



DEFTA

Strategic Vision and Concept for NBO

WP0

Danish Defence Target Architecture (DEFTA)

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 0 (WP0). The objective of WP0 is to formulate the connections between the general policies and strategy work. This report contains the initial analysis of the national strategic vision and concept for Network Based Operations (NBO) and the general perception of the developments in this area.

This page is left intentionally blank

Summary

This report contains the initial analysis of the national strategic vision and concept for Network Based Operations (NBO) as 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 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 WP0 is to formulate the connections between the general policies, strategy work, ICT development and DEFTA. It contains the initial analysis of the national strategic vision and concept for NBO and the general perception of the developments in this area. The results of WP0 will be applied to the WP1, which defines the Operational Scenarios for the Danish Armed Forces.

The connections between Danish Defence Vision and Mission, Corporate Strategic goals and the underlying Strategies are shown in Figure 0-1. The ICT strategy is the central element, with the Target Architecture as a primary supporting document.

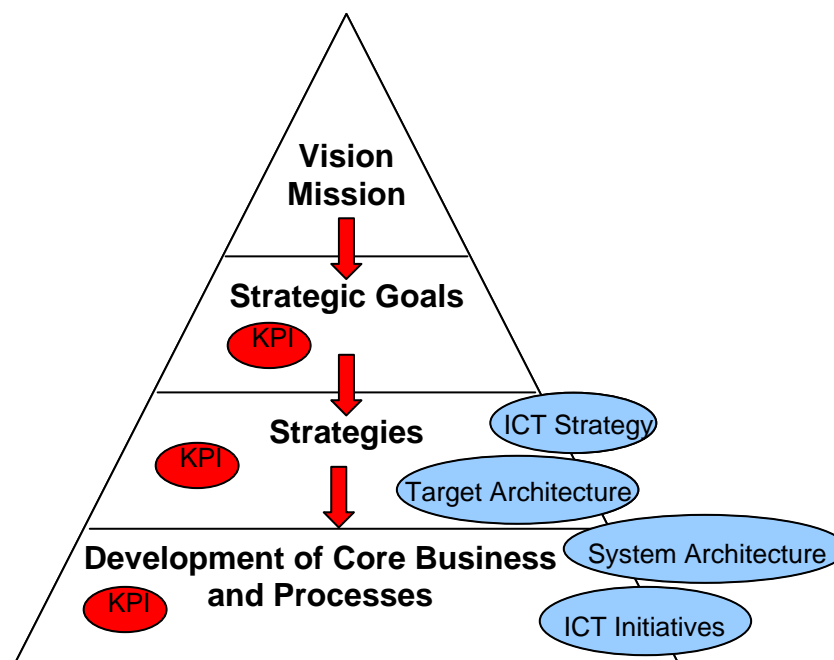


Figure 0-1: Strategy pyramid

To make sure that ICT solutions give value to the core business, ICT initiatives should only be initiated in support of the corporate Vision, Mission and Strategies.

The content of the Defence Commission Report (DCR08) and the Defence Agreement (DDA14) is the basis for focusing on the cornerstones of Danish security and defence policy, national level of ambition, tasks for the armed forces and their future operational environments and the requirements for a robust force.

DCR08 stresses the need for NBO in the Danish defence and the ability to interoperate with allies and coalition partners, and therefore appropriate technical interoperability. It points out that NBO prospectively will have significant impact on the defence structure and activities. It mentions improved command and control systems, with the aim to enhance the operational capabilities ability to participate in international operations with coalition partners.

According to DDA14, Danish Armed Forces must be able to perform a wide variety of tasks and must remain able to participate in difficult and intensive operations, including the continued contribution to the Danish engagement in Afghanistan in the coming years in accordance with Denmark's Afghanistan Strategy. However, the Danish Armed Forces must also preserve and develop the ability to execute other types of stabilisation tasks and international policing operations, including such mission types as the KFOR mission in Kosovo and the operations against piracy off the Horn of Africa.

With reference to DCR08 the support to the operational units will be based on a network-based approach, where each single acquisition is coordinated in order to create networks-of-networks and systems-of-systems.

In conclusion, the statements in DCR08 and DDA14 should be used as the basis for development of operational scenarios in WP1.

The main principle behind Danish Defence approach to NBO is that the development of the ability to operate in networked environments must be pragmatic and realistic. Danish Defence has therefore chosen to follow and influence the NNEC developments within NATO and will follow the trends among our strategic partners, rather than implementing own costly prototypes. The focus is on national activities since the last report (2005), the general status of NNEC in NATO, and the latest developments in USA and GBR. The national NBO-developments and the development in NATO are closely connected. The ability to interoperate with allies and coalition partners is of outmost importance, and therefore appropriate technical interoperability is required. Interoperability through NATO has been chosen as a way to achieve this goal, and national focus will be on development of common joint systems instead of dedicated systems.

The Networking and Information Infrastructure (NII) is the collection of NATO and national information infrastructure and communications infrastructure capabilities. The NII implements standardised information services including information transport, storage, security, management and other enabling capabilities to technically support NNEC.

There is a need for closer development of systems-of-systems, where the Danish national systems must be able to connect seamlessly to other systems, national as well as international. Joint and combined development is therefore required.

Table of Contents

Abstract.....	iii
Summary.....	v
Table of Contents.....	vii
List of Figures.....	ix
1 Introduction.....	1
1.1 Overview of DEFTA.....	1
1.2 Objective and Scope of DEFTA/WP0.....	3
1.3 Structure of DEFTA/WP0 Report and DEFTA.....	4
2 Assumptions on ICT Strategy and DEFTA.....	7
2.1 Business Value.....	7
2.1.1 ICT Vision.....	8
2.1.2 ICT Strategy.....	8
2.1.3 ICT Target Architecture.....	8
2.1.4 ICT System Architecture.....	9
2.1.5 ICT initiatives.....	9
2.2 Summary.....	9
3 Defence Commission Report & Defence Agreement.....	11
3.1 Defence Commission Report.....	11
3.2 Defence Agreement 2010-2014.....	11
3.2.1 Cornerstone of Danish Security and Defence Policy.....	12
3.2.2 Level of Ambition.....	12
3.2.3 Tasks.....	13
3.2.4 Future Operational Environment.....	14
3.2.5 Requirements for Robust Forces.....	14
3.3 Summary.....	14
4 Status of NBO.....	17
4.1 National NBO Development.....	17
4.1.1 Concept for the development of ability to operate in NBO environment.....	18
4.1.2 Concept for the Operational Development.....	18
4.2 NATO.....	19
4.2.1 NATO Requirements to NEC.....	19
4.2.2 The NATO Bi-SC Strategic Vision.....	20
4.2.3 NATO Political Guidance.....	21
4.3 Strategic Partners.....	22
4.3.1 NEC Strategy in GBR.....	22
4.3.2 NCW Strategy in USA.....	23
4.4 Summary.....	23
5 Discussion and Conclusions.....	25
References.....	27
Acronyms.....	29

This page is left intentionally blank

List of Figures

Figure 0-1: Strategy pyramid.....	v
Figure 1-1: Overview of DEFTA work process and the WP contributions to NAF views.....	3
Figure 1-2: NNEC Services Framework.....	4
Figure 2-1: Strategy pyramid.....	7
Figure 2-2: Connections to and from DEFTA.....	10
Figure 4-1: Approach, Co-evolution of Functional Areas.....	17
Figure 4-2: The NNEC Value Chain, as developed in the USA by OSD/OFT.....	20
Figure 4-3: NNEC Feasibility Study development model.....	21

This page is left intentionally blank

1 Introduction

The purpose of this report is to describe the strategic ICT vision and concept leading towards network based operations (NBO) as part of Danish Defence Target Architecture (DEFTA). The report is the result of work package 0 (WP0) of the DEFTA work.

