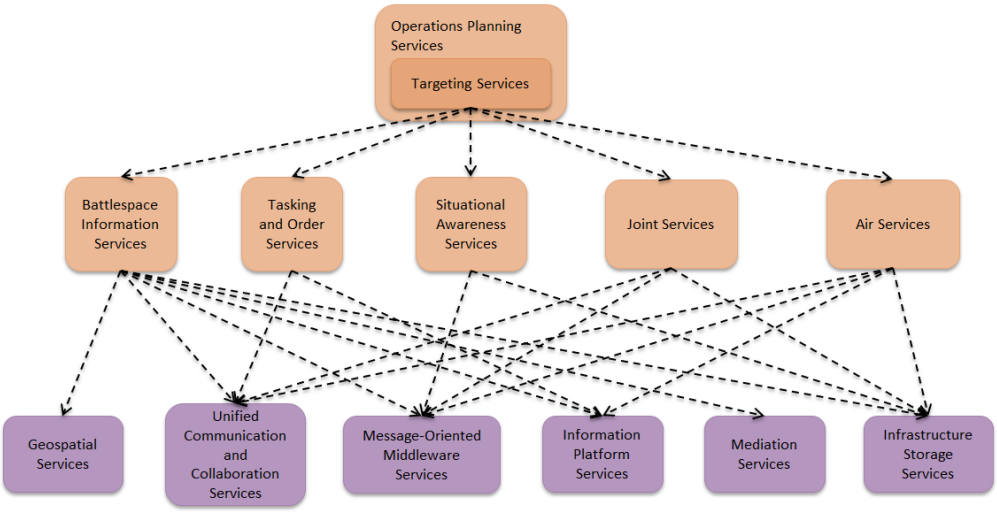


Figure 4.7 Mapping COI Services to Core Services for the Targeting task.

4.3 Dynamic replanning

The Dynamic replanning task is concerned with reassigning time-sensitive tasks in response to changes in battlespace conditions. It is characterized by diverse tasks with time windows, heterogeneous resources with fuel and payload limitations, and multiple competing objectives. Requirements and constraints continuously change over time. In the air domain, undertaking dynamic replanning in a timely manner is critical due to the highly dynamic environment. The COI Services that best represent this task are the Deployment Plan Services within Operations Planning Services. In the C3 Taxonomy, the Deployment Plan Services are described as providing

> "…the means for the coordination of air, sea, rail and road movements, tracking, reprioritization and re-routing. It supports alternative routes and the assessment of the implications and results of such alternatives, providing deconfliction and validation of plans feasibility."

The relationship between Deployment Plan Services and COI-Enabling and COI-Specific Services is shown in Figure 4.8. Within the COI-Enabling Services, Deployment Plan Services rely on Battlespace Information Services, Recognized Picture Services (within Situational Awareness Services), and Tasking and Order Services. Within the COI-Specific Services, Targeting Services rely on several classes of services within Air Services: Air Asset List Services, ACO Services, ATO Services, Air Mobility Analysis Services, Airlift Services and Airspace Management Services.

Deployment Plan Services have been broken down into Core Services in Figure 4.9. The Business Support Services they rely on are Geospatial Network Analysis Services and Geospatial Terrain Analysis Services (within Geospatial Services), and Unified Communication and Collaboration Services. Deployment Plan Services rely on several services within SOA Platform Services: Direct Messaging Services (within Message-Oriented Middleware Services); Information Discovery Services and Information Aggregation Services (within Information Platform Services); and Mediation Services. Finally, Infrastructure Storage Services (within Infrastructure Services) are also used.

In Figure 4.10 a mapping of COI-Enabling and COI-Specific Services to Core Services is presented for Deployment Plan Services. Battlespace Information Services require all six Core Services. Tasking and Order Services require Unified Communication and Collaboration Services and Information Platform Services, and Situational Awareness Services require Message-Oriented Middleware Services and Infrastructure Storage Services. Air Services require Unified Communication and Collaboration Services, Message-Oriented Middleware Services, Information Platform Services and Infrastructure Storage Services.

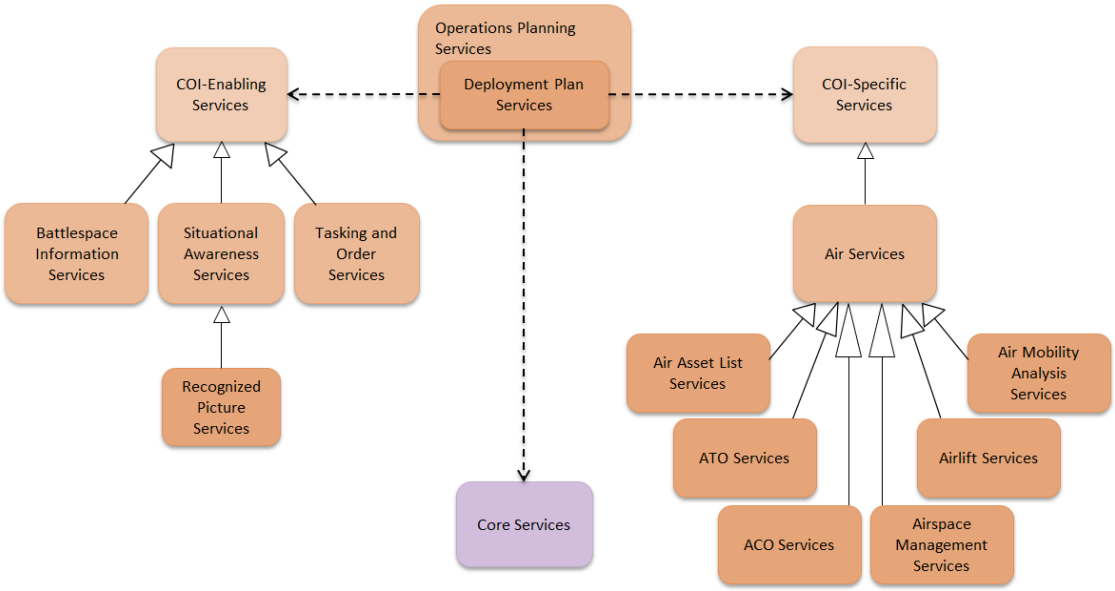


Figure 4.8 COI Services for the Dynamic replanning task.

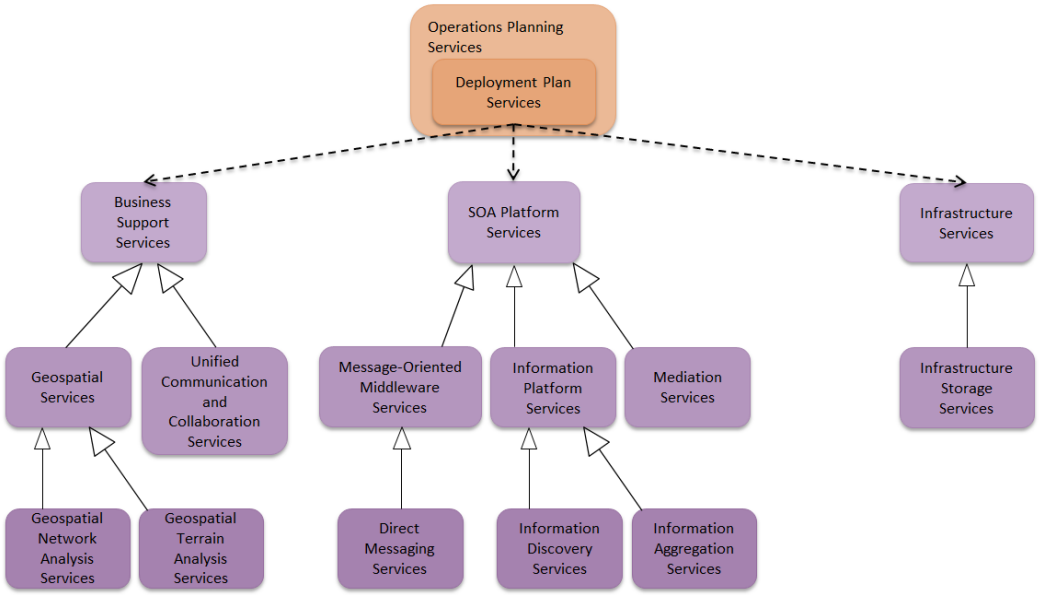


Figure 4.9 Core Services for the Dynamic replanning task.

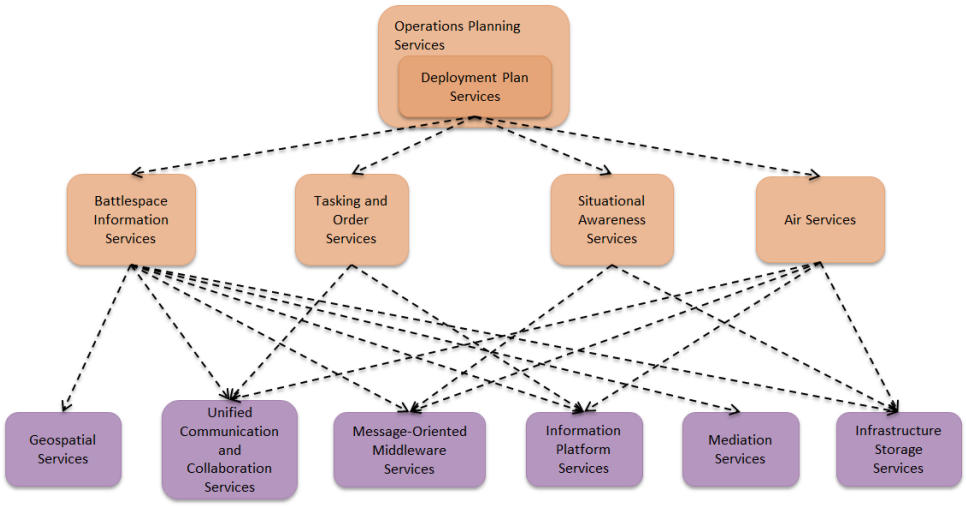


Figure 4.10 Mapping COI Services to Core Services for the Dynamic replanning task.

