284 23-3064 Uen Rev B

C4ISR FOR NETWORK-ORIENTED DEFENSE

October 2006

White Paper

Service-based C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance) solutions for network-oriented defense will improve operational capabilities, flexibility and cost efficiency. The realization can be evolutionary, starting with networking of existing systems.

ERICSSON

TAKING YOU FORWARD

Contents

1 Executive Summary

The prime objective of network-oriented defense concepts – such as Network-Centric Warfare (NCW), Network Enabled Capability (NEC), and Network-Based Defense (NBD) – is to improve and extend operational capabilities by connecting decision makers, effectors, and information sources to a common network. Advantage is taken of the great advances within civilian information and communication technology.

In the approach presented here, service-based C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance) solutions for network-oriented defense are based on

- Service-Oriented Architecture (SOA)
- Networks-of-networks using a variety of communication technologies
- Situation adapted combinations of units and systems

The functionality of the interconnected systems is made generally available as “services on the net”, and the ultimate goal is that all systems shall be connected. By means of real time configuration of interacting systems, it is possible to combine the functionality of the most useful systems in each situation.

The approach is aimed to improve and extend C4ISR capabilities such as high-performance communication; gathering, processing, and dissemination of situation information; decision quality and speed of command; and interoperability. The service-based C4ISR solutions are flexible, secure, robust, and cost efficient. The approach gives the possibility to interconnect and utilize existing system, and to extend capabilities by successively adding functionality and systems in an evolutionary way. Suitable technology and solutions for implementing service-based C4ISR solutions for network-oriented defense exist and an implementation is possible to initiate today.

The service-based C4ISR solutions lead to improvement of traditional military capabilities. Furthermore, the solutions also provide new capabilities that make it possible to conduct a broad spectrum of operations. The service-based C4ISR solutions offer opportunities to deal with even the most challenging threats and environments, today and in the future.

Altogether, the service-based network-oriented defense concept offers a path to allow defense organizations to develop excellent operational capabilities in a cost efficient way.

2 Introduction

There is today a worldwide trend toward a greatly extended use of information and communication technology in defense systems in order to improve operational capabilities and cost efficiency. In most cases the main approach is a strive toward network orientation, meaning the formation of networks of interconnected decision makers, effectors, information sources etc. This development takes advantage of the great advances within information and communication technology. The network-oriented defense concept has been developed in slightly different directions and has been given names such as Network-Centric Warfare (NCW) [1], Network Enabled Capability (NEC) [2], and Network-Based Defense (NBD) [3].

The concept is aimed to improve and extend important capabilities such as

- Information gathering, processing and dissemination.
- Decision quality and speed of command.
- Collaboration between different units and different organizational levels.
- Flexibility in the use of defense units and systems.

These enhanced capabilities also involve new or developed methods for how to conduct operations. This means that the introduction of these capabilities may result in a profound transformation of defense organization, regarding the use of technical system but also regarding, e.g., tactics and training.

The development of the concept also coincides with the efforts to adapt to the global political strategic situation in the post cold war era with its fragmented and sometimes diffuse security threats. Among other things, this situation has put emphasis on the interoperability aspects of the network-oriented defense concept.

In this white paper, C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance) solutions for network-oriented defense are presented. The solutions are based on

- Service-Oriented Architecture (SOA)
- Networks of networks using a variety of communication technologies
- Situation adapted combinations of units and systems

The approach gives the possibility to interconnect and utilize existing systems in a more cost efficient way, making the functionality of these systems generally available as “services on the net”. The approach also involves utilization of widely used civilian technology whenever it meets the requirements relevant in each application.

Figure 1: In the network-oriented defense concept decision makers, effectors, and information sources are interconnected in a common network. Functionality of a system is available as “services on the net”.

There is today an excellent opportunity to realize the great potential of a service-based and network-oriented defense concept, starting with networking of existing systems followed by an evolutionary growth, i.e. a gradual process involving successive improvements.

The concept of network-oriented defense is also well in harmony with the principles of Effects-Based Operations (EBO), which is a concept that makes use of a broader and more strategic perspective in all actions in a conflict and involves tailoring of the efforts in order to achieve a desired outcome in the broader perspective [4].

Many of the ideas of network-oriented defense are relevant also in other contexts, e.g. within public safety and security, enterprise safety and business efficiency. For instance, methods and solutions for interoperability are very relevant for collaboration between civilian agencies and authorities. A concept closely related to network-oriented defense is described in the Ericsson White Paper “Communication and Information Services for National Security and Public Safety” [5].

3 Service-Oriented Architecture

The C4ISR solutions for network-oriented defense are based on a Service-Oriented Architecture (SOA). The service concept means that the functionality of a communication, information or command & control system is made available as services that can be accessed by any authorized user connected to the network, mobile or stationary. The concept is in accordance with the general trend within the information and communication industry.

