Policy for military adaptation and use of **information and communication technology** in the Norwegian Armed Forces

Approved 1st September 2005

Contents

1. Purpose

The purpose of this policy is to establish a foundation for the Norwegian Armed Forces' common organisational culture regarding adaptation and use of information and communication technology (ICT) for military purposes. This in particular implies that a common vision and central guidance must be provided to all stakeholders. The policy therefore serves an explanatory as well as a governing function.

The policy builds on the intentions and guiding principles expressed in previous long-term defence plans and parliamentary proposals, and provides an increased focus on the adaptation and use of ICT in an operational context.

2. Area of application

This policy applies to all military adaptation and use of ICT in Norwegian Armed Forces. In cases where ICT is used exclusively in connection with research, development and experimentation, this policy is intended as guidance.

3. Vision

Technology, in particular ICT, is instrumental to the transformation of the Armed Forces. Secure exchange and distribution of information through networks will provide our forces with more comprehensive and updated bases for decision and enable rapid and synchronised action, with the appropriate means to respond to all types of situations.

Innovations within ICT provide substantial possibilities for further improved efficiency related to the operational activities, in particular operational support, as well as administration. Through increased use of standardised solutions combined with a reduction in both types and number of applications, as well as improved system interoperability, substantial savings can be generated.

The ICT core adapted and used for military purposes will in this document be referred to as the defence information infrastructure. This infrastructure includes information, processes, standards and technology as well as the necessary operations and maintenance personnel. The future information infrastructure shall support network based operations by facilitating an interactive, network oriented organisation of the Armed Forces' resources, from strategic to tactical level , both nationally as well through interaction with allied or coalition forces, including relevant civil agencies. Thus interoperability is the guiding principle for the defence information infrastructure. Priority will also be given to improvements regarding important operational characteristics like flexibility, response time and deployability.

4. Reference model for the information infrastructure

Figure 1 depicts the new reference model for the defence information infrastructure. The model reflects design work in the Armed Forces as well as equivalent results from Alliance partners and civil sector. Military adaptation and use of ICT shall focus on solutions that, to the extent possible adhere to the reference model, subject to financial and technical limitations at the time of realisation.

The defence information infrastructure consists of functionally oriented decision support services and core services, interconnected by the communications infrastructure.

- *The functionally oriented decision support services support user groups with common requirements for information and process support. These services build on and utilize the core services.*

- *The information infrastructure core services are common and describe available basic information and process* *support. The fact that the services are common, does not imply that they are universally available, but rather that these services are standardised throughout the Armed Forces.*

- *The communications infrastructure provides quality tested mechanisms interconnecting the functionally oriented decision support services and core services as well as various decision, effector and sensor components.*

In principle, all the services are independent of one another and of the communication solutions. The interfaces between the information infrastructure and the decision, effector and sensor components are represented by the various services.

The services in the reference model are further described on page 11.