4.4 Requirements

The operational environment in the air domain is highly dynamic, and because of this, air C2 systems are highly mobile and have real-time or near real-time requirements. Further, as the communication systems in the air domain typically have throughput limitations and the space on board aircrafts are limited, air C2 systems have severe limitations on data throughput and physical space. Therefore, the non-functional requirements most important to air C2 systems are performance, reliability and safety. These impact the implementation of the Core Services detailed above. For example, Message-Oriented Middleware Services for air C2 will need to use direct messaging (rather than brokered) with guaranteed delivery in order to meet the real-time or near real-time requirements typical for this domain. Therefore, an appropriate standard to implement the real-time aspect of these services is the Object Management Group's Data Distribution Service for Real Time Systems (Object Management Group, 2018).

Due to their characteristics, we posit that real-time or near real-time performance and guaranteed delivery is required for air C2 tasks for the following Core Services: Geospatial Services, Unified Communication and Collaboration Services, Message-Oriented Middleware Services, Information Platform Services, Mediation Services and Infrastructure Storage Services.

According to our experience this is not necessarily the case for Information Management Services, thus for this class of Core Services we believe that the non-functional requirements are non-real-time and best effort.

5 JISR service decomposition

JISR is vital for all military operations. It provides information and intelligence to decision-makers and action-takers, helping them make informed, timely and accurate decisions. While surveillance and reconnaissance can answer the questions “what,” “when” and “where”, the combined elements from various intelligence sources and disciplines provide the answers to “how” and “why”.

Allied Joint Publication (AJP) 2-7 (NATO, 2016) defines JISR as follows: *A set of intelligence and operations capabilities, to synchronize and integrate the planning and operations of all collection capabilities with the processing, exploitation, and dissemination of the resulting information in direct support of the planning, preparation and execution of operations.*

Furthermore, the JISR process is defined as *a coordination process through which intelligence collection disciplines, collection capabilities and exploitation activities provide data, information and single source intelligence to address an information or intelligence requirement, in a deliberate, ad hoc or dynamic time frame in support of operations planning and execution. The JISR process consists of five steps: Task, Collect, Process, Exploit and Disseminate, referred to as TCPED.* (NATO, 2016)

The aim of JISR operations is to satisfy collection requirements (CRs) across all echelons of command in a timely and efficient manner. This means that the JISR staff is responsible for coordinating, synchronizing, and de-conflicting multi-disciplinary JISR collection capabilities and associated processing and exploitation capabilities. The JISR process constitutes a framework where each collection requirement is satisfied by a JISR asset following the five sequential steps that were listed above: Task, Collect, Process, Exploit and Disseminate (TCPED). This is illustrated in Figure 5.1 below.

1. *Task*: JISR tasking is the initial step of the JISR process. It is initiated with the clear articulation of CRs and consists of developing collection, exploitation and dissemination guidance/directives/orders to coordinate and control JISR operations and assets. JISR tasking is to be coordinated among all levels of command in order to enable mutual support between services/component commands and to make the most efficient use of available collection and exploitation capabilities.

2. *Collect*: This is the actual gathering of data and information by JISR capabilities and assets. Collection encompasses the detailed scheduling of JISR tasks to available JISR assets and the execution of those tasks by JISR capabilities. JISR assets collect the requested data and information and make it available for further processing.

3. *Process*: This is the conversion of collected data and information into appropriate readable or useable formats that enable further exploitation, storage or dissemination.

4. *Exploit*: In this step processed data and information is further exploited. There can exist different levels of exploitation for each JISR capability or asset. The levels range from rapid and preliminary assessment of collected JISR data or information up to a more time consuming in-depth assessment via reach-back capabilities.

5. *Disseminate*: This is the timely provision of JISR results to those who need it, in the requested format, and through the communication means as specified by the JISR task.

These steps apply at all levels of command, across components, for any type of mission, and in all operational environments. Figure 5.1 illustrates the JISR cycle with its five steps and the "customers" of each step.

JISR supports the full spectrum of NATO operations ranging from combat operations to humanitarian assistance.

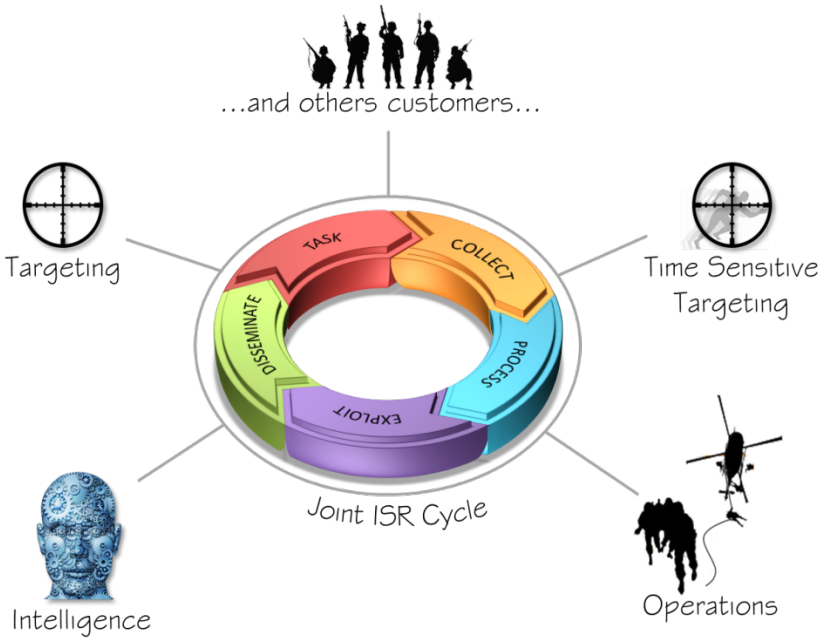


Figure 5.1 The JISR cycle (MAJIIC2/OWG, 2013).

The Multi-intelligence All-source Joint Intelligence Surveillance and Reconnaissance Coalition (MAJIIC 2) project was a multi-national effort to build technology based on standards and to test implementations to support the JISR cycle (MAJJIC, 2015). Within the MAJIIC 2 context, some work has already been done in mapping the different MAJIIC 2 services into the C3 Taxonomy (see Figure 5.2). However, no work has been done on further decomposing these services. In our work, we have therefore selected one of the services from the mappings done by MAJIIC 2, and then decomposed this service further within the C3 Taxonomy.

The service we chose to decompose is the Request service from the JISR COI Specific Layer (see Figure 5.2). The Request service enables Information Requirement Management &

Collection Management (IRM & CM) and exploitation capabilities to submit and receive Requests for Information (RFIs) and ISR requests, report and monitor their workflow status across the different nodes of the coalition, and retrieve resulting ISR products, both un-exploited and exploited. Figure 5.3 shows a high-level view of the COI-Specific Services that the ICM & RM capability depends on.

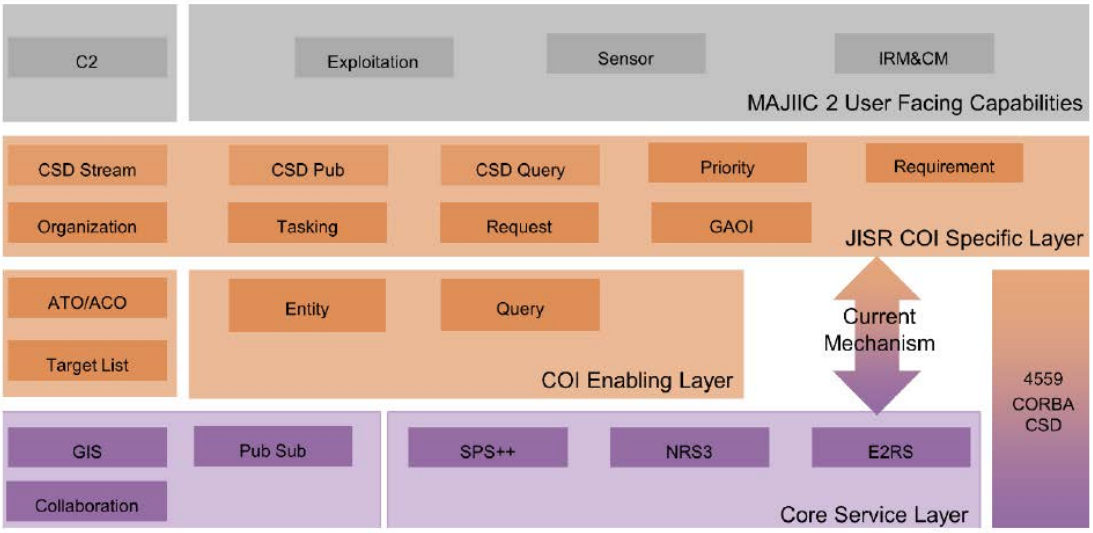


Figure 5.2 MAJIIC 2 service taxonomy as specified by the MAJIIC community (MAJIIC, 2015).