The target audience of WP0 is mainly enterprise architects responsible for the NBO visions in architecture development and other architectural stakeholders with strategic and conceptual interests. The summary is targeted to decision makers at high level.

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.
- 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.

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.

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).

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

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).

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.

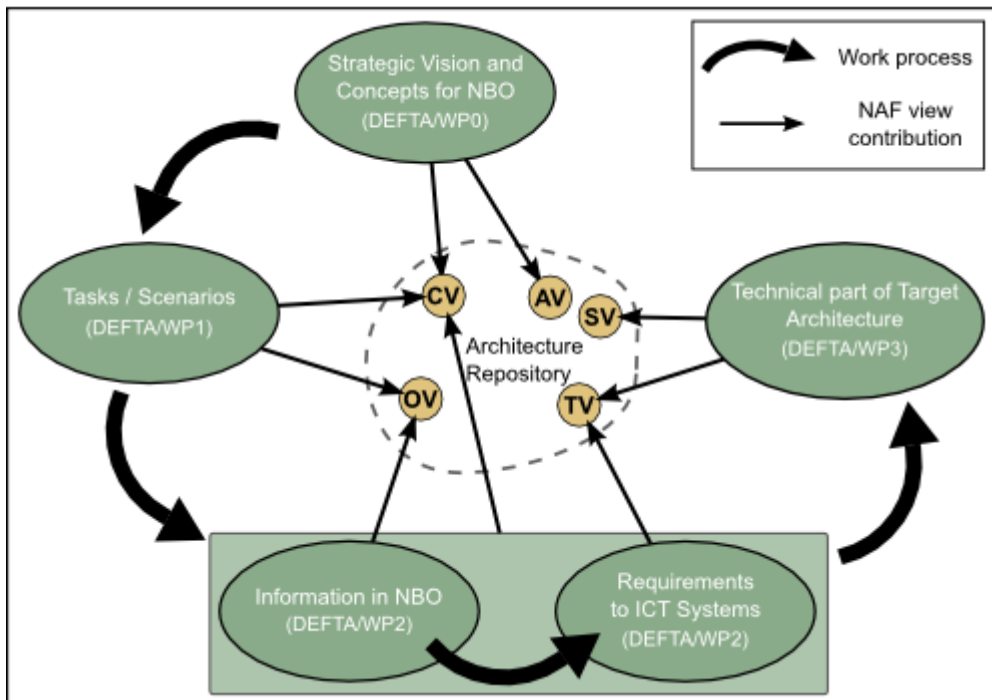


Figure 1-1: Overview of DEFTA work process and the WP contributions to NAF views

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).

1.2 Objective and Scope of DEFTA/WP0

The objective of WP0 is to formulate the connections between the general policies, strategy work, ICT development, and DEFTA. It contains the initial analysis of the national strategic vision and

⁵ The first version - denoted DEF COMM - is from 2005 and consisted of three reports denoted WP1, WP2, and WP3. In 2007, DEF COMM 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.

concept for NBO and the general perception of the developments in this area. The results of the work will be applied to the WP1, which defines the Operational Scenarios for the Danish Defence.

DEFTA not only describes the vision for the ICT-systems in Danish Defence, but also principles and standards to be followed by future acquisitions of ICT capabilities in Danish Defence.

DEFTA has been closely linked to the work within NATO Networked Enabled Capabilities (NNEC), NATO Overarching Architecture, and the developments of NNEC Services Framework.

By emphasising capability-based defence planning and focusing on interoperability, this report provides guidance for the development and implementation of the robust ICT capabilities needed to meet the operational and administrative challenges.

1.3 Structure of DEFTA/WP0 Report and DEFTA

This first chapter of WP0 contains the general background, scope and objectives of WP0.

The second chapter of WP0 is a general discussion on how to map this DEFTA work up to the overall Vision, Mission and Strategies, and a model is presented.

The third chapter of WP0 describes the content of the Defence Commission Report (DCR08) [8] & Defence Agreement (DDA14) [9], focusing on cornerstones of Danish security and defence policy, national level of ambition, tasks for the armed forces and their future operational environments and the requirements for a robust force.

The fourth chapter of WP0 gives a short view of the developments in the area of NBO. Focus in this chapter will be on activities in the national arena since the last report (2005) and general status of NNEC in NATO, and the latest developments in USA and GBR.

The fifth chapter of WP0 contains a conclusion and general guidelines based on the analysis from the other chapters. A number of recommendations for further work are included.

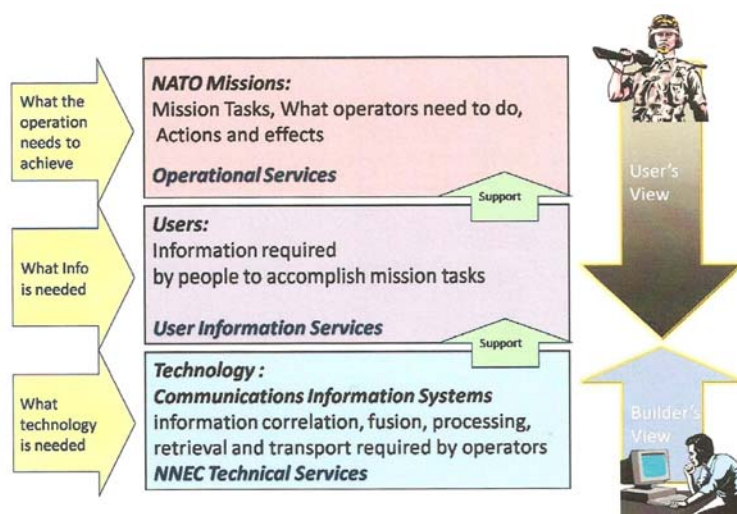


Figure 1-2: NNEC Services Framework

The NNEC Service Framework – as shown in Figure 1.2 – gives another view on how DEFTA is structured. NATO Missions relate to WP1 with “Operational Tasks and Vignettes”. Users related to WP2 with “Information in Network Based Operations”. Technology relates to WP3 with “Technical Architecture for ICT systems in Danish Defence”.

