



DEFTA

Information in Network Based Operations

WP2

Danish Defence Target Architecture (DEFTA)

Version 1.0
Released June 2011

This page is left intentionally blank

Abstract

This report is part of the Danish Defence Target Architecture (DETFA) for information and communication technology (ICT) systems. The report describes the result of work package 2 (WP2) of DEFTA, and the report deals with information in Network Based Operations (NBO). It includes an analysis of the requirements to the ICT systems in the Danish Armed Forces based on information and its desired characteristics. The requirements are analysed in a number of generic tasks derived from vignettes. Capability requirements are derived from the tasks, and this report contains the parts of these requirements that deal with information. The capability requirements cover the main ICT aspects of NBO and lead to a set of requirements to the information and consequently to the information systems in a number of relevant mission types. This includes both systems that are restricted to the military defence and systems that will also be used by the Total Defence. The derived requirements constitute a fundamental input to the technical target architecture of the Defence ICT Systems Architecture in the transformed Armed Forces.

This page is left intentionally blank

Summary

This report deals with information in network based operations (NBO) and is part of the Danish Defence Target Architecture (DEFTA). DEFTA is a high-level architecture spanning 10-15 years ahead, and DEFTA serves as the vision for evolutionary development of all information and communication technology (ICT) systems to be used in Danish Defence. The vision includes network and infrastructure development, sharing of information for operational and administrative domains, and interoperability for NBO. The work on DEFTA has been divided into four work packages (WP):

- WP0: Strategic vision and concepts for NBO
- WP1: Operational tasks and vignettes
- WP2: Information in NBO
- WP3: The technical architecture for the ICT systems.

The objective of WP2 is to derive a number of functional and technological requirements on DEFTA. WP2 is thus one important prerequisite for the establishment of the technical part of DEFTA and system architectures for the defence ICT systems.

The outcome of WP2 is an analysis of the information requirements in the Danish Armed Forces, and hence requirements to the ICT systems. The requirements have been developed from three points of view:

- The general mission independent requirements, i.e. requirements that to some degree are always present in military communication and information processing.
- Mission dependent requirements derived from selected tasks and vignettes of WP1 and the derived capability requirements.
- A number of technological requirements and other constraints have been identified.

The requirements will serve as constraints for the technical target architecture, and they are partly dealt with in WP2 and partly in WP3. Some of the requirements are related to the present situation, while most are future requirements, i.e. requirements to be fulfilled in the transformed military with its anticipated tasks. These requirements may not be completely fulfilled with the presently available technology, either because of economic constraints, or because the technology has not completely reached the adequate level of maturity.

It must be emphasised that the three points of view do not give a complete picture of the needs for communication and information processing in all three services nor in relation to the Total Defence enterprise. It is, however, deemed to be sufficient for the present objective: Establishing a target architecture framework that is able to take into account the foreseeable technological development. Thus, WP2 is just one - but important – input to WP3.

Communication is exchange of information. It is therefore possible to deduce the requirements for ICT systems from desired properties of information. Similarly, the information attributes will also be decisive not only for the information systems themselves but also for the required degree of interoperability between the systems. By focusing on information, and defining requirements to the information in form of desired values for its attributes, a number of requirements on the target (and later system) architecture may be derived, and it is therefore possible to evaluate a given form of architecture in terms of the degree to which it accommodates the required information attributes.

The attributes selected to characterise the information are shown in the Table 0-1. To clarify the applicability, a scale from 0 to 5 for each attribute has arbitrarily chosen. Table 0-1 shows the definitions of these values for the information attributes.

		ATTRIBUTE VALUE					
		0	1	2	3	4	5
Reach	Physical	None	Local/personal	Local area	Regional, LOS	Regional, BLOS	Global
	Logical	None	Point-to-point with no further disclosure	Multicast with limited disclosure	Networked with limited disclosure	Networked with some disclosure	Networked with full disclosure
	Organisational	None	Own unit	Own service	Joint	Combined	All actors, including but not limited to joint and combined
Richness	Richness	None	Single, predefined message	Predefined, limited message catalogue	Message catalogue including free text	Text, voice, picture	Full multimedia
Actuality	Timeliness	None	Best effort	Guaranteed delivery	Low jitter, isochronous	Soft real-time	Strict real-time
	Lifetime	None	> Years	Months / Weeks	Hours / Days	Seconds / Minutes	< Seconds
	Continuity	None	Sporadic update		Many updates (bursts)		Continuously update (streaming)
Assurance	Availability	None	Very low	Low	Medium	High	Very high
	Integrity	None	Tampering possible		Tampering is detected		Tampering not possible
	Confidentiality	None	Very weak	Weak	Medium	Strong	Very strong
	Authenticity	None	No source identification		Traceable source		Authorised identifiable sources only
	Non-repudiation	None					Guarantee
Intrinsic Quality	Precision	None	Low		Adequate (medium)		High
	Accuracy	None	Far from true value		Acceptable distance to true value		Close to true value
	Consistency	None	Many contradictory versions		Some contradictory versions		Homogeneity (high)

Table 0-1: Values of the information attributes and their definitions

By stating the information requirements as requirements on the information attributes we derive requirements for the communication and information systems and hence for the overall ICT architecture. This is shown in Figure 0-1.

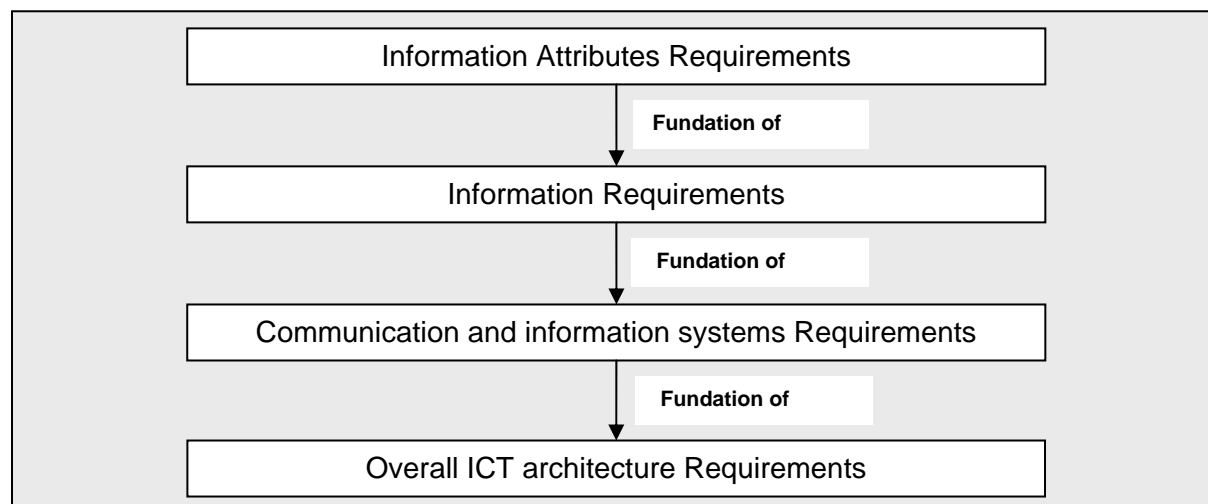


Figure 0-1: Information requirements inference

The above mentioned information attributes apparently have a significant impact on the degree of fulfilment of the requirements on the ICT systems. Other attributes such as completeness, cohesion and correctness (except for integrity issues) are not decisive for the ICT architectures, but certainly for the information systems themselves. They are therefore not considered in any significant detail. Completeness is mainly a property of the information source such as a sensor suite, and is therefore partly outside the scope of this work. Correctness has both roots in the information source and information assurance in the form of assurance of integrity, and falls partly outside the scope of this work package.

It must be noted that the concatenation of vignettes in the discussion of selected tasks has led to different types of communication and information processing. It is therefore not assumed that the derived requirements should be fulfilled by just one type of system, or by the activities of one organisational level.

The analysis is restricted to requirements to information and thus to communication and information systems in an NBO context. It does not to any significant extent include financial or organisational aspects, but is strictly for the purpose of establishing the technical target architecture.

Information Management (IM) is a key component for fulfilling the requirements to information. The requirements for the ICT systems in the NBO context are based on support of IM, i.e. getting the right information to the right system or person in the right format at the right time.

Based on the analyses, a number of conclusions may be drawn:

- The physical and logical reach of the information will be decisive for the design of communication infrastructure. The ability to exchange information with many different collaboration partners is important at all levels. Particularly regional Beyond Line of Sight (BLOS) communication is important.
- Information actuality (even real time) is particularly important, but time criticality is always present.
- The availability of services (including communications) will play an important part for the architecture, and forces redundancy to be built in.
- The task and its nature are not very stable, and in many cases it must be possible to improvise.
- Operating in cyberspace will increase in importance.

These requirements must be seen in relation to the overall assumption that all operations should be network based, and that agility in executing operations must be supported.

Several other attributes may often have to be adapted to the actual circumstances. As an example, the requirements for richness and precision may be compromised if the transmission capacity is limited.

The support for agility in organisation, and in command and control is a basic requirement. This will inevitably lead to use of adaptive or adaptable technologies such as ad hoc networks, software defined and cognitive radios, mobile code, and service-oriented architectures. These systemic aspects have been considered and lead to a mixture of absolute and desirable requirements. It is to be expected that many of the discretionary requirements will become absolute, mandatory, within the time span of 10 to 15 years. It is therefore an imperative that the target architecture supports both kinds of requirements to the fullest possible extent.

The demands for rich and accurate information with many stakeholders show an apparently never ending increase. The basic properties of information show that storage capacity and processing power to some extent can relieve the demands for high capacity communication. Whether these facilities shall be local to the unit or the single soldier or dispersed in the cloud of networks and computers remain to be seen. The implications for the technical part of DEFTA are far reaching.

Finally it should be mentioned that non-functional requirements such as flexibility, scalability, using civilian ICT, and cost effective solutions will also influence the technical part of DEFTA.

Contents

Abstract.....	iii
Summary.....	v
Contents.....	ix
Figures.....	xi
Tables.....	xi
1 Introduction.....	1
1.1 Overview of DEFTA.....	1
1.2 Objective and Scope of WP2.....	4
1.3 General Background and Constraints.....	4
1.4 The Method Used.....	4
1.5 The Organisation of the Report.....	5
2 Information and Information Management.....	7
2.1 Information Management.....	7
2.1.1 Facilitators for IM.....	7
2.1.2 Vision and Target for IM.....	8
2.2 Basic Definitions of Data and Information.....	8
2.3 Information Quality.....	9
2.4 Information and its Properties.....	10
2.4.1 Information Reach.....	11
2.4.2 Information Richness.....	12
2.4.3 Intrinsic Qualities of Information.....	13
2.4.4 Information Actuality.....	14
2.4.5 Information Assurance.....	15
2.4.6 Information Attribute Summary.....	16
3 Military Information Exchange Requirements.....	19
3.1 The Evolution of Military Communications.....	19
3.2 Communications in Network Based Operations.....	20
3.3 Strategic Communication.....	21
3.4 Tactical Communications.....	22
3.5 Communication and Total Defence.....	24
3.6 Communications and Enterprise Resource Management.....	25
3.7 Other General issues.....	27
3.8 Information Systems - the Applications.....	27
3.9 Requirements from the Three Services and the Total Defence.....	28
4 Requirements Derived from Vignettes.....	29
National tasks.....	29
International tasks.....	29
Vignettes.....	29
4.1 Vignette 1: National Task Denmark.....	30
4.1.1 Summary of requirements.....	33
4.2 Vignette 2: National Task North Atlantic.....	33
4.2.1 Summary of requirements.....	36
4.3 Vignette 3: International Task Afghanistan.....	36
4.3.1 Summary of requirements.....	39
4.4 Summary of Information Requirements.....	39
5 Technological Requirements on Defence ICT Systems.....	41
5.1 Local and Personal Communications.....	41
5.2 Communication between C2 Elements.....	42
5.3 Communications, Targeting and Tracking.....	43
5.3.1 Sensor Networks.....	43
5.3.2 Effector Networks.....	44

5.4	Beyond Line Of Sight Communications.....	44
5.5	Naming and Addressing	45
5.6	Real Time and Other Quality of Service Issues	47
5.7	Network Management	48
5.8	Information Systems and Constraints	48
5.9	Loose Coupling and Late Binding – Service Oriented Architecture (SOA)	49
5.10	Cyberspace	50
5.11	Other Requirements	50
6	Discussion and Conclusions	55
	References.....	57
	Acronyms	59
Appendix A	Definition of Terms and Terminology.....	63
Appendix B	Information Theory	65

Figures

Figure 0-1: Information requirements inference	vi
Figure 1-1: Overview of DEFTA work process and the WP contributions to NAF views	3
Figure 1-2: Method used in work package WP2.....	5
Figure 2-1: Information requirements inference	10
Figure 2-2: Information richness	12
Figure 2-3: Accuracy versus Precision	13
Figure 2-4: Circular measures of absolute and relative accuracy.....	14
Figure 2-5: Timeliness in a hard real time system	15
Figure 2-6: Radar diagram instance (webogram) of information attributes on a 1 to 5 scale	17
Figure 3-1: Generic attributes for strategic communication and information processing.....	22
Figure 3-2: Generic requirements for tactical communication	23
Figure 3-3: Generic requirement for communications in Total Defence.....	25
Figure 3-4: Generic information requirements for Enterprise Resource Management	26
Figure 4-1: Head of State Summit. (OV-1).....	31
Figure 4-2: Information requirements in the National Task Denmark.....	33
Figure 4-3: Oil Tanker Burgas (OV-1).....	34
Figure 4-4: Information requirements in the North Atlantic Incident.....	36
Figure 4-5: Afghanistan (OV-1).....	37
Figure 4-6: Information requirements in International Task Afghanistan.....	39
Figure 5-1: Late binding and creation of applications require a broker mechanism and orchestration	49
Figure B-1: Schematic diagram of a general communication system.....	65

Tables

Table 0-1: Values of the information attributes and their definitions	vi
Table 2-1: Values of the information attributes and their definitions	17
Table 3-1: Generic attributes for strategic communication and information processing	21
Table 3-2: Generic requirements for tactical communication.....	23
Table 3-3: Generic requirement for communications in Total Defence.....	24
Table 3-4: Generic information requirements for Enterprise Resource Management.....	26
Table 4-1: Summary of characteristics of National Task Denmark.....	32
Table 4-2: Information requirements in the National Task Denmark.....	32
Table 4-3: Summary of characteristics of National Task North Atlantic	35
Table 4-4: Information requirements in the North Atlantic Incident.....	35
Table 4-5: Summary of International Task Afghanistan.....	38
Table 4-6: Information requirements in International Task Afghanistan	38

This page is left intentionally blank

1 Introduction

The purpose of this report is to describe functional and technological requirements for the ICT target architecture as part of the Danish Defence Target Architecture (DEFTA). This is the result of Work Package 2 (WP2) of the DEFTA work.

The target audience of WP2 is mainly military decision makers, but it also includes system engineers and people involved in acquisition and production of defence information and communication systems. The report can be read by persons without a detailed technical background, but some parts presuppose a certain background in communications and information technology.

1.1 Overview of DEFTA¹

The Danish Defence is heavily engaged in a transformation from platform centric operations towards Network Based Operations (NBO). At the same time, the Danish public sector is moving towards the digitized society. Therefore, there is a requirement to be able to share information not only within the military operational and administrative domains, but also between coalition partners, across ministerial boundaries, with international and local organisations, suppliers and even private citizens. One of the most important prerequisites for NBO is the establishment of a networked information infrastructure.

The Danish Defence Target Architecture² (DEFTA) supports this transformation and is a vision for the infrastructure development of the Danish Defence aimed for the future. Therefore, DEFTA is the guideline for other architectural considerations which include development of system architectures and planning of the acquisition and maintenance of Information and Communication Technology (ICT) systems. DEFTA is an overarching and high-level architecture spanning 10 to 15 years from now, and it serves as a vision for evolutionary development of ICT systems supporting the mission of the Danish Defence, i.e. both its operational and administrative tasks. All ICT architectures in Danish Defence must comply with DEFTA.

The main purposes of DEFTA are to contribute to the following goals:

- Ensure that present and future operational requirements on ICT systems can be met.
- Ensure that development of ICT systems is coordinated with Defence ICT-Strategy³.
- Ensure that ICT systems support the national strategic vision and concept for NBO and the general perception of the developments in this area.
- Ensure that ICT systems support operational scenarios for the Danish Defence.
- Establish functional and technological requirements for the Danish Defence ICT systems.
- Ascertain system interoperability.
- Increase the quality of the combined systems-of-systems that forms the ICT infrastructure.

¹ Note that this section is common for all work packages of DEFTA.

² The term “**target architecture**” is different from the similar NATO term, which describes a detailed, project related system implementation target.

³ Current version of the Defence ICT-Strategy covers the period 2011-2014.

- Facilitate the use of open standards and COTS products.
- Ensure that acquisitions both from usability and technological point of views have a reasonable life time.
- Make the acquisition and sustainment processes more straightforward, i.e. providing basis for better coordinated and cheaper ICT development.

Another purpose of DEFTA is to provide a mean which encompasses essential main architectures and principles of corporation partners. This generates some compliancy requirements for DEFTA:

- No discrepancies with NATO Overarching Architecture or the major NATO Reference Architectures.
- Coordination with the architectures provided by the Danish digitized society, - in particular regarding administrative ICT systems.
- Compliancy with visions and target architectures of major coalition partners, e.g. USA and GBR.

The DEFTA work has been divided into four Work Packages (WP's), which provide a DEFTA description being compliant with the NATO Architecture Framework (NAF)⁴. The overall DEFTA work process is visualised in Figure 1-1. The same figure also shows how the DEFTA architectural components - identified in the four WP's - contribute to NAF views.

- **WP0: Strategic Vision and Concept for NBO.**

The objective of WP0 is to formulate the relations between the general policies and strategy work on ICT development. It contains the initial analysis of the national strategic vision and concept for NBO and the general perception of the developments in this area. Referring to NAF, WP0 will mainly provide architectural components used in All Views (AV) and to some extent Capability Views (CV).

- **WP1: Operational Tasks and Vignettes.**

The objective of WP1 is to describe a set of overall operational scenarios, and describe a set of representative vignettes which can establish the basis for the analysis of information exchange requirements in WP2. Referring to NAF, WP1 will mainly provide architectural components used in Operational Views (OV) and Capability Views (CV).

- **WP2: Information in Network Based Operations.**

WP2 deals with information in NBO. The objective is to derive a number of functional and technological requirements for DEFTA. The requirements are derived from the tasks and vignettes of WP1. Referring to NAF, WP2 will mainly provide architectural components used in Operational Views (OV) and to some extent Capability Views (CV) and Technical Views (TV).

- **WP3: The Technical Architecture for ICT Systems in Danish Defence.**

The objective of WP3 is to describe the technical part of the target architecture. This technical architecture is a high level vision of future ICT systems-of-systems. The WP3 report looks at different technical aspects as they are expected to develop (evolve) in a 10-15 years of time. WP3 describes the technical solution for the requirements from the other WP's, in particular WP2. Referring to NAF, WP3 will mainly provide architectural components use in System Views (SV) and Technical Views (TV).

⁴ The NATO Architecture Framework (NAF version 3) specifies how architecture is described by use of different views: Capability Views (CV), Operational Views (OV), System Views (SV), Technical Views (TV), Service Oriented Views (SOV), Programme Views (PV), and All Views (AV).

Each WP is documented in a separate report, thus DEFTA consists of four reports which should be regarded as a unified whole. However, each of the four WP reports can be read independently of each other.

Referring to NAF, DEFTA does not contribute significantly to Programme Views (PV) and Service-Oriented Views (SOV). However, service orientation is a key element of DEFTA, and DEFTA provides contributions to SV and TV being a prerequisite for the technical implementation of Service Oriented Architecture (SOA). The definition, taxonomy, and orchestration of actual services to be provided in SOV must be with basis in doctrine, operational procedures and other business processes. This is outside the scope of DEFTA. In the same way, DEFTA does not define programme portfolios and projects for PV. Some PV contributions may be found in the roadmap part of the Defence ICT-Strategy.