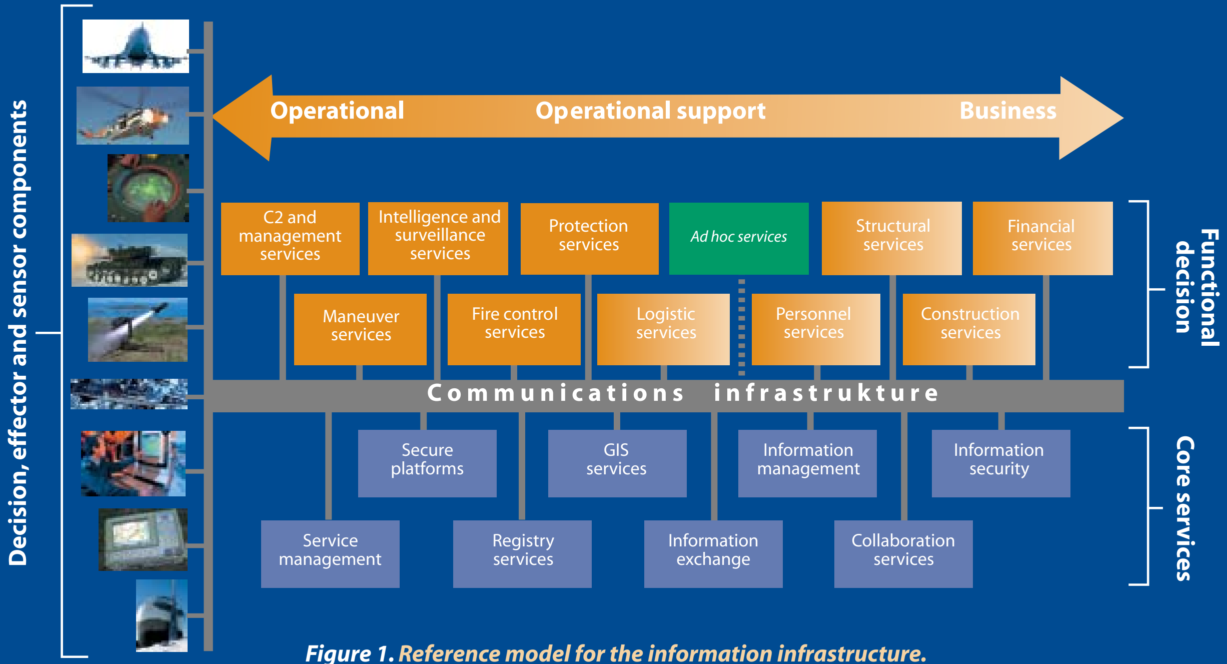

Figure 1. Reference model for the information infrastructure.

5. Guidance for military adaptation and use of ICT

5.1 Central management

ICT is instrumental to the desired transformation towards more network based operations. In order to avoid incurring substantial costs through suboptimization of technology application and lack of comprehensive gains analysis, there is a need for strategic level central management focusing on three particular areas:

- *Unified planning and structuring of military adaptation and use of ICT in the Armed Forces.*

- *Overall management and control of ICT investments and operations.*

- *Political and military guidance with respect to possibilities and limitations in military adaptation and use of ICT.*

Military adaptation and use of ICT shall be managed through the use of architectures. Identifying the essential characteristics of the Armed Forces' activities shall be the focus, including the interfaces and information flow between different organisational units.

5.2 ICT as a catalyst for change and the realisation of gains

The information infrastructure shall enable the Armed Forces to increase the effectiveness of other investments and create potential cost reductions. To achieve maximum benefit from modern ICT, the Armed Forces are also required to introduce necessary changes in related processes and organisational structures.

Viewed in isolation, modern ICT may seem expensive and contribute disproportionately to increase investment expenditures, By actively utilizing ICT as an integral part of a broader restructuring, it is still possible to achieve overall cost savings through gains achieved in other affected areas of the organisation.

Through the active use of ICT, Norwegian authorities aim at simplifying its interaction with private citizens as well as business enterprises. Therefore all Armed Forces electronic interfaces with both private citizens and businesses must support this public commitment.

5.3 Focus on the user

The information infrastructure services shall, to the extent possible, use a common user interface. The services shall provide relevant user guidance, and shall be resistant to possible user errors. New services shall be thoroughly tested prior to introduction and necessary time shall be made available to users for training.

It is paramount to develop the skill level of the user in sync with the evolving spectrum and availability of the information infrastructure services. This includes the ability to take advantage of modern ICT, and utilize this resource discriminately and creatively for both learning and work purposes.

5.4 Adaptation and use

Military adaptation with subsequent usage shall be given preference over development of proprietary solutions. The information infrastructure shall hence, as far as possible, be based on existing technology adapted and used to meet the Armed Forces' requirements. The relevant processes of the Armed Forces shall, if necessary, be adapted in order to utilize standard software and standard processes wherever possible.

Technology that are to be adapted and used for military purposes should normally be in production.

5.5 Process model for military adaptation and use of ICT

Figure 2 shows a generic model, describing how research and development, experimentation, concept development, lessons learned from exercises and operations all contribute to developing knowledge about how modern ICT can be adapted and used for military purposes.

We aim to learn from our experiences, both failures and successes, and we must manage the lessons learned in a manner that benefits both individuals as well as the entire military organisation.