This page is left intentionally blank

2 Assumptions on ICT Strategy and DEFTA

This chapter describes the assumptions on how DEFTA should be related to the strategic goals for ICT involvement and utilisation in Defence. The description is not necessarily a picture of the present situation; however, it describes the relations between facts, prerequisites, business, and ICT solutions, and how this provides value to the core business.

2.1 Business Value

ICT initiatives should only be initiated in support of the corporate vision, which is formed of a wish to increase the value creation of the corporation. Increase of the business value in a commercial company can typically be simplified into: to make more profit and continue to make more profit. In public companies the directors will have to state what creation of value for their company is defined as. In a defence organisation increased value can be manifested in less loss of own troops, less collateral damage, more effect with the same force etc. On the internal lines it could be subjects related to management such as economic controlling, spare parts management etc. Figure 2-1 gives an overview of the chain of the strategy pyramid.

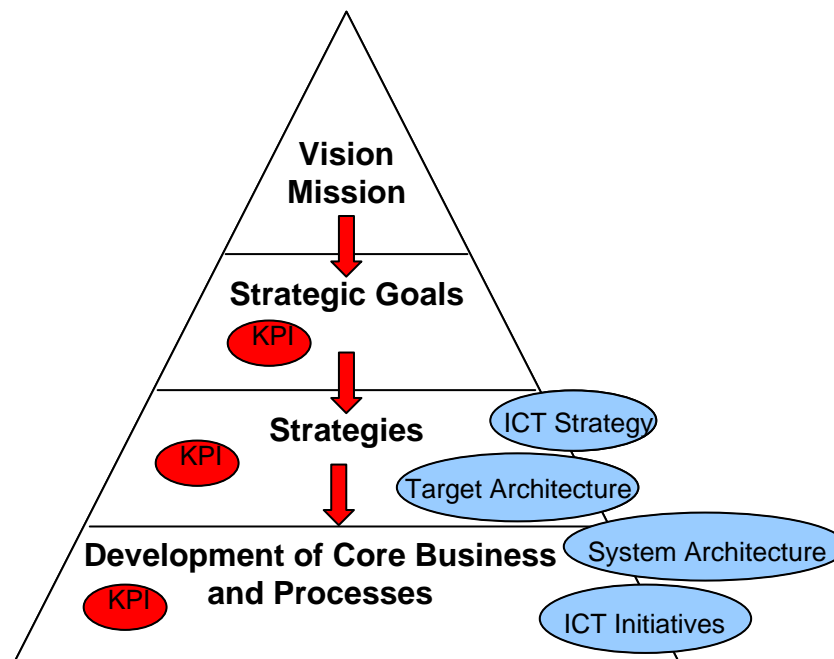


Figure 2-1: Strategy pyramid

The vision for a company should be based on how much the company should increase its value creation. The overall value creation of the Danish Defence is to 1) prevent conflicts and war, 2) upholding the sovereignty of Denmark and securing continued existence and integrity of the country and 3) furthering peaceful development in the world with due respect for human rights. The increasing of values must be expressed in strategic goals by key performance indicators (KPI) and

then broken down in strategies further down in the development of the Core Business⁷ and the Processes with related KPIs. KPI's will be the tool to measure to what degree the value creation of any initiative supports the strategic goals. ICT initiatives must as well support the increase of values directly and indirectly. If not, the initiative is not formed correctly or the values (expressed in KPIs) are not broken down into an adequate level of detail. In ICT initiatives, this will normally mean that the required change in core business and processes has not been sufficiently identified and documented.

The ICT Strategy, this target Architecture and underlying system architectures and ICT initiatives, including ICT projects must support the value creation. Details are found in the sections below.

2.1.1 ICT Vision

The ICT vision for Danish Defence is:

“Information should be available in right form, at right time at right place”.

2.1.2 ICT Strategy

The ICT strategy is one of a number of corporate strategies – one for each strategic business unit – to support the achievement of the strategic goals. It is important that business units develops and maintains their own strategy in order to support corporate strategic goals and not just own goals.

The ICT strategy describes how the ICT supports the strategic goals by taking the recognised creation of value into consideration. The ICT strategy supports both the core functions and the supporting functions. The ICT strategy defines the route to achieve the strategic goals by the use of ICT in a manner which motivates decision makers to use it. Since the primary tasks for the defence forces are military operations both internationally and nationally, the partners should be identified as well as the approach to interoperability in order to support the strategic goals - including a prioritization.

The ICT Strategy for the Danish Defence has defined four areas of significant importance for the implementation of the ICT Strategy:

- changing requirements to the business in the military domain,
- the developments inside the ICT area,
- new governmental goals in the ICT area, and
- ICT developments in NATO and at strategic partners.

2.1.3 ICT Target Architecture

The purpose of the target architecture⁸ is to provide a set of goals for the evolution of the ICT for the ICT community within the defence forces as well as with vendors by setting the standards and

⁷ A business value is the effect of an initiative (e.g. an ICT initiative) contributing - directly and indirectly - to reach the strategic goals of a corporation.

⁸ The target architecture is DEFTA consisting of the four work packages WP0, WP1, WP2, and WP3.

preferred technologies. The target architecture is considered as an appendix to the ICT strategy and address the ICT solutions based on the demands from both the primary business (military operations) and the support functions (management, logistics, human resource etc.). The operational requirements and support function requirements are ideally stated in the strategies for these areas. Based on these requirements the target architecture should describe how the creation of values is best supported within the foreseen given resources.

2.1.4 ICT System Architecture

The purpose of system architecture is to describe ICT architectures to form the basis for acquisition, implementation and sustainment of ICT systems. All system architectures must be compliant with DEFTA.

The Danish Defence Overarching System Architecture (DEFOSA) covers all services, training, educational and supporting systems, i.e. the scope is similar to DEFTA. However, DEFOSA is limited to a shorter timeframe (app. 5 years) giving a more detailed setting of standards and technologies. The compliancy with DEFTA is realised by focusing on baseline and the first step on the way towards the target.

System architecture in general has always a specific purpose. The purpose is normally related to acquisition or updates of ICT systems. However, it can also provide the frame for a collection of basic system architectures, e.g. within a service or as reference architecture.

2.1.5 ICT initiatives

ICT initiatives are specific plans for ICT involvement to support the strategic goals. It takes form of roadmaps, program and project business cases, acquisition plans, upgrade plans, etc. The associated ICT system architecture should be enclosed as appendix to the plans. The initiatives should be compliant to DEFTA and DEFOSA. If that compliance for some reason is not obtainable, a waiver should be created and approved.

2.2 Summary

This chapter describes how the connection between facts, prerequisites, business, and ICT solutions should be connected in a way which gives value to the core business and the links between ICT Strategy, ICT Target Architecture, ICT System Architecture and ICT initiatives are defined. See figure 2-2 for connections to and from DEFTA.