DEFTA is an updated version of the Danish Defence Target Architecture⁵, and will be published as an annex to Defence Command Denmark (DCD) directive for maintenance of architectures⁶. Updates of DEFTA are set to be released every second year.

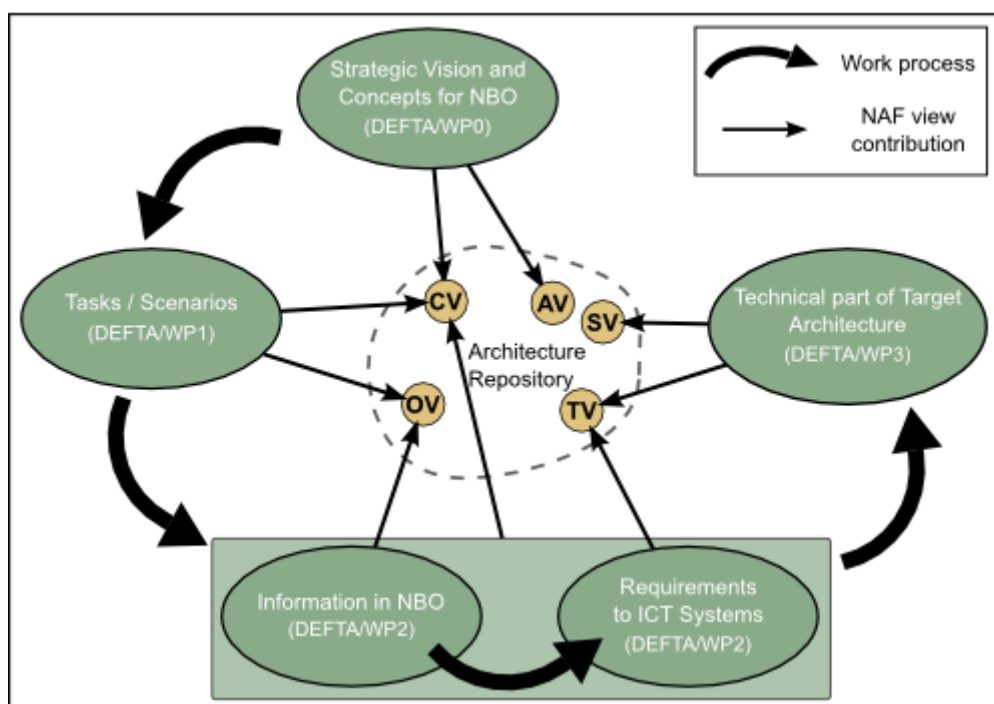


Figure 1-1: Overview of DEFTA work process and the WP contributions to NAF views

The DEFTA work is tasked by Information Technology Policy CIS Staff of the DCD and conducted with the Danish Acquisition and Logistics Organisation (DALO) as lead. Most of the work is also carried out by DALO; - however, major part of WP0 is made by DCD, and WP1 has substantial contribution from Royal Danish Defence College (RDDC).

⁵ The first version - denoted DEFComm - is from 2005 and consisted of three reports denoted WP1, WP2, and WP3. In 2007, DEFComm was approved by the Defence Top Management as the vision for evolution of the ICT systems in the Danish Defence.

⁶ The reference is FKODIR 380-2.

1.2 Objective and Scope of WP2

This work package (WP2) deals with information in NBO. The main objective of WP2 is to derive a number of functional and technological requirements for DEFTA. The requirements are derived from the vignettes of WP1 [2] and the NBO visions/concepts from WP0 [1]. WP2 with its focus on information is thus one important prerequisite for the establishment of the technical part of DEFTA and ICT system architectures.

WP2 deals mainly with functional requirements as derived from the vignettes and the information need in the situations. However, some obvious non-functional requirements, i.e. performance requirements, have also been identified. These will serve as constraints for DEFTA.

The analysis is restricted to information requirements and thus for communication and information systems in an NBO context. It does not to any significant extent include financial or organisational aspects, but is strictly for the purpose of establishing the technical part of DEFTA.

The emphasis on information naturally leads to the observation that information management (IM) is and will remain a key discipline for conduction modern warfare. IM is therefore a theme that permeates this work.

1.3 General Background and Constraints

The technology requirements that are put forward in this report do not specifically take legacy systems (i.e. already existing information and communication systems ~ baseline) into account. The report, however, treats in some detail the anticipated future context of Military and Total Defence operations and their influence on the technological requirements.

A prerequisite for the report is the tasks with vignettes that are outlined in WP1, and the identified capability requirements. Another important basis is that the systems must support NBO, in a national as well as in a combined and joint context. Also the cohesion with the administrative, logistic and national crisis response systems is considered.

The report is focused on the functional requirements, so that non-functional requirements (including mandatory standards, use of Commercial Off The Shelf (COTS) products, etc.) are only considered to a limited extent. These non-functional requirements are briefly mentioned in section 5.11.

1.4 The Method Used

The information and communication systems process store and disseminate information. The information may be described by a number of characteristics or attributes such as richness, reach, actuality (including real time aspects), assurance (the degree of trust in the information), precision and accuracy (exactness or correctness) [3].

The report takes as its starting point the information attributes which can be utilised for identifying and, where possible, quantifying requirements for the communication systems and information systems, in brief the Defence Info Structure. The info structure includes tools and methods for IM.

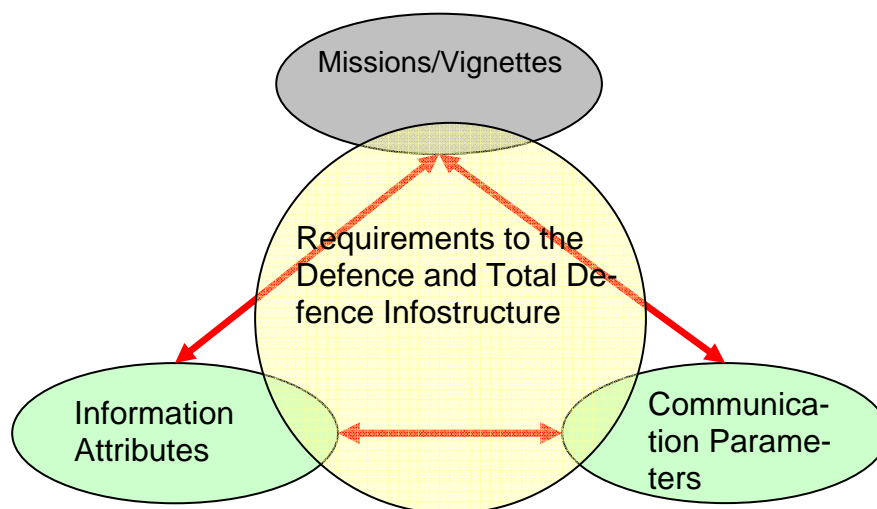


Figure 1-2: Method used in work package WP2

The requirements are derived by comparing the tasks, mission types and capabilities from the vignettes and the needed properties of the involved information and communication parameters from WP1. The vignettes point to the need to be able to conduct certain types of missions, and such general abilities are capabilities. The information required in the different mission types is the focus of the work.

1.5 The Organisation of the Report

The first chapter (this chapter) of the report contains the general background, scope and objectives of WP2.

. Chapter 2 deals explicitly with information and IM. The chapter further defines the information attributes that are decisive for the ICT architecture. The chapter also gives a relatively thorough discussion of information in NBO and its characteristics. These information attributes span a multidimensional space, where the different points contain the requirements from the vignettes. Even if the different attributes logically are independent, financial and technological constraints will force developers and acquisition authorities to make trade-offs between desired and needed properties, and thus introduce dependencies. One illustrative example is precision in position data. A high degree of precision requires the position to have many significant digits. And this again will require transmission capacity. So there may be a trade-off between precision and transmission capacity. This may have further implications in the sense that a limited transmission capacity will cause a delay so that precision (many bits) must be balanced against actuality (real time requirements).

Chapter three of the report poses general military communications requirements, with a focus on tactical communication, strategic communication and NBO. The requirements are tightly coupled to the information characteristics.

In the fourth chapter of the report, more specific requirements are identified based on the vignettes of DEFTA/WP1. Communication and information parameters are found from the vignettes, and these are briefly summarised. The analysis is conducted so that the specific information characteristics and requirements are met in the given context, i.e. in the vignette. Special emphasis is put on the NBO aspects, because network centricity will be dominant for the future deployment of military forces.

The fifth chapter is a survey of a number of issues that are specific for military and Total Defence communication and information systems, but independent from the concrete mission. In this context a number of technological requirements for the communication and integration of information systems are identified. Some of the precedents for the requirements are also discussed. The requirements are described generically, so that they fit into the further work on the technical part of DEFTA (i.e. WP3) that broadly serves the fulfilment of requirements for the communication and information systems of the Armed Forces.

The final chapter of the report contains a conclusion based on the analysis from the other chapters.

The two appendixes contain a list of definitions of the used terms, and a more in-depth discussion of information.

2 Information and Information Management

The ability to perform NBO is crucially dependent on having the right information at the right place with a sufficient quality.

2.1 Information Management

The era of netcentric warfare is dominated by an understanding of the importance of shared information, and this sharing is made possible by the progress in ICT. This means that information management (IM) is a key discipline in NBO. IM gives another perspective on requirements to the information. It must be emphasised that IM used to be a librarian task, but that today it is much more than dealing with printed information in libraries.

In short we define IM as *the capture, recording, organising, storage, dissemination, and retrieval of information*. IM has the sole goal of getting the right information to the right system or person in the right format at the right time. This means that a large part of the ICT architecture may be seen as supporting IM and tools for conducting IM.

This is very much in line with the UK MOD definition of IM [18]:

A set of integrated management processes and services that enable and support the capability of collectors, producers and users to store, locate, retrieve and transform information, allowing it to become the right information in the right form and of adequate quality to satisfy the demands of the commander or organisation.

IM must take into account all actual constraints such as information overload, limited bandwidth, operation security, confidentiality requirements, processing capacity, cyber attack, etc. when providing the right information in the right form at the right time. This means that all information is not necessarily available for everyone at any time in all scenarios, but the visions for IM generates a requirement for flexibility and scalability of the ICT architectures.

2.1.1 Facilitators for IM

To manage the asset that information is, we need to establish routines and practices [18], comprising:

- PROCESSES AND DOCTRIN – ensuring that key information activities are embedded into the normal routine - how information is organised, stored, secured, protected, shared, labelled, tagged, and disseminated;
- ORGANISATION – establishing structure, lines of communication, roles and responsibilities, authority, delegation in the enterprise;
- CULTURE AND EDUCATION – building the right culture to value, communicate, share, protect and preserve information, together with developing individual and team skills; the ability of conduction NBO depends on the individuals willingness to share information and knowledge;
- INFORMATION INFRASTRUCTURE – deploying, supporting and maintaining the appropriate hardware, software and networks for capturing, storing, processing, communicating and retrieving information.

IM may be seen as an overarching theme in the ICT architecture. The overall requirements to information may largely be met by having efficient and effective IM. In the next chapters we deal explicitly and in more detail with the issues met in this chapter. More specifically, we link the quality parameters to the likely tasks and vignettes outlined in DEFTA/WP1.

2.1.2 Vision and Target for IM

The long term vision is to have a mature NBO environment which is about management and control of shared information, i.e. IM must be supported by all parts of the underlying technical ICT architecture. The evolution taking place in the DEFTA timeframe should aim towards the long term vision, i.e. the DEFTA target is a state which should be realistic according to development in business processes, doctrines, organisations, cultures and technology.

The short term target for IM is to put in place the facilitators lined up in section 2.1.1 above. This means that a set of practices for information push and information pull must be established. The efficiency and effectiveness of IM are both dependent on meta-information, i.e. information about the information such as tagging and mark-ups. Dependent on the granularity of the tagging, the use goes far beyond efficient storage and retrieval of information. The tagging may also be used for managing access rights and for enforcement other parts of a security policy. Tagging and mark-ups should be standardised broadly in the Defence enterprise.

Information pull is greatly enhanced by well known mechanisms such as search machines and web portals, known from the Internet. Such mechanisms and enhancers for information sharing such as social media must be placed at the disposal of communities of interest and practice.

Parts of the information to be exchanged will be true multimedia such as video streams and large images. This of course puts high demands on the information infrastructure in terms of capacity and reliability. Although the requirements for capacity in principle are insatiable, we must continuously enhance the infrastructure by exploiting the rapid technological advances.

2.2 Basic Definitions of Data and Information

This section contains a basic definition of data, information, semantics, pragmatics, meta-data, and meta-information. A more in-depth survey of the concepts is given in Appendix B.

Data is defined as a stable representation of one or more facts, be they events or objects.

Information is defined as the data which lead to a decrease in the uncertainty of an event or an object, at the receiver.

Both data and information are measured in bits. Eight bits are defined as one byte (1 B).

The definition of information includes a utility aspect because data that do not diminish uncertainty about an event or an object at the receiver end do not contain information. This of course means that information includes a dependency of the context of the receiver.

It must be noted that the above definition of information does not take into account the meaning of the information and the actual use of the information. The meaning of information can be divided into semantics and pragmatics. **Semantics** is the first stage of the meaning

of the information, and **pragmatics** is the second stage where the meaning of the information is taken in the actual context. The theories of semantics and pragmatics are not considered, beyond the fact that information must tell something new to the receiver. The pragmatic and semantic aspects are taken into account in the following sections of this work package, where the relevant information attributes or characteristics are discussed.

An important consequence of the properties of information is that the need for transmission capacity may be decreased by increasing the a priori (known) knowledge at the receiver. This may be effectuated by having stored information and large information processing capacity at the receiver's end, but also by having highly trained personnel.

The ultimate goal of sending, receiving and processing information is to add to knowledge and understanding, so that the right actions can be performed. We as human beings are the ultimate receivers of information, but also machines may need information to perform their duties. The meaning of the information must therefore be unambiguous and understandable. This is the semantic dimension to information. Understanding is conveyed by use of information context, either tacit or explicit in the form of **metadata** (data about data) or **metainformation** (information about information). The metainformation usually has the form of data-models or more general ontologies (formal representation of the knowledge). This metainformation must be available to all parties in an information exchange. Modern information and communication systems must be able to deal with semantic amplifiers. Otherwise we can only achieve basic forms of interoperability.

2.3 Information Quality

To be really useful information must be of good quality (see [12] and [18]). Ideally, we want it to be accurate, unambiguous, concise, clear, consistent and timely. The information the user needs to know is its origins (source, provenance) and status (such as historic or current, draft or final) and the user wants it in a form that he/she/it can access and use. The user also wants to be able to find and retrieve it easily and quickly, confident that it remains protected from those people who shouldn't be able to see it. Accessibility, security and privacy are competing themes, so skills and sound judgement are needed to strike the appropriate balance between them. Whatever the information, it has certain requirements. It should be:

- **Available** – accessible when needed
- **Relevant** – pertinent to the present situation and the receiver
- **Accurate** – must be correct
- **Precise** – the uncertainty and stochastic errors must be small
- **Timely** – much information is useless if it arrives too late (or too early)
- **Complete** – the whole story should be told
- **Secure** – including information integrity, confidentiality and non repudiation
- **Directed** – adapted to the receiver, no superfluous details and to the point.

2.4 Information and its Properties

Communication is exchange of information. It is therefore possible to deduce the requirements for information and communication systems from desired properties of information. Similarly, the information attributes will also be decisive not only for the information systems themselves but also for the required degree of interoperability between the systems. By focusing on information, and defining requirements to the information in form of desired values for its attributes, a number of requirements on the target (and later system) architecture may be derived, and it is therefore possible to evaluate a given form of architecture in terms of the degree to which it accommodates the required information attributes.

The **information attributes** that we have selected to characterise the information in DEFTA are *richness*, *reach*, *actuality (timeliness)*, *assurance*, *precision*, and *accuracy (exactness)*. Precision and accuracy together are the *intrinsic quality* of information.

By stating the information requirements as requirements on the information attributes [14] we derive requirements for the communication and information systems and hence for the overall ICT architecture.

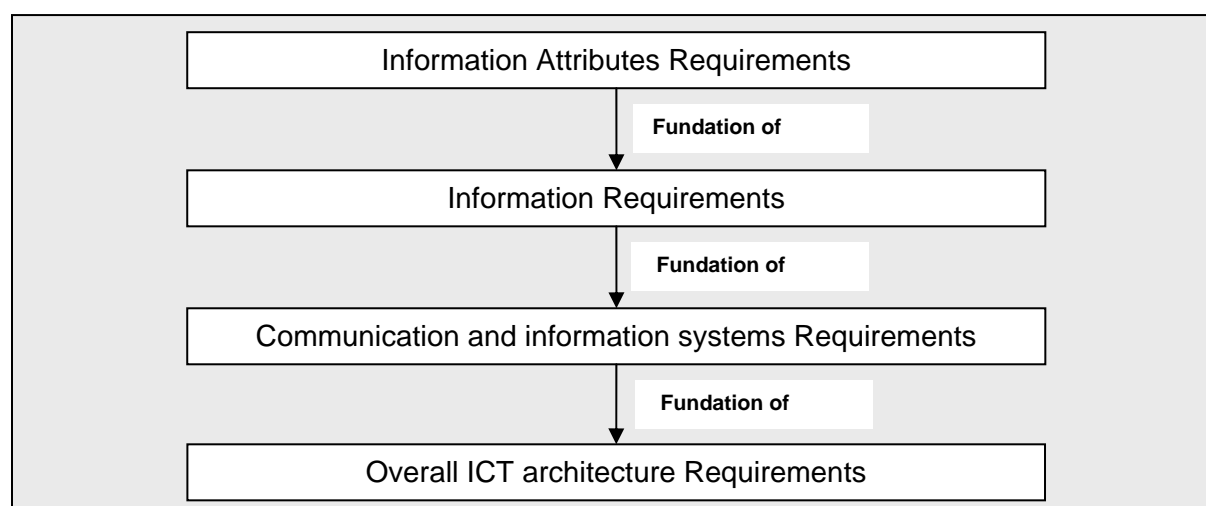


Figure 2-1: Information requirements inference

In the following subsections, we describe the selected information attributes, and show how their values lead to requirements on the communication and information systems. Again, the NBO related issues are in focus.

It must be noted that in this report emphasis is put on the information attributes that apparently have a significant impact on the degree of fulfilment of the requirements on the ICT systems. We treat them under the headings of reach, richness, intrinsic quality, actuality and assurance. Other attributes such as completeness, cohesion and correctness (except for integrity issues) are not decisive for the ICT architectures, but certainly for the information systems themselves. They are therefore not considered in any significant detail. Completeness is mainly a property of the information source such as a sensor suite, and is therefore partly outside the scope of DEFTA. Correctness has both roots in the information source and information assurance in the form of assurance of integrity, and falls partly outside the scope of DEFTA/WP2.

2.4.1 Information Reach

Information reach is a measure of which and how many subjects (humans, systems, processes) the information potentially can be at the disposal of. The reach has both a physical and a logical dimension. Included in the information reach is also the granularity with which the subjects can be reached, such as broadcast, multicast or individually addressed.

The *physical information reach* depends on the geographical propagation of signals. High frequency (HF, short wave) communication may reach beyond line of sight (BLOS) while Super High Frequency (SHF) transmission is strictly Line Of Sight (LOS) communication. But also the number of units that are coupled to a local, regional or global communication grid is important for the degree to which it is possible to disperse the information.

The physical reach is only one part of the information reach, but logical aspects are at least as decisive for whom the information may reach. This *logical information reach* sets limits for the community of interest. This means that as important as physical reach is, the way the information is presented and how access to the medium and to the information is controlled are decisive for the actual use of the information. In a network based defence system that conducts NBO, mechanisms such as naming and addressing, directory information and coding become key parameters. The logical reach can be influenced by encryption, by language and by the selected character set. It is of no use that a message physically reaches a Danish unit but is in Japanese. In a more comprehensive way, to obtain a useful exchange of information, both message syntax and semantics must be agreed upon by the participants. One of the main advantages of XML is that metadata about syntax and semantics may accompany the real information and thus make the possible reach much larger than by more traditional representations. One example is the data packets that are used by the RAC 3D (deployable medium range radar). Because of a very limited transmission capacity, a very compact specially tailored data format was chosen. If the RAC 3D data are to be of any broader use, a conversion to a standard format is necessary. Without such a translation the possible (logical) reach is very limited.