3.1 Overall architecture

The basic idea behind the service-oriented architecture is to avoid large “stovepipe” systems, designed only for a specific purpose, and instead make it possible to combine individual systems into systems-of-systems. This means that the individual systems, that may be geographically distributed, are used as modular building blocks that are interconnected. The output of these building blocks is made available as generally accessible services permitting the blocks to be combined in different ways. Among the advantages with such an approach are a more cost efficient use of systems, and the possibility to adapt to the needs of the particular situation by reconfiguration in real time of the building blocks into so-called situation-adapted systems.

The overall architecture of C4ISR solutions for network-oriented defense is depicted in Figure 2. The two main parts are Services and Infrastructure. The Services part includes services for Communication & Collaboration, Situation Information, Information Operations, Command & Control and Engagement Support. The Infrastructure part includes a Control Layer, a Convergence Layer and a Connectivity Layer.

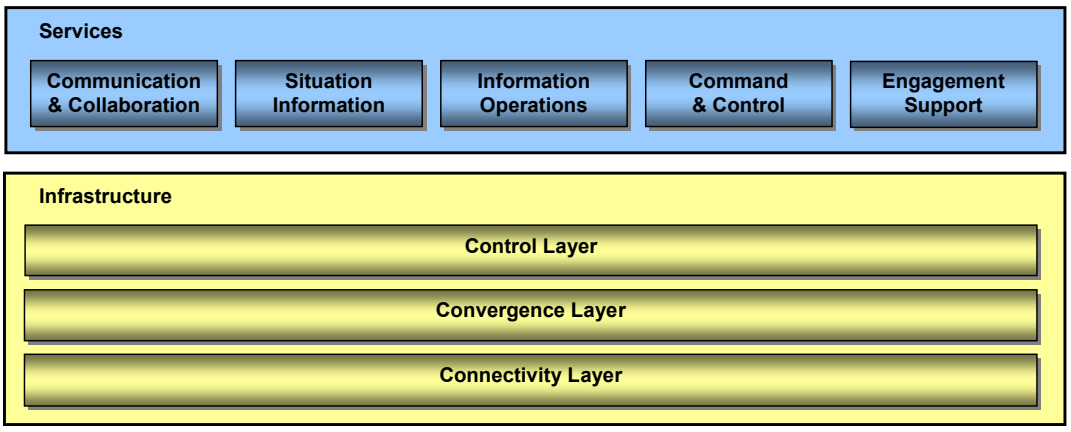

Figure 2: Service-oriented architecture for network-oriented defense.

The Communication & Collaboration services provide functionality for communication and information sharing. Situation Information services involve gathering, processing and dissemination of situation information. Information Operations include services for assessment and influence on other parties' situation information and also for protection of the own situation information. Command & Control involves services for decision support and order handling. Engagement systems and effectors are connected to the C4ISR environment and are involved in the information flow and controlled by Engagement Support services.

The Control Layer contains functionality and support services that are used to give all the services mentioned above the required characteristics and features such as security, mobility, and accessibility. The Convergence Layer ensures that connectivity can be accomplished in a unified manner based on the Internet Protocol (IP) and that different types of fixed and wireless networks, belonging to the Connectivity Layer, can be used.

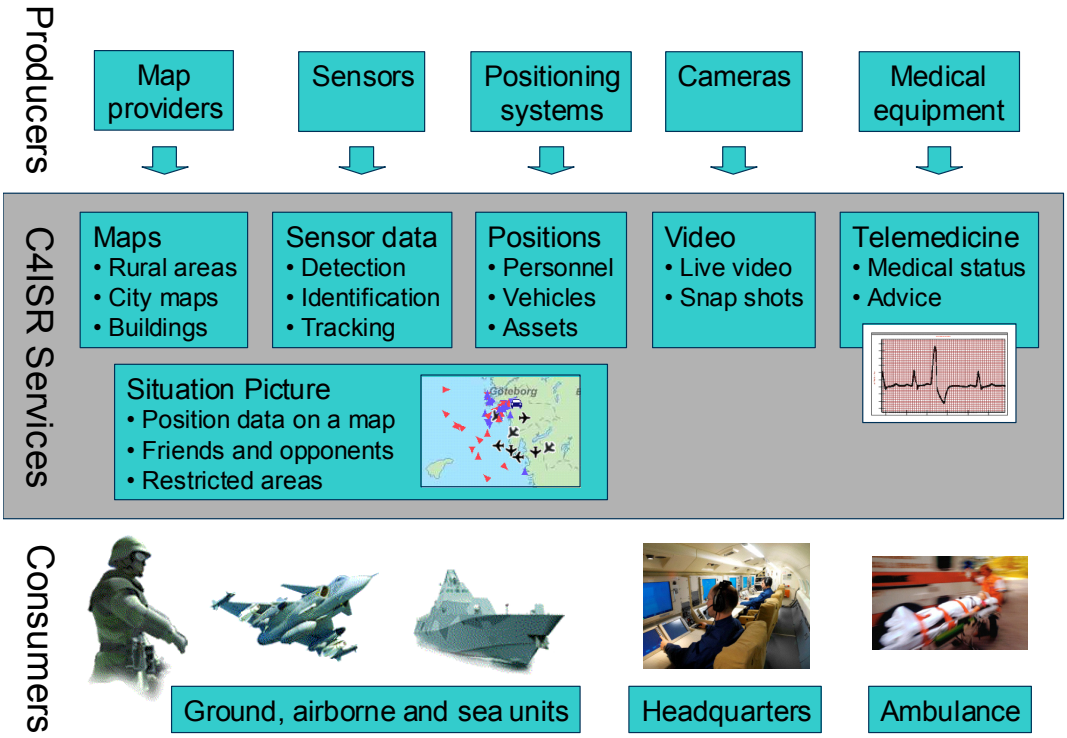

Figure 3: Examples of C4ISR services, their producers and consumers. The situation picture service is an aggregation of the map, sensor data, and positioning services. All services can be used by any authorized consumer.