It is stated that ICT initiatives should only be initiated in support of the corporate Vision, Mission and Strategies.

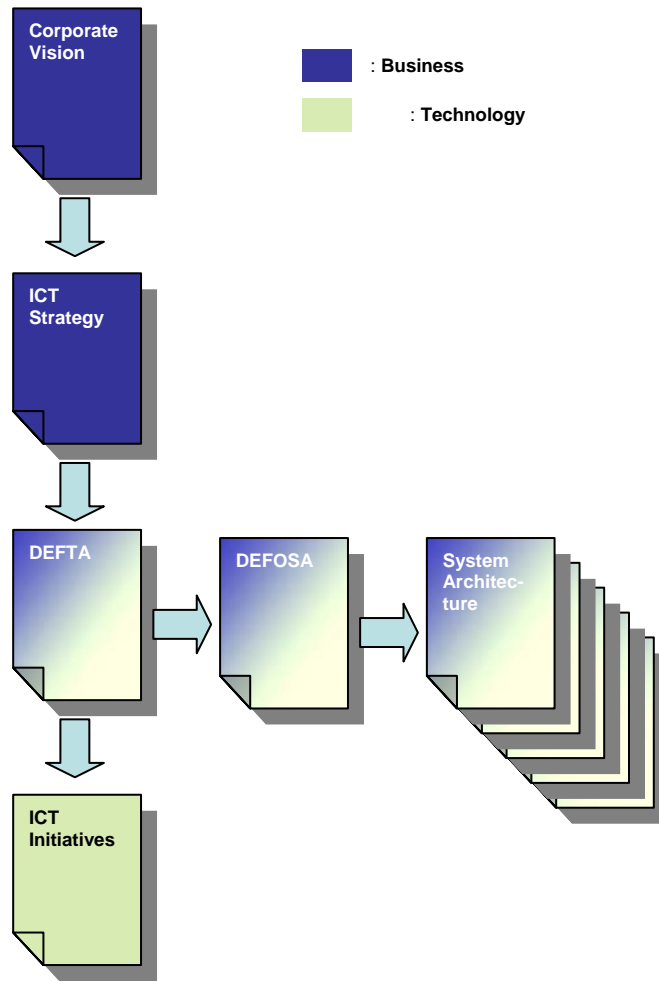


Figure 2-2: Connections to and from DEFTA

3 Defence Commission Report & Defence Agreement

This chapter describes the content of DCR08 and DDA14, focusing on cornerstones of Danish security and defence policy, national level of ambition, tasks for the armed forces and their future operational environments and the requirements for a robust force.

3.1 Defence Commission Report

The Defence Commissions Report [8]: Danish Defence Global Engagement was published in 2008 (DCR08). The report is looking forward 15 years until 2025 and, has broad political support. One of the main issues in the report was that the security policy challenges to a substantial degree, still needs to be tackled and addressed far away from Denmark's own borders. Hence the Danish Armed Forces must to a greater extent be able to fight asymmetric wars, besides maintaining the ability to fight conventional wars.

The report covered the following areas:

- The premises of security policy
- The Danish Armed Forces – aims and tasks
- The Danish Armed Forces – present structure
- Technology and equipment
- People – roles and conditions
- The support structure
- The Danish Armed Forces - development
- Resources

The Danish Defence Commission proposed that new capabilities should be established in two areas.

- Computer Network Operations (CNO), which partly aims at securing the ICT systems of the Danish Armed Forces against attacks in cyberspace.
- Capacity Building, which ranges from, assisting the East-African countries in building a peacekeeping unit that can be deployed in troubled areas elsewhere in Africa, or training a unit of the Afghan government forces to be able to perform some of the tasks we perform today.

The report later formed the basis for the Defence Agreement 2010-2014.

3.2 Defence Agreement 2010-2014

Danish Defence Agreement [9] for the period 2010-2014 (DDA14) was signed in Copenhagen, 24 June 2009. The basis for this agreement was the Defence Commissions Report: Danish Defence Global Engagement published in 2008 (DCR08).

The DDA14 establish the premises of national security policy, and the Danish Armed Forces – aims and tasks, structure, roles and conditions and future development.

3.2.1 Cornerstone of Danish Security and Defence Policy

Concerning premises the following cornerstone are identified:

- **NATO**⁹ “Denmark’s membership of NATO is a cornerstone of Danish security and defence policy. In a strategic perspective Denmark’s sovereignty is secured through NATO’s Article 5 commitment to collective defence of Alliance territory. At the same time, NATO provides a framework for the participation of the Danish Armed Forces in international missions. Denmark will thus continue to work in favour of a transformation of the Alliance in tandem with the transformation of the military forces of Member States, seen also in relation to a strengthening of the demands placed by the Alliance on the usability of these military forces.”¹⁰
- **United Nations**¹¹ “An active Danish involvement in the UN is another cornerstone of Danish security and defence policy. Denmark should therefore work to ensure that the UN continues to constitute the foundation of the international system as the source for global legitimacy and the establishing of universal norms. Furthermore, Denmark should contribute to enhancing the UN’s capability for the conduct of peacekeeping operations. This could be achieved partly through focused cooperation in Nordic circles. The already ongoing Nordic cooperation on the training and instruction of African peacekeeping forces will be continued and intensified, and potential opportunities for joint Nordic peacekeeping operations within the UN framework will similarly be pursued.”
- **EU**¹² “Furthermore, in the event of the discontinuation of the Danish EU defence opt-out, the Danish Armed Forces must be able to participate in EU operations outside Union territory relating to peacemaking, peacekeeping, conflict resolution and humanitarian assistance as well as to strengthening international security in accordance with the principles of the UN Charter.”

3.2.2 Level of Ambition

The Defence Commission Report recommends that the present national level of ambition regarding the ability of the Danish Armed Forces to contribute to international operations should be maintained. Thus the sustaining of deployed capabilities corresponding to up to some 2,000 soldiers, sailors and airmen should be achieved through a combination of some of the examples as described below.

- **ARMY**¹³ “The Army should be capable of simultaneously deploying up to two units organised as battle groups, as well as a number of smaller contingents. In terms of the structure of the

⁹ DDA14 p.10

¹⁰ DDA14

¹¹ DDA14 p 11

¹² DDA14 p.11

¹³ DDA14 p.7

battle groups, their composition will be tailored to task and they will thus vary in size, typically from approx. 300 and up to approx. 800 soldiers. Similarly, smaller-sized contingents of company size – typically approx. 150 soldiers – are also to be configured to task.”

- **NAVY**¹⁴ “The Navy should, with the commissioning of three new frigates, be capable of simultaneously deploying two frigates, support ships or ocean patrol vessels. Additionally deployment of the Royal Danish Navy’s Task Group is a possibility.”
- **Air Force**¹⁵ “The Air Force should be capable of simultaneously deploying up to three contingents, which will typically consist of transport aircraft, helicopters, combat aircraft, as well as surveillance and early warning contingents. Furthermore, the Air Force should be capable of contributing with an expeditionary staff along with a range of specialised personnel in the form of, for example, support crews for loading and unloading aircraft as well as for air base operations, etc.”
- **Others**¹⁶ “Additional contributions from the Army, Navy, Air Force and Home Guard might encompass Special Operations forces, smaller units and elements designed for military capacity building, as well as individuals dispatched to staffs and as observers, etc.”