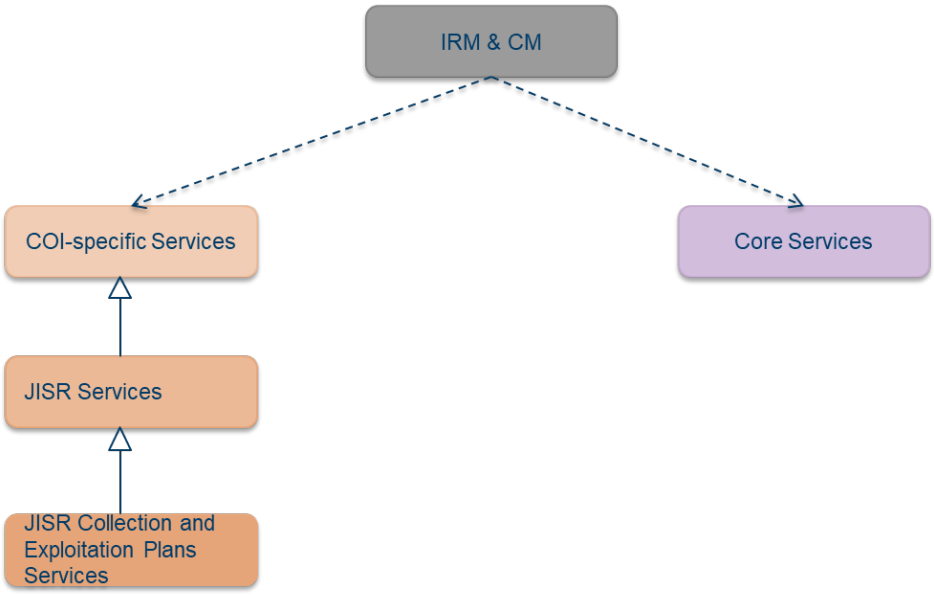


Figure 5.3 COI-Specific Services for the user-facing capability ICM & RM.

The reason for choosing the Request service is that this service is central for the workflow management that fulfils the RFI/ISR request choreography. In addition, the service interacts with a number of other COI Specific Services, and Core Services, and therefore serves as a good candidate for service decomposition.

5.1 Request for Information (RFI)

We assume that Unit 1 needs information from Unit 2, and therefore creates an RFI, specifying the information needed. The IRM & CM capability at Unit 1 creates the RFI, together with a Geographical Area Of Interest (GAOI). This information is then transferred to Unit 2 by means of the replication process between the SPS++ (Simple Persistence as a Service) service instances (the purpose of SPS++ is to store and disseminate business entities such as RFIs, order of battle, tasks, intelligence requests, etc).

In Figure 5.4, the sequence of events at Unit 1 is illustrated. The IRM & CM capability at Unit 1 first defines the Geographical area of interest (GAOI), which is stored in the SPS++ and replicated to other SPS++ instances. The IRM & CM capability then creates a new RFI, addressed to Unit 2, and with reference to the defined GAOI. Using a WS-Notification broker, the SPS++ then creates a notification about the event, which is then disseminated to all subscribers. The content stored in SPS++ at Unit 1 is then replicated to other SPS++ instances, including the one at Unit 2.

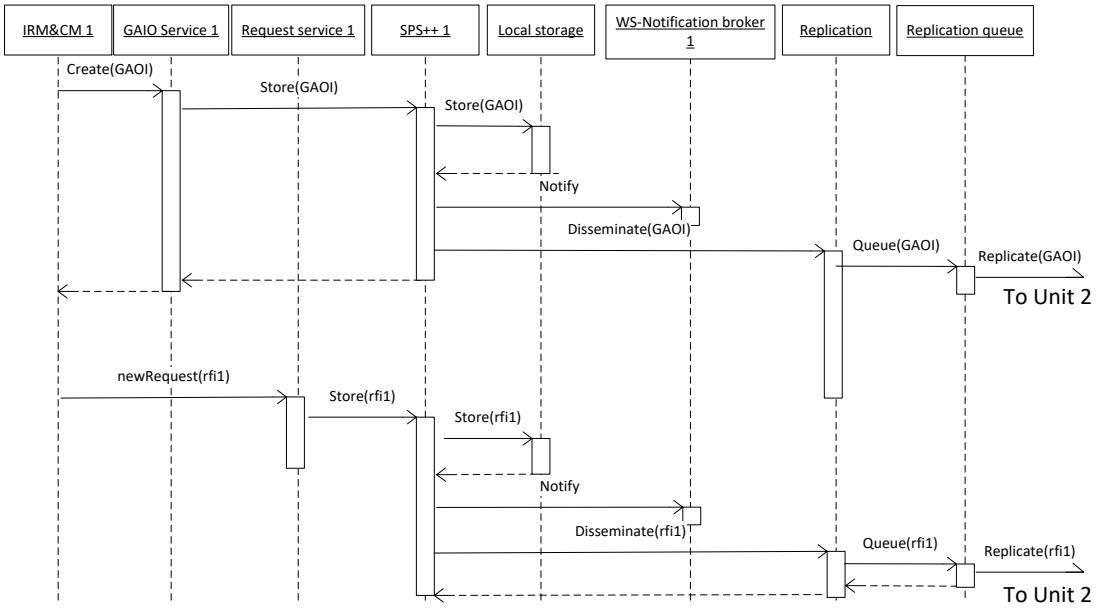


Figure 5.4 Unit 1 creates GAOI and RFI, which are replicated to Unit 2.

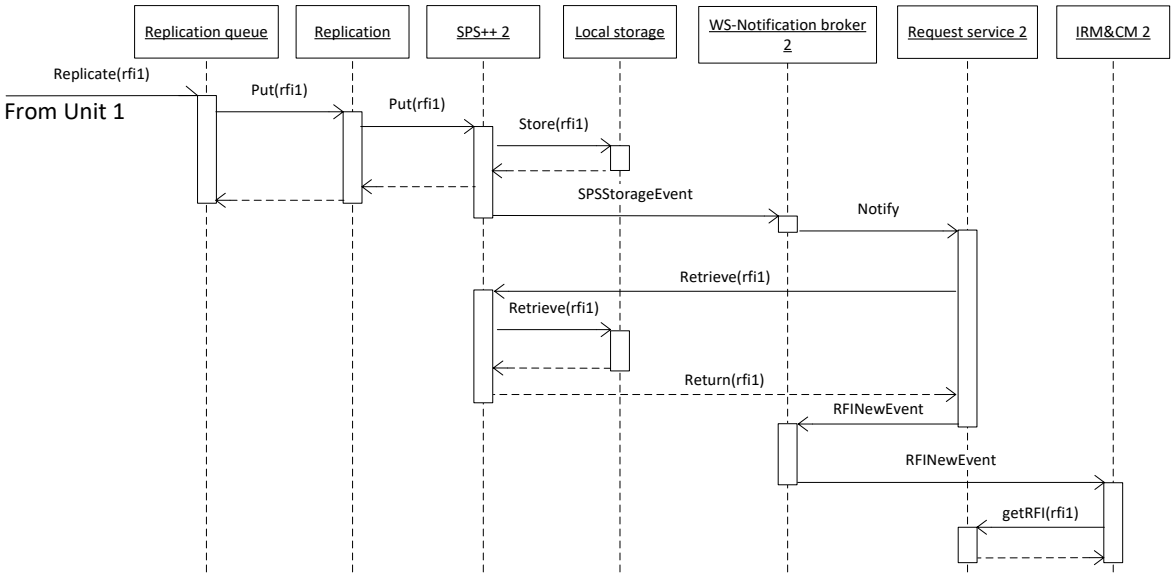


Figure 5.5 Unit 2 receives RFI from Unit 1.

Figure 5.5 shows the sequence of events at Unit 2. For simplicity reasons, the replication of GAOI is not shown at Unit 2, but this process would be equal to the synchronization of the RFI. After having received the RFI, the SPS++ at Unit 2 sends a notification about its new content to the local WS-Notification broker, which in turn notifies Request service that the SPS++ has new data. Via the WS-Notification broker, the Request service then notifies IRM & CM at Unit 2 that a new RFI has arrived. Finally, the IRM & CM at Unit 2 retrieves the RFI from the local request service.

Summarizing, we have one user facing capability:

- User-facing capability: IRM & CM

In addition, we have the following set of technical services:

- COI-Specific Services: Request service and GAOI service

- Core Services: SPS++, Replication service and WS-Notification (denoted WS-Notification broker in the figures) services. Note that these services are not shown in Figure 5.2, since the decomposition work done in MAJIIC 2 did not go beyond COI-Enabling Services.

These services and the dependencies between them are illustrated in Figure 5.6.

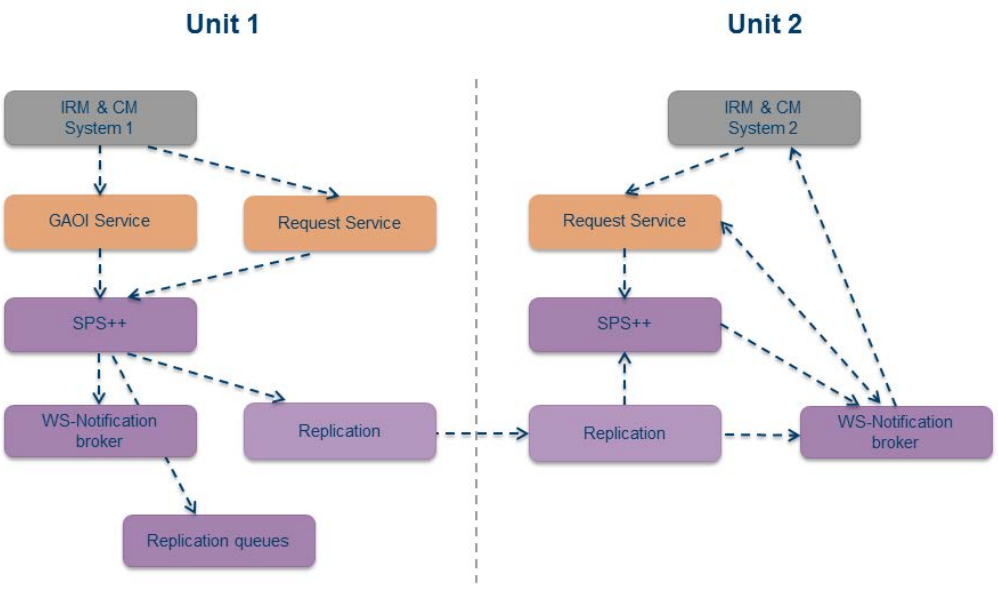


Figure 5.6 Identified services for the Replication service as used by the IRM & CM capability.