3.2 System principles

The C4ISR “system” is not to be regarded as a single system, but rather as a distributed system-of-systems where each system is producing and/or consuming services. A cornerstone in the service-oriented concept is the separation of the producers and consumers of functionality. The services are not necessarily produced for a single particular purpose; they are instead produced independently of the consumers and are made generally available for any authorized consumer to use.

The systems-of-systems concept also means that services and information residing in existing and new systems are integrated and aggregated. Thereby services and information with a higher value are created.

Neither the infrastructure nor the technical systems producing the services need to be new systems, even though new systems may of course also be included. Existing legacy systems can be integrated into the service environment by means of encapsulation. The C4ISR solutions are completely scalable; services and capabilities can be further developed and the range of services and systems can be extended over time in an evolutionary fashion.

Another very important principle is that of situation adaptation. The objective is to use the resources, including human individuals, technical systems and information, that are best suited in a given situation. To enable this, the services to be accessed by different users, and the combination of technical systems producing the services, do not have to be predetermined but can be adapted according to the needs at each time. The system combinations can be predefined, or can be defined and connected in runtime, for an example see Figure 4. In the case of resource conflicts, intelligent priorities can be set.

Interoperability with external organizations, e.g. in international assignments, is also based on the service concept. Systems belonging to external organizations can be connected using bridges enabling their functions to be exhibited according to the service concept in the same way as the internal systems. However, different systems and organizations often use different information models and different operational processes. Therefore, in addition to the technical bridges, providing connectivity and common syntax, agreements concerning information exchange models and content interpretation, i.e. semantics, and collaboration methods on the operational level, must be maintained.

The C4ISR solutions are based on an open architecture using open standards on various levels and commonly used interfaces – some examples are IP, the information exchange model JC3IEDM, and XML. Common standards and interfaces facilitate compatibility among new systems as well as encapsulated legacy systems. The open standards also allow different system and service developers to be engaged.