3.2.3 Tasks

According to DDA14, the tasks of the Danish Armed Forces can be divided into national and international tasks.

“The national tasks comprise – besides monitoring of the national territory and enforcement of sovereignty – a range of more civilian-oriented tasks in support of Danish society, such as search and rescue operations, environmental tasks as well as providing support to a number of other public authorities, such as the police, the emergency rescue services and the tax authorities.”¹⁷

“The international tasks will typically fall within the following main areas: armed conflict, stabilisation tasks and international policing”.¹⁸

In relation to the international tasks, the Defence Commissions Report points out that the Danish Armed Forces’ deployable capabilities in principle should be capable of being deployed globally. This means, for example, that the Danish Armed Forces should have the ability to deploy forces in areas which feature demanding climate and terrain conditions, such as desert and mountain areas. In addition, the Danish Armed Forces should be able to operate in areas with limited infrastructure as well as in urbanised areas. Combined, these operational conditions will therefore place great demands on the Danish Armed Forces’ personnel, equipment, training, logistical capability and mobility, including for example strategic maritime and air transport capability.

¹⁴ DDA14 p.7

¹⁵ DDA14

¹⁶ DDA14

¹⁷ DDA14 p.2

¹⁸ DDA14 p.3

3.2.4 Future Operational Environment

It is expected that the future operational environment will continue to place great demands on the operational units of the Danish Armed Forces, with regard also to training and equipment. In the DDA14 it is stated:

“Past developments and expected future developments within international operations indicate, for example, that the future operational environment could be characterised by a high threat level. The accompanying need to protect personnel places great demands on the equipment, personnel and training of contingents.

At the same time, it is expected that the Danish Armed Forces, in connection with international missions, must increasingly be prepared to encounter both asymmetric instruments of warfare (e.g. improved explosive devices (roadside bombs) and suicide attacks) and more conventional instruments of warfare (e.g. indirect fire from rockets and mortars).

More technologically advanced instruments of warfare, such as long-range rockets and missiles as well as cyberspace attacks against computer systems, must also be expected to be used against Danish contingents from all three armed services.

At the same time, the possibility of having to conduct operations against more conventionally organised and operating opponents still exist. The Parties to the Defence Agreement are in agreement that the Danish Armed Forces must also maintain the ability to fight and win this type of conflict”.

3.2.5 Requirements for Robust Forces

The demand for Danish contributions to international operations will not diminish in the future and that such operations will often be long-term in nature. The DDA14 states that there is a “need for the operational capabilities of the Danish Armed Forces – of all services – to be, as a whole, sufficiently robust and capable of a sustained effort in order to support long-termed international engagements. Moreover, in special situations the Danish Armed Forces should possess the ability to deploy additional or larger contingents for shorter periods of time as well as the ability to deploy contingents at short notice in connection with crisis management, humanitarian disasters, evacuation operations, demonstrations of solidarity or of NATO’s commitment, etc., which can be ensured through, among other things, participation in NATO’s response forces”.¹⁹

3.3 Summary

In DDA14 the overall conclusion was that the Danish Armed Forces must be able to perform a wide variety of tasks.

“The Danish Armed Forces must remain able to participate in difficult and intensive operations, including the continued contribution to the Danish engagement in Afghanistan in the coming years

¹⁹ DDA14 p.4

in accordance with Denmark's Afghanistan Strategy. However, the Danish Armed Forces must also preserve and develop the ability to execute other types of stabilisation tasks and international policing operations, including such mission types as the KFOR mission in Kosovo and the operations against piracy off the Horn of Africa."

The content of DCR08 and DDA14 is used in further detail in WP1: Operational Tasks and Vignettes.

This page is left intentionally blank

4 Status of NBO

The main principle behind Danish Defence approach to NBO is that the development of the ability to operate in networked environments must be pragmatic and realistic. Danish Defence has therefore chosen to follow and influence the NNEC developments within NATO and will follow the trends among our strategic partners, rather than implementing own costly prototypes. .

This chapter gives a short view of the developments in the area of NBO. Focus will be on activities in the national arena since the last report in 2005 and general status of NNEC in NATO. Finally the latest developments in USA and GBR are described.

4.1 National NBO Development

Danish Defence NBO-development has been based on *The Preliminary NBO Report*" (DEC 2004)²⁰ and *The Follow-up NBO Report*" (OCT 2005²¹). These reports identified a number of recommendations and actions, which created a solid foundation for Danish Defence approach to the NBO. Its recommendations and actions were mainly focused on technological issues, where ICT Target Architecture and the Defence Overarching System Architecture (DEFOSA) was significant contributions to the development of Danish Defence capabilities. These reports have also been used as basis for studies in the training and logistics area.

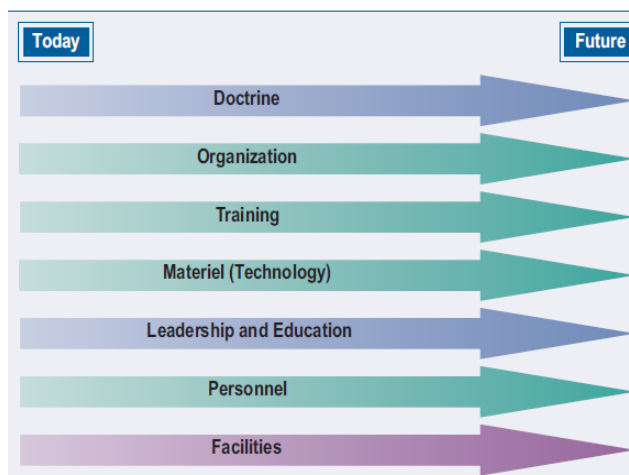


Figure 4-1: Approach, Co-evolution of Functional Areas

DANISH DEFENCE has been active contributor to the NBO developments within NATO, where focus today is the co-evolution of doctrine, organization, training, technology, training, personnel and facilities as shown in figure 4-1.

²⁰ Den indledende NBO rapport 2004 [3].

²¹ Den opfølgende NBO Rapport 2005 [10].

4.1.1 Concept for the development of ability to operate in NBO environment

Based on these initial reports Danish Defence drafted a new concept in 2008: "Concept for the development of Danish Defence ability to operate in a network-based environments" was presented. This draft defined the new objectives and targets for Danish Defence development of the ability to operate in networked environments. Based on these objectives and a generic description of the networked environment and the operations within, a number of NBO-related requirements and recommendations were given.