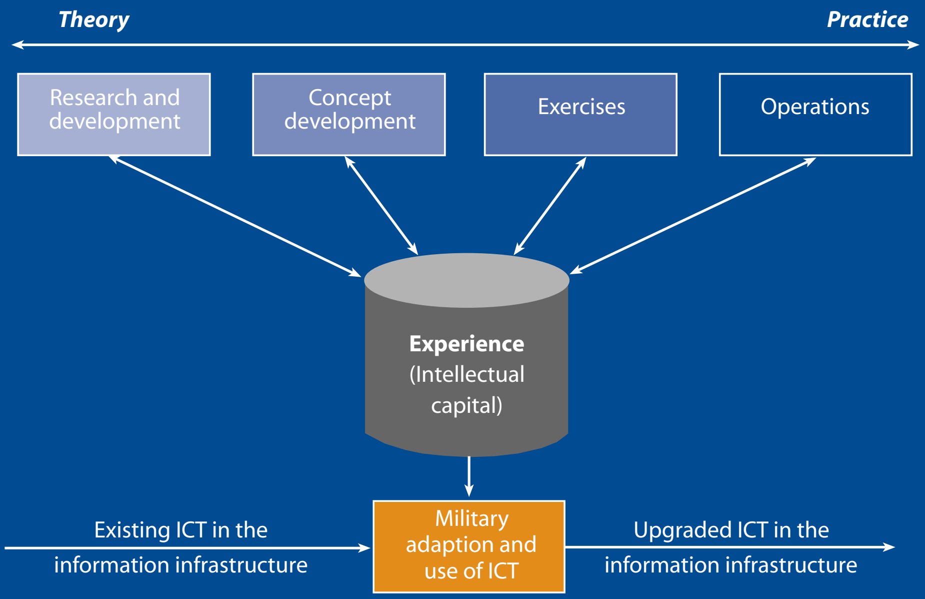
Theory
Practice
Research and development
Concept development
Exercises
Operations
Experience
(Intellectual capital)
Existing ICT in the information infrastructure
Military adaption and use of ICT
Upgraded ICT in the information infrastructure

Figure 2. ***Cultivation of defence information infrastructure***

When planning ICT investments, alternative procurement strategies shall always be considered, e.g. various public - private partnership solutions. During the planning phase, it is also essential to identify which operating and maintenance costs that will be financed through direct funding and which will be covered through internal invoicing.

5.6 Standardisation and variant limitation

The aim is a development towards limited types and number of ICT solutions with improved co-ordination both within and between the different levels of security classification. This will in itself be an important contribution to interoperability. Common solutions across the military services have priority and shall be used wherever possible.

Increased emphasis should be put on standardised, lightweight and preferably less expensive end-user equipment, which may be deployed with units both nationally as well as internationally.

An improved consensus concerning the content of the relevant operational processes is also required.

5.7 Modularity and standardised interfaces

In order for the defence information infrastructure to support network based operations, it is necessary to change focus from the actual applications towards solutions which facilitate access to information and services through standardised interfaces.

A key element is open industry and alliance standards which already have a minimum critical mass of users. The standards must be flexible and accommodate specific requirements. The design of the information infrastructure, including the inherent standards, shall enable the Armed Forces to cooperate effectively with existing as well as new partners in both national as well as international operations. Emphasis must be put on the development of interoperable modules which can be organised to provide rapid and flexible support in accordance with different requirements.

5.8 Continuous adaptation and upgrade

New solutions should be developed to allow continuous adaptation and upgrades rather than be designed for future replacement. Flexibility shall be a fundamental principle, facilitated through continuous evaluation of new solutions. Developing the defence information infrastructure is a long term process, achieved through expansions, extensions and improvement of the existing infrastructures. This implies that development of a comprehensive infrastructure is a continuous process.

Focus shall be on applying military adapted ICT for personnel who plan, support, implement and conduct operational activities, i.e. those elements that are involved in exercising military power.

5.9 Information management support

Information management first and foremost relates to what information the different services provide access to, how it is processed and disseminated, and to a lesser extent to technology. In regards to this, the defence information infrastructure must ensure that not only the data provider, but all relevant users, get access to usable information (contextual data, messages) rather than just unprocessed data. Services that describe data in a manner that provides context and relevance are hence important.

Effective information management is affected by culture and attitudes. Hence it is necessary to develop skills related to sharing and re-using information electronically, and also to develop and promote sharing and reuse practices in the organisation.