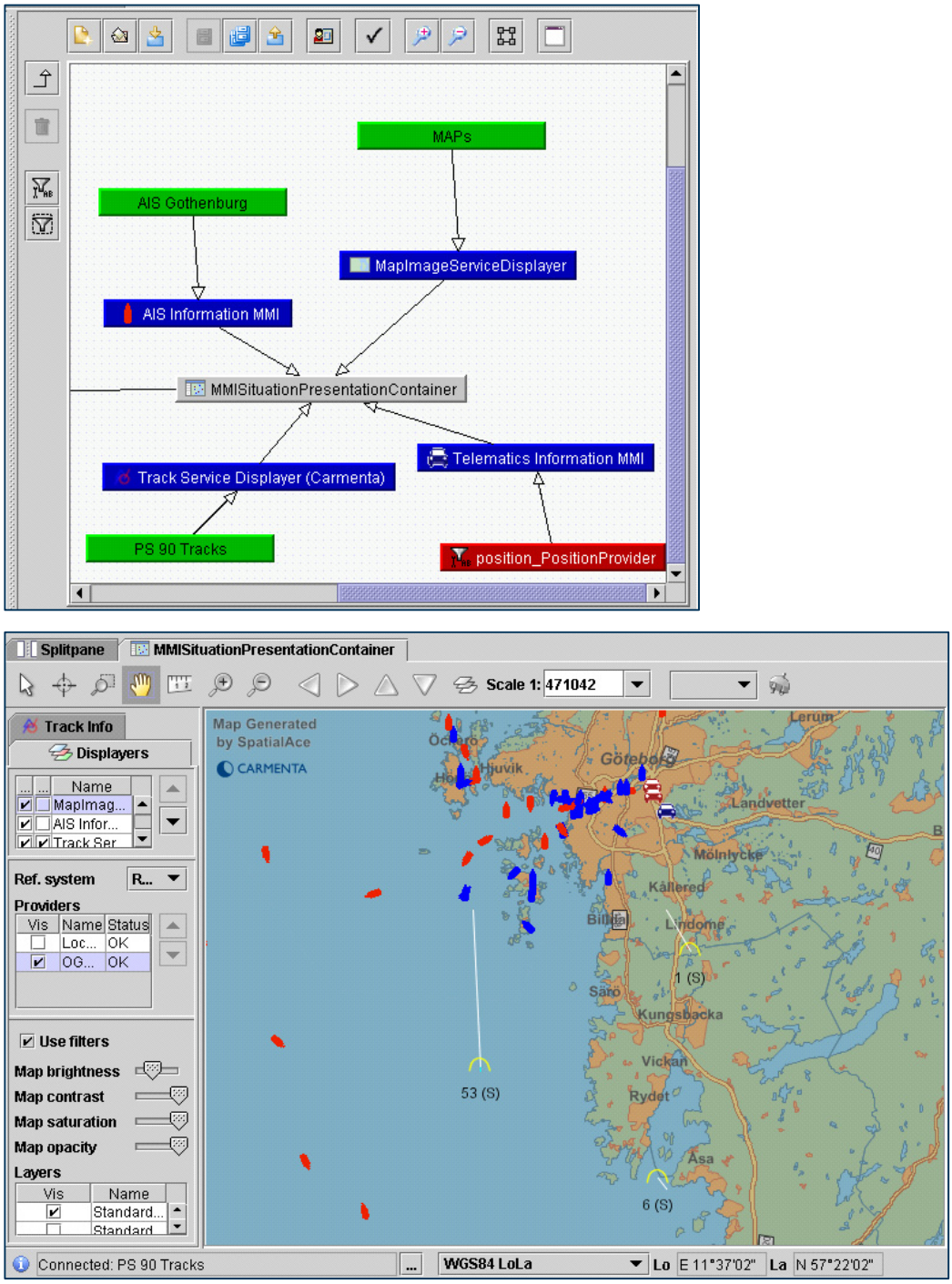

Figure 4: Example of a tool for building situation-adapted systems. The upper panel shows the configuration window with a number of interconnected services. The lower panel shows the corresponding result, in this case a combined ground, air, and sea situation picture.

3.3 Security aspects

Defense organizations usually have their own specific security policies and the C4ISR solutions must therefore be capable of supporting the appropriate overall security policy for each organization.

The technical security solutions are only parts of the overall security solutions related to the respective security policies and must be coordinated with the solutions regarding methods, organization, and competence. Technical solutions are used to fulfill security objectives such as identification and authentication, authorization and access control, protection against intrusion and attacks, maintaining confidentiality, integrity and privacy of information, non-repudiation, and auditing. The quantitative requirements related to the different security objectives should be dynamic and situation adapted. The requirements are determined by the process of risk management in order to keep a balance between security and other system performance properties; the preferred balance depends on the operational situation.

The security solutions are often based on concepts such as classifying information, maintaining different isolated security zones, and defining user roles with respect to access and authority. Separation of different information classes may be facilitated by an infrastructure consisting of overlaid virtual networks, all using a common physical network, in combination with physically separated access equipment for different security domains. It is also necessary to have a “reaction force” in the network that can take care of an intrusion before a grave harm has been caused.

The technical components for implementing the security solutions include encryption, firewalls, digital signatures and certificates, user smartcards, logging, and of course also physical mechanisms such as restriction of admittance.

3.4 Communication technologies

To have a separate dedicated communication network for each operational context is expensive and often superfluous. The approach presented here supports the use of network of networks utilizing a variety of communication technologies, so-called heterogeneous communication networks. The communication networks may have different origins: defense, governmental, and public, and may include tactical radio, broadband networks, fixed telephony, and mobile networks.

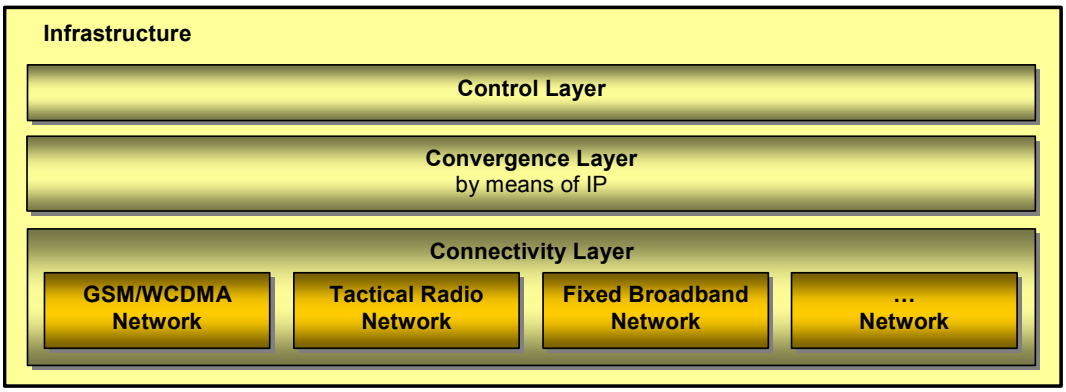

Figure 5: The SOA infrastructure part. The Connectivity Layer can contain networks based on different communication technologies (examples are displayed above) that are interconnected by means of IP in the Connectivity Layer.

The mechanism to create a network of interconnected networks is to use the Internet Protocol (IP) as the common communication protocol. IP is a standard that governs addressing and routing of data packets through different types of underlying transmission networks, both fixed and wireless. An IP network of networks can be used for all types of local and global communication like voice, video, real-time data, messaging, Internet traffic etc. Dedicated non-IP networks may sometimes be necessary, e.g. in cases of extreme real-time performance requirements.