NBO is not regarded as a separate doctrine, but a tool which will gradually be developed by enhancing the operational capabilities opportunity to be part of networks-of-networks and contribute to the development of a common operational picture that forms the basis for:

- Increased ability to fight asymmetric warfare through an increased awareness.
- Increased operational tempo and awareness of risks.
- More flexible use of effects and better resource management.
- Improved intelligence and more rapid and accurate assessment of the achieved effects.

This draft concept included a dynamic plan (roadmap) for the development Danish Defence ability to operate in networked environments.

As part of the preparatory work up to the Danish Defence Agreement (DDA14), the draft concept was set on hold, and later in 2009 it was integrated into a new concept. "*Concept for the Operational Development of Danish Defence*"

4.1.2 Concept for the Operational Development

The concept aims to contribute to the establishment of the strategic basis for the military professional advice in relation to the Armed Forces' operational capability development.

It is based on NATO strategic guidance, strategic partners trend, the Danish Defence Mission, Vision and Strategies (MVS) and recommendations from the *Defence Commission Report dated 2008* (DCR08), including the threat assessment report developed by Danish Defence Intelligence and the report from the Committee regarding Defence Equipment from 2007.

The concept defines the direction of development for Danish Defence operational capabilities in the medium (5-15 years) and long (15-30 years) term. The following conclusions were given:

- The development of Danish Defence capabilities has to ensure doctrinal and technical interoperability in order to operate in multinational combined environments and national joint operations within specific task based on the principle of supported / supportive units. The technical and doctrinal development should also consider cooperation with civilian organizations.
- Within the material development and acquisition the focus will be increased modularization and use of "commercial of the shelf" or "military of the shelf" (COTS / MOTS) products to ensure low development cost and the fast implementation.
- In the technology area, the rate of development continues to be high and irregular adversaries innovative use of open standards can potentially have an impact on the tactical level. This requires that the defense doctrinal, organizational and technological possess a high degree of adaptability and continuous upgrading or renewing procedures and equipment.

- It should be regularly assessed across the armed services whether the technological development in specific areas of capability allows for the provision of the desired operational effect of reduced personnel resources, including the possibilities offered by the recovery of modern surveillance and sensor technology.
- In situations where there are several possible directions of developments, priorities must be set for the benefit of the strategic partners.
- Interoperability and the ability to operate in networked environments will be key parameters for future development or acquisition of capabilities.

Development of capabilities should take into account; Resources required, safety of own personnel, Life Cycle Cost, effect, logistics support and personnel required. This should be accomplished through a modular and incremental approach. During the process synergies can be achieved through solutions that can support two or more services which is an important parameter in the development of future capabilities. Lessons from national and international deployments (Lessons Identified / Lessons Learned) are another important factor in the development of all capabilities.

4.2 NATO

In the following NATO Network Enabled Capability (NNEC) is described with requirements, strategic vision, and political guidance.

4.2.1 NATO Requirements to NEC

“SHARE TO WIN” is the new slogan of Allied Command Transformation, who is responsible for the transformation of NATO into the NNEC-future. The requirement for the NNEC is based on the following principles (see figure 4-2):

- A robustly networked force improves information sharing.
- Information sharing and collaboration enhances the quality of information and shared situational awareness
- Shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command; it should be viewed as a force multiplier.
- These in turn dramatically increase mission effectiveness.

Recognising that in the Information Age military transformation is essential, NATO pursues a course of transformation towards achieving NNEC, which “encompasses the elements involved in linking collectors, effectors, and decision makers together to enable the development of a NATO, network enabled, and effects-based, operational capability”²². In the NATO Network Enabled Capability resides a coherent approach to the development of technical and operational interoperability standards and targets for adoption and aims to harmonize NATO and national NEC and NBO programmes. Security is part of the “Share to Win”, only people with “need to know” can access information – this is done defining groups, not individuals. The “need to know” personnel can change over time.

²² 3 MCM-0032-2006, NATO Network Enabled Capability (NNEC) Vision and Concept, dated 19 Apr 2006.

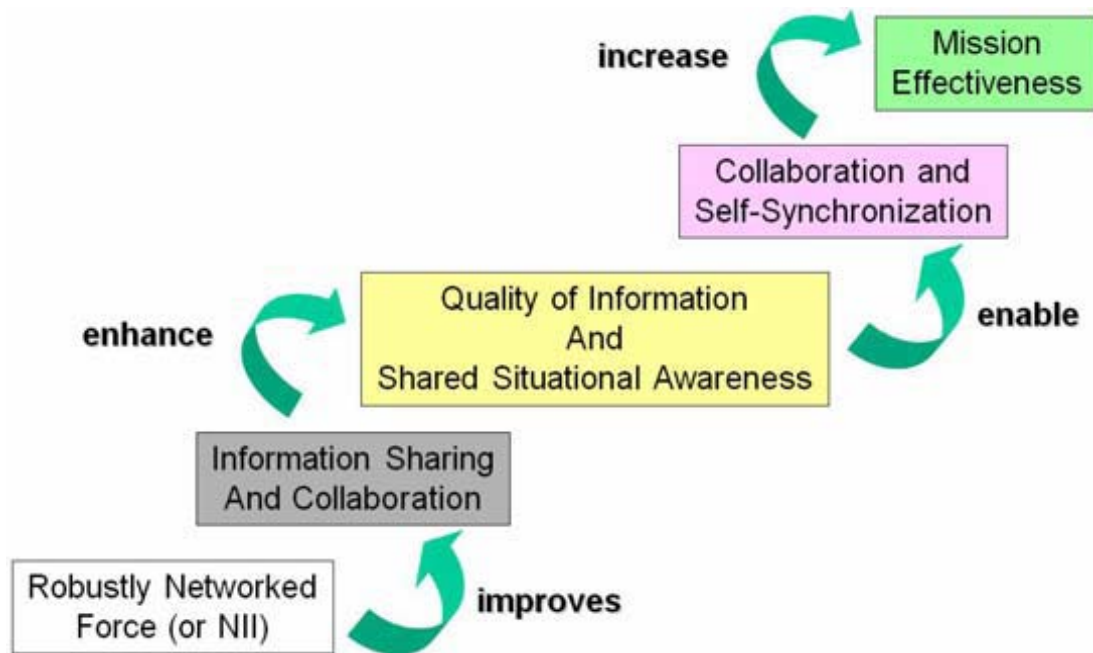


Figure 4-2: The NNEC Value Chain, as developed in the USA by OSD/OFT.

The Networking and Information Infrastructure (NII) is the collection of NATO and national information infrastructure and communications infrastructure capabilities. The NII implements standardised information services including information transport, storage, security, management and other enabling capabilities to technically support NNEC.

4.2.2 The NATO Bi-SC Strategic Vision

The Bi-SC Strategic Vision – “The Military Challenge” points to future Alliance operations being expeditionary, multi-dimensioned, and effects based.