It is worthwhile to consider the *organisational information reach*, which is a special aspect of the logical reach. This is a measure of how widely the information can be disseminated in the enterprise network. Should it reach everybody in the organisation, or is it to be limited to certain categories or organisational roles? It may be desirable to limit the information dispersal to one's own unit, own service, joint services, combined services or to all actors (including but not limited to joint and combined). The organisational reach is very often coupled to the concept of role, not to the individual. Organisational reach is usually dependent on the establishment of identification, authentication and authorisation schemes.

The information reach is closely related to the concept of interoperability. Interoperability may be defined as the ability of humans or systems to collaborate in performing a given task. The fact that two entities can reach each other information-wise is a necessary but not sufficient precondition for a meaningful collaboration. A huge information reach means that there are many potential recipients, and hence many units, who in some sense can be made interoperable with the information source. But a huge information reach does not necessarily implicate a high degree of interoperability (e.g. everyone has access to the information, but it is in Japanese). Further, cultural doctrinal and organisational compatibility must be present. Still the most distinguishing characteristic of NBO is the possibility of a large information reach through the network or information grid (see [3]).

2.4.2 Information Richness

The *information richness* is a measure of the expressive power of the message language. In other words, the information richness expresses how many different messages that may be exchanged. If text based messages from a fixed message catalogue are to be exchanged, the richness is much more limited than if free text of arbitrary length is possible. For multimedia information, the difference in richness may be much more conspicuous.

There may be many reasons for restricting the richness of information. The most important ones are:

- The need for a simple machine processing of information
- A wish to restrict the number of unambiguous interpretations of the messages, and hence avoid misunderstandings
- Limited available transmission capacity that enforces an efficient encoding.

The limitations in richness are often caused by the above mentioned precautions, but they are frequently a product of the fact that information is considered to be very specific for a given mission or a given stove piped system, and of no interest beyond that. If the information is to be applied within a very specific part of the application space, e.g. targeting, richness may be limited without loss of generality. It must be emphasised that if the information use is unpredictable, it is not very prudent to decrease richness. A classic example of such limitations is the use of an artillery tracking radar. In this case it is customary to filter all information of slow moving objects away. Such objects might be helicopters or slow fixed-wing aircraft. But exactly these objects could be of great interest as a valuable contribution to the general common operating picture, but of course of low interest to the artillery officer.

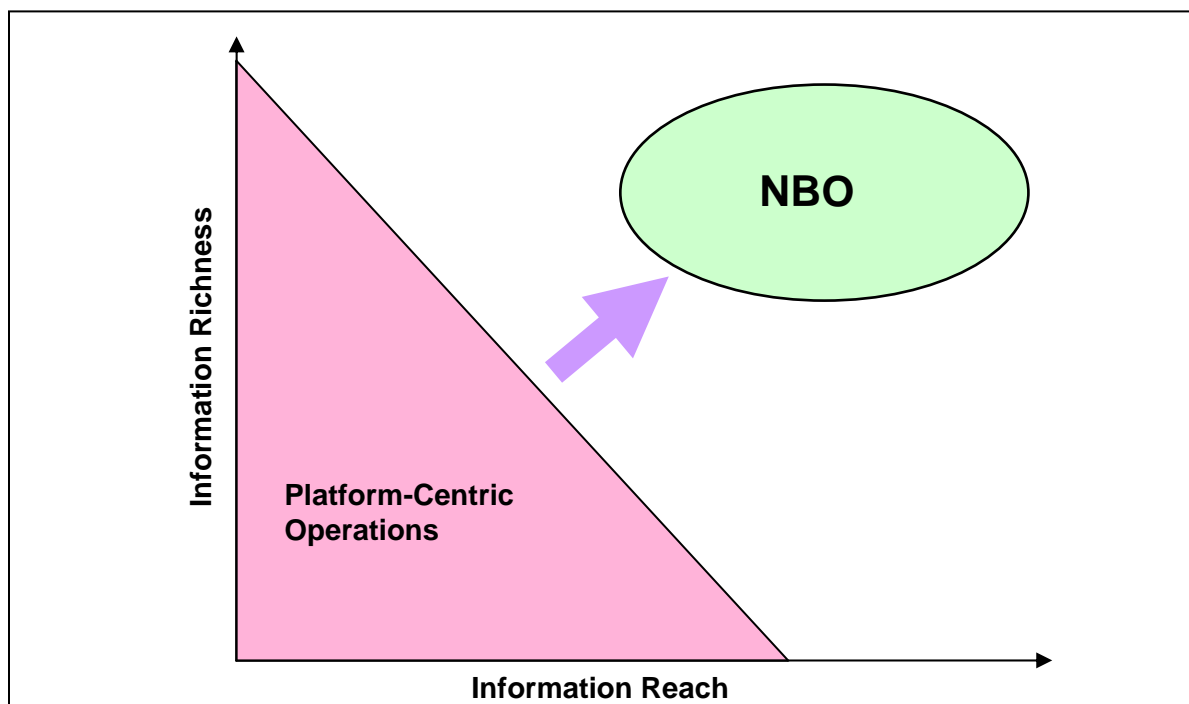


Figure 2-2: Information richness

Traditionally, rich information required people to be physically close to one another. Modern technology allows rich information to be exchanged by entities which are not close to each other. The Internet allows much greater reach for much richer information than the telegraph. As semantic technology evolves, it enables association of different additional types

of information to allow a much broader and richer information discovery and exchange. This pushes out the limit at which the trade-off between richness and reach must be made. The ultimate result is that much richer information can be exchanged by a much wider audience. Where platform-centric operations used to have poor reach if the information was rich, it is now possible in NBO to have both adequate information reach and richness. This is illustrated in Figure 2-2.

2.4.3 Intrinsic Qualities of Information

The *intrinsic qualities of information* that we deal with in this context are precision, correctness (accuracy and exactness), and consistency.

The *information accuracy or correctness* is the measure of the distance between the information and the true value. The accuracy is mainly determined by whether one measures the right thing or transmits the right thing.

Information precision is the degree to which several outcomes or measurements provide answers very close to each other. It is primarily a function of the properties of an observation instrument and the ambient noise. If a measurement has a large noise component its precision is small. One example is information from a radar sensor. If the radar sensor coordinates are wrong (e.g. an error in northing of the sensor), the precision may still be high, but the accuracy is low. Another example is the coordinate set of a position. High precision requires a large number of digits in the position, which causes high load on the transmission channel. The number of bytes to represent an image is yet another example. To give precise and accurate colour and luminance information, many bits per pixel will be needed, again with consequences for transmission and storage capacity. Figure 2-3 shows the difference between precision and accuracy.

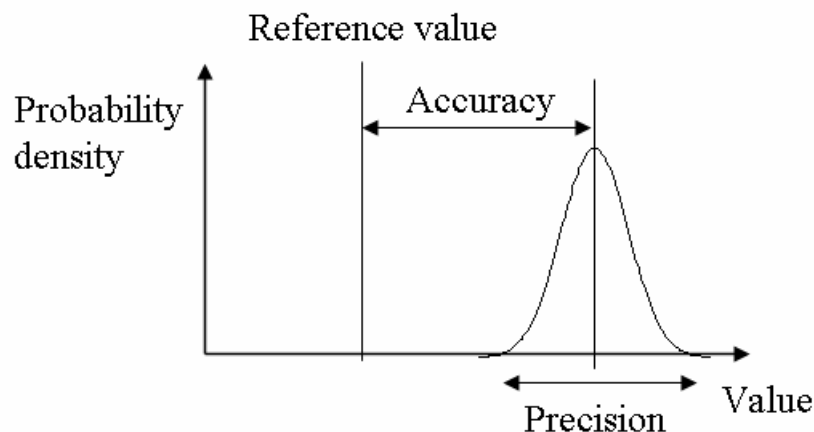


Figure 2-3: Accuracy versus Precision

Figure 2-4 is another illustration of the concepts of accuracy and precision. Inertial navigation Systems (INS)/GPS guided munition all use circular measures of absolute and relative accuracy at 50% probability that reflect the intended uses of these systems. The 50 percent Circular Error Probable (CEP) figure is the radius of a circle around the target within which 50% of the weapons should fall. The remaining 50% fall outside the CEP.

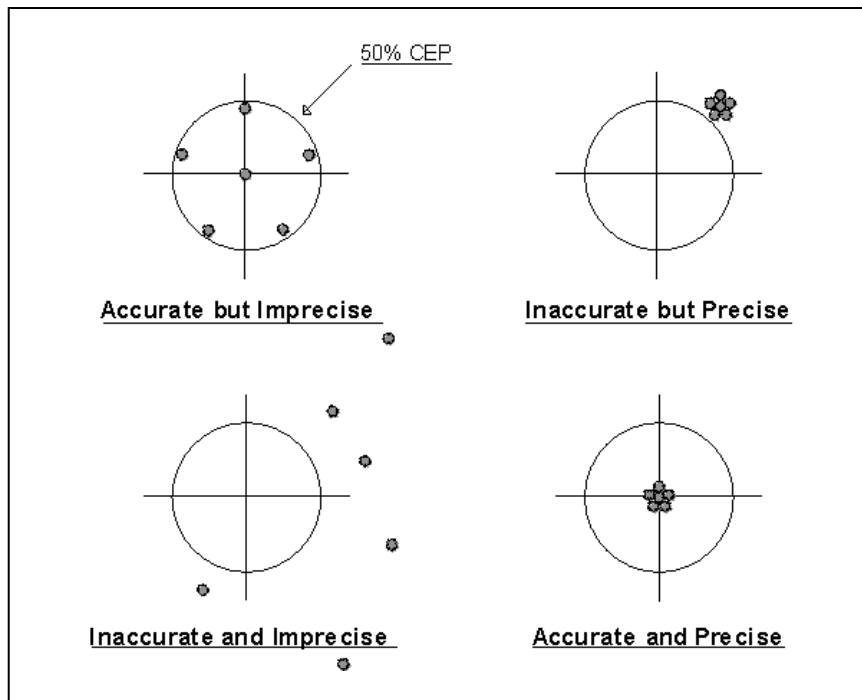


Figure 2-4: Circular measures of absolute and relative accuracy

It must be emphasised that lack of data integrity (see also section 2.5 on information assurance) potentially can influence the accuracy of the information. One example is injection of false signals in a satellite navigation system like GPS. In this case the precision may be unchanged or even improved, while the accuracy suffers badly.

Information consistency (cohesion) is a measure of the homogeneity with which the same information is available and represented in the network at different nodes and at different times. If the same information is found in contradictory versions, the consistency is low. Consistency may pose requirements both on the communication and the information systems, because data must be replicated with small latencies. The ability to perform distributed transactions is one way of assuring consistency, but at costs of many transmissions.

2.4.4 Information Actuality

Information actuality properties are timeliness, useful lifetime, and continuity.

Timeliness is a measure of the degree to which the information is available at the right place at the right time. The intrinsic or utility value of the information may be extremely degraded if given requirements to the actuality attribute are not met.

Some pieces of information are only of any use if they reach their destination within a given time period, e.g. before a given deadline. Controlling signals to a UAV is one example. Timeliness is directly related to real time requirements. We define *strict* or *hard real time* systems as systems that fail if timeliness requirements are not met. *Soft real time* systems are systems that still work, but have a degraded performance if data are not available within a given time frame.

The useful *lifetime of the information* is the next actuality property. The lifetime is a derivative of the age of the information. One example is a weather forecast. If the forecast is 5 days

old, its value is probably nil. From a communication and processing point of view, the lifetime is related to the latency and processing time which are always present. In the UAV example, it is of no use that the controlling information is at the UAV in time to prevent a crash, if the direction information is no longer valid because the target has moved. Lifetime considerations are also important when protecting information. Tactical information usually has a short useful lifetime, so that simple cryptographic means may suffice, while strategic information has a long lifetime.

Another actuality property is the *continuity of the information*. This property expresses an ability to continually update the information or to maintain sequences of data (e.g. time series). Examples are situational pictures that are continuously updated and displayed at several nodes in the network. Data and information fusion may be critically dependent on the continuity.

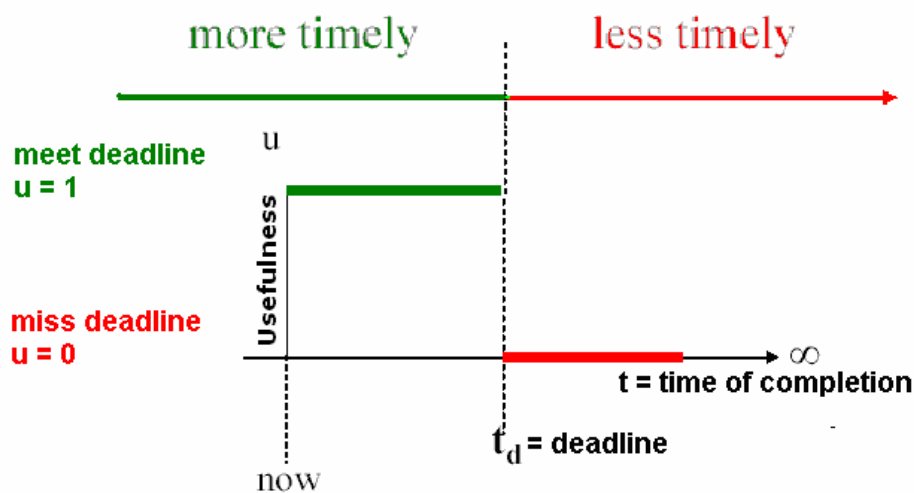


Figure 2-5: Timeliness in a hard real time system

One of the most familiar example of timeliness is a time constraint in terms of a deadline (t_d), which can be (properly) defined as the time until which an activity's completion is more useful to a system ($u=1$), and after which the activity's completion is less useful or of no use ($u=0$). If the usefulness of the system after the deadline is zero, i.e. the system has failed; we have a hard real time requirement.

2.4.5 Information Assurance

Information assurance comprises the usual security properties in the sense that if the security procedures and architecture fulfil the overarching security requirements, the information may be trusted. The concept includes a dynamic dimension because changes in network and IT architectures and their responses to attacks must be continuously accommodated in order to maintain the information assurance.

The most important security properties in ICT systems are traditionally grouped under the headings of confidentiality, integrity, availability and non-repudiation. In this report we consider both security aspects of the exchange of information, and the security aspects of the data processing inside the nodes.

The *confidentiality property of information* implies that only intended (authorised) entities may access the information. The *confidentiality of the information* includes restrictions on

access to the information and thus to both the logical and physical reach. Confidentiality is very often achieved by use of cryptographic means or by use of media which cannot be listened to, e.g. special optical fibres. Cryptography is in many cases implemented in a network as an infrastructure component which among other things takes care of the distribution of cryptographic keys. Because of the limited useful lifetime of tactical information, relatively weak cryptographic measures may suffice, while very strong protection means may have to be enforced for strategic information.

Information integrity means that the received information has not been tampered with by unauthorised subjects - or at least not undetected. Integrity is typically assured by cryptographic means, including an electronic signature (that also assures non-repudiation). The use of an electronic signature presupposes a dedicated infrastructure component, e.g. a public key infrastructure (PKI).

The *availability of information* and services means that authorised users at any time have access to the data, so the communication works and the information services are delivering the data. Robustness in the context of deliberate attacks or accidents must be present so that intrusions, denial of service attacks or unintended load situations do not prevent access.

Availability is often obtained by redundancy of both information sources and transmission channels. This means that availability uses resources both between processing nodes and at the nodes. The resources are transmission channels, transmission capacity (e.g. for distributed updates of data bases), data storage and processing power. To obtain a high degree of availability some extra or redundant capacity must therefore be taken into account when designing the systems, i.e. in the architecture.

Information authenticity is a measure of the assurance that the information comes from an authorised identifiable source. The information must be traceable back to the source. Besides electronic signatures, also restricted and controlled access to the network is important to obtain authenticity.

The *non-repudiation* is a measure of the assurance that the sender (or recipient) cannot deny that the transmission has taken place. This usually includes the fact that neither the authenticity nor the integrity can be denied. A digital signature is one way of obtaining this.

2.4.6 Information Attribute Summary

The information attributes in a given vignette may be shown in a *web-o-gram (radar diagram)*. The greater the area of the polygon is - the greater the information requirements in the vignette will be. To clarify the applicability we have arbitrarily chosen a scale from 0 to 5 for each attribute.

Table 2-1 shows the definitions of the values 0-5 of the information attributes.

Figure 2-6 shows a diagram with arbitrarily chosen values for the attributes.

		ATTRIBUTE VALUE					
		0	1	2	3	4	5
Reach	Physical	None	Local/personal	Local area	Regional, LOS	Regional, BLOS	Global
	Logical	None	Point-to-point with no further disclosure	Multicast with limited disclosure	Networked with limited disclosure	Networked with some disclosure	Networked with full disclosure
	Organisational	None	Own unit	Own service	Joint	Combined	All actors, including but not limited to joint and combined
Richness	Richness	None	Single, predefined message	Predefined, limited message catalogue	Message catalogue including free text	Text, voice, picture	Full multimedia
	Timeliness	None	Best effort	Guaranteed delivery	Low jitter, isochronous	Soft real-time	Strict real-time
Actuality	Lifetime	None	> Years	Months / Weeks	Hours / Days	Seconds / Minutes	< Seconds
	Continuity	None	Sporadic update		Many updates (bursts)		Continuously update (streaming)
	Availability	None	Very low	Low	Medium	High	Very high
Assurance	Integrity	None	Tampering possible		Tampering is detected		Tampering not possible
	Confidentiality	None	Very weak	Weak	Medium	Strong	Very strong
	Authenticity	None	No source identification		Traceable source		Authorised identifiable sources only
	Non-repudiation	None					Guarantee
	Precision	None	Low		Adequate (medium)		High
Intrinsic Quality	Accuracy	None	Far from true value		Acceptable distance to true value		Close to true value
	Consistency	None	Many contradictory versions		Some contradictory versions		Homogeneity (high)

Table 2-1: Values of the information attributes and their definitions

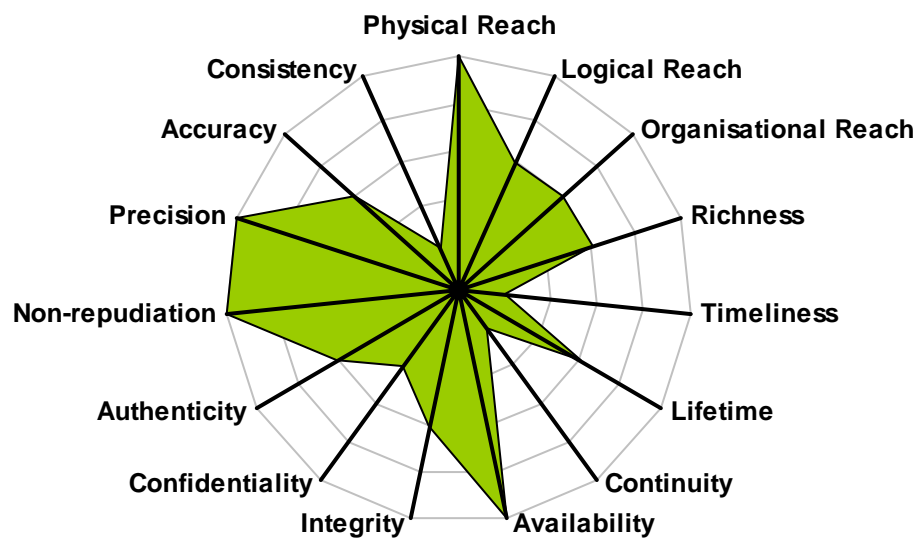


Figure 2-6: Radar diagram instance (webogram) of information attributes on a 1 to 5 scale

This page is left intentionally blank

3 Military Information Exchange Requirements

In this chapter we look at some general communication requirements in the Danish Armed Forces, mainly with regard to operational communications. The requirements will be associated with the information characteristics delineated in chapter 2. Taking recent developments in military communication, information systems, and the anticipated future developments as one's starting point a number of requirements are identified. We then look at the communications at the strategic and the tactical levels followed by the more specific aspects of relevance to NBO. Finally some requirements in connection with important specific systems and the Total Defence are described.