The main advantages of the networks-of-networks approach are:

- Combined use of different networks leading to improved efficiency and a reduction of equipment and operational costs, as compared to traditional vertically integrated networks (“stovepipe networks”).
- The networks-of-networks can be dynamically composed depending on where network resources are needed for the moment.
- Due to the distributed network architecture and packet-based transmission there is no single point of failure. If a piece of equipment is damaged, others continue to operate and joint communications are maintained using alternative paths. If all connections to other networks are lost, sub-networks are formed that may operate autonomously and later be reconnected.

The networks-of-networks approach puts special requirements on infrastructure functionality like routing, addressing, mobility, quality of service, and security. In order to fulfill these requirements it is advantageous to make use of IP version 6.

The infrastructure can to a large extent be based on public communication technologies with necessary additions to fulfill security, robustness, and flexibility requirements of interoperating defense organizations and other authorities. These solutions can at the same time be cost efficient and make use of the most advanced components available. Several programs around the world are currently exploring these opportunities, e.g. in creating solutions for tactical communication networks based on widely used telecommunication technologies.

The mobile telecommunication technology GSM is used by more than two billion people across more than 200 countries. Its successor WCDMA has a more efficient use of radio spectrum and an improved data communication capacity. Communication systems that make use of GSM and/or WCDMA can be adapted for different environments and made transportable and placed in containers, mounted on vehicles, or even carried by people.

4 Benefits

The proposed approach to service-based C4ISR solutions for network-oriented defense has several distinct benefits that will enhance and improve operational capabilities:

- **Flexibility** is achieved on all time scales, from long-term system development to momentary adaptation to an unexpected situation.
    - Flexibility on the time scale of new system development is facilitated by the modular architecture, admitting easy addition of new types of systems and services without changing the existing systems. By removing dependencies between different types of functionality, different systems can follow their own lifecycles.
    - Flexibility in developing the capabilities of an organization is achieved by the situation adaptation concept in that new or improved services can be obtained by combining systems and services in new ways, or by successive addition or replacement of systems. This is done as a “runtime” feature which makes it very cost efficient since only a small technical development effort is required. To a large extent, organizational staff can accomplish this kind of development without involving external technical specialists.
    - Flexibility in preparing an organization for a mission or operation is obtained in that the C4ISR solutions can be adapted to the needs of different situations. This flexibility is crucial for achieving organizations that can effectively handle the full spectrum of conflicts.
    - Flexibility within an ongoing operation, e.g. when an organization is faced with an upcoming new situation, is again achieved by the possibility to adapt services to the needs of a specific situation. The systems behind the services can be allocated in a way that gives adequate performance and enables efficient collaboration between the different actors that are involved. If necessary, continuous adaptations to changes during the operation can be obtained.
- **Cost Efficiency** results from:
    - Existing systems and infrastructure are integrated and utilized; this creates additional value without the cost for acquisition of new systems.
    - Full advantage of the technological development generated by the commercial driving force of mass markets.

  - The fact that there is large degree of freedom in how resources can be combined leads to an optimized use of resources. For various purposes and in various types of conflicts, resources can be allocated and combined to give the right performance. By selecting just enough resources in every situation, unoccupied resources are made available for other purposes. This means that there is a less need to duplicate similar resources.

  - The enhanced potential for collaboration admits cost saving through sharing of systems, functions, and capabilities between different units and different organizations.

- **Evolutionary growth,** i.e. a gradual process involving successive improvements, is facilitated by the service concept, situation adaptation, and the concept of modular system-of-systems, which make it easy to add new functionality, services, and systems. As a consequence, it is not always necessary to acquire a “complete” C4ISR system all at once; instead one can primarily concentrate on solutions for immediate operational needs and then successively add functionality in an evolutionary fashion.

- **Interoperability** is based on the service concept. External systems can be accessed via bridges enabling their functions to be exhibited according to the service concept and enabling service access for authorized users. Interoperability is further facilitated through the use of open standards and established and widely used technologies.

- **Ubiquitous Service Availability:** The service-based C4ISR solutions and the infrastructure consisting of networks-of-networks utilizing heterogeneous communication systems imply that all authorized and connected users, mobile or stationary, can access in principle all functionality, anytime and anywhere.

- **Robustness** is a characteristic of both the services and the networks-of-networks.

  - Different producers may provide the same type of service and the service concept allows consumers to find and use services produced by other systems if some producers disappears.

  - Connectivity for all services is based on IP, which was designed to deal with problems where some of the infrastructure is absent. The long establish vision that everything will be delivered using a packet-based method is coming into reality. It should be noted that it was more than 30 years ago when ARPANET was commissioned by the US Department of Defense for research into networking. The principles and technology worked then and it works now; in fact, it works even better now. And the continued evolution is expected to yield an even better experience.

- **Security** in the C4ISR solutions is achieved by adapted security functions based on widely used communication and information technologies. Useful technologies already exist and are expected to be further developed. A driver for this development is the emphasized need for usable security solutions within various parts of the society. However, defense organizations will probably continue to require specific solutions for certain needs.