In order to accomplish this, NATO will need to become more efficient in utilizing all the instruments of power, Military and Political, available to the Alliance, and ultimately to learn how to integrate these activities into a coherent plan of action that will increase the impact and overall effectiveness to deliver rapid, decisive operational and strategic outcomes inside and outside its traditional area of responsibility (cf. Articles 5 & 6 of the Treaty). As a part of this process, NATO will have to utilize smaller force structures that will need to move farther and faster than ever before, and be able to operating with a speed and precision that allows doing more with less.

The immediate area of attention within ACT and NATO HQ is to develop a roadmap that will modernize Alliance capabilities and enable NATO to create a truly networked Force. This will require the exploitation of modern and emerging technologies, particularly in the area of information collection, synthesis and dissemination and the development of strategies to make the transition from legacy systems and processes into an integrated network centric environment.

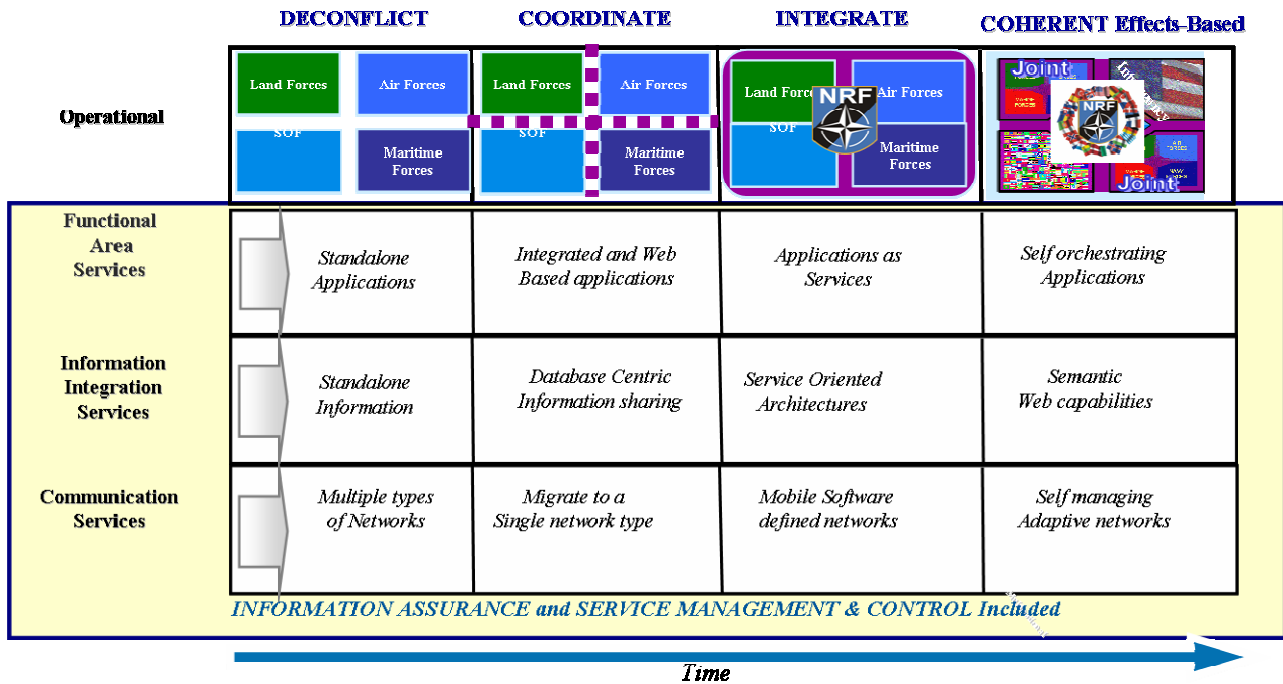


Figure 4-3: NNEC Feasibility Study development model

4.2.3 NATO Political Guidance

NATO Strategic Concept is a cornerstone in the development of the Alliance. The new NATO Strategic Concept, “Active Engagement, Modern Defence”, adopted at the Lisbon Summit in November 2010 defines three core tasks for the Alliance:

- Collective Defence. By deterrence and defence protecting all members from attack in accordance with the Article 5 of the Washington Treaty.
- Crisis Management. NATO possesses a unique and robust set of capabilities that address the full spectrum of crisis.
- Cooperative Security. NATO will engage actively with all relevant countries and international organisations to enhance international security.

The Political Guidance was agreed in March 2011 as a Strategic Concept implementation document. The Political Guidance defines roles and responsibilities in addressing the growing threat of cyber attacks directed at the Alliance. The focus of NATO cyber defence will be on the implementation of a robust fundamental defensive construct for the centralised protection of all NATO’s own communication and information systems both in NATO Military and Civil bodies to take into account the interconnected nature of cyber space and propagation of relevant risks. Planning should presume that future operations will be conducted in a contested and often degraded network environment, and take into account associated cyber defence requirements on a prioritised basis. Due to the interconnected nature of cyberspace, vulnerabilities of individual Allies can create risks for the Alliance as a whole. Allies are responsible for the security of their national networks.

NATO requires forces which are robust, mobile and deployable in order to carry out both Article 5 and non-Article 5 crisis response operations. Hence, the focus of defence planning and capability development will be on modern, interoperable and sustainable forces and capabilities to undertake the full spectrum of operations and tasks. The approach to interoperability has to be holistic, consistent and coherent, starting with definition of interoperability requirements, identification of solutions, followed by implementation of solutions by all parties involved.

4.3 Strategic Partners

One of the main conclusions from the Preliminary NBO report of 2004, was the definition of the principle of Strategic Partners. Denmark has, besides NATO, chosen GBR and USA as main Strategic Partners and a short description of the latest NBO-developments in GBR and USA is described below.

4.3.1 NEC Strategy in GBR

The MOD's NEC strategy is a fundamental element of the GBR Defence Vision. The GBR vision of NEC goes wider than defence. In overseas operations, NEC involves networking with other departments and Government agencies like the Foreign Office and DFID (Department for International Development), as well as non-Governmental organisations like Doctors Without Borders and the Red Cross. At home, the intent is that NEC will allow better networking with other Government departments, the security services and the emergency services.

The implementation of the GBR vision of NEC is a step-by-step evolution through what are known as the three NEC maturity states. The aim is to achieve the initial maturity state by 2012, based on current doctrine, organisations, processes and equipment where improvements in operational capability can be made in the short term.

In the initial state the intention is to ensure that a rudimentary but increasingly capable NEC capacity is achieved. Achieving the initial state will also require considerable work on ensuring security and resilience for information and communication systems. Moreover, a process for improving interoperability within the GBR Armed Forces needs to be set in place alongside the additional needs for interoperability between GBR Defence and other GBR elements, as well as with our allies and coalition partners.