It is customary to structure military communications in three levels, namely the strategic/political level, the operational level, and the tactical level. From an information point of view, the main differences between the levels are reflected in requirements on information life time, actuality, and reach. We therefore frequently meet strict real time requirements at the tactical level that are absent at the other levels, while requirements on reach are more pronounced at the operational and strategic levels.

The introduction of NBO will probably mean a reduction in the importance of the operational level (see [6], [13] and [14]), at least for the national forces. Communication will be much more direct between the strategic and the tactical level, and in combined operations; also communication between coalition partners will take place at the tactical level. The extent to which our national forces will operate at brigade level in international operations is believed to be limited (see [2], [11], and [17]).

3.1 *The Evolution of Military Communications*

Military communications channels have traditionally very much reflected the military organisation hierarchy. Changes in the organisation have therefore had a profound effect on how the communication was orchestrated, and new communication possibilities have vice versa influenced the military structure. The movement towards smaller and more mission or task-oriented organisational units, such as Joint Task Forces, Rapid Reaction Forces, and Expeditionary Forces makes the distinction between traditional levels of tactical, operational, and strategic communications less important.

The appearance of NBO and the accompanying net centricity have a number of important consequences. First of all, the ubiquitous communication network of NBO allows communication that does not follow the hierarchy. Secondly, the task orientation will make the strategic and the tactical levels more important; so much that in many cases the operational level will cease to exist. Originally the operational level was a barrier between politics and military professionalism. The operational level of command makes the plans and decides how the force structure is to be deployed ([3] and [7]). When it comes to participation in coalition operations and particularly in NBO, the operational level will, when the operations are taking place, mainly be involved in monitoring and logistics. The communication involved in logistics will have great resemblance to strategic communications (see below).

The vignettes in WP1 [2] show that the three levels are not easily identified in the missions and tasks in which the Danish Armed Forces are anticipated to be involved. Unit sizes as large as corps and division or even brigade are not or only seldom met. The Danish contribution to multinational joint and combined task forces are deployed at the tactical level, and still

the lower level units will be able to commandeer weapon systems that used to be rigidly controlled by higher levels. The need to deploy mixed military and civilian units will pose new challenges both to command and control, and to the supporting ICT systems. It is beyond the scope of this report to propose organisational and doctrinal solutions to the new challenges, but it must be stated that the traditional partitioning into the strategic, the operational, and the tactical levels is challenged.

Contact to civilian organisations has traditionally been created at the operational level. With the use of military forces in all conflict phases, and the close collaboration with e.g. non-military emergency and disaster relief organisations, tactical military communication must be interlinked with the non-military communication means.

The new task set [16] of the Danish Armed Forces and the technological development have led to network centricity. Buried in this is the requirement of being able to act in non-anticipated situations. This requirement for flexibility and agility must be reflected in the way the ICT systems are organised. This is in contrast to the cold war scenarios, where predictability made it possible to define the sorts of messages that were to be exchanged, and thus to reduce the richness of the information. In such a situation it is possible to plan the communications in great detail, and to elaborate Information Exchange Requirements (IERs) in great detail. IERs are still useful, but they are not sufficient to guarantee meaningful interoperability and hence collaboration between relevant systems and organisations. New tools must be used to facilitate the collaboration between disperse organisations, and by focusing on the information attributes, this report is an attempt to give such new tools. The IERs will be complementary to requirements of net readiness, i.e. the ability to plug into the *Network* at a given level. Be it in the role of service provider or service consumer, or maybe in both roles.

3.2 Communications in Network Based Operations

For the conduct of Network Based Operations, information and hence communication is a decisive factor. The *Network* guarantees that communication between all relevant partners can be established. Adherence to a Service Oriented Architecture assures that meaningful collaboration based on a common situational awareness can take place. This means that where collaboration earlier was considered to be between platforms, one must now consider collaboration based on communication to and from the network, and in communities of interest that consume and supply services.

The network, i.e. the involved host systems and dedicated network units, must thus supply services and data to the systems that are plugged into the network and their users. The network basis will give flexibility; because it is not necessarily decided in advance which entities will exchange information, or supply or consume services. This flexibility will support agility, precision and speed in the conduct of operations.

In principle, three types of information are supplied and consumed via the network: Sensor Information, information for Command and Control (C2) and effector information, e.g. information for fire and weapons control. The network should in principle support the exchange of all three types of information in spite of their different attributes.

3.3 Strategic Communication

On a national basis strategic communication includes the communication to and from the operational commands (army, navy, and air force) and the Defence Command Denmark. At the political level communication to the Ministry of Defence (MoD) and between ministries takes place.

		ATTRIBUTE VALUE					
		0	1	2	3	4	5
Reach	Physical	None	Local/personal	Local area	Regional, LOS	Regional, BLOS	Global
	Logical	None	Point-to-point with no further disclosure	Multicast with limited disclosure	Networked with limited disclosure	Networked with some disclosure	Networked with full disclosure
	Organisational	None	Own unit	Own service	Joint	Combined	All actors, including but not limited to joint and combined
Richness	Richness	None	Single, predefined message	Predefined, limited message catalogue	Message catalogue including free text	Text, voice, picture	Full multimedia
	Timeliness	None	Best effort	Guaranteed delivery	Low jitter, isochronous	Soft real-time	Strict real-time
Actuality	Lifetime	None	> Years	Months / Weeks	Hours / Days	Seconds / Minutes	< Seconds
	Continuity	None	Sporadic update		Many updates (bursts)		Continuously update (streaming)
Assurance	Availability	None	Very low	Low	Medium	High	Very high
	Integrity	None	Tampering possible		Tampering is detected		Tampering not possible
	Confidentiality	None	Very weak	Weak	Medium	Strong	Very strong
	Authenticity	None	No source identification		Traceable source		Authorised identifiable sources only
	Non-repudiation	None					Guarantee
Intrinsic Quality	Precision	None	Low		Adequate (medium)		High
	Accuracy	None	Far from true value		Acceptable distance to true value		Close to true value
	Consistency	None	Many contradictory versions		Some contradictory versions		Homogeneity (high)

Table 3-1: Generic attributes for strategic communication and information processing

The main generic requirements are given below. Please note that the list does not imply a prioritisation.

- Information assurance meaning high availability, confidentiality, and integrity is important. This implies *transmission security* and *communication security* requirements.
- Large reach.
- Requirements for multimedia information, hence large richness.
- Actuality and precision requirements are less important.

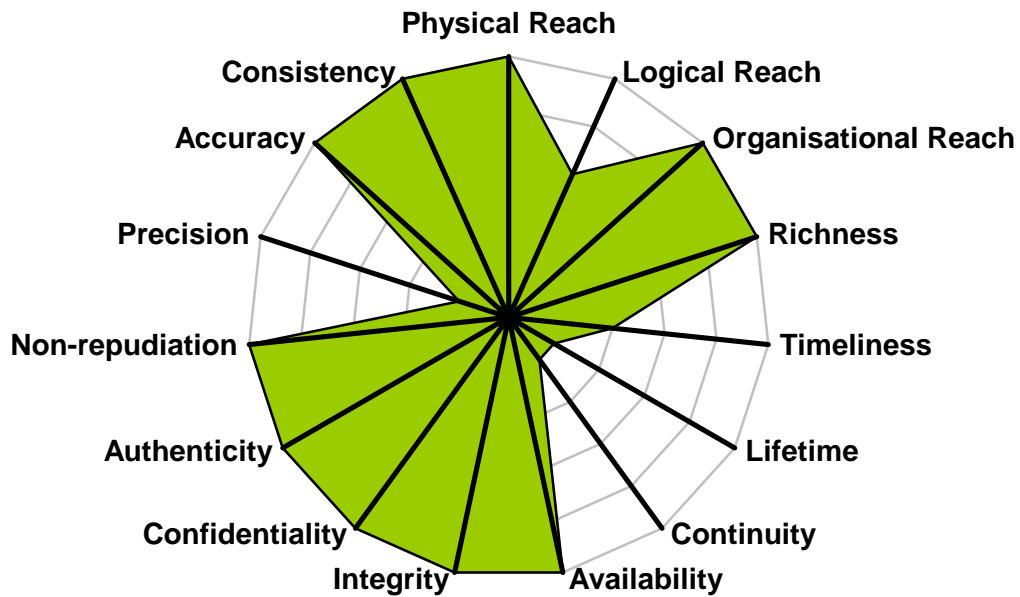


Figure 3-1: Generic attributes for strategic communication and information processing

3.4 Tactical Communications

The requirements on military ICT systems at the tactical level differ from civilian needs in a number of important ways. Add to this the general requirement for flexibility. It is still possible, however, to set up a number of generic requirements, requirements that are to be fulfilled in all scenarios. Based on chapter 2 in WP1 [2] it is relatively easy to make a list of these generic requirements, but the dependence on mission type makes it impossible to prioritise the requirements.

The generic requirements are:

- Mobility and deployability, both of infrastructure and hosting nodes
- Some degree of information assurance, mainly *communication security*, to assure availability, integrity and confidentiality. The tactical data will have a limited lifetime.
- Strict real time requirements and requirements for accuracy and precision.
- Robustness of all equipment, including the ability to operate under adversary climatic conditions.
- Limited logical and physical reach, but including the ability to participate in combined operations.

Other non-functional requirements are:

- Low cost, use of dispensable equipment in e.g. unattended ground sensor nets.
- Movement from analogue voice to digital multimedia in e.g. tactical internets.

		ATTRIBUTE VALUE					
		0	1	2	3	4	5
Reach	Physical	None	Local/personal	Local area	Regional, LOS	Regional, BLOS	Global
	Logical	None	Point-to-point with no further disclosure	Multicast with limited disclosure	Networked with limited disclosure	Networked with some disclosure	Networked with full disclosure
	Organisational	None	Own unit	Own service	Joint	Combined	All actors, including but not limited to joint and combined
Richness	Richness	None	Single, predefined message	Predefined, limited message catalogue	Message catalogue including free text	Text, voice, picture	Full multimedia
Actuality	Timeliness	None	Best effort	Guaranteed delivery	Low jitter, isochronous	Soft real-time	Strict real-time
	Lifetime	None	> Years	Months / Weeks	Hours / Days	Seconds / Minutes	< Seconds
	Continuity	None	Sporadic update		Many updates (bursts)		Continuously update (streaming)
Assurance	Availability	None	Very low	Low	Medium	High	Very high
	Integrity	None	Tampering possible		Tampering is detected		Tampering not possible
	Confidentiality	None	Very weak	Weak	Medium	Strong	Very strong
	Authenticity	None	No source identification		Traceable source		Authorised identifiable sources only
	Non-repudiation	None					Guarantee
Intrinsic Quality	Precision	None	Low		Adequate (medium)		High
	Accuracy	None	Far from true value		Acceptable distance to true value		Close to true value
	Consistency	None	Many contradictory versions		Some contradictory versions		Homogeneity (high)

Table 3-2: Generic requirements for tactical communication

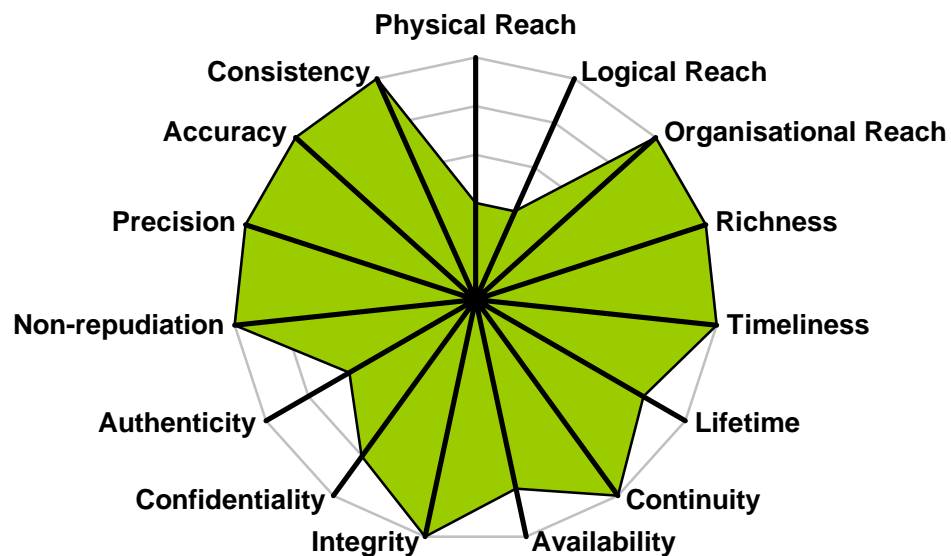


Figure 3-2: Generic requirements for tactical communication

The requirements reflect that even for tactical military communication, the conformity with commercially available communication in the shape of mobile phones (regular and smart phones) and PDAs is so pronounced that the expectations of the military user are created by what is common in his home from the commercial market. This underscores that for units deployed far from Denmark it is important that there is access to civil communication back to the homeland. Likewise communication internally in headquarters (HQ) and with local authorities must be supported. This is to be regarded as an extended tactical communication with both operative and social aspects. There will be a mixture of command in the field, command from HQs and communication with non-military organisations, from patrols and from moving convoys. This will affect the ICT systems and not least the information assurance.

3.5 Communication and Total Defence

The information services and exchange in Total Defence operations are relatively similar to tactical military communication [15]. Most Total Defence operations will be limited in time, space and the number of involved units. However, it is believed that such operations will be under close scrutiny both by the press and by the political level.

		ATTRIBUTE VALUE					
		0	1	2	3	4	5
Reach	Physical	None	Local/personal	Local area	Regional, LOS	Regional, BLOS	Global
	Logical	None	Point-to-point with no further disclosure	Multicast with limited disclosure	Networked with limited disclosure	Networked with some disclosure	Networked with full disclosure
	Organisational	None	Own unit	Own service	Joint	Combined	All actors, including but not limited to joint and combined
Richness	Richness	None	Single, predefined message	Predefined, limited message catalogue	Message catalogue including free text	Text, voice, picture	Full multimedia
	Timeliness	None	Best effort	Guaranteed delivery	Low jitter, isochronous	Soft real-time	Strict real-time
Actuality	Lifetime	None	> Years	Months / Weeks	Hours / Days	Seconds / Minutes	< Seconds
	Continuity	None	Sporadic update		Many updates (bursts)		Continuously update (streaming)
	Availability	None	Very low	Low	Medium	High	Very high
Assurance	Integrity	None	Tampering possible		Tampering is detected		Tampering not possible
	Confidentiality	None	Very weak	Weak	Medium	Strong	Very strong
	Authenticity	None	No source identification		Traceable source		Authorised identifiable sources only
	Non-repudiation	None					Guarantee
	Precision	None	Low		Adequate (medium)		High
Intrinsic Quality	Accuracy	None	Far from true value		Acceptable distance to true value		Close to true value
	Consistency	None	Many contradictory versions		Some contradictory versions		Homogeneity (high)

Table 3-3: Generic requirement for communications in Total Defence

The generic requirements are:

- Mobility, both of infrastructure and hosting nodes
- Limited degree of information assurance, mainly *communication security*, to assure availability and integrity. The exchanged data will have a limited useful life time.
- Some real time requirements and limited requirements for precision.
- Robustness of all equipment, including the ability to operate under adversary physical conditions.
- Logical reach, including the ability to collaborate with a number of civil emergency operators. Very often reach is limited to a region.

The information assurance requirements will in general be lower than for strictly military operations.

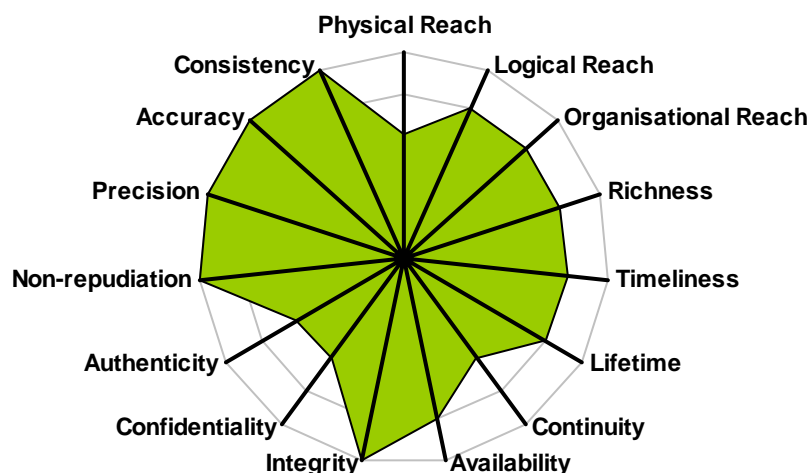


Figure 3-3: Generic requirement for communications in Total Defence

3.6 Communications and Enterprise Resource Management

There is a general trend towards not discerning between administrative and operational systems, which certainly is true for the Defence ICT systems. In connection with NBO this tendency will be even more pronounced. C2 systems must therefore be seen in a greater context, because some of the traditionally administrative systems are directly involved in operational tasks. Examples are the Danish Defence Management and Resource System (DeMars) and the staff support systems (SSS). DeMars will among other things be used in a logistical context, which pose a number of requirements on the ICT systems.

In principle there is a requirement for full access to all DeMars functions including logistics, human resources and budgets in all HQs and onboard all larger ships. The logistics functionality will be particularly important. The information must therefore have a large reach, a high degree of accuracy and integrity. Modern logistics systems with RF and bar code ID tags on equipment and adhering to *just in time* principles will be rather demanding.

		ATTRIBUTE VALUE					
		0	1	2	3	4	5
Reach	Physical	None	Local/personal	Local area	Regional, LOS	Regional, BLOS	Global
	Logical	None	Point-to-point with no further disclosure	Multicast with limited disclosure	Networked with limited disclosure	Networked with some disclosure	Networked with full disclosure
	Organisational	None	Own unit	Own service	Joint	Combined	All actors, including but not limited to joint and combined
Richness	Richness	None	Single, predefined message	Predefined, limited message catalogue	Message catalogue including free text	Text, voice, picture	Full multimedia
Actuality	Timeliness	None	Best effort	Guaranteed delivery	Low jitter, isochronous	Soft real-time	Strict real-time
	Lifetime	None	> Years	Months / Weeks	Hours / Days	Seconds / Minutes	< Seconds
	Continuity	None	Sporadic update		Many updates (bursts)		Continuously update (streaming)
Assurance	Availability	None	Very low	Low	Medium	High	Very high
	Integrity	None	Tampering possible		Tampering is detected		Tampering not possible
	Confidentiality	None	Very weak	Weak	Medium	Strong	Very strong
	Authenticity	None	No source identification		Traceable source		Authorised identifiable sources only
	Non-repudiation	None					Guarantee
Intrinsic Quality	Precision	None	Low		Adequate (medium)		High
	Accuracy	None	Far from true value		Acceptable distance to true value		Close to true value
	Consistency	None	Many contradictory versions		Some contradictory versions		Homogeneity (high)

Table 3-4: Generic information requirements for Enterprise Resource Management

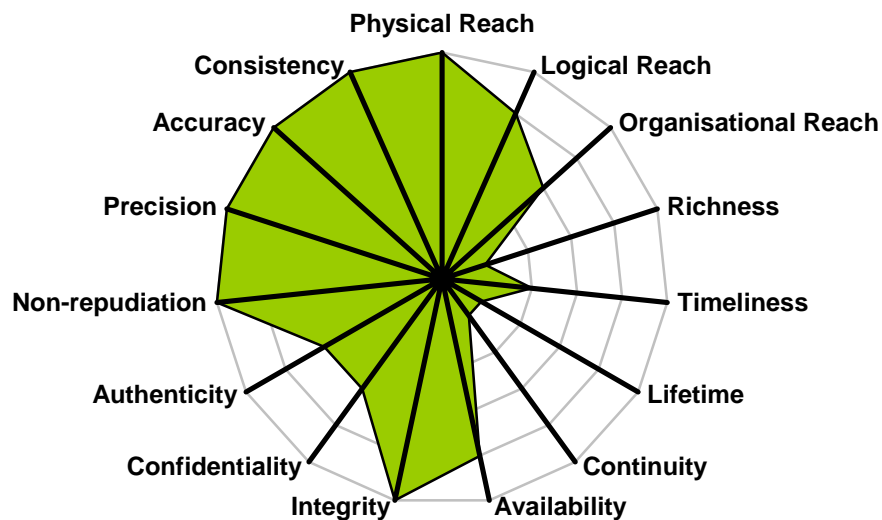


Figure 3-4: Generic information requirements for Enterprise Resource Management

3.7 Other General issues

The focus on capabilities has a very direct influence on the requirements on the target architecture. From a technological point of view, the emphasis will always be on systems. From a user's point of view, the services offered by the systems are important. Therefore the architecture must accommodate a service-oriented approach. The systems must be components in a system of systems, which in a flexible and transparent fashion gives the user the suite of services needed in a specific mission.