Service-based solutions for network-oriented defense are as a whole superior to solutions based on traditional stovepiped systems and a so-called platform-centric defense. The C4ISR solutions can be adapted to the needs of different situations and allow units to operate across organizational as well as technological borders. Furthermore, the solutions lead to cost efficiency and the possibility to give the desired information and functionality **to anyone authorized, anytime, anywhere.**

5 C4ISR Capabilities

The approach presented here for the network-oriented defense concept leads to a wide range of opportunities to create exceptional C4ISR system capabilities. Below follows a discussion of some aspects of the capabilities within the service areas depicted in Figure 2.

5.1 Communication & Collaboration

Improved communication based on networks-of-networks and heterogeneous communication systems – including widely used technologies such as GSM and WCDMA as well as dedicated defense communication technologies – is at the heart of the network-oriented defense concept. Communication with high capacity and performance is a main driver for the concept as a whole, even though adaptations can also be made to situations where only low capacity communication is available.

Authorized people and systems in the network will, anywhere and anytime, be able to use secure and robust high quality communication services, e.g. for voice, data, video, and group call. Compatible communication together with the service-based interoperability and other collaboration services facilitate information sharing and a multitude of other new opportunities for collaboration both within and between organizations.

5.2 Situation Information

The service-based network-oriented defense concept together with widely accessible high-performance communication services fundamentally change the basis for the capability to achieve situation information. This capability is taken to an entirely new level:

- Gathering of information is obtained from a substantially increased number of sources of different kinds: sensors, intelligence, databases, collaborating authorities and organizations, and other external sources such as news, media, weather forecasts, websites etc.
- Processing and fusion of information is used to create situation information that is accurate, with a low level of ambiguities, and that fully utilizes the complete underlying information set. This is an area in rapid development due to advances in technology and methods.
- Role-based situation pictures, i.e. excerpts of the situation information, can be accessed by any authorized user anywhere and anytime.

The above promotes trustworthy and recognized situation pictures, shared in real time, that support all actors in obtaining situation awareness, i.e. an understanding of the overall situation. The above also enables access to key information for different types of actions; the critical piece of information required for an action often exists somewhere – it is all about getting it where it is needed.

Furthermore, the above leads to improved opportunities to combine information from complementary sensors – such as radar, electro-optics, and signal intelligence sensors – and other sources. Thereby, it is possible to obtain accuracy and quality meeting the challenging operational needs, e.g. regarding ground situation pictures in urban environments.

The service-based concept and the modular principle facilitate flexible and adaptive configuration of surveillance system-of-systems, including various sensor systems and their platforms. Surveillance management can be performed to continually optimize the use of sensor resources in order to adapt to the dynamical environment of an operation. For instance, in a situation with a temporary threat or a specific planned activity there may be a need to move mobile platforms to preferable geographical locations, tune the sensor usage, or to add supplementary sensor resources.

Altogether, the service-based network-oriented defense concept results in enhanced situation awareness based on common situation information.

5.3 Information Operations

The area of information operations encompasses intelligence, influencing and suppressing the opponent's situation information, protecting the own situation information, and managing the information flow to external parties. Intelligence includes, e.g., human intelligence and signal intelligence. One interesting aspect of intelligence is the assessment of the opponent's situation information. Information operations may be conducted in the human dimension, in the electromagnetic dimension, as well as in the information network dimension, so-called computer network operations. Within all these fields the service-based network-oriented defense concept can lead to considerable improvements.

Intelligence capabilities are improved in much the same way as the capability to achieve situation information. Particularly important is the possibility to manage a large number of sources and the wide access to high-performance communication services. When being in control of the public infrastructure, this can be used for secure communication, e.g. to support human intelligence, as well as a useful source of intelligence from opponent use of public infrastructure.

The capability to influence and suppress the opponent's situation information is improved through a greater possibility to perform coordinated actions in time and space, e.g. electronic attacks against the information systems of the opponent. This is partly due to the fact that effectors and other resources are connected to a common network, and partly due to the access to high quality situation information. Furthermore, in order to counter the imposed actions the opponent may change its behavior, which gives an additional opportunity to achieve information about the opponent. The areas of situation information and information operations are thus closely related and the activities should be coordinated in order to fully exploit all opportunities.

The network-oriented approach can also lead to considerable improvements in the protection against information operations directed toward the own situation information. The extensive information gathering and processing reduces the vulnerability against deception. Redundancy and graceful degradation features of the service-based network-oriented defense concept will enhance electronic protective measures and the ability to keep a low electronic signature. For instance, with sufficient knowledge of emitters the surveillance systems can be dynamically adapted to mitigate jamming. Alarming and subsequent distribution of acquired jamming information to individual sensors and command & control nodes also enhance the surveillance system robustness.

Management of the information flow to media and other external parties is an important part of effects-based operations. Thorough situation information, such as awareness of the situation in a wide sense including opinions among the civilian population, supports this capability. The system can give access to suitable information content to be released, and selection of target groups is also facilitated.