Next, we decompose the Core Services, listed above, together with descriptions of the services. We have also used the service specifications in MAJIIC 2. Since the level of detail in the JISR use cases and the MAJIIC 2 technical descriptions of the services varies, the level of decomposition for the different Core Services varies correspondingly.

As mentioned above, the purpose of the SPS++ service is to store and disseminate business entities such as RFIs, orders of battle, tasks, intelligence requests, etc. Based on the available information, we have decomposed SPS++ into the set of Core Services from the C3 Taxonomy, shown in Figure 5.7.

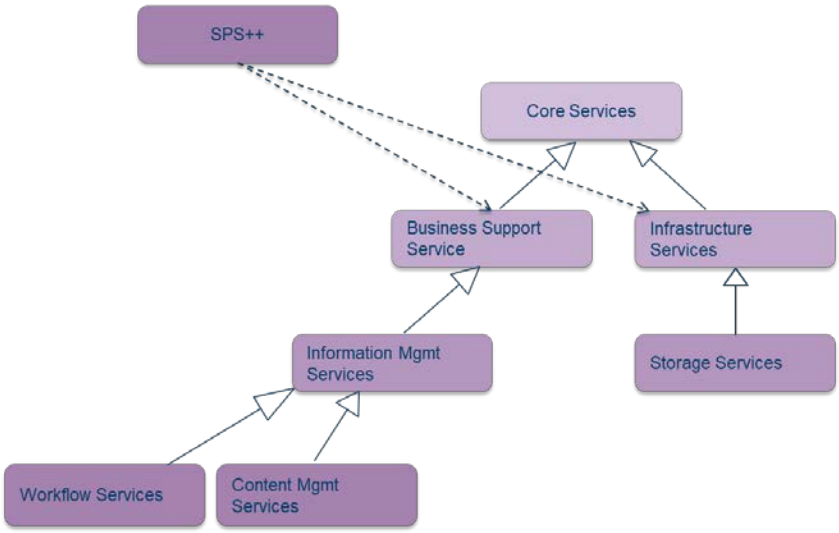


Figure 5.7 Decomposition of the SPS++ service.

Next, we decompose the Replication service, as shown in Figure 5.8.

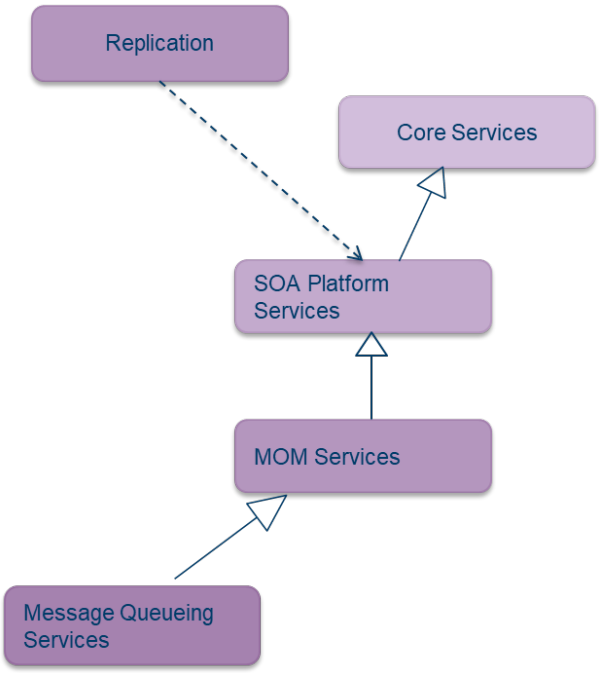


Figure 5.8 Decomposition of the Replication service.

Finally, the WS-Notification service is decomposed as shown in Figure 5.9.

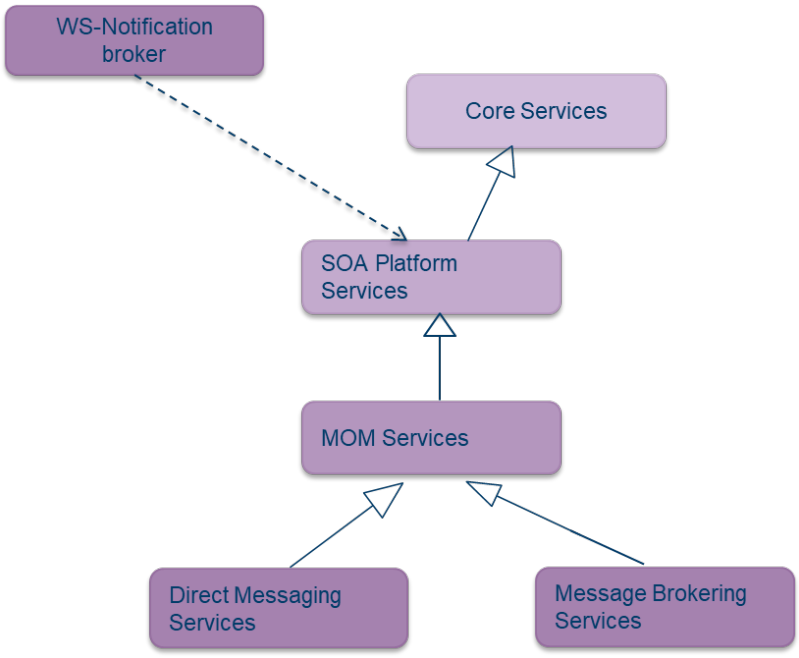


Figure 5.9 Decomposition of the WS-Notification service.

In Figure 5.10 we have placed all the identified services together. This figure effectively shows the C3 Taxonomy version of Figure 5.6, and thus, identifies the Core Services necessary for realizing the Request service, as used by the IRM & CM capability (note that this is not a complete decomposition of the IRM & CM capability; other use cases can include additional COI-Specific, COI-Enabling and Core Services).

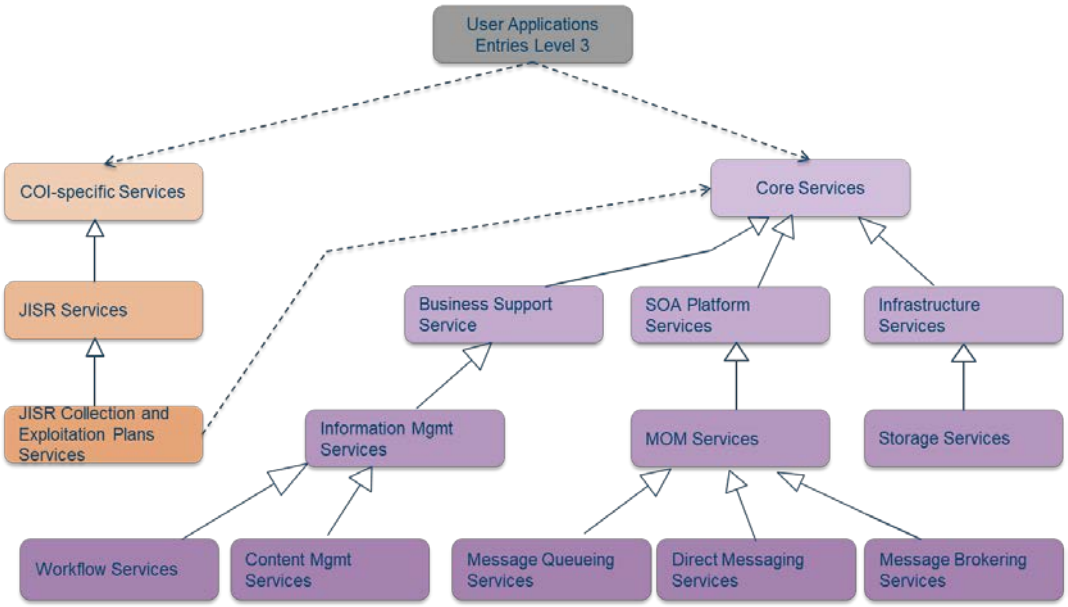


Figure 5.10 Classification of services included in the Request Service use case, according to the C3 Taxonomy.

5.2 Requirements

The MAJIIC documents do not provide much detail with respect to requirements to these services. There are, however, some non-functional requirements listed for the SPS++ service (MAJIIC, 2015):

- The service must be able to handle up to 64,850 business entities per day, with an average size of 20 kB per business entity.
- The implementation of SPS++ must use an asynchronous message pattern when exchanging business entities with other SPS++ instances.
- For the SPS++ Local storage, all storage action must be guaranteed to be performed, i.e., corresponding to the transaction concept in database systems.

For the replication service, the SPS++ documentation specifies that the inbound queue is recommended to support “a few thousand” elements in the queue. In addition, entities must not be removed from the inbound queue until they are stored locally. The outbound queue must be unlimited in size, and support durable write (i.e., information must not be lost).

6 Modeling and simulation service decomposition

Modeling and Simulation (M&S) encompasses a COI that focuses on applying specialist software and techniques to model and simulate military networks, military units and other aspects of defense. Examples of M&S use cases include C2-sim, which focuses on feeding C2 systems with simulated information to train commanders in using the C2 system in a realistic setting, and computer-assisted exercises (CAX), where modeling and simulation techniques are used to augment and enhance the overall training experience.