The time of large scale big bang acquisitions is over. The speed of the technological development and the unpredictability of the mission in terms of space, time and cooperation partners force a move towards iterative acquisition and development, either in the form of incremental or evolutionary development. The latter will lead to incremental models such as spiral models for the development (or acquisition).

The mixture of legacy systems, dedicated systems and COTS, will virtually make it impossible to have homogeneous solutions. The architecture must be able to encompass the many different components and subsystems. This will not only be the case for national systems but also for NATO systems and for the systems of collaboration and cooperation partners.

Finally, although we do not explicitly deal with economy aspects in this work package, it is important to note that the above principles will reduce the project risk in several ways. Firstly, it retains a loose coupling between the systems, and the service orientation makes it easier to discuss requirements with the end users. There is a greater probability that they get systems that add value to their ability to accomplish missions. Secondly, it will be possible to use common commercially available components to a larger extent than earlier- and thus obtain a reduced cost and faster acquisition. Finally spiral development and acquisition make the fulfilment of the actual and up to date user requirements easier. However, the loose coupling and the incremental acquisition may pose new challenges to fulfilment of the information requirements.

From the vignettes from WP1 [2] and from the discussion in [7] it appears that small groups in new combinations will be important. These technical teams (the term is used in [7] for small groups) must be supported by the technical architecture of the ICT systems. Their information and communication systems will most likely not be of the same kind, so a simple principle to allow their interoperability must be applied. This principle must also allow the systems to develop and function autonomously.

3.8 Information Systems - the Applications

We have so far dealt with the information and the requirements on the information as expressed by information attributes and their values. These requirements will translate into requirements on the communication, and on the information systems that capture, process and store the information. The information systems include the applications that are directly seen by the end user, e.g. the military decision maker, but also comprise services that are necessary to operate and manage the systems of systems and functions such as data and information fusion. The information systems must of course deliver information with the required values of the attributes, but other requirements must also be met by the systems. These requirements may be divided into requirements for usability (e.g. user friendliness)

and requirements for their ability to plug into the network of networks that is one of the prerequisites for NBO, and a precondition for obtaining a sufficient information reach. This net worthiness requirement is at the lowest level a requirement for using the right protocols, including methods for authentication and authorisation of users and processes. At a higher level requirements for meaningful collaboration with other systems become important. These interoperability requirements are very often requirements on data and information, from requirements on presentation via syntax to semantics and pragmatics. One way of obtaining a high degree of interoperability is to use a common data model in the systems such as the JC3IEDM (see e.g. [8]). Such a model may be the native model of the systems, or it may be used as a data interchange model. A common data model may be an important step towards semantic interoperability. A less complex example is the use of ADatP3 messages.

Data interoperability in itself is not very flexible. The applications are of course able to exchange meaningful information, but the systems that deliver and process the information will have to be defined in advance. A more flexible way of doing things is necessary, so that the end users or consuming systems can pick freely from services provided by systems that are connected to the net, and thus if necessary on the fly define new and specially tailored applications dedicated to the concrete mission or even to the actual situation by combining services. Use of meta-information (e.g. XML and XML schema) and service orientation (with service descriptions) is one way of obtaining this flexible formation of applications, but at the cost of a significant overhead in terms of the volume of data and in terms of the service orchestration. The service orientation, however, allows inhomogeneous systems to interoperate and to be federated in a meaningful way.

3.9 Requirements from the Three Services and the Total Defence

The three services (army, navy and air force) and the Total Defence authorities have traditionally had different mission types, and different collaboration partners.

From [2], [4], [5], [6], [10], [11], [13], and [15] it is clear that for each service and for the Total Defence the union of all requirements encompasses all information attributes, and forces them to be at their highest level. Therefore it does not make any sense to consider all mission types when stating the requirements. It will be necessary to look at a specific mission and even at specific tasks within the missions. In this work we accomplish this by using the vignettes of the overall tasks. Coalition partners could be NATO members, Partnership for Peace countries and others. From a communications point of view this brings back the focus on interoperability, where *networthiness* is one important parameter. Despite of this, there are obvious differences in general terms between the services, mainly with respect to reach and actuality. It is important to note that the requirements on military information with few exceptions are much higher than on civilian information. The demands for the properties of the ICT systems are thus significantly higher- and possibly costlier to meet.

4 Requirements Derived from Vignettes

This chapter deals with the requirements that follow from the vignettes from WP1. It is possible to define generic tasks from the vignettes that deal with a smaller number of different requirement sets. The use of the vignettes makes the traceability of the requirements clearer. Besides WP1, also reports from the three services and the Total Defence (see [6], [10], [11], [13], and [15]) are used. As stated in WP1, the vignettes are selected so that they cover most of the ICT requirements to meet the challenges in the tasks outlined below. The 10 main tasks and 3 vignettes from WP1 are:

National tasks

- Denmark – Monitoring of national territory and enforcement of sovereignty
- Denmark – Civilian-oriented tasks (ie. Environmental tasks, Search-and-Rescue)
- Denmark – Emergency Services / Disaster Response
- Denmark – Defence against a Cyber Attack
- North Atlantic – Monitoring of national territory and enforcement of sovereignty

International tasks

- Armed conflict (i.e. Counter Insurgency (COIN) and Peacemaking)
- Stabilization / Peacekeeping
- Nation Building / Capacity Building / Reconstruction
- International Maritime Policing (Piracy)
- Disaster response / Humanitarian assistance

Vignettes

1. National Task Denmark.
2. National Task North Atlantic.
3. International Task Afghanistan.

The information exchange requirements for the 3 vignettes will be described through the identified *information attributes* described in chapter 2 and summarised in Table 2-1. In order to deduct the *information attribute values*, some characteristics of the vignette are derived.

First, the vignettes will be evaluated by analysing seven communication related parameters. These parameters are:

- **Area.**
The nature of conflicts today deviates from the traditional scenario, where the area behind a frontline was considered secure. It is therefore necessary to consider presence of hostile forces a possibility, even when the area of operation is in traditionally friendly area. Typical values of this attribute are friendly, hostile, or adverse environmental conditions.
- **Mobility.**
The requirement on mobility will also create a requirement on the mobility of the communication equipment. Typical values of this attribute are high, moderate, or none
- **Collaboration partners.**
The collaborating partners are a factor, when defining the communication requirement of a system. The interoperability and richness of the communication can be increased, when communicating with a pre-defined set of partners using advanced communication standards. Typical values of this attribute are Police, DEMA, Home Guard, NGO, Nation, or NATO.

- **Stability in tasks.**
When a task deviates too much from the standard task, it will limit the ability to communicate. E.g. when one can use well defined communication patterns, the semantics of the information will be much richer, than when one needs to communicate with parties that do not have the necessary equipment or the ability to interpret a set of pre-defined messages. Typical values of this attribute are high, low, or changeable.
- **Space.**
The physical area of operation is a significant factor, when dimensioning/selecting the communication equipment. Typical values of this attribute are small, regional, or cyberspace.
- **Time.**
The time span of an operation. Typical values of this attribute are short, possible long, or long.
- **Conflict Intensity.**
The intensity of the operation usually measured as high/low, etc. Typical values of this attribute are high, middle, or low.

Second, six selected *Information System Attribute values* will be described for each of the vignettes. These Attributes are:

- **Information Types.**
What kind of information is required? Typical values could be tracking data, voice, video, images or other data.
- **Real-time.**
Does this vignette have any real time requirement, and what kind?
- **Interoperability.**
The required interoperability (spanning from not connected to highly integrated). Example on exchange goes from a purely syntactical level to some degree of semantic data exchange.
- **Network based.**
Yes/no
- **Civilian infrastructure.**
Do we need access to a civilian infrastructure?
- **Level.**
Usual parameters go from tactical, operational and strategic to the political level.

When the characteristics consisting of the seven parameters (or vignette attributes) and the six Information System Attributes are described for a vignette then it is possible to deduct the *information attribute values*. The deduction is a best match based on how the characteristics mentioned above may influence the *information attributes*.

4.1 Vignette 1: National Task Denmark

A Heads of State summit is held in Denmark, with participants from many nations. Danish Security and Intelligence Service⁷ has received a credible threat that a group of unknown terrorist will try to kill a head of state at this summit. To help the Police the Danish Home Guard⁸, the national SOF⁹, the Navy and the Air Force are tasked with securing the perime-

⁷ Danish: Politiets Efterretningstjeneste (PET)

⁸ Danish: Hjemmeværnet

⁹ Danish: Frømandskorpset and Jægerkorpset

ter of the summit. The Police will handle crowd control. All of this is coordinated from an operational HQ located within the protected perimeter.

As soon as the summit was announced hackers have tried to hack into Police, Danish Armed Forces and governmental computer systems. DK-Cert, GOV-Cert and MIL-Cert are all involved in protecting the ICT- infrastructure.

During the summit different radical NGOs attempt to get access to the summit grounds by land, sea and air. But all attempts are discovered and repelled.

An act of sabotage de-rails a commuter train close to the Conference Center where the summit takes places. This causes casualties as well as a major disturbance in the commuter-traffic between Copenhagen and the airport. The Home Guard (additional units) and DEMA are activated to help control and alleviate the situation. The assessment is that the purpose of this event is to divert the attention of the authorities from the Head of State summit and cause a chaotic situation that will enable the terrorist organisation to accomplish its intended assassination.



Figure 4-1: Head of State Summit. (OV-1)

The following *Information Exchange Requirements* have been identified:

- Real-time data communication between sensor network (costal radars, mobile and long range air-defence radars) and Headquarters (National and summit).
- Real-time voice and data communication between military entities, DEMA and the Police.
- Real-time voice and data communication between military entities (SOF, land, sea and air).
- Real-time voice and data communication between HQ and SOF units.
- Real-time network monitoring.

The following *Information Requirements* have been identified:

- Common Operational Picture (COP). For small scale maps also in 3D.
- Real-time air picture for Headquarters (National and summit).
- Live video from ground and air.

- Which computer systems are compromised and what is affected.

By distilling the *Information Exchange Requirements* and *Information Requirement*, it is possible to assess seven communication related parameters and six selected *Information System Attributes with their appropriate values*. This is shown in Table 4-1.

Vignette Attribute Values	Information System Attribute Values
Area: Friendly	Information types: Voice, images and video, data.
Mobility: High	Real-time: Yes
Collaboration partners: Police, DEMA, Home Guard	Interoperability: Syntactical, preferably semantic.
Stability in tasks: Moderate to high	Network based: Yes
Space: Small, but up to national size + Cyberspace	Civilian infrastructure: Available
Time: Short time span	Level: Up to strategic/political.
Conflict intensity: High	

Table 4-1: Summary of characteristics of National Task Denmark

The information attribute values deduced from the vignette characteristics are shown in Table 4-2.

		ATTRIBUTE VALUE						
		0	1	2	3	4	5	
INFORMATION ATTRIBUTE	Reach	Physical	None	Local/personal	Local area	Regional, LOS	Regional, BLOS	Global
		Logical	None	Point-to-point with no further disclosure	Multicast with limited disclosure	Networked with limited disclosure	Networked with some disclosure	Networked with full disclosure
		Organisational	None	Own unit	Own service	Joint	Combined	All actors, including but not limited to joint and combined
	Richness	Richness	None	Single, predefined message	Predefined, limited message catalogue	Message catalogue including free text	Text, voice, picture	Full multimedia
		Actuality	Timeliness	None	Best effort	Guaranteed delivery	Low jitter, isochronous	Soft real-time
	Lifetime		None	> Years	Months / Weeks	Hours / Days	Seconds / Minutes	< Seconds
	Continuity		None	Sporadic update		Many updates (bursts)		Continuously update (streaming)
	Assurance	Availability	None	Very low	Low	Medium	High	Very high
		Integrity	None	Tampering possible		Tampering is detected		Tampering not possible
		Confidentiality	None	Very weak	Weak	Medium	Strong	Very strong
		Authenticity	None	No source identification		Traceable source		Authorised identifiable sources only
		Non-repudiation	None					Guarantee
	Intrinsic Quality	Precision	None	Low		Adequate (medium)		High
		Accuracy	None	Far from true value		Acceptable distance to true value		Close to true value
		Consistency	None	Many contradictory versions		Some contradictory versions		Homogeneity (high)

Table 4-2: Information requirements in the National Task Denmark

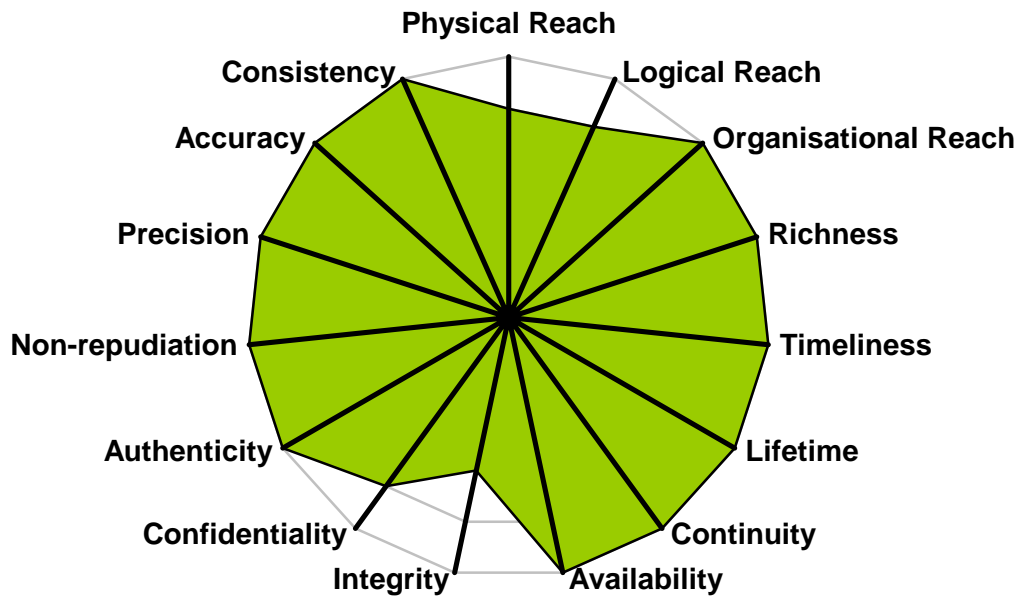


Figure 4-2: Information requirements in the National Task Denmark

Defending cyberspace will be as important as defending physical space. The implications of cyber attacks may be far reaching and go from defacing attacks on official websites to non availability of vital assets and obstructions of disaster relief operations. This leads to demands for a high availability and robust communication network of networks. Such a *protected core* is an important national infrastructure asset with many stakeholders, among them the Danish Armed Forces.

4.1.1 Summary of requirements

Means for protection of cyberspace and among these a protected core should be established. Real-time high bandwidth mobile communications with regional physical reach is in demand. The many stakeholders, military and emergency services, point to the need for a federated network of networks based on standard protocols. SOA can support interoperability between stakeholders' command and control systems and should be mandated.

4.2 Vignette 2: National Task North Atlantic

On September 12th a violent explosion-like fire broke out in the 156 thousand ton Russian oil tanker Burgas. The ship was on its way through the newly opened north-west passage with a cargo of crude oil from the Siberian Salym oil field intended for refining in the city of Garyville. The fire in the ship caused a major oil leak that with the current wind and sea conditions seem bound for Disko Bay. The crew had to abandon the ship and find themselves in two life rafts in the sea (sea state 5). Both the Canadian and the Danish environmental authorities are extremely concerned about the situation and both countries are sending ships

and planes to the area. Canada has two Maritime Patrol Aircrafts (MPA) in the area and a marine environmental ship is under way. To monitor the situation and help with the rescue of the crew, the Ocean Patrol Vessel THETIS, and the Arctic Patrol Ship KNUD RASMUSSEN. is on the way to the area. In addition, two F-16 fighters with recce pods and a Challenger aircraft have been sent to Sondrestrom Air base to assist in the area. The disaster is followed very closely by the news media both in Europe and North America. The Russian frigate NOVIK is expected to come to the area since it was on patrol between Greenland and Iceland. Environmental organisations, including Greenpeace, have previously requested strict rules for sailing these waters with large oil tankers, and have threatened blockades of ports and actions against ships.

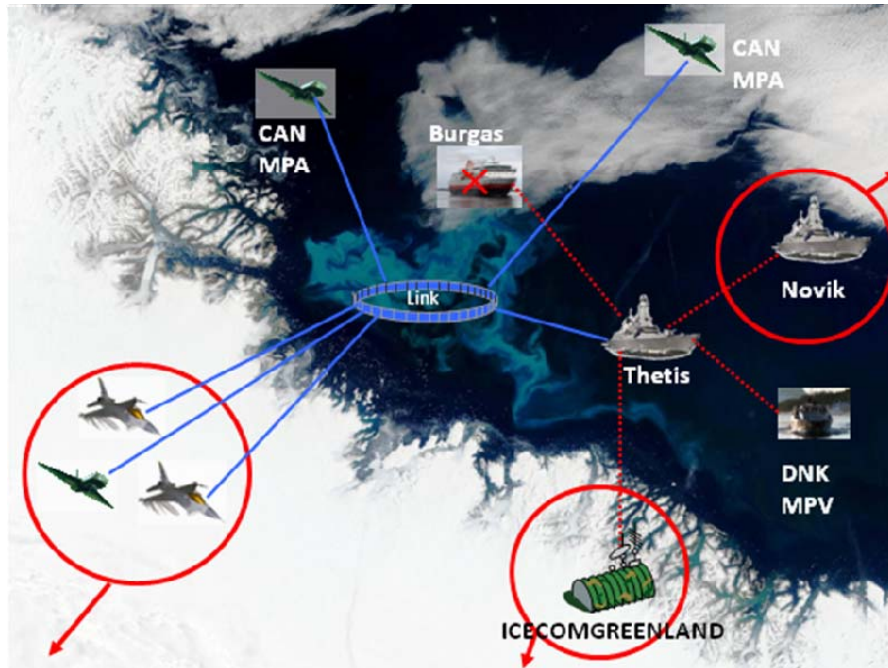


Figure 4-3: Oil Tanker Burgas (OV-1)

The Danish minister of Defence and the Government of Greenland want to be constantly updated on the situation. The defence minister has in a statement stressed the importance of a coordinated and rapid response. There must, as soon as possible, be established an emergency organisation, to prevent and possibly reduce the impact of the disaster on the vulnerable nature of Greenland.