5.4 Command & Control

The service-based network-oriented defense concept leads to enhanced quality and speed of command & control. The concept encompasses several ways to obtain accuracy, flexibility, speed, and efficiency of the command & control process, thereby leading to decisions that give as favorable operational effects as possible.

Although the situation information will always be limited for decision makers in a military operation, the improved availability of information in a network-oriented defense gives a much more thorough basis for decision making on all kinds of organizational levels. The large flexibility of a service-based network-oriented defense, in particular the situation adaptation concept, allows for an increased number of action alternatives. This, together with the improved availability of information, opens up new possibilities for effects-based operations. In order to make full use of these possibilities there is a need for development of the operational concepts of command & control.

Sharing of information about ongoing activities between various decision makers facilitates synchronized parallel planning and effectuation of operations. In particular, an improved coordination between organizational levels can be achieved. Parallel planning can lead to shorter decision cycles and gain of initiative, which are often decisive factors in a conflict situation.

The networking environment will enable the rapid formation of virtual decision cells consisting of participants that can be selected regardless of their geographical location. Together with advanced collaboration support, this permits dynamical command structures and geographical distribution of command & control in an efficient way.

Other essential factors that improves decision quality are the ubiquitous access to advanced support services, e.g. for resource optimization, decision support, and simulation including evaluation of possible action alternatives.

Finally, the network-oriented concept gives an improved capability of distribution of orders and commander's intent throughout the organizations.

The service-based network-oriented defense concept opens up many new opportunities for how to conduct command & control in order to increase operational effectiveness. The best way to explore these opportunities is by trying out new ways of conducting operations in real-life situations. The ability for evolutionary growth makes it possible to introduce new capabilities in a stepwise fashion.

5.5 Engagement Support

Connecting engagement systems and effectors to the service-based and network-oriented environment will enhance engagement capability and cost efficiency. This is resulting from the fact that the entire range of command & control systems, effectors, and information resources are made available for the engagement functions. As an example, situation adapted sensor-to-weapon loops – that utilize the "best" information source, "best" command & control function, and "best" effector – can be established, regardless of organizational location.

The information flow involving the engagement functions is accomplished by the ordinary serviced-based C4ISR solutions whenever possible. Other specific solutions may be needed to establish a sufficient performance in critical situations. However, this does not necessarily imply the use of dedicated systems, but may e.g. involve flexible communication resources on mobile platforms.

The enhanced and improved situation information provided by the network-oriented environment will give new possibilities for achieving a balanced use of engagement based on effects-based operations principles. It will also enhance the capability of executing balanced and precise engagement in complex situations, such as in urban environments.

6 Excellent Operational Capabilities

The prime objective of the network-oriented defense concept is to improve and extend operational capabilities. This section contains examples of important operational capabilities – in particular those presenting outstanding challenges in various current conflicts – and how the service-based C4ISR solutions support successful conduct of operations through excellent operational capabilities.

6.1 Traditional military capabilities

The traditional military capabilities, like conquest of an area and surveillance of a territory, are clearly among the fundamental requirement drivers for the network-oriented defense. Certain aspects have recently grown in importance, in particular the ability to minimize casualties. This has lead to changes in preferred way of conducting operations, e.g. fewer forces on the ground and extended use of airborne operations, and more moderate and precise use of engagement capabilities. A key requirement is the ability to conduct operations according to the principles of effects-based operations, maneuverist approach, and mission command (“Auftragstaktik”).

Driven by traditional military requirements, the C4ISR capabilities have undergone a strong continuous development during the last decades, taking advantage of the emerging information and communications technology. Various C4ISR capabilities to support new preferred ways of conducting operations are also under development, e.g. the versatility and capability of airborne operations have been dramatically improved, largely due to enhanced ground situation information and coordination with ground forces. The introduction of service-based C4ISR solutions improves the above-mentioned military capabilities even further. The maneuverist way of operations and the capability to improvise are supported by means of C4ISR capabilities such as situation adaptation, dynamical decision processes, distributed collaboration and command, and rapid dissemination of key information to where it is most needed.

6.2 Broad spectrum of operations

A further set of challenging requirements on operational capabilities is generated by the recent shift in threat situations. A prominent consequence is the requirement to be able to manage a broad spectrum of operations from traditional to asymmetrical conflicts under various circumstances, including full-scale conflict, peace enforcement, peacekeeping, and reconstruction of the civil society. This also involves the requirement to be able to act within a multi-organizational coalition and to handle a changing character of an operation.

The service-based C4ISR solutions admit rapid and flexible situation adaptation to obtain an appropriate combination of units and systems in order to meet a wide variety of missions and threats. Such combinations are not limited to the resources of a singular organization, but also involve interoperability between different types of coalition partners. The relation between partners may range from full trust to loose collaboration, and may possibly change over time.

6.3 Challenging threats and environments

Another requirement that has been emphasized due to the recent shift in threat situations is the ability to deal with opponents that are not regular armed forces, but rather paramilitary units, militias, terrorist organizations etc. A further consequence of the recent shift in threat situations is the increased emphasis on the extraordinary difficult task of performing missions in urban environments. Such missions are even more challenging in situations between peace and war, e.g. peace enforcement, where very few casualties of own and opposing forces are tolerable and where disturbances of civilian activities of the normal life must be limited. Historically, such missions have lead to very high numbers of casualties and devastation of urban areas, or alternatively, necessary missions, e.g. to protect civilian populations, have been left unattended.