Current M&S systems are mostly stovepiped, involving monolithic software approaches and vendor-specific packages (Siegfried, Lloyd, & Van Den Berg, 2018). NATO is moving towards a SOA approach with composable, reusable services with well-defined interfaces, which is also reflected in current trends in Federated Mission Networking (FMN). Hence, the future of M&S needs to align with this approach as well. Not only to remain viable in joint NATO exercises, but also from a national perspective it makes sense to avoid vendor lock-in by adopting services where the interfaces are well defined. In key with this approach was the NATO Modeling and Simulation Group on M&S as a Service, MSG-136 for short. This recently concluded group focused on how one could start transitioning from legacy modeling and simulation approaches involving stovepipes, towards future-oriented and FMN-aligned approaches involving virtualization of software, containerization of components and finally leveraging hybrid deployments where services could reside inside or outside a cloud (Siegfried, Lloyd, & Van Den Berg, 2018). Since training is an important part of preparations for operations, and M&S can be used for training purposes, the approach of MSG-136 is interesting. Hence, we will investigate a specific M&S use case from that group in this report. The group concluded in 2017, and the group's final report was a publication in several volumes, covering central aspects such as architectural overview, technical architecture recommendations, and suggested standards to employ (MSG-136 vol 1-3, 2018). It is important to note that the service decompositions presented in this report were performed using the same style and approach as the operational use cases already covered. Hence, our M&S service decomposition may differ from that of the MSG-136 group in certain areas.

From a bird's eye perspective, the group's outcome is a proposal called Allied Framework for M&S as a Service (MSaaS), which is illustrated in Figure 6.1. The figure was fetched from (Siegfried, Lloyd, & Van Den Berg, 2018), which presents a synopsis of the MSaaS and the group's work.

The Allied Framework for MSaaS is the common approach of NATO and Nations for implementing MSaaS. It enables:

1. The community of users to discover new opportunities to train and to work together.

2. Users to enhance their operational effectiveness, saving costs and effort in the process.

3. M&S services that are readily available on-demand and deliver a choice of applications in a flexible and adaptive manner.

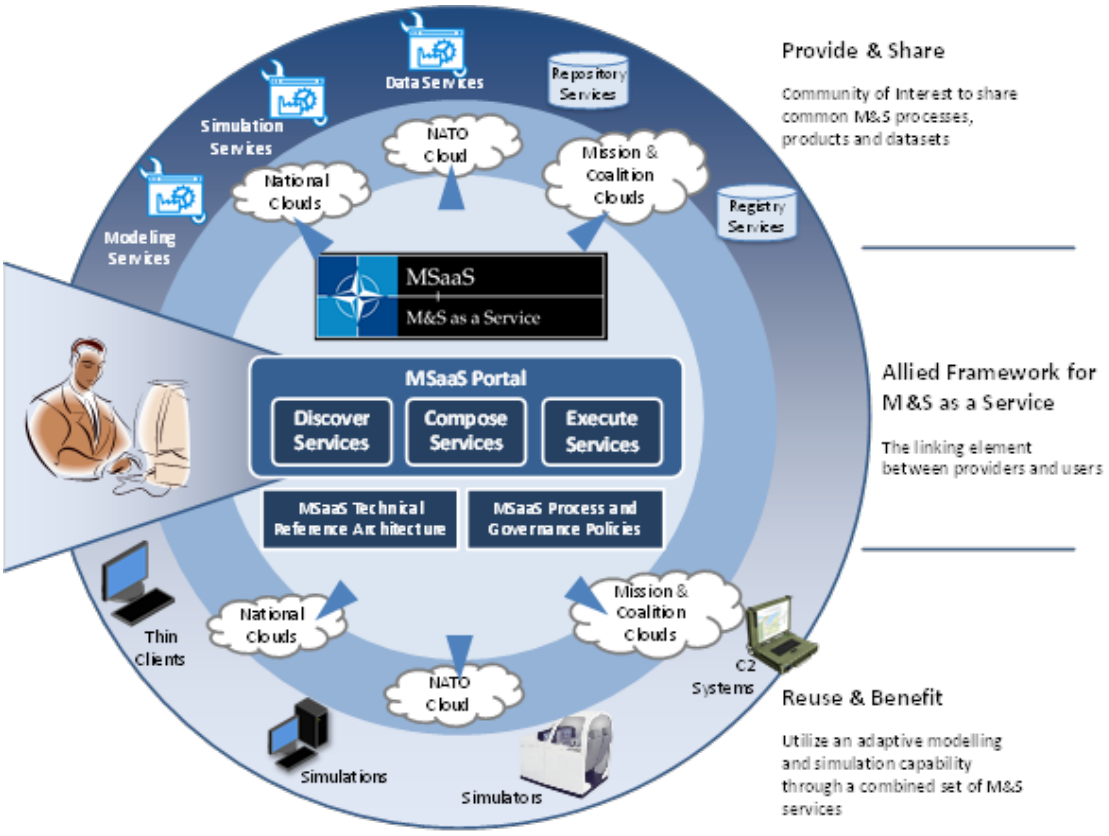


Figure 6.1 MSaaS Concept (Siegfried, Lloyd, & Van Den Berg, 2018).

6.1 MSaaS use case

The MSG-136 group has shown the MSaaS concept to be viable through a proof-of-concept implementation using Docker for containerization and various cloud providers, including Amazon Web Services public cloud, to host the services (Siegfried, 2017). The technical demonstration concept is illustrated in Figure 6.2.

In the proof of concept, C2-sim was chosen as the use case. In this use case, M&S services interact with an actual C2 system. This C2 system belongs to a given COI, e.g., land or air. When decomposing M&S services, we focus on the M&S specific services, and do not include the C2 system as such in the M&S COI. Hence, we do not discuss the C2 component further here, but suggest that the reader pursues the C2 specific chapters of this report for further details. As for the M&S COI, a tool named PAXSEM was being used:

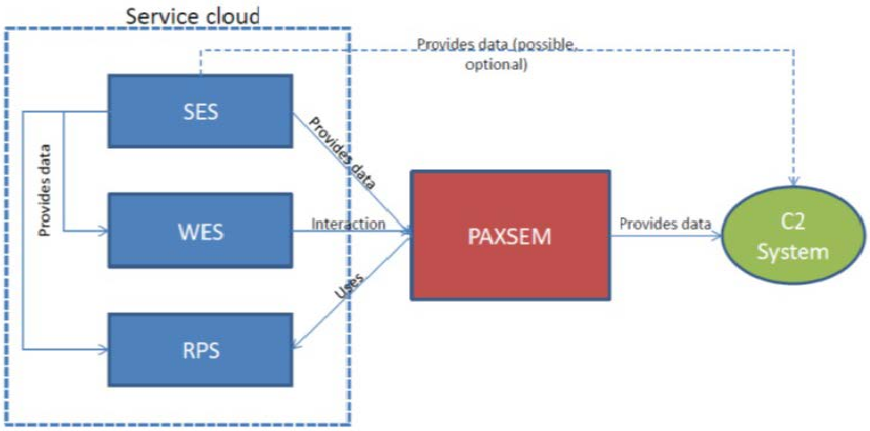


Figure 6.2 Technical demonstration concept – use case C2-sim. Components include SES (Synthetic Environment Service), WES (Weapons Effect Service), RPS (Route Planning Service) and how these support the PAXSEM tool, which drives the simulation and provides data to the C2 system.

> "PAXSEM is an agent-based simulation model developed by CASSIDIAN since 2008 on behalf of the German Bundeswehr. PAXSEM enables a detailed, physically based representation of technical systems as regards the combined application of sensors (optical/infrared/radar) and effectors (point/area weapons, rockets/controlled missiles/fire-and-forget). All contained agents act according to their predefined complex rule sets just like in the real world. Within PAXSEM, as a multi-agent system, their individual behavior is coined by mutual influences. Unlike their isolated behavior, the collective behavior of all agents cannot be accurately predicted. PAXSEM hence represents complex systems. Furthermore, it allows the highly resolved 3D visualization of technical-tactical scenarios and plots. Within these, military units are represented as agents in a granularity from single entity to enforced company level. The simulation environment offers a flexible level of detail which is to be aligned with the examination subject. In order to generate even more added value, its expandability comprises the combination with third party models (e.g., weapon effect service), detailed modules (e.g., communication model), free-to-choose landscapes and real systems (e.g., in a testbed)." (Kallfass & Schlaak, 2012)

Here, PAXSEM represents a legacy (but modular) system that can be coupled with an MSaaS approach. We will treat PAXSEM as a "black box" between the services and C2 system here, and not delve further into its innards. However, its modular approach allows us to deploy services to a cloud that can provide certain functionality to PAXSEM. This aspect was leveraged in the MSG-136 proof-of-concept, where PAXSEM was coupled with a Synthetic Environment Service (SES), a Weapons Effects Service (WES), and a Route Planning Service (RPS) as shown in Figure 6.2:

1. SES provides scenario data to RPS and PAXSEM.

2. PAXSEM uses RPS for route planning in the scenario.

3. PAXSEM uses WES for calculating weapons effect in the scenario.

4. PAXSEM provides data to C2 System (or equivalent) (optional: Battlefield Markup Language (BML) orders).

In our opinion, these three services (SES, WES, RPS) used by PAXSEM are in key with current trends in NATO, which looks towards SOA for building loosely coupled, interoperable systems. Hence, we will have a closer look at these services in context of the NATO C3 Taxonomy, in an effort to decompose them all the way down to specific Core Services.

6.2 Service placement in the C3 Taxonomy

When considering the services SES, WES, and RPS it is evident that they are definitely of use to the M&S COI. However, this does not necessarily prescribe that they should be considered COI-Specific Services. These services can be used by the M&S COI, true, but if they can be considered usable also by other COIs then they need to be considered COI-Enabling Services. Or, if a service can be considered so basic, so foundational, that it can even be usable across different higher-level COI-Enabling Services, then it should be considered a Core Service.