The following *Information Exchange Requirements* have been identified:

- Real-time Communication between MPA and recce aircraft from DNK and CAN.
- Sensor information in real time from Challenger to F16 and THETIS and KNUD RASMUSSEN.
- Real-time Information for THETIS.
- Transfer of (processed) sensor information from the area to Arctic Command, CHODDEN and Environmental Ministry.
- The data and images for/from NOVIK.
- Video and data from field to Danish MoD, Greenland and CHODDEN.
- Voice and data for NGOs (Greenpeace).
- Direct access to environmental and meteorological databases, including from DMI.

The following *Information Requirements* have been identified:

- Maps of region including 3D depth maps.

- Real-time air and satellite pictures.
- Processed sensor information.
- Environmental data, including updated maps of currents in the region.
- Meteorological data (including DMI)

By distilling the *Information Exchange Requirements* and *Information Requirement*, it is possible to assess seven communication related parameters and six selected *Information System Attributes with their appropriate values*. This is shown in Table 4-3.

Vignette Attribute Values	Information System Attribute Values
Area: Friendly, possibly adverse environmental conditions	Information types: Voice, images and video, data.
Mobility: High	Real-time: Yes
Collaboration partners: Canada, Russia, NGOs (Greenland Greenpeace)	Interoperability: Syntactical, preferably semantic.
Stability in tasks: High.	Network based: Yes
Space: Usually small, but up to regional size.	Civilian infrastructure: Available
Time: May be long.	Level: Up to strategic/political.
Conflict intensity: Middle	

Table 4-3: Summary of characteristics of National Task North Atlantic

		ATTRIBUTE VALUE						
		0	1	2	3	4	5	
INFORMATION ATTRIBUTE	Reach	Physical	None	Local/personal	Local area	Regional, LOS	Regional, BLOS	Global
		Logical	None	Point-to-point with no further disclosure	Multicast with limited disclosure	Networked with limited disclosure	Networked with some disclosure	Networked with full disclosure
		Organisational	None	Own unit	Own service	Joint	Combined	All actors, including but not limited to joint and combined
	Richness	Richness	None	Single, predefined message	Predefined, limited message catalogue	Message catalogue including free text	Text, voice, picture	Full multimedia
		Actuality	Timeliness	None	Best effort	Guaranteed delivery	Low jitter, isochronous	Soft real-time
	Lifetime		None	> Years	Months / Weeks	Hours / Days	Seconds / Minutes	< Seconds
	Continuity		None	Sporadic update		Many updates (bursts)		Continuously update (streaming)
	Assurance	Availability	None	Very low	Low	Medium	High	Very high
		Integrity	None	Tampering possible		Tampering is detected		Tampering not possible
		Confidentiality	None	Very weak	Weak	Medium	Strong	Very strong
		Authenticity	None	No source identification		Traceable source		Authorised identifiable sources only
		Non-repudiation	None					Guarantee
	Intrinsic Quality	Precision	None	Low		Adequate (medium)		High
		Accuracy	None	Far from true value		Acceptable distance to true value		Close to true value
		Consistency	None	Many contradictory versions		Some contradictory versions		Homogeneity (high)

Table 4-4: Information requirements in the North Atlantic Incident

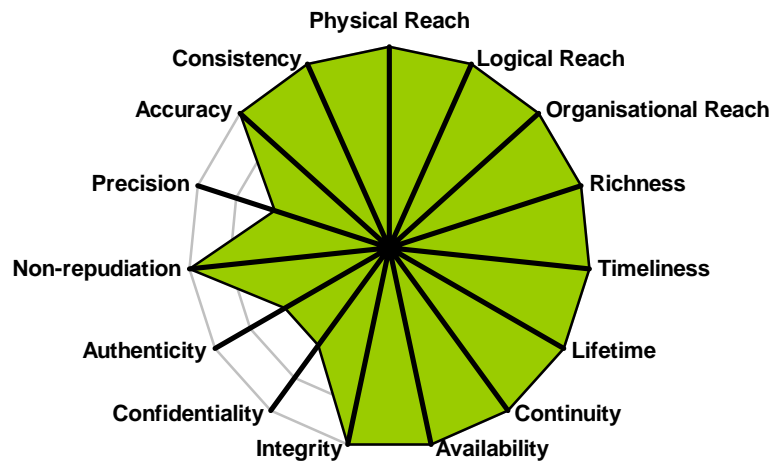


Figure 4-4: Information requirements in the North Atlantic Incident

The tasks of enforcing sovereignty and dealing with environmental disasters in the North Atlantic lead to demands for interoperability with unforeseeable partners. This means that the information exchange to a large extent will have to be based on a common denominator, most likely commercial providers and internet technology. The need for reach-back to Denmark and Greenland puts emphasis on BLOS communication means.

The information attribute values deducted from the vignette characteristics are shown in Table 4-4.

4.2.1 Summary of requirements

Exchange of real-time sensor data and tasking between the military actors can for a long time only be accommodated by joint or federated data links. The obvious interests of non military organisations lead to a demand for information gateways between the military communication systems and civilian networks. The gateways serve as interoperability points that allow rich information to be exchanged without compromising security and safety of the operations. The military C2 systems must be able to interoperate with e.g. environmental and local authorities. The regional communications must have a global reach.

4.3 Vignette 3: International Task Afghanistan

Danish military units are involved in a NATO lead operation in Afghanistan. Main contribution is an army battalion, organized as a part of a UK brigade. Main task is controlling and stabilizing an area in southern part of Afghanistan. The battalion is supported by an Afghan National Army (ANA), police, rescue preparedness unit from Danish Home Guard and other units from the Danish government and NGOs. The battalion has established a main HQ and

a number of smaller forward operation bases where Danish and ANA military personnel work close together.

During a visit from the Danish Minister of Defence, where he was accompanied by a British general, at one of the forward operation post, his convoy was hit by a road bomb, and two soldiers were killed. The convoy was afterwards attacked by the enemy with small arms fire, machineguns, and RPG. The VIP vehicle was hit.

Two wounded soldiers and a wounded Danish journalist from a major newspaper were picked up by a British rescue helicopter. Short after takeoff the helicopter was forced to make an emergency landing and the British helicopter crew and the Danish journalist were captured by the enemy.

A joint rescue operation was established, with participation from, British, Danish and Afghan army units, reconnaissance and close air support aircrafts, UAV and SOF. National HQs in UK and DNK are heavily involved with NATO HQ and Deployed Army HQ. The incident was followed very closely by the media.

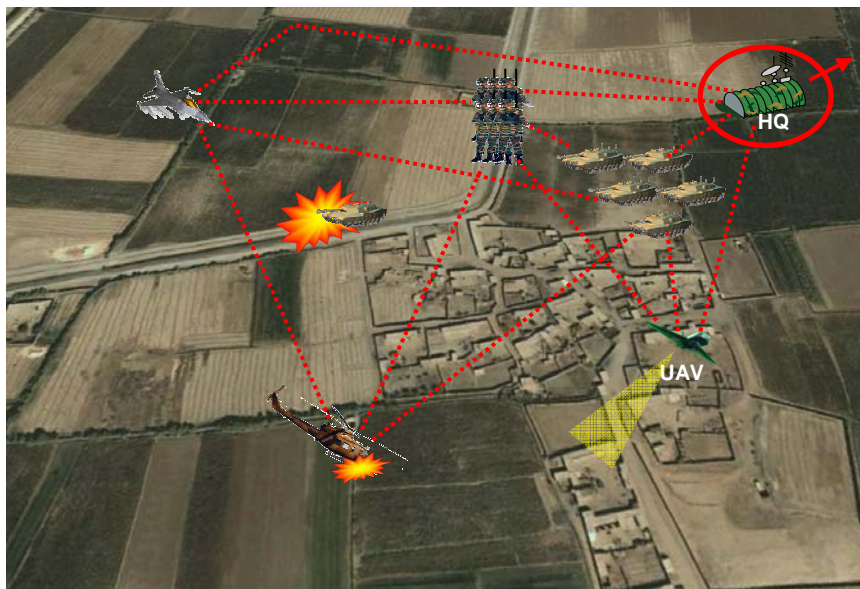


Figure 4-5: Afghanistan (OV-1)

The following *Information Exchange Requirements* have been identified:

- Real-time data communication between sensor network (air-defence radars, UAV, aircrafts) and Headquarters (National and NATO).
- Real-time voice and data communication between military C2-units and political HQ.
- Real-time voice and data communication between military units (SOF, land, sea and air).
- Near real-time communication between national HQs and the BTN HQ in Afghanistan.
- Role based access to information

The following *Information Requirements* have been identified:

- Real-time sensor information from air-defence radars, UAV, and aircrafts.
- Live pictures from UAV and aircrafts.
- Common operation picture, including 3D.
- Real-time effector information such as status and location, and engagement and firing orders.

- Large reach of rich information, including regional Beyond Line of Sight (BLOS) communication.

By distilling the *Information Exchange Requirements* and *Information Requirement*, it is possible to assess seven communication related parameters and six selected *Information System Attributes* with their appropriate values. This is shown in Table 4-5.

Vignette Attribute Values	Information System Attribute Values
Area: Hostile	Information types: Voice, images and video, data.
Mobility: High	Real-time: Yes
Collaboration partners: International (GBR and NATO)	Interoperability: Syntactical, preferably semantic
Stability in tasks: Low, changeable.	Network based: Yes
Space: Usually small, but up to regional size.	Civilian infrastructure: No or limited.
Time: Relatively short.	Level: Tactical, including up to strategic/political.
Conflict intensity: High	

Table 4-5: Summary of International Task Afghanistan

		ATTRIBUTE VALUE						
		0	1	2	3	4	5	
INFORMATION ATTRIBUTE	Reach	Physical	None	Local/personal	Local area	Regional, LOS	Regional, BLOS	Global
		Logical	None	Point-to-point with no further disclosure	Multicast with limited disclosure	Networked with limited disclosure	Networked with some disclosure	Networked with full disclosure
		Organisational	None	Own unit	Own service	Joint	Combined	All actors, including but not limited to joint and combined
	Richness	Richness	None	Single, predefined message	Predefined, limited message catalogue	Message catalogue including free text	Text, voice, picture	Full multimedia
		Timeliness	None	Best effort	Guaranteed delivery	Low jitter, isochronous	Soft real-time	Strict real-time
	Actuality	Lifetime	None	> Years	Months / Weeks	Hours / Days	Seconds / Minutes	< Seconds
		Continuity	None	Sporadic update		Many updates (bursts)		Continuously update (streaming)
		Availability	None	Very low	Low	Medium	High	Very high
	Assurance	Integrity	None	Tampering possible		Tampering is detected		Tampering not possible
		Confidentiality	None	Very weak	Weak	Medium	Strong	Very strong
		Authenticity	None	No source identification		Traceable source		Authorised identifiable sources only
		Non-repudiation	None					Guarantee
Intrinsic Quality	Precision	None	Low		Adequate (medium)		High	
	Accuracy	None	Far from true value		Acceptable distance to true value		Close to true value	
	Consistency	None	Many contradictory versions		Some contradictory versions		Homogeneity (high)	

Table 4-6: Information requirements in International Task Afghanistan

The information attribute values deduced from the vignette characteristics are shown in Table 4-4.

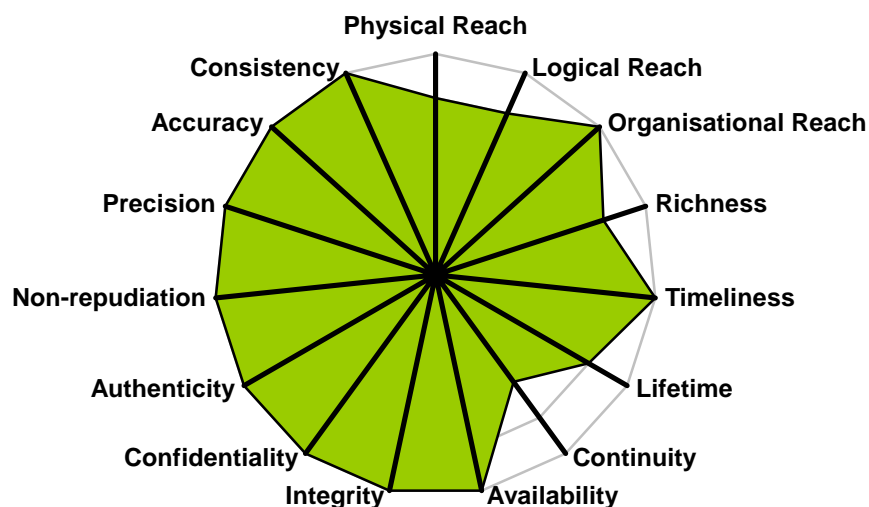


Figure 4-6: Information requirements in International Task Afghanistan

4.3.1 Summary of requirements

The vignette *International Task Afghanistan* demonstrates the emphasis on reach, precision and real-time information. An important and needed asset is regional BLOS communication means. The ability to plug into the coalition network of networks (including Afghan mission network (AMN)) together with the need for reach-back to Danish HQ and the political level shows the need for high availability communication. The need for interoperability between the Danish C2 systems and coalition partner systems may in the short term be accommodated by exchange of data models and data replication such as Multilateral Interoperability Programme (MIP). However, requirements for flexibility and wider interoperability will in a longer time frame point towards more open and commercially available interoperability mechanisms, e.g. web based cloud or grid computing. The demand for joint and combined high capacity data links is obvious. The IM task in this situation is a difficult balance between the democratic need for openness and the requirements for operations security.

4.4 Summary of Information Requirements

From the analysis, it is obvious that regional BLOS reach is important, and that availability and other assurance characteristics must be met. The intensity and speed point towards exchange in real-time. The need for accuracy is becoming increasingly important because of the far reaching consequences of mistakes in the missions. As the dependency on information sharing increases, information assurance becomes even more important.

This page is left intentionally blank

5 Technological Requirements on Defence ICT Systems

This chapter introduces a number of technical requirements that are consequences of the vignettes of WP1 [2] and the transition towards NBO [3] and bridges the gap between the functional requirements of the former chapters and the technical part of DEFTA (see WP3).

One of the most important requirements from the vignettes is that of agility. Agility in command and agility in execution means the possibility to make changes, to improvise and to exploit new opportunities as the mission evolves. Therefore, the ICT systems must be able to adapt to the current situation, and the common operating picture must be available in an appropriate level of detail for all relevant actors. The following sections do not constitute an exhaustive list of technical requirements, but rather take into account aspects specific to NBO.

The chapter is divided into sections and subsections that address issues decisive for technical part of DEFTA. The issues are:

- 1) Local and personal communications.
- 2) Communication between C2 systems.
- 3) Communication involved in targeting and tracking, with its specific real time requirements.
- 4) Beyond line of sight communication. This is important for reach back.
- 5) Addressing and naming
- 6) Real time and other Quality of Service issues.
- 7) Communication management.
- 8) Information systems and constraints.
- 9) Loose coupling and late binding – service oriented architecture (SOA).
- 10) Cyberspace aspects.

A number of additional technological aspects outside the above mentioned issues, but also of importance to the design of the communication and information systems are briefly discussed in section 5.11.

5.1 Local and Personal Communications

Local and personal communication is limited to a small geographic area, and usually takes place within military units, inside C2 installations, inside a vehicle or inside a limited environment such as a ship. The sender and receiver in end-to-end (E2E) will in all cases be attached to a local or personal communication network. Physical organisational reach will not in general entail any requirements, but very often logical reach will. Real time requirements will be soft. The information will often be very rich, free text or speech, video, imagery or information from a variety of sensors.

There must be support for *communication security* and means for preventing unauthorised use of the systems.

The local means of communication for future units must be able to manage both strategic and tactical communication. This requirement for multimode and multirole communication is a consequence of the network centrality, and the means for obtaining it is in this case connectivity to the global network of networks.

Local communication is important in a number of the vignettes and tasks that are discussed in chapter 4. From them, the following requirements can be deduced:

- Fully portable in the sense that the equipment may be carried by one person.
- Local communication and data processing must be available in mobile C2 installations
- Local communication and data processing must be available in stationary and semi-stationary C2 installations
- Some local communication assets should be able to function as a relay, switch or base station for users in the local environment. This is particularly important if it cannot be assumed that a fixed infrastructure is available. Examples of users are patrols and transport convoys.

Local communication must therefore be able to function at different levels, from the single soldier, within the aircraft, to the local unit. There is a need for communication technology that reflects the convergence in Personal Area Networks (PANs), Local Area Networks (LANs) and Wide Area Networks (WANs). This means that for instance the single soldier may connect to his unit, a battalion and a fully mobile division.

5.2 Communication between C2 Elements

Future use of C2 systems will put great demands on the reach of the information, especially the logical and organisational reach (e.g. vignettes 1, 2 and 3 in WP1 [2]). The system must be able to be used across a wide spectrum of threats and scenarios of deployment, which spread from conventional wars through limited Crisis Response Operations, asymmetric conflicts, terrorism and in operations with coalition partners (Combined) and also with other branches (Joint). The ability to participate in multilateral collaboration is in general important, but planning must increasingly be created from scenarios, which are hard to predict. Furthermore these situations will arise with short notice. The build-up of such a defence structure, which accommodates these military requirements, must be based on flexible C2 systems.

To accomplish this, we must ensure interoperability between C2 systems. Decision makers must have access to timely information. This also means that the C2 system must be able to exchange information across organisational lines, national borders and cultural and language boundaries. Furthermore, tactical C2 systems must be able to send information to both operational and strategic command levels and governmental agencies. Military forces must be able to communicate with non-government organisations such as international relief organisations. The requirement for interoperability will require a well-developed communication and information structure and establishment of well-defined interfaces to information systems (C2IS).

It will be required that the different command levels should be able to use different WANs. Combat Net Radio (CNR), satellite links, phone, Internet technology and broadband microwave links and also different network topologies may be in use in order to optimize the communication infrastructure and information systems. The architecture must enable net-centricity hereby providing access to the heterogeneous communication systems in an integrated way.

For NBO purposes the term “C2 network” is understood as a logical network, which is used for exchange of C2 information. The C2 entities can therefore be regarded as connected in

their own virtual network on top of, or as an integrated part of existing heterogeneous communication infrastructures.

5.3 Communications, Targeting and Tracking

Target acquisition for deployment of weapons and tracking are two types of assignments, which will increase the demands on the communication infrastructures in a net-centric environment. There will often be hard real-time requirements on the communication infrastructures. The real-time requirements are described in generic terms in section 5.6. Tracking data should in general be transmitted with minimum delay. However, the requirements are less strict, since loss of a limited amount of data may be acceptable to the tracking algorithm.

In an NBO environment the information for target acquisition, deployment of weapons, and tracking information will be communicated in the form of sensor and effector information. This information will be handled by two types of networks, i.e. a sensor network (see section 5.3.1) and an effector network (see section 5.3.2). These networks will often be virtual networks, and be hosted by the overall communication infrastructure, but in some cases also by means of dedicated networks.

5.3.1 Sensor Networks

There will be a requirement to utilize many different sensors, including radar, electro optical, acoustic, magnetic, seismic and also sensors for automatic target acquisition, identification (e.g. Combat ID), and tracking. The interesting point here is not the increased use of sensors, but the fact that the sensors are interconnected in their own virtual network.

These sensor networks will use a very large number of different sensors to collect information from the environment. Through the sensor network, this information will be transmitted to other sensors or information consumers.

Some sensor networks must be able to collect information for a central analysis centre. Contemplating the capacity of the network, local aggregations or data manipulation will be done offhand.

Other sensor networks use the information in a distributed way, i.e.:

- The information is not collected centrally, but is utilized in multiple places in the network (geographically or logically), just as applications continually are updated and should not be polled for new information. I.e. the continuity of the information is the decisive factor.
- The information can be depending on time and place. Often it is acceptable that the precision of the information is decreasing with the distance to the event.

The sensor network can therefore have a logical architecture, which is different from other networks. They can be very limited in their use of resources, often have wireless connectivity and ad-hoc networks can be established when unattended ground sensors are randomly deployed in the field.

Three properties characterise the architecture of sensor networks:

- The heterogeneousness in the network architecture; it must cover a large number of disparate sensors
- Both the network topology and the means for data extraction must be configurable
- Security and survivability during an unexpected or malicious attack.