5.10 Security

Network based operations create an increased dependence on the defence information infrastructure, and hence sensitivity with respect to manipulation, degradation or loss of this infrastructure. The security aspect shall therefore be treated as an integral part of the defence information infrastructure, and incorporated in the adaptation- and development processes from the very start. Supporting secure operations and maintenance, ensuring the ability to detect security breaches and managing incidents, including subsequent

restoration, is vital. When selecting solutions, the security aspect of integration and interoperability shall be emphasised in order to avoid infrastructure fragmentation and subsequent interruption of information flow and services.

The capability to share information in flexible and dynamic networks, including utilization of available military and commercial communication resources, is prerequisite for network based operations. Future security solutions shall therefore focus more on securing confidentiality, integrity, authentication and access control associated with information and services, and less on the physical hardware used to convey the information. The security related to physical transmission shall focus on availability and capability to utilize alternative communication resources.

The use of Public Key Infrastructure (PKI) represents a considerable asset in ensuring the security of services in the information infrastructure. When utilising PKI for classified services, compliance with Norwegian National Security Authority requirements, which are based on NATO's "PKI Certification Policy", is mandatory. The Armed Forces must also be cognizant of the national initiative to establish a public sector security portal for relevant services.

6. Implementation

This policy is implemented with effect from 1st September 2005. It supersedes previous versions of Armed Forces ICT policies.

Brief explanation of the services in the reference model

The classification of the functional services and the common core services may include overlaps and omissions. It must be expected that the extent and subdivision of the services will have to be amended as experience is generated through application of the model.

Functional decision support services

- **Command, control and management services** - Services for planning, management and control of Armed Forces activities. For example, services for the development of plans, orders and missions, as well as for simulation and analysis.
- **Manouver services** - Services for conduct of military activities, i.e. in support of the various forms of operation (land operations, air operations, maritime operations, amphibious operations, air and missile defence, information operations, special operations and crisis management).
- **Intelligence and surveillance services** - Services for building relevant operational pictures, for example intelligence, reconnaissance, surveillance and sensor control.
- **Fire control services** - Services for controlling and synchronising various types of fire. For example, services for localisation and target processing, target engagement, choice of weapon and effect analysis.
- **Protection services** - Services for NRBC, fortification and protection measures.
- **Logistic services** - Services for acquiring and maintaining combat capability (materiel).
- **Personnel services** - Services for recruiting, development, utilisation and discharge of personnel.
- **Structural services** - Services for planning, realisation and evaluation of organizational structures.
- **Works services** - Services for management of defence property, buildings and installations. For example services to support the establishment and unrigging of camps.
- **Financial services** - Services for pay and accounting.
- **Ad hoc adapted services** - This type of service is included in order to indicate that we must have flexibility to assemble specially adapted groups of services to meet operational needs as they arise.

Common core services

- **Service management** - Services such as system monitoring, availability assurance and various kind of service desks.
- **Secure platforms** - Secure runtime environments with standard support tools (For example FISBasis Secret/NATO Secret and FISBasis Restricted/Unclassified).
- **Registry services** - Administration and provision of the services in the information structure, for example a look-up service («electronic Yellow Pages»).
- **Geographic services** - Services for administration and use of geographic information. For example, a map engine capable of displaying military symbols, overlay handling and basic tracking.
- **Information exchange** - Standards and solutions for information exchange nationally, with allied forces and coalition partners and with other appropriate civil agencies. Examples of this type of service include military message handling, e-mail, data links and replication.
- **Information management** - Services for the capture, storage, fusion and correlation, recovery and use of information.
- **Collaboration services** - Services for audio and video telephony and other online interaction.
- **Information security** - Public Key Infrastructure (PKI), IP encryption and other types of service to ensure confidentiality, integrity and availability.

Policy for the military adaptation and use of
information and communication technology
in the Norwegian Armed Forces

Issued by
The Royal Norwegian Ministry of Defence
Glacisg. 1
P.O. Box 8126 Dep
NO-0032 Oslo

Tel: +47 23 09 80 00 - Fax: +47 23 09 61 05

www.mod.no

ISBN 978-82-7924-064-8

FORSVARSDEPARTEMENTET

The Ministry of Defence