The development of Britain's armed forces is based on a growing ability to conduct operations in a combined joint environment including GO and NGO, with more extensive use of technological solutions for improving communications and the ability to act (Strike Capability) on land, sea and air. Overall, Britain will invest in platforms and capabilities that can support the ability to operate in network-centric operations and the use of precision engagements. Following this, Britain will also focus on developing solutions that will strengthen the military capabilities the ability to achieve information superiority

4.3.2 NCW Strategy in USA

The United States Department of Defence Office of Force Transformation (OFT) was established October 29, 2001 in the Office of the Secretary of Defence. Secretary of Defence Donald Rumsfeld called for the creation of this new office to support his transformation vision along with President George W. Bush's broad mandate to transform U.S. military capabilities. OFT transformation plan includes changing the force and its culture from the bottom up through large amounts of experimentation, increased sharing of new knowledge and experiences, and by broadening military capabilities while mitigating risk. One of the pillar theories driving OFT was Network Centric Warfare (NCW), also known as Network Centric Operations (NCO). The OFT was closed in 2006 and the transformation activities transferred to the services.

The development of U.S. military capabilities will in future be based on the most likely threat scenarios rather than the most dangerous scenarios. The nature and complexity of the conflicts that the U.S. has been and is engaged in, is pointing to U.S. involvement in future conflicts in time will be prolonged periods (5 - 10 years).

There is an increased need for the ability to act globally (Strike Capability) within a very short time - down to an hour - and micro - seconds concerning operations in Cyber Space.

Concerning acquisition of military equipment the United States will focus on capabilities that can be rapidly updated or adjusted if the opponent changes tactics. The technological development is therefore seems to point at flexible (general purpose) hardware, which can be maintained through situation-specific software updates. In conclusion, USA will strengthen its military leader's ability to improvise and to take appropriate and in-time situation-specific decisions.

4.4 Summary

This chapter presented an over all view of the developments in the area of NBO. Focus was on national activities after the NBO Follow-up report (2005) and gave a general status of NNEC with our Strategic Partners NATO, USA and GBR described.

The Networking and Information Infrastructure (NII) is the collection of NATO and national information infrastructure and communications infrastructure capabilities. The NII implements standardised information services including information transport, storage, security, management and other enabling capabilities to technically support NNEC.

The national NBO-developments and the development in NATO are closely connected. The ability to interoperate with allies and coalition partners is of outmost importance, and therefore appropriate technical interoperability is required. Interoperability through NATO has been chosen as a way to achieve this goal, and national focus will be on development of common joint systems instead of dedicated systems.

Developments points to the need for closer development of systems-of-systems, where the Danish national must be able to connect seamlessly to other systems. Joint development is therefore required.

This page is left intentionally blank

5 Discussion and Conclusions

The Networking and Information Infrastructure (NII) is the collection of NATO and national information infrastructure and communications infrastructure capabilities. The NII implements standardised information services including information transport, storage, security, management and other enabling capabilities to technically support NNEC.

The national NBO-developments and the development in NATO are closely connected.

In the DDA14 the overall conclusion is that the Danish Armed Forces must be able to perform a wide variety of tasks and must remain able to participate in difficult and intensive operations, including the continued contribution to the Danish engagement in Afghanistan in the coming years in accordance with Denmark's Afghanistan Strategy. However, the Danish Armed Forces must also preserve and develop the ability to execute other types of stabilisation tasks and international policing operations, including such mission types as the KFOR mission in Kosovo and the operations against piracy off the Horn of Africa

The report from the Defence Commission Report (DCR08) stresses the need for NBO and the ability to interoperate with allies and coalition partners, and therefore appropriate technical interoperability. DCR08 points out that NBO prospectively will have significant impact on the defence structure and activities. DCR08 mentions improved command and control systems, with the aim to enhance the operational capabilities ability to participate in international operations with coalition partners. Moreover, as explained in DCR08, there has to be focus on development of common joint systems instead of dedicated systems.

With reference to DCR08 the support to the operational units will be based on a network-based approach, where each single acquisition is coordinated in order to create a networks-of-networks and a systems-of-systems.

The statements in DCR08 and DDA14 must therefore be basis for the developments of Operational Scenario's in WP1. As a roadmap for this work chapter 2 describes the connections between Danish Defence Vision and Mission, Corporate Strategic goals and the underlying Strategies. The ICT strategy is the central element, with the DEFTA as a primary supporting document.

This page is left intentionally blank

References

- [1] Thyge Arum: DEFCOMM, Operational Scenarios, WP1, DDRE report M-17/2005 (Sep 2005).
- [2] David S. Alberts, John J. Garstka and Frederick P. Stein: Network Centric Warfare, 2nd edition, CCRP 1999.
- [3] Koordinationsgruppen vedr. Netværksbaserede Operationer, Indledende Rapport, FAK 21 DEC 2004 (Danish).
- [4] DOD Architecture Framework 1.0, 9 February 2004.
- [5] Network Enabled Capability, *Unified Message 1. draft*, UK MOD SEP 2004.
- [6] David S. Alberts, John J. Garstka, Richard E. Hayes, and David A. Signori: Understanding Information Age Warfare, CCRP August 2001, Chapter 3-5.
- [7] David S. Alberts and Richard E. Hayes: Power to the edge, CCRP June 2001, Chapter 5.
- [8] Defence Commission Report (DCR08) - Forsvarskommissionens rapport 2008 (Danish).
- [9] Defence Agreement (DDA14) - Forsvarsforliget 2010-2014 (Danish).
- [10] Koordinationsgruppen vedr. Netværksbaserede Operationer, Opfølgende Rapport, OKT 2005 (Danish).

This page is left intentionally blank

Acronyms

AV	All View [from NAF]
CCRP	Command and Control Research Program
CIS	Communication and Information System
CNO	Computer Network Operations
COTS	Commercial, off-the-shelf
CV	Capability View [from NAF]
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 (used previous version of the Target Architecture)
DEFOSA	Danish Defence Overarching System Architecture
DEFTA	Danish Defence Target Architecture
DFID	Department for International Development
DoD	Department of Defense
EU	European Union
FAK	Forsvarsakademiet (Danish for Royal Danish Defence College)
GBR	Great Britain
GO	Government Organisation
HQ	Headquarter
ICT	Information and Communication Technology
KFOR	Kosovo Force
KPI	Key Performance Indicator
MoD	Ministry of Defence
MOTS	Military Of The Shelf
MVS	The Danish Defence Mission, Vision and Strategies
NAF	NATO Architectural Framework
NATO	North Atlantic Treaty Organization
NBO	Network Based Operations
NCO	Network Centric Operations
NCW	Network Centric Warfare
NEC	Network Enabled Capability
NGO	Non-Government Organisation
NII	Networking and Information Infrastructure
NNEC	NATO Network Enabled Capability
OFT	United States Department of Defence Office of Force Transformation
OV	Operational View [from NAF]
PV	Programme View [from NAF]
RDDC	Royal Danish Defence College
SOA	Service Oriented Architecture
SOV	Service Oriented View [from NAF]
SV	System View [from NAF]

TV	Technical View [from NAF]
UK	United Kingdom
UN	United Nations
USA	United States of America
WPx	Work Package x (x=0, 1, 2, 3)