The above needs will create a demand on the communication, which must be robust, reliable and flexible, and must also be adaptable given the available bandwidth.

Data aggregation and fusion will have a decisive role for the efficiency and effectiveness of the whole sensor network. This is among other things due to limitations in bandwidth of the network.

The real challenge in large heterogeneous sensor networks is often in the management part of these networks. The management part must ensure a secure and fault tolerant network structure, which includes both high-speed infrastructure and wireless or ad-hoc networks and channels. Routing protocols must ensure the preservation of the information exchange despite failure of nodes and links. To accommodate fault tolerance in equipment and to avoid that all applications are critically dependent on the same sensors, the network architecture should have built-in flexibility in configuration, filtering and data extraction.

In the future raw sensor data is expected to be available to a much higher degree than previously, i.e. a *publish-before-process* principle. The argument partly being that data will be available quickly and partly that the user can select the necessary processing method (the user will know better than anyone for what purpose the data in a given context should be used). Such a methodology will create a new set of requirements on the transmission capacity of the network.

5.3.2 Effector Networks

The third of the logical NBO networks is called an effector network. This network carries the information, which directly guides and controls the engagement. Typical information will be target data, fire control data, status data for artillery and close air defence and certain data from the sensor network. The effector network will very often have to deliver hard real time data, just as a number of status data will have to live up to soft or hard real time requirements. Some of the data, which are transmitted in the effector network, could previously have been transmitted in separate networks with little or no gateway based coupling to e.g. C2 systems. The effector systems have to a certain degree been independent from their own sensors and with a modest exchange of information to other networks. They have therefore only given a modest contribution to the combined common operating picture and benefited little from it.

5.4 Beyond Line Of Sight Communications

Communication beyond line of sight (BLOS) includes the strategic communication and other types of communication for units deployed in mission spaces far from the homeland. Also communication within regions and between spots with local communication may be BLOS communication. One important example is *reach back* in international operations, where deployed national units must be able to communicate with the operational or strategic level back home. Logistics communication to the homeland is another similar example. A third

example is communication from a logistics centre (HQ) at a harbour to a number of C2 installations maybe several hundreds of kilometres from the harbour.

Regional communication is a borderline. Monitoring a larger area, where both solutions based on a collection of local communication assets and BLOS to a number of local assets may be possible solutions.

Military radio communication in the high frequency (HF) range, very high frequencies (VHF), ultra high frequencies (UHF) or in the micro and millimetre wave regions (EHF) has been used for many years. Even communication based on infrared light (IR) is applied. VHF, UHF, EHF and IR are BLOS when using relays (i.e. satellites, planes). Each frequency range has particular propagation properties. There is a need to take into account geographic, meteorological, and atmospheric conditions that may cause the propagation to behave unexpectedly. A sandstorm may destroy communication in microwave link systems, but allow UHF communication and even further troposcatter communication. In general: The higher the carrier frequency, the larger the potential bandwidth and hence transmission capacity.

The atmosphere and its ionised layers cannot be controlled, so it is important to have a number of frequency ranges to pick from to achieve the optimal solution in a given situation. BLOS communication is very often used for tasks where high availability is required, i.e. 24 hours in all months of the year, even in periods of high solar activity.

All this leads to four basic ways of radio transmission over the horizon:

- Use of HF radios (1.6- 30 MHz). This does not require access to satellites. The HF signal is reflected by the ionosphere.
- Use of satellite communications. Using a satellite radio implies a transmission to the satellite that retransmits the signal to the receiver. Hence there must be at least one satellite accessible for both sender and receiver. Requirements on the maximally allowable latency will have implications for the choice of satellite type.
- Use of earth or space bound relay stations. A relay station must be placed between the two stations that are beyond line of sight (BLOS). It is of course necessary that the relay station at all times can see the two communicating stations.
- Use of scattering of radio waves in the troposphere (troposcatter).

It is customary to add a BLOS capacity to mobile ad hoc networks, because of the built-in relay function in the nodes of the ad hoc network. Mobile ad hoc networks are self-organising, and they do not depend on a central base station or an established infrastructure. Each node in an ad hoc network is a possible information source, a relay station and a destination. This multi hop functionality makes communication between nodes that are outside their own radio coverage possible. By connection of ad hoc networks to e.g. a fixed infrastructure, it is possible to achieve a regional coverage, even a global coverage.

5.5 Naming and Addressing

A substantial aspect in development, maintenance and extension of media and large scale networks is in the design of network names and addressing plans. Although this is not a significant factor in the overall network design, a poorly designed address structure can degrade the network performance and limit the scalability.

A well documented and scalable networks address plan is fundamental for an optimal implementation and operation of an information infrastructure, which can be supported globally.

It is crucial in the addressing plans to compare the logical, physical and organisational structure of an organisation with the purpose of obtaining an optimal usage of the networked infrastructure.

Scalable network addressing is often insignificant or even trivial in small or medium sized networks; however, as the network increases in size, it will quickly reach the limit of its natural maximum scalability, which will result in a costly redesign of the address plans. Scalable address plans can guarantee a smoother expansion of the network, and a good network design can optimize the bandwidth using a hierarchical address structure combined with optimal routing protocols.

Addressing and communication structures must be transparent against a global addressing concept, i.e. that communicating C2 systems do not have the responsibility to maintain routing tables or name server facilities for other C2 systems. Each C2 system must inform other C2 systems of names and addresses of its own recipients.

There is a tendency towards *mobile networking* and especially *Mobile Ad Hoc NETWORKING* (MANET). A static addressing model will not be sufficient for this, so a dynamic configuration must take place, when:

- One or more MANETs, which used to be independent, collide.
- A MANET is connected to a static infrastructure.
- A new node in the network is assigned a unique address.

In larger networks, there is a demand for white and yellow pages (directory services). With the increasing demand for scalability of networks and with the emergence of tools such as firewalls and dynamic dial-in VPNs, etc, there is an increasing demand for configuration and management of politics for properties such as authentication, authorization, Quality of service (QoS), configuration and bandwidth. The enormous amounts of data will increasingly be exposed and coordinated through directory services and protocols. In service-oriented architectures such functionality will be taken over by brokers.

The development goes towards separating address plans and protocols. There is in principle no reason for using only a single protocol for lookup service. E.g. the Domain Name System (DNS) can be an initial implementation of a hierarchical directory service, which is not incompatible with the long time goal of utilizing other networking protocols. Transition between systems can be established with ease, just as parallel systems which use the same data can be established. The drawback of redundant directory services is that the task of keeping data consistent will increase.

In order to enable NBO there is a requirement that all connected units can be addressed. This requires a global addressing scheme, and that the network and its protocols support routing. Since some of the terminals connected to the network participate on an ad hoc basis, it is required that these terminals are reachable. Management of large networks is still a difficult problem, but a meticulous choice of routers, routing protocols and gateways can contribute to a solution. To make life easier for the users it is necessary to have a global, scalable and dynamic directory system for mapping between names and network addresses. Since the armed forces will have multiple collaboration partners, it is important that the proposed communication solution should live up to prevailing standards for addressing, routing and directory services.

5.6 Real Time and Other Quality of Service Issues

The requirement on real time communication is related to the actuality of the information, since there is a direct coupling to the timeliness of the information.

There will always be a delay in communication. The delay covers a span from a few nano-seconds to hours and possible days. The requirement on real time communication is to control this delay, both with regard to the actual delay and in the jitter of the delay.

The delay and jitter consist mainly of the following elements:

- The preparation of the information for transmission, incl. coding, encryption, packing, adding header information, and handling of the transmission queue.
- The access to the communication media (e.g. the channel or network). Possibly establishment of a session is also included.
- The transmission time, - which also is affected by a potential sharing of the transmission media.
- Receipt of the information after transmission, incl. decoding, decryption and unpacking. In principle this is analogous with the preparation of the transmission.

All these elements must be controllable. Other elements might also delay the transmission, such as acknowledgements or re-transmission caused by bad connections or congested networks.

There is a distinction between soft- and hard real time requirements. Hard real time requirements exist if a system fails because the information arrives too early or too late. An example of this is systems, which must receive target information in order to engage a target. Soft real time requirements exist, if systems which receive the information too late have a reduced efficiency or put an unnecessary strain on the users. Quite a few systems used for creation of a common operating picture have such soft real time requirements.

It must be possible to establish connections, which accommodate hard real time requirements. Although a connection is deterministic time-wise i.e. it guaranties that the communications take place within a predefined time span, it is not synonymous with living up to the hard real time requirements. From the reverse perspective, it is possible for a non-deterministic connection in practice to live up to hard real time requirements.

In NBO where the communication must be facilitated by the network, the fulfilment of many requirements will be part of the *Quality of Service (QoS)* of the network. When it comes to real time requirements, QoS will directly include requirements for guaranteed or an average bit velocity, as well as delay and jitter. These requirements depend on a vast number of other properties of the network, QoS will therefore also deal with properties as a limitation in the loss of packages and thereby re-transmission, control of priorities of classes of traffic, time limitation for recovery or disrupted connections, and other forms of error handling.

The access to the communication media is guided by the method and interfaces for regulation of access to the media, the method of delivery of the media, and of the load, i.e. how many systems (stations) which are active and want to transmit. The access can be centrally regulated, e.g. by using polling as in link 11, or controlled decentrally as in link 16 with time division. The access can also be unregulated and therefore controlled decentrally as in contention net, exemplified by WLAN (as defined in the 802.11 standards). In such networks the delay is in principle stochastic, while link 16 can guarantee delivery of information within a certain time span (i.e. it is deterministic) - link 16 is a real time system.

Sharing of the transmission media can in principle take place in the time or frequency domain. This leads to techniques such as TDMA (time division multiple access) and FDMA (frequency division multiple access). The concept of multiplexing is often used synonymously with the concept of multiple accesses. The more advanced method Code Division Multiple Access (CDMA) can here be seen as a generalization of the previously mentioned two fundamental methods.

Therefore one can see a clear connection between real time requirements and the selected communication technology. A number of the most widespread types of networks and their protocols (e.g. the TCP/IP suite) are not designed for real time communication, while some of the tactical data links have particularly good real time properties.

5.7 Network Management

It is a requirement that all communication systems and infrastructures can be monitored and controlled based on operational and technical requirements. This requires Network Management (NM), which can partly inform on and visualize the network and partly be used to govern and control the usage of the network. It includes handling of network errors, all forms of configuration including updates, performance analysis, governance of the real time communication and prioritization of the communication, and handling of security governance. NM should be possible at all levels, from the physical level, logical network level including protocols, and at service and application level.

NM is especially important in an NBO context, because the efficiency of the communication is an absolute prerequisite for NBO. There is no doubt that NM in this network of networks setting will have a crucial significance for the communication and information systems. It will be decisive that the operational requirements for guidance of the communication can be converted into technical NM.

NM has technically a specific meaning, but there might be a requirement for other systems, that are related to the normal use of the network by the armed forces. An example from Cyber Defence is Intrusion Detection systems, which might be relevant from a security point of view with regard to a proper response in case of an intrusion.

5.8 Information Systems and Constraints

A recurrent theme (see [2], [4], [5], and [15]) is the wide scope of the operations. In addition you have the agility and flexibility issues. In [7] the problems of forming task groups or ad hoc groups that are gathered just for the solution of specific problems or taking part in just one or a few missions together are dealt with, and it is shown that the consequences of not having a long common history may be that the groups do not function optimally because of lack of trust. This leads to requirements for the information systems in the sense that they must be trustworthy. They should be easy to modify, easy to integrate in new ways, and easy to use by personnel with little training in their use and experienced as secure and safe. This leads to a requirement for using a familiar user interface, and to use to the widest possible extent COTS application and middleware. One obvious candidate is Internet technology and more specifically the Web technology as a common platform for most applications.

The security issues in the foreseen setting must be dealt with explicitly. In many cases, the non-military information systems are based on COTS products that are developed to capture as large a market segment as possible. This has led to products with emphasis on a multitude of functions, but not with simple and efficient security properties. There is a gradual increase in security awareness among the producers of COTS information systems [9], but this has not yet manifested itself in information systems that immediately fulfil military security requirements. The implications of this will be that it may still be necessary to constrain the use of such systems and their integration. The expectations of the users gained from their daily use of information systems technology at work or at home may therefore not be met. This may again lead to reduced or even lacking use of the information systems.

Legacy systems must be able to take part in NBO even before they are superannuated within a foreseeable future. This means that old applications may have to be given new interfaces and that they may have to be integrated via new protocol stacks and other middle-ware. The legacy systems may even force integration between systems to be less efficient than otherwise foreseen.

5.9 Loose Coupling and Late Binding – Service Oriented Architecture (SOA)

The basic components in the NBO infrastructure will be services that are produced by service providers, and service consumers or clients. It is important that the service consumers do not have to deal with the inner workings of the services. Further, it is imperative that different services can evolve at their own pace and that new improved versions do not enforce large changes in other services or in clients. It is therefore a requirement that the different components are loosely coupled. One way of obtaining this loose coupling is by transitioning to a Service Oriented Architecture.

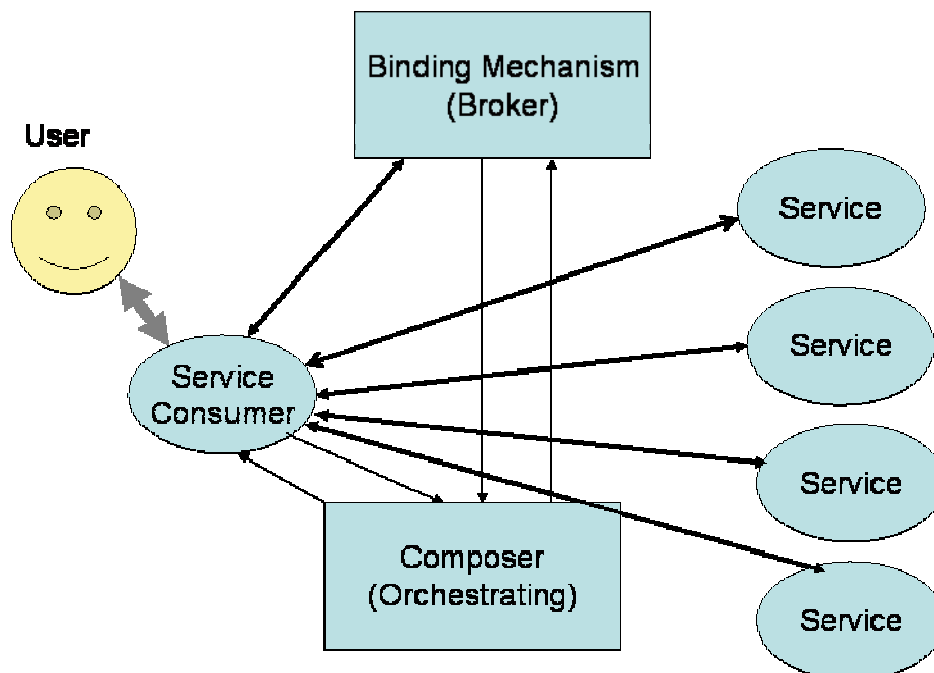


Figure 5-1: Late binding and creation of applications require a broker mechanism and orchestration

The requirement of agility in planning and executing missions [2] has the cost that it may not in advance be possible to know which applications (read: services) are most appropriate in a given context. The nature of the mission dictates the services to be used. It should therefore be possible to compose the applications nearly at execution time. The architecture must accommodate this late binding between service providers and service consumers [3].

The principle of loose coupling between the components in the total system is important. Loose coupling means that the components expose coarse grained interfaces to the network, and that as much lifetime control of software objects and processes as possible is done locally, at the node where they reside. Communication between components is as a principle done via messages, and wherever possible by asynchronous (non-blocking) message passing e.g. via queuing systems. The loose coupling reduces the overall complexity and allows the components to evolve at their own pace. A change in technology in one component does not affect the other component. SOA is one method for obtaining loose coupling.

Figure 5-1 shows that in a loosely coupled architecture with late binding between consumer and service, components like brokers and application composers are helpful. The broker knows which services are available, and the composer puts their invocations together. The service consumer uses the services in the way that the composer has decided.

The loose coupling may not be the best solution in all cases. If e.g. there are strict real time requirements, the overhead may be so large that they cannot be fulfilled. SOA will in principle make it possible for the end user to develop new applications composed of more basic services. Further, the development of new applications may itself be exposed as a service. Again, SOA gives high flexibility.

A related but somewhat different concept, cloud computing, is dealt with in WP3.

5.10 Cyberspace

Cyberspace is an important part of NBO. Defending cyberspace will be as important as defending physical space. A battle can be won or lost in cyberspace. The implications of cyber attacks may be far reaching and go from defacing attacks on official websites to non availability of vital assets and obstructions of disaster relief operations. This leads to demands for a high availability and robust communication network of networks. Such a *protected core* is an important national infrastructure asset with many other stakeholders than the Danish Armed Forces.

Computer Network Operations (CNO) has three components, namely defence, attack, and exploitation. The offensive parts, attack and exploitation, can be implemented with their own infrastructure and applications. They will thus not have specific requirements to the overall architecture of the defence ICT systems.

5.11 Other Requirements

In the previous sections, a number of mainly functional requirements and their influence on the technology have been discussed. These have been selected because they have a deci-

sive influence on the technical architecture of the ICT systems. However, there are many other needs that must be fulfilled in the technical architecture, both in the form of technological and not technical requirements. Most of these requirements are already mentioned directly or indirectly, but in the list below the most important of these requirements are briefly summarised:

- **Security, including military security.** The security field is closely related to information assurance. The whole area of cryptography and the necessary infrastructure to manage this are also part of this. The core network must be black (i.e. encrypted), meaning that users must have the possibility of encrypting classified information. Data link encryption in parts of the infrastructure to increase the security should not be ruled out.
- **Frequency management.** Frequency is becoming an increasingly scarce resource, and requirements from civil agencies are restricting the military use of frequencies for wireless communication. The problems of interference and congestion are part of this.
- **Code management.** Because of frequency scarcity, an increase in co-existence of different equipment in the same frequency bands is foreseen. This will force users to use codes and other schemes that are orthogonal. A consequence is that the code space must not be divided in a manner similar to the frequency space. The enforcement of code restrictions is much harder than enforcement of frequency restrictions.
- **Physical media, including antennas.** Electronic Compatibility Measures (ECM), robustness in case of atmospheric and environmentally adverse conditions, and influence on the radio propagation. Also signature control including stealth is a part of this.
- **Weight, size and robustness and the trade-off against mobility.**
- **Use of standards.** The architecture shall implement as many functions as possible based on open standards, in terms of protocols, underlying technologies and methodologies. It is important to facilitate and encourage reuse and commonality both at component and at systems level. The access to services must be independent of the network type and the inner workings of the service. In this context, the Internet Protocol (IP)-suite is of paramount importance. IP is not mentioned as a functional requirement, but considering the need for use of commercial technology (COTS) certainly forces the use of the IP to obtain interoperability and an acceptable price tag.
- **Education, training, user friendliness and other usability issues.**
- **Costs.**
- **Scalability.** The converged network infrastructure must be scalable in the sense that it must be a simple task to add new capacities, services, applications and users to the structure. In principle, this should be possible on demand. The same scalability requirement applies for removal of capacities, services, applications and users.
- **Location Transparency.** The physical placement of users and resources must be transparent to the consumers and the producers of services. Functions that used to be only accessible in headquarters are to be available overall and for all legitimate users. This does not preclude a central management.