Let us explore the three services in turn, in order to establish their logical placement in the C3 Taxonomy. The conclusion of the discussion below is presented in Table 6.1.

A SES provides synthetic environment data that can be fed into either a simulator or a C2 system (in the case of C2-sim). Hence, a SES can be seen as the M&S counterpart of a Map service, which would provide actual map data and not merely synthetic terrain. Map services, e.g., Web map services, are considered Core Services. Should then a SES be considered a Core Service as well, since it may implement the same interface, but deliver data that is synthetic rather than a representation of an actual physical area? To better be able to decide on a suitable placement in the taxonomy, we will specifically consider the use case from MSG-136, in which case this service, and the other two, were being used in a C2-sim scenario. Further, let us consider that the case is to support a land C2 system in this simulation. Then, the synthetic environment service must be able to deliver a synthetic land environment, and this land environment is delivered both to the land C2 system (to visualize it and the simulated forces to the commander) as well as being fed into the simulator (PAXSEM) which moves the simulated forces in this synthetic environment. This means that the SES is being consumed both by a land C2 system as well as a simulation system. Hence, it makes sense to consider the SES a COI-Enabling Service in this use case, since it can support systems from two different COIs.

The WES provides synthetic data on weapons effects that can be used by the simulator (PAXSEM) to decide effects of weapons in a given terrain and potentially also effects on nearby

simulated forces. Hence, the WES provides data to the simulation system, but it is also a consumer of the SES in order to determine the effect of a given weapon in a specific area of the synthetic environments, taking any geographical implications into account. For this specific use case of C2-sim, the WES can typically be considered a COI-Specific Service since it applies only to the M&S COI. On the other hand, if we generalize, a WES could potentially be considered a COI-Enabling Service, in that effects of weapons (and potentially visualizing that in a C2 system) could be considered a welcome and future application of such a service in manoeuver planning, for example. Here, however, we focus on its current application and implementation as used in the MSG-136 proof-of-concept, in which case the WES is arguably a COI-Specific Service.

The RPS is generic enough to be considered a Core Service. We can envision that route planning could be a part of Geospatial Services, which are situated at the Core Services level. However, we could also argue that route planning needs to be specialized with regard to the domain it is supporting. For example, route planning for land forces, who typically move across the terrain would be different than route planning for air forces, who would have different needs here not only because they have an extra dimension (altitude) to consider in their route planning, but also a matter of timeliness constraints since some air forces typically move much faster than land forces. So, it would make sense to offer different RPS for different COIs. Conversely, for the MSG-136 specific use case for its RPS for land forces C2-sim, it makes sense to consider the RPS as a COI-Enabling Service. The RPS can take land terrain data into account (for example as provided by the SES) and plan a route across the terrain, be it synthetic or real. The way the RPS was being used, though, was as a COI-Specific Service, since for the proof-of-concept it was fed only synthetic data and provided routes to the simulator (PAXSEM) based on this data. However, a land forces RPS will, in a broader context be of use both to the land COI for navigation as well as to the M&S COI for pure simulation purposes or as a cross-COI effort in the case of land C2-sim. So, it is probably the best approach to consider the RPS COI-enabling at this point.

Service	***Placement in C3 Taxonomy***
Synthetic Environment Service (SES)	COI-Enabling Service
Weapons Effect Service (WES)	COI-Specific Service
Route Planning Service (RPS)	COI-Enabling Service

Table 6.1 Service placement in the C3 Taxonomy.

6.3 Service decomposition

Following the categorization of the SES, WES, and RPS as COI-Enabling, COI-Specific, and COI-Enabling Services, respectively, we need to consider further decomposition of said services in an attempt to establish how they rely on other services from the C3 Taxonomy.

Figure 6.3 shows the services in context of the C3 Taxonomy.

Figure 6.4 shows decomposing the RPS into its reliance on various Core Services. Note that at this level the RPS will decompose into the same building blocks as the SES (as illustrated in Figure 6.5), since there are no fundamental differences between them in this context. However, if we further decompose the Geospatial Services component (see Figure 6.6), then the differences become evident. Here, the RPS will typically rely on Geospatial Web Map Services and Geospatial Terrain Analysis Services. The SES, on the other hand, will have no need for the Geospatial Terrain Analysis Services. Note that this and the other services are intended to be deployed as cloud services to fully realize the MSaaS concept. Hence, they rely on Infrastructure Services, namely Infrastructure Processing Services, Infrastructure Storage Services, and finally (not shown for brevity) Infrastructure Networking Services.

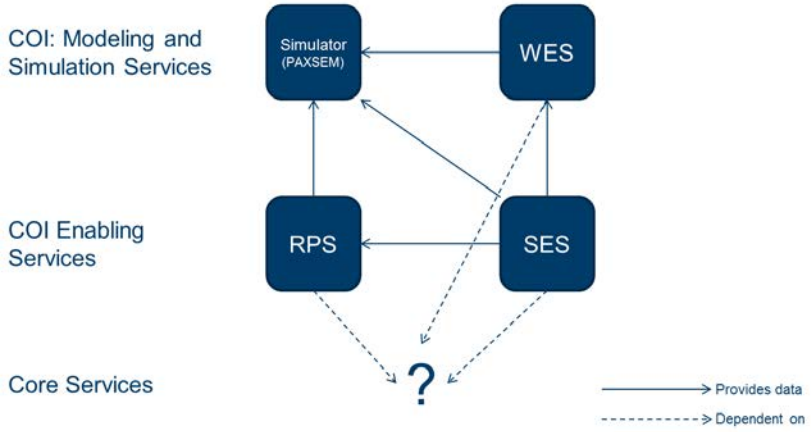


Figure 6.3 The Synthetic Environment Service (SES)/Weapons Effect Service (WES)/Route Planning Service (RPS) in context of the C3 Taxonomy.

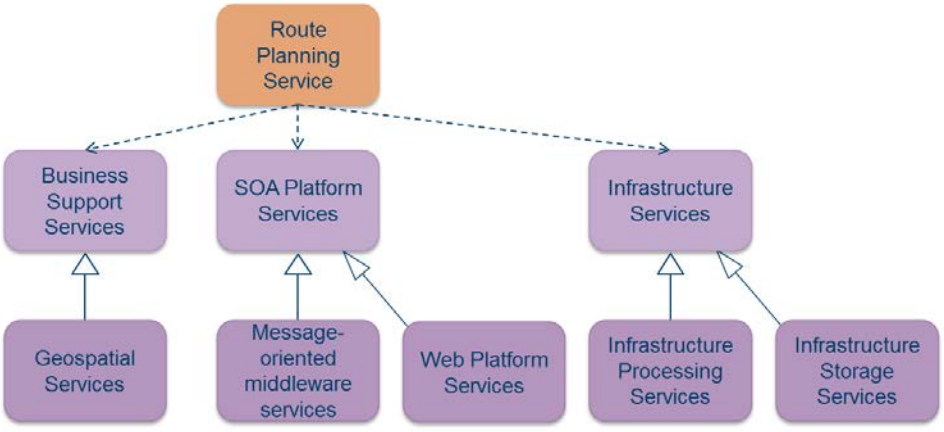


Figure 6.4 Decomposing the Route Planning Service.

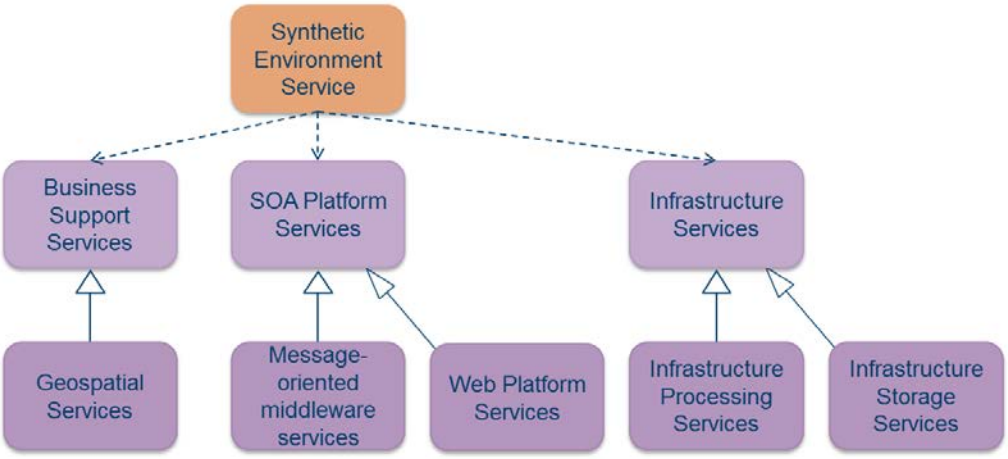


Figure 6.5 Decomposing the Synthetic Environment Service.