- **Open Architecture and Innovation.** The use of an open architecture will facilitate cooperation or partnering between producing companies and the military users and acquisition people. The open architecture will encourage competition and prevent dependence on a single supplier. The use of proprietary and special military standards should be avoided. The architecture must itself be able to evolve and support the technological evolution.
- **Flexibility.** An open architecture means an increase in the number of suppliers of functionalities, and the development of the system of systems will be dictated more by the users than by the commercial and military market. The roll-out or deployment of new functionalities in the form of e.g. services will be faster and easier, both in terms of geographical coverage and in terms of number of users. The converged network structure will favour a consistent span of services independent of the underlying transport mechanism. This will make it possible to choose the most appropriate transmission channel in a given situation.
- **Network Management (NM)** The open and converged network architecture will make it possible to monitor and control the whole network of networks by one team in stead of having a number of independent and isolated groups taking care of networks and services. Because all resources are harboured on the same network, the exploitation of the resources can be efficient.
- **Quality of Service (QoS).** The converged network must be able to deliver a broad spectrum of QoS, which includes the support of time critical applications and isochronal services.
- **Reliability and Security (Availability).** The converged system of systems must have redundancy to maintain high availability of all critical resources. Examples of loss of availability could be jamming and satellite denied environment (ships at the poles).
- **Transmission Capacity.** The networked infrastructure must offer the necessary capacity and signal processing to accommodate both voice and video applications, and the supply of timely information where necessary.
- **Control of Electrical Power** - Parts of the communication system must apply technologies with low power consumption, including protocols that do not require frequent keep-alive signalling. This is particularly important for unmanned devices with a limited battery capacity (larger platforms usually bring their own power generator). Power supplies including battery technology and careful selection of protocols are parts of this.
- **Mobility.** Mobility comprises the independence from geographical location and the ability to be operational on the move. It must be possible to establish ad-hoc networks to accommodate this and thus obtain communication without having to rely on e.g. a fixed infrastructure.

- **Network Basis.** In all cases, the operations must be network based. The most important properties of the network centricity may be summarised as a movement from as-is to the desired out-come, to-be:

AS-IS (Today, Platform Oriented)	TO-BE (Network Based)
Platform based	Capability based
Point-to-Point	Net-centric
Stow-piped information and services	Shared information and services
Emphasis on systems and their functions	Emphasis on services

The movement towards Network Based Operations will have implications for all applications and for the architecture of both the communication systems and the information systems.

- **ICT civilian Development.** The general technological development is an underlying aspect of the technical target architecture. As mentioned above, this includes use of civil ICT systems and standards. However, some specific standards and technologies are of major interest for the technical target architecture. This includes:
 - The IP-suite - in particular the IPv6-suite.
 - SOA standards – in particular web-services.
 - SATCOM, Software Defined Radio (SDR) and other transmission technologies.
 - NBO security technology – in particular crypto devices and security gateways.
 - Human computer interaction (HCI).

This page is left intentionally blank

6 Discussion and Conclusions

In this report, the requirements on communications and information systems have been developed from three points of view:

- The general mission independent requirements, i.e. requirements that to some degree are always present in military communication and information processing.
- Mission dependent requirements derived from selected tasks and vignettes of WP1 and the derived capability requirements.
- A number of technological requirements and other constraints have been identified.

Few of the requirements are strongly related to the present situation, while most are future requirements, i.e. requirements to be fulfilled in the transformed military with its anticipated tasks. These requirements may not be completely fulfilled with the presently available technology, either because of economic constraints, or because the technology has not completely reached the adequate level of maturity.

It must be emphasised that the three points of views do not give a complete picture of the needs for communication and information processing in all three services nor in relation to the Total Defence enterprise. It is, however, deemed to be sufficient for the present objective: Establishing a target architecture framework that is able to take into account the foreseeable technological development. WP2 is thus just one input, but an important contribution, to WP3, where the technical part of DEFTA is described.

It must be noted that the concatenation of vignettes in the discussion of selected tasks has led to different types of communication and information processing. It is therefore not assumed that the derived requirements should be fulfilled by just one type of system, or by the activities of one organisational level.

A number of conclusions can be drawn from the analyses of this work:

- The physical and logical reach of the information will be decisive for the design of communication infrastructure. The ability to exchange information with many different collaboration partners is important at all levels. Particularly regional BLOS communication is important.
- In two of the vignettes the information actuality (even real time) is particularly important, but time criticality is always present.
- The availability of services (including communications) will play an important part for the architecture, and forces redundancy to be built in.
- The task and its nature are not very stable, and in many cases it must be possible to improvise.
- Operating in cyberspace will increase in importance.

These requirements must be seen in relation to the overall assumption that all operations should be network based, and that agility in executing operations must be supported.

Several other attributes may often have to be adapted to the actual circumstances. As an example, the requirements for richness and precision may be compromised if the transmission capacity is limited.

The support for agility in command and control is a requirement. This will inevitably lead to the use of adaptive or adaptable technologies such as ad hoc networks, cognitive radios, mobile code, and service-oriented architectures. These systemic aspects have been considered and lead to a mixture of absolute and desirable requirements. It is to be expected that many of the discretionary requirements will be absolute, mandatory, within the time span of

10 to 15 years. It is therefore a requirement that the technical part of DEFTA supports these requirements to the highest extent possible.

The demands for rich and accurate information with many stakeholders show an apparently never ending increase. The basic properties of information show that storage capacity and processing power to some extent can relieve the demands for high capacity communication. Whether these facilities shall be local to the unit or the single soldier or dispersed in the cloud of networks and computers remain to be seen. The implications for the technical part of DEFTA are far reaching.

Finally, the importance of non-functional requirements on the ICT systems should be noted. Requirements such as flexibility, scalability, using open standards, using open architectures, military security and the use of civilian ICT must be taken into account when the technical architecture is developed. Behind all these requirements is also the need for cost effective solutions, - including costs for acquisition, maintenance, configuration, education, and training.

References

- [1] DEFTA, Strategic Vision and Concept for NBO, WP0, Danish Defence Target Architecture (DEFTA), November 2010.
- [2] DEFTA, Operational Tasks and Vignettes, WP1, Danish Defence Target Architecture (DEFTA), November 2010.
- [3] David S. Alberts, John J. Garstka and Frederick P. Stein: Network Centric Warfare, 2nd edition, CCRP 1999.
- [4] NATO Network Enabled Capability (NNEC) Study vol. 2, NC3A JUL 2005. 4.a
- [5] NATO Network Enabled Capability (NNEC) Study vol. 1, NC3A JUL 2005. 4.b
- [6] Koordinationsgruppen vedr. Netværksbaserede Operationer, Indledende Rapport, FAK 21 DEC 2004. (Danish)
- [7] Ni Noter om Netværksbaseret Forsvar, Forsvarets Högskola 2005.
- [8] Anthony W. Isenor: A Brief Assessment of LC2IEDM, MIST and Web Services for use in Naval Tactical Data Management, DRDC Atlantic TM 2004-148, 1 JUN 2004.
- [9] Hvidbog om IT arkitektur (Whitebook on IT Architectures), Ministeriet for Videnskab, Teknologi og Udvikling 2004. (Danish)
- [10] Netværksbaserede Operationer i Flyvevåbnet, AG/NBO/FLV, OCT 2004. (In Danish)
- [11] Udkast til Hærens strategi for netværksbaserede operationer, HOK, AG/NBO/HRN SEP 2004. (Danish)
- [12] David S. Alberts, John J. Garstka, Richard E. Hayes, and David A. Signori: Understanding Information Age Warfare, CCRP August 2001, Chapter 3-5.
- [13] Koordinationsgruppen vedr. Netværksbaserede Operationer, Opfølgende rapport, 14 OKT 2005.
- [14] David S. Alberts and Richard E. Hayes: Power to the edge, CCRP June 2001, Chapter 5.
- [15] Rapport fra Arbejdsgruppen vedrørende Netværksbaserede Operationer i Totalforsvaret, udkast juni 2005. (Danish)
- [16] Danish Defence Global Engagement, Report by the Danish Defence Commission of 2008 (DCR08)
- [17] Danish Defence Agreement 2010-2014 (DDA14)
- [18] JSP 747 Information Management Policy v1.1, 2009-12-15

- [19] Shannon, C. E.: A Mathematical theory of communication, Bell Sys. Tech. J. 27. 379-423, 1948.
- [20] Kolmogorov, A. N: Combinatorial foundations of information theory and the calculus of probabilities, Russian Math. Surveys 38(4), 29-40, 1983.

Acronyms

3D	Three Dimensional
ADatPn	Allied Data Publication number n
AG	Arbejdsgruppe (Danish for Working group)
AMN	Afghan Mission Network
AV	All View [from NAF]
B	Byte
BLOS	Beyond Line Of Sight
BTN	Battalion
C2	Command & Control
C2IS	Command & Control Information System
CAN	Canada
CCRP	Command and Control Research Program
CDMA	Code Division Multiple Access
CEP	Circular Error Probable
CHODDEN	Chief of Defence of Denmark
CNR	Combat Net Radio
COIN	Counter Insurgency
COP	Common Operational Picture
COTS	Commercial, off-the-shelf
CV	Capability View [from NAF]
CWS	Control and Warning System
DALO	Danish Defence Acquisition and Logistic Organization
DCD	Defence Command of Denmark [in Danish: Forsvarskommandoen]
DCR08	Defence Commissions Report (2010-2025)
DDA14	Danish Defence Agreement (2010-2014)
DDRE	Danish Defence Research Establishment
DEFCOMM	Defence Communication
DEFOSA	Danish Defence Overarching System Architecture
DEFTA	Danish Defence Target Architecture
DEMA	Danish Emergency Management Agency [in Danish: Beredskabsstyrelsen]
DeMars	Danish Defence Management and Resource System
DK-Cert	Danish Computer Emergency Response Team
DMI	Danish Meteorological Institute
DNK	Denmark
DNS	Domain Name System
DoD	Department of Defense
DRDC	Defence Research and Development Canada
E2E	End-To-End
ECM	Electronic Compatibility Measures
EHF	Extremely High Frequency
FAK	Forsvarsakademiet (Danish for Royal Danish Defence College)
FDMA	Frequency Division Multiple Access
FLV	Flyvevåbnet (Danish for Air Force)
FOFT	Forsvarets Forskningstjeneste (Danish for Danish Defence Research Establishment)
GOV-Cert	Government Computer Emergency Response Team
GPS	Global Positioning System
HCI	Human Computer Interaction
HF	High Frequency
HF	High Frequency
HKOM	Hærens Kommunikation (Communication in the Army)
HQ	Headquarter

HRN	Hæren (Danish for Army)
ICT	Information and Communication Technology
ID	Identity
IER	Information Exchange Requirements
IM	Information Management
INS	Inertial navigation Systems
IP	Internet Protocol
IPv4	IP version 4
IPv6	IP version 6
IR	InfraRed
IT	Information Technology
JC3IEDM	Joint C3 Information Exchange Data Model
JSP	Joint Service Publication
LAN	Local Area Network
LC2IEDM	Land C2 Information Exchange Data Model
LOS	Line Of Sight
MANET	Mobile Ad-hoc wireless NETWORKS
MB	Mega Byte
MIL-Cert	Military Computer Emergency Response Team
MIP	Multilateral Interoperability Programme
MIST	Maritime Information Sharing Technology
MoD	Ministry of Defence
MPA	Maritime Patrol Aircraft
MPLS	Multi Protocol Label Switching
NAF	NATO Architectural Framework
NATO	North Atlantic Treaty Organization
NBO	Network Based Operations
NC3A	NATO Consultation, Command and Control Agency
NCOW	Net-Centric Operations and Warfare
NGO	Non-Government Organisation
NM	Network Management
NNEC	NATO Network Enabled Capability
OV	Operational View [from NAF]
PAN	Personal Area Network
PDA	Personal Digital Assistant
PET	Politiets Efterretningstjeneste [Danish for Danish Security and Intelligence Service]
PKI	Public Key Infrastructure
PV	Programme View [from NAF]
QoS	Quality of Service
RDDC	Royal Danish Defence College
RF	Radio Frequency
RPV	Remotely Piloted Vehicle
SATCOM	Satellite Communication
SDR	Software Defined Radio
SHF	Super High Frequency
SOA	Service Oriented Architecture
SOF	Special operation Forces
SOV	Service Oriented View [from NAF]
SSS	Staff Support System
SV	System View [from NAF]
TACOMS	Tactical Communication
TBCE	Type B Cost Estimate
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TM	Technical Memorandum

TV	Technical View [from NAF]
UAV	Unmanned Air Vehicle
UHF	Ultra High Frequency
UK	United Kingdom
UK	United Kingdom
VHF	Very High Frequency
VIP	Very Important Person
VPN	Virtual Private Network
WAN	Wide Area Network
WAS	Wide Area Subsystem
WEAO	Western European Armaments Organisation
WLAN	Wireless LAN
WPn	Work Package n
XML	eXtensible Mark-up Language

This page is left intentionally blank

Appendix A Definition of Terms and Terminology

In this appendix, we briefly for the sake of completeness define a number of terms that are widely used throughout the report.

Communications means exchange of information. *Communications* is broadly used in connection with all systems that are involved in exchange of information. Consequently, it comprises among other things the transmission medium, access to the medium, waveforms, protocols, cryptography, network management, as well as related processes and applications.

Communication security is a common term for all security controls that assures availability, confidentiality, and integrity of the exchanged information. *Communication security* includes *transmission security*, crypto security and physical security.

End-to-End (E2E) communication is the exchange of information all the way from source to destination. The destination or source (sender) may be a process, a terminal, a microphone, a PDA, a human being etc.

Information Assurance is an information characteristic that means that you can trust the information, among other, because the information security is in place. Information assurance thus includes information availability, integrity, non-repudiation, and information confidentiality.

An **Information Attribute** is used to describe property of information. High level examples of *Information Attributes* are Richness, Reach, Actuality, Assurance, Intrinsic quality, Completeness, and Cohesion. See Chapter and Table 2-1 for details.

Information Attribute Value defines the value of the *Information Attribute*. In DEFTA a scale from 0 to 5 and a textual value is used. The scales and textual values may differ in other contexts.

Information Attribute Requirement is shown by specifying the actual *Information Attribute Value* of the *Information Attribute* for a given task, scenario or vignette.

Information System Attribute is used to describe requirements for information systems. Examples of Information System Attributes are Information Type, Real-time, Interoperability, Network based, Civilian infrastructure, and Level. See Chapter 4 for details.

Information System Attribute Value defines the value of the *Information System Attribute*. E.g. the Information Type attribute may have values like tracking data, voice, video, or images. See Chapter 4 for other value examples.

Information Management (IM) may be defined as methods, practices and tools for making sure that the right information is available to the right entities with the right quality. It thus comprises collection, storing, retrieval and dissemination of information. In the times where most information was written in books or in papers, IM was very much considered a librarian task. The advent of digital information has broadened both the scope and the tools of IM.

Information Quality is about the information being available, relevant, accurate, precise, timely, complete, secure, and directed.

Information Requirement is an operational requirement for information, e.g. COP, RT Air Picture, Maps of a region, or Meteorological Data.

Target architecture is a version of architecture that forms a goal to be reached. The target architecture is an ideal form of architecture, and as such not very detailed. It will be based on general principles and requirements for the ICT systems. The target architecture is described via a number of *architectural views*, where a view considers one logical aspect of the architecture. It must be stressed, that the term *target architecture* is not identical to the similar NATO term, which describes a detailed, project related system implementation target (Type B cost estimate (TBCE)). The target architecture described in this document has a stronger resemblance with the NATO concept *overarching architecture*. Target architecture is evolvable by nature, since it is a model of a desired system, and does not designate any specific products. Target architecture must therefore be capable of adapting to changes in technology and capability requirements, and must as such be regularly updated.

The **Total Defence** concept (in Danish: Totalforsvaret) is a term that is used for the cooperative organisation of the military forces, the emergency services including police, fire fighting, and ambulances to deal with national (and international) crises or catastrophes. It is thus akin to the US term Homeland Security.

Transmission is the part of the communication that refers to the physical medium and access to the medium. This includes some basic network software such as parts of a protocol.

By **Transmission Security** all security means to protect the transmission against being compromised are meant, but excluding cryptographic means.

Vignette Parameter is a *communications* related parameter describing characteristics of the vignette. Examples of *Vignette Parameters* are Area, Mobility, Collaboration partners, or Time. See Chapter 4 for other examples.

Vignette Attribute is the same as *Vignette Parameter*.

Vignette Attribute Value defines the value of the *Vignette Attribute*. An example is the Area attribute having typical values of Friendly, Hostile, or Adverse environment conditions. See Chapter 4 for other examples.

Appendix B Information Theory

This appendix contains a definition of information and gives an introductory survey of the concept. It is slightly technical and may be surpassed in a first reading.

The crucial role of information means that an understanding of the concept is important for some sections of the report. Claude Shannon is the founder of modern information theory. This appendix gives therefore a brief discussion of the concept of information, and introduces a definition. The definition is in accordance with the Shannon concept [19] but reconciled with Kolmogorov's algorithmic complexity [20].

Information in the form of a message is generated at a source and sent to a receiver through a transmission channel. The transmission channel may compromise the message by introducing noise or a deliberate change of the content and hence compromise the integrity of the message. Shannon's model of a communication system is shown in Figure B-1.

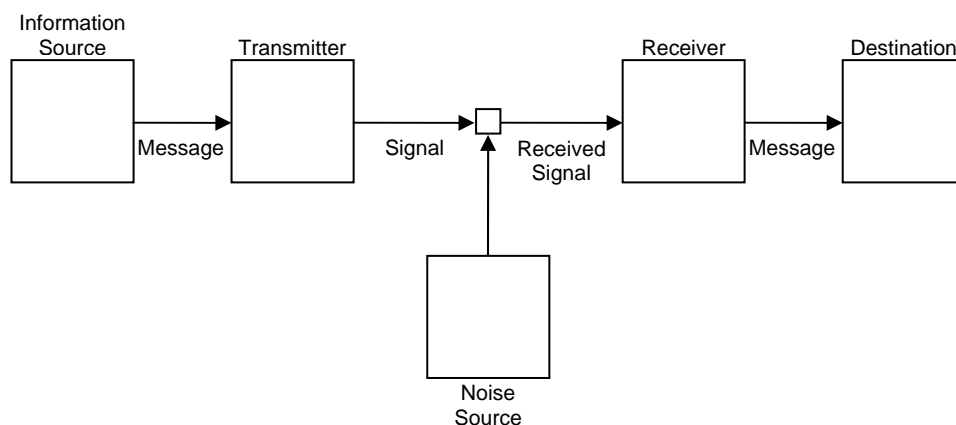


Figure B-1: Schematic diagram of a general communication system

In WP2, we define information as the data which lead to a decrease in the uncertainty of an event or an object, at the receiver. Data is simply defined as a stable representation of one or more facts, be they events or objects. Both data and information are measured in bits. Eight bits are defined as one byte (1 B). A consequence of the definition is that information is linked to events (facts, objects) in the real world, and that information is dependent on the apriori knowledge of these events. Shannon gives a probability theoretic definition of information in the form of entropy, which relates information to the information source (sender) and the relative frequency of the symbols that it sends.

An alternative approach to the concept of information is from the complexity of the object to be described. More complex objects demand more information for their description. Kolmogorov's algorithmic complexity [20] defines the information content of an object as the length of the smallest algorithm that is able to generate the object. The object in this case is an encoding of real world objects. As an example, consider a 6 digit printed table of the sine function. This table contains a lot of data, maybe as much as 10 MB. An efficient algorithm, i.e. a computer program that may generate all these data will have a length of less than 0.01 MB. If the object is a completely random sequence of bits, the Kolmogorov complexity (algorithmic information) will be approximately of the same length as the sequence, in good accordance with the Shannon measure of information. The definition of information that we apply in this work is a synthesis of the ideas of both Shannon and Kolmogorov.

Our definition of information includes a utility aspect because data that do not diminish uncertainty about an event or an object at the receiver end do not contain information. This of course means that information includes a dependency of the context of the receiver.

It must be noted that the above definition of information does not take into account the real meaning of the information and the actual use of information. The semantics and pragmatics are not considered, beyond the fact that information must tell something new to the receiver. The pragmatic and semantic aspects are taken into account in the following sections of this work package, where the relevant information attributes or characteristics are discussed.

An important consequence of the properties of information is that the need for transmission capacity may be decreased by increasing the a priori knowledge at the receiver. This may be effectuated by having stored information and large information processing capacity at the receiver's end, but also by having highly trained personnel.