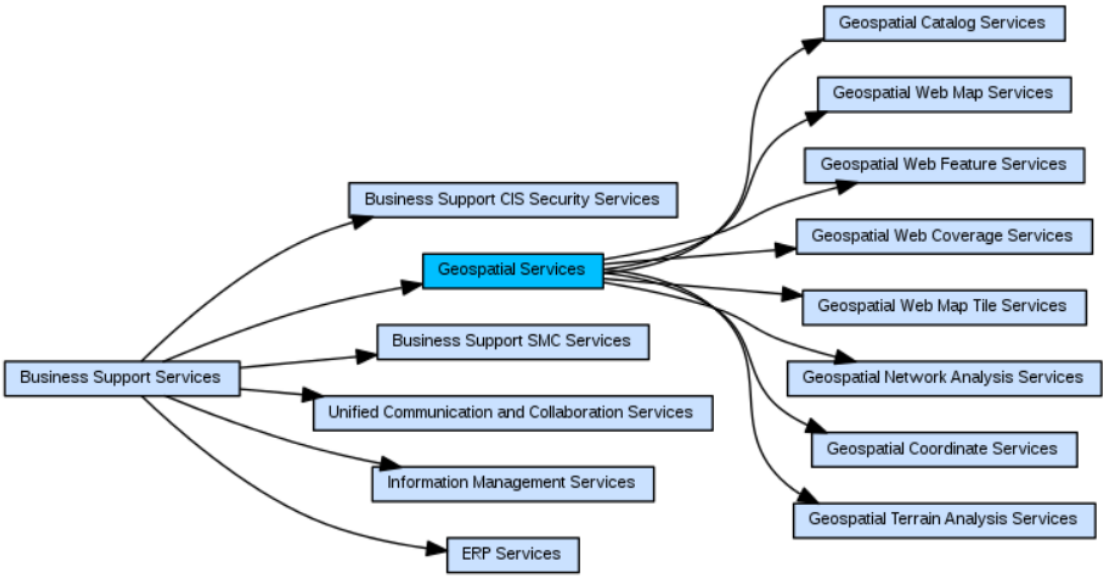


Figure 6.6 Decomposing the Geospatial Services.

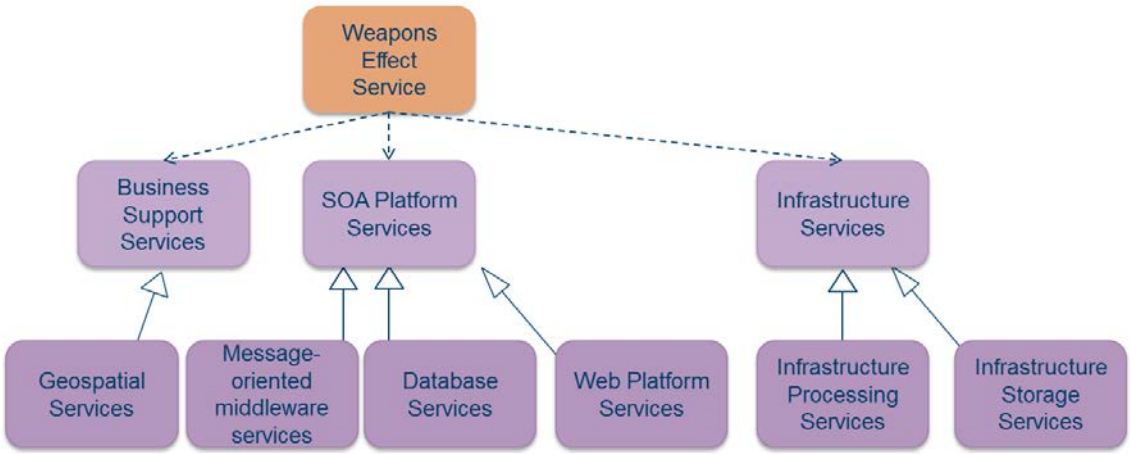


Figure 6.7 Decomposing the Weapons Effect Service.

Figure 6.7 shows the decomposition of the WES. Here we see that the WES has many of the same Core Service needs as the RPS and the SES. Note, however, the addition of Database Services, since the WES will need to access a database on weapons effects to be able to provide its service. Further, if we look closer at the Geospatial Services aspect, the WES will consume synthetic environment data as provided by the SES. Furthermore, it relies on a form of Geospatial Terrain Analysis Services (see Figure 6.6), but for a different purpose than the RPS. In the WES, the terrain analysis will pertain to how the terrain affects applying a certain weapon to a certain (synthetic) area. This is in contrast to the RPS, where the analysis is geared towards whether it makes sense to suggest a route for moving a unit across a certain portion of the (synthetic) terrain.

6.4 Requirements

The M&S COI has diverse requirements, depending on what the specific application of M&S is. In this chapter we have focused on C2-sim aspects, which model and simulate complex operations involving highly mobile units operating in synthetic terrain. To be useful as support in an exercise, the services involved need to meet real-time or near-real time requirements. Hence, the most important non-functional aspects here are performance and reliability of the services. Performance-wise the services must be supported by adequate processing, storage, and networking capacity to handle the load during the exercise. Leveraging cloud computing aspects is key here, since it allows for on-demand and elastic scaling of resources. Further, M&S typically needs both direct messaging (as the case of SES/RPS/WES) as well as brokered messaging to drive the M&S bus, which typically has real-time and reliability built in. For direct messaging, typically Web services are useful (e.g., the RPS implements a Representational state transfer (REST) Web Processing Service API (OGC, 2018)). For brokered messaging, there are

specific solutions that are employed for M&S that meet the demands of the COI, typically the High-Level Architecture (HLA) (IEEE, 2010).

The M&S COI will need to rely on service management and control (SMC) aspects to control, monitor and meter service use (some capabilities involve a pay-as-you-go principle, with higher fidelity models costing more to use than low fidelity models). Also, service discovery, part of SMC, is important to look up and choose appropriate services to use in a certain exercise, based on fidelity, cost, availability, and other parameters the operator may consider. Further, though not explicitly shown in this chapter, where focus has been on technical machine-to-machine aspects of the services, it is also necessary to use Unified Communication and Collaboration Services for those parts of M&S that require human interactions. For example, in the phase prior to running the simulation when everything is being set up, communicating with the owners of different M&S services will be necessary. Finally, security is an important aspect that permeates all applications of services; hence it was also not made explicit in the service decomposition here. However, adequate measures to support integrity, confidentiality and availability must be applied.

7 Additional considerations

In the use cases in Chapters 3, 4, 5, and 6, we have identified both the COI Services and Core Services needed to perform a given task within the different COIs. However, these analyses are limited to identifying the direct dependencies – only the services that are directly required to perform a task are mentioned in the previous chapters. In addition to these direct dependencies there are other services, particularly at the Core Services level, which must be present in the information infrastructure.

Furthermore, our use case analyses do not cover any potential dependencies between the Core Services themselves.

In this chapter we highlight some important Core Services that are not a part of the use cases, but are required either as indirect dependencies, or because they are used by other Core Services.

7.1 Security and Service Management & Control

Though not merely a part of the Core Services, Security and Service Management & Control (SMC) permeate the C3 Taxonomy as vertical bars as illustrated in Figure 2.1. This indicates that for all services and at all levels, security and SMC aspects must be considered and provided for.

Without support from these services categories, the Core Services highlighted in our analysis would be lacking essential security properties like confidentiality, integrity, and availability, as well as SMC capabilities like service discovery (the process of finding service descriptions that enable a consumer to properly utilize a service), leaving a service-oriented information infrastructure with severe deficiencies.

7.2 Dependencies between Core Services

Some Core Services depend on others to provide their functionality. This is in alignment with SOA principles, where functionality is broken down into specific building blocks that implement well-defined application programming interfaces (APIs) to feature loose coupling, late binding and the re-use of existing components.

In order to illustrate this point, consider for example Geospatial Services. Such services will rely on Message-Oriented Middleware Services, Web Platform Services and Database Services (to name a few) to be able to realize the communication, storage and provisioning needed for these services.

8 Analysis Summary

Given the analysis in chapters 3-6, we created the matrix in Figure 8.1 to identify the different COI's reliance on specific Core Services. It can be seen that the Core Services that are highly relied on, and thus are the top candidates when considering which Core Services to implement in a service-oriented information infrastructure, are:

- Geospatial Services (particularly Geospatial Network Analysis Services, Geospatial Coordinate Services and Geospatial Terrain Analysis Services)
- Message-Oriented Middleware Services (particularly Direct Messaging Services, Message Brokering Services and Message Queueing Services)
- All of the Infrastructure Storage Services

The Core Services that are somewhat relied on are:

- Unified Communication and Collaboration Services (specifically for C2 applications)
- Information Management Services (particularly Content Management Services, Workflow Services and Analytics Services)
- Information Platform Services (specifically for C2 applications)
- Mediation Services (specifically for C2 applications)

In addition to this, we emphasize the need to include security and service management and control services as well as identify whether the Core Services listed here have important dependencies to other Core Services which in case also should be considered for inclusion in an infrastructure.

			Communities of Interest			
			Air C2	Land C2	Joint ISR	Modelling & Simulation
Business Support Services	Unified Communication and Collaboration Services	Military Messaging Services	✓	✓		
		Informal Messaging Services	✓	✓		
		Fax Services	✓	✓		
		Calendaring and Scheduling Services	✓	✓		
		Video-based Communication Services	✓	✓		
		Audio-based Communication Services	✓	✓		
		Text-based Communication Services	✓	✓		
		Whiteboarding Services	✓	✓		
		Presence Services	✓	✓		
		Time Zone Data Distribution Services	✓	✓		
		Application Sharing Services	✓	✓		
	Information Management Services	Content Management Services		✓	✓	
		Workflow Services		✓	✓	
		Search Services		✓		
		Analytics Services	✓	✓		
		Language Support Services		✓		
		Archiving Services		✓		
	Enterprise Resource Planning Services	Financial Resource Management Services				
		Human Resource Management Services				
		Supply Chain Management Services				
		Project Planning Services				
	Geospatial Services	Geospatial Catalog Services		✓		✓
		Geospatial Web Map Services		✓		✓
		Geospatial Web Feature Services		✓		✓
		Geospatial Web Coverage Services		✓		✓
		Geospatial Web Map Tile Services		✓		✓
		Geospatial Network Analysis Services	✓	✓		✓
		Geospatial Coordinate Services	✓	✓		✓
		Geospatial Terrain Analysis Services	✓	✓		✓
SOA Platform Services	Message-Oriented Middleware Services	Direct Messaging Services	✓	✓	✓	✓
		Message Brokering Services		✓	✓	✓
		Message Routing Services		✓		✓
		Message Proxying Services		✓		✓
		Message Queueing Services		✓	✓	✓
		Message Caching Services		✓		✓
	Web Platform Services	Web Hosting Services				✓
		Web Presentation Services				✓
	Database Services	Non-relational database Services				✓
		Directory Services				✓
		Relational Database Services				✓
	Information Platform Services	Information Discovery Services	✓	✓		
		Information Access Services		✓		
		Information Aggregation Services	✓	✓		
		Metadata Repository Services	✓	✓		
		Information Annotation Services	✓	✓		
		Business Rules Services		✓		
	Composition Services	Orchestration Services				
		Choreography Services				
		Transaction Services				
	Mediation Services	Protocol Transformation Services	✓	✓		
		Data Format Transformation Services	✓	✓		
Infrastructure Services	Infrastructure Processing Services	Operating System Services				✓
		Virtualized Processing Services				✓
	Infrastructure Storage Services	Block-Level Storage Services	✓	✓	✓	✓
		File System Storage Services	✓	✓	✓	✓
		Blob Storage Services	✓	✓	✓	✓
	Infrastructure Networking Services	Caching Services				
		Proxying Services				
		Host Configuration Services				
		Network Load Balancing Services				
		Printing and Scanning Services				
		Data Transfer Services				
		Domain Name Services				
		Distributed Time Services				
		Remote Access Services				

Figure 8.1 A summary of the different COI applications' reliance on specific Core Services.

9 Conclusion

Both FFI and the DST Group are planning experiments in order to provide advice to their respective armed forces regarding the development of information infrastructures with the necessary characteristics for military use. As the prevailing way of building such infrastructures is according to the principles of service orientation, a part of the preparations for such experiments is to identify what services are essential to implement in the information infrastructures. In this report we have followed a use case driven approach to start identifying these services.

The use cases were chosen from four different military communities of interest in order to provide the analysis with sufficient variety without promising to be exhaustive:

- Establishing situational awareness and performing targeting and dynamic planning in the air domain.
- Establishing situational awareness and planning a tactical manoeuver in the land domain.
- RFI submission in JISR.
- Providing M&S as a service.

In this work, the NATO C3 Taxonomy was used as a common tool and language for decomposing the above use cases. The use cases were first decomposed into functional services from the COI Services. This decomposition was then used to identify the Core Services that each use case relies on. By utilizing the C3 Taxonomy in this way we have shown that it is applicable across disparate domains.

The analysis in this report identified the following Core Services as candidates to first inclusion in the information infrastructures due to their importance across the use cases:

- Infrastructure Storage Services.
- Message-Oriented Middleware Services.
- Geospatial Services.

In addition to this, there is a need to include security and service management and control services as well as to identify whether the Core Services listed here have important dependencies to other Core Services which in case should be considered for inclusion.

Future work in this area will involve the development of experimental systems and information infrastructure. This development should begin with the three Core Services identified above and will be guided by the C3 Taxonomy. As the development of the C3 Taxonomy is an ongoing process, the insights gained from these experiments can also enable the identification of areas where the C3 Taxonomy requires further development.

References

ACT. (2016). *The C3 Taxonomy.*

ADF Warfare Centre. (2009). *ADDP 00.1 Command and Control, 1st edition.* Canberra.

Bartolomasi, P., Buckman, T., Campbell, A., Grainger, J., Mahaffey, J., Marchand, R., et al. (2005). *NATO network enabled capability feasibility study. Version 2.0.*

Erl, T. (2004). *Service-Oriented Architecture: A Field Guide to Integrating XML and Web Services.* Prentice Hall PTR.

Erl, T. (2005). *Service-Oriented Architecture: Concepts, Technology, and Design.* Prentice Hall PTR.

IEEE. (2010). *1516-2010 - IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA)-- Framework and Rules.*

Kallfass, D., & Schlaak, T. (2012). NATO MSG-088 Case Study Results to Demonstrate the Benefit if Using Data Farming for Military Decision Support. *Proceedings of the 2012 Winter Simulation Conference.*

MAJIIC. (2015). *MAJIIC 2 Business rules and use cases, DOP-MAJIIC2-026, version 6.0.*

MAJIIC. (2015). *MAJIIC 2 Simple persistence as a service (SPS++) documentation. Service version 4.4. Document version 4.0.*

MAJIIC2/OWG. (2013). *JISR TTP Draft v3.0.*

MAJJIC. (2015). *MAJIIC 2 JISR Interoperable capabilities concept within a coalition environment, DOP-MAJIIC2-115, Version 2.0.*

MSG-136. (2018). *Modelling and Simulation as a Service, Volume 1: MSaaS Technical Reference Architecture.*

MSG-136. (2018). *Modelling and Simulation as a Service, Volume 2: MSaaS Discovery Service and Metadata.*

MSG-136. (2018). *Modelling and Simulation as a Service, Volume 3: MSaaS Engineering Process.*

NATO. (2016). *AJP-2.7 Allied Joint Doctrine for Joint Intelligence, Surveillance, and Reconnaissance. Edition A, version 1.*

NATO ACT. (2015). *C3 Taxonomy Perspective, Baseline 2.0.*

NATO ACT. (2018). *Enterprise Mapping wiki*. Hentet fra https://tide.act.nato.int/em/index.php/C3_Taxonomy

Nordbotten, N. A. (2009). XML and Web services Security Standards. *IEEE Communications Surveys & Tutorials, 11*(3).

Object Management Group. (2018). *About the Data Distribution Service Specification Version 1.4.*

OGC. (2018). *Web Processing Service.*

Royal Australian Air Force. (2013). *The Air Power Manual, 6th edition.* Canberra.

Siegfried. (2017). M&S as a Service Briefing about NATO MSG-136 for SISO ENGTAM SG . Hentet fra https://www.sisostds.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=45262&PortalId=0&TabId=

Siegfried, R., Lloyd, J., & Van Den Berg, T. (2018). A New Reality: Modelling & Simulation as a Service. *Journal of Cyber Security and Information Systems, 6*(3).

Singhal, A., Winograd, T., & Scarfone, K. (2007). Guide to Secure Web services. I NIST, *Recommendations of the National Institute of Standards and Technology, NIST Special Publication* (ss. 800-95).

Sliwa, & Amanowicz. (2011). *Success Factors for SOA implementation in Network Centric Environment.*

Tilkov, S. (2007, March). *10 Principles of SOA, A frame of reference – for –SOA-related discussions*. Hentet fra SOA World Magazine: http://soa.sys-con.com/node/346363

About FFI

The Norwegian Defence Research Establishment (FFI) was founded 11th of April 1946. It is organised as an administrative agency subordinate to the Ministry of Defence.

FFI's MISSION

FFI is the prime institution responsible for defence related research in Norway. Its principal mission is to carry out research and development to meet the requirements of the Armed Forces. FFI has the role of chief adviser to the political and military leadership. In particular, the institute shall focus on aspects of the development in science and technology that can influence our security policy or defence planning.

FFI's VISION

FFI turns knowledge and ideas into an efficient defence.

FFI's CHARACTERISTICS

Creative, daring, broad-minded and responsible.

Om FFI

Forsvarets forskningsinstitutt ble etablert 11. april 1946. Instituttet er organisert som et forvaltningsorgan med særskilte fullmakter underlagt Forsvarsdepartementet.

FFIs FORMÅL

Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som kan påvirke forutsetningene for sikkerhetspolitikken eller forsvarsplanleggingen.

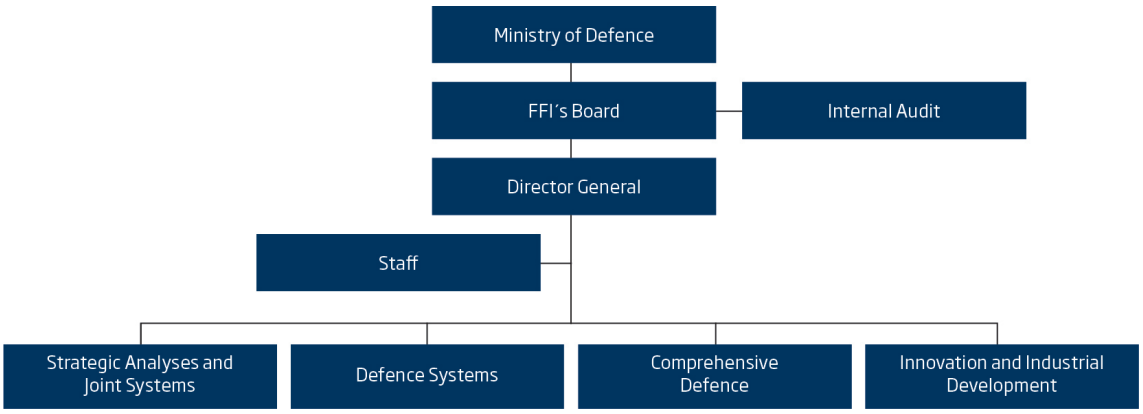
FFIs VISJON

FFI gjør kunnskap og ideer til et effektivt forsvar.

FFIs VERDIER

Skapende, drivende, vidsynt og ansvarlig.

FFI's organisation



Forsvarets forskningsinstitutt
Postboks 25
2027 Kjeller

Besøksadresse:
Instituttveien 20
2007 Kjeller

Telefon: 63 80 70 00
Telefaks: 63 80 71 15
Epost: ffi@ffi.no

Norwegian Defence Research Establishment (FFI)
P.O. Box 25
NO-2027 Kjeller

Office address:
Instituttveien 20
N-2007 Kjeller

Telephone: +47 63 80 70 00
Telefax: +47 63 80 71 15
Email: ffi@ffi.no

FFI Forsvarets forskningsinstitutt