The service-based C4ISR solutions open up several ways of meeting the challenges concerning the variety of opponents and threat situations. Dynamical situation adaptation facilitates best use of all available resources, including non-military resources. Many valuable pieces of information often exist widely scattered throughout various forces, partners and allies. In order to deal with an elusive opponent it is of utter importance to utilize as many relevant pieces of information as possible. A key system capability is the rapid gathering of information and efficient establishment of coherent overall situation information. This is achieved, e.g., through efficient communications and systems for filing and correlating human intelligence and other types of information. Efficient information dissemination and exchange of information between all organizational levels can be achieved. A key component in this context is the extensive interoperability and collaboration with various military and civilian partners and allies, both regarding information gathering and dissemination of shared situation information.

The C4ISR functionalities discussed above are also important in order to address the huge challenges of operations in urban environments. A key capability of service-based C4ISR solutions in an urban environment is to be able to gather and process very large amounts of information, allowing a large number of relevant sources to be utilized. The sources can involve both people and technical systems, e.g. advanced sensor network for surveillance of buildings or restricted zones. The communication approach based on networks-of-networks, heterogeneous systems, and suitable mobile terminals will ensure a high connectivity even in difficult communication environments of the urban area. Even when forces are highly fragmented, this facilitates efficient gathering of information, dissemination of key information, as well as horizontal communication and collaboration. The ability for all units to utilize appropriate excerpts of the advanced situation information will support their operations in several ways: rapid decision making and keeping the initiative, finding and putting opponents out of action, avoiding unnecessary or misdirected force, avoiding collateral damage etc. Another important aspect is the possibility to operate well protected, still with good situation awareness.

6.4 Information superiority and decision superiority

The service-based C4ISR solutions discussed above can be interpreted as involving a strive towards information superiority and decision superiority. In any type of conflict, major advantages can be obtained by having a superior capability, relative to the opponent, to gain sufficient situation awareness in order to make decisions and act. Since the information need generally differ on the opposing sides, the objective is not necessarily to have more or better information than the opponent but to ensure that the information needed for the decisions and actions of the own organization can be obtained more swiftly than for the opponent.

The examples above show how the principles of network-oriented defense and in particular information and decision superiority lead to the establishment of excellent operational capabilities. When networked military and civilian resources are used in an optimized way to achieve the desired impact – then we have reached the goal of effects-based operations. Moreover, the service-based C4ISR approach makes it possible to achieve this in a cost efficient way.

7 Implementation

There are many possible ways to implement a network-oriented defense. Below follows a brief proposal for how to proceed when realizing service-based C4ISR solutions for network-oriented defense:

- **Specify the foundation.** A necessary prerequisite step is to establish common overall system principles, architecture and design rules to a level that is sufficient for detailed specification and implementation of systems within different C4ISR capability areas. This involves elaboration from basic principles such as a service-oriented architecture, networks-of-networks and heterogeneous communication systems, and situation adaptation of interconnected resources. The design rules constitute a set of governing rules for development of systems for network-oriented defense that is also a tool for reusing design solutions for recurring problems. It is preferable that this foundation is based on existing standards when applicable and also subject to further standardization.

- **Roadmap according to operational needs.** It is important to formulate objectives in terms of operational capabilities in different time frames. However, there is no general need to perform complete detailed specifications toward a long-term end-state regarding doctrines, threat situations, operational strength etc. For a network-oriented defense there does not have to be a predefined end-state. Instead there is a flexibility to continuously develop capabilities according to changing needs and technological progress and opportunities. As a first step, specifications can be prepared to a level motivated by the currently most urgent needs and that is sufficient to start developing initial operational capabilities, i.e. an implementation plan for a set of primary systems resulting in such capabilities.

- **Functional design.** Based on the roadmap for operational capabilities, technical system solutions are formulated through the functional design process. This process includes operational analysis, design of C4ISR system solutions, and evaluation to ensure that the solutions result in the desired operational capabilities. The process should be performed on a systems-of-systems level and preferable in an iterative manner.

- **Experiments and trials.** In order to have a successful development it is highly useful to continuously conduct experiments and trials to support the work on foundation, roadmap for operational capabilities, functional design, as well as system implementation. In particular, the mutual influences between operational needs and technological opportunities can be efficiently explored in this way.

- **System implementation.** The principles of service-oriented architecture allow work on different system areas to be carried out to a large extent independently of each other. The implementation plan for the primary systems can to a high degree be based on networking of existing systems.

- **Continuous evolution.** When having implemented the primary systems, related to the most urgently needed operational capabilities, the further development can be performed in an evolutionary fashion. This means that the further development of operational capabilities can be decided in successive manner.

A close collaboration between stakeholders, users and industry – from the initial specification of foundations and throughout the implementation process – is desirable in order to obtain a fruitful and innovative coupling between technological and operational driving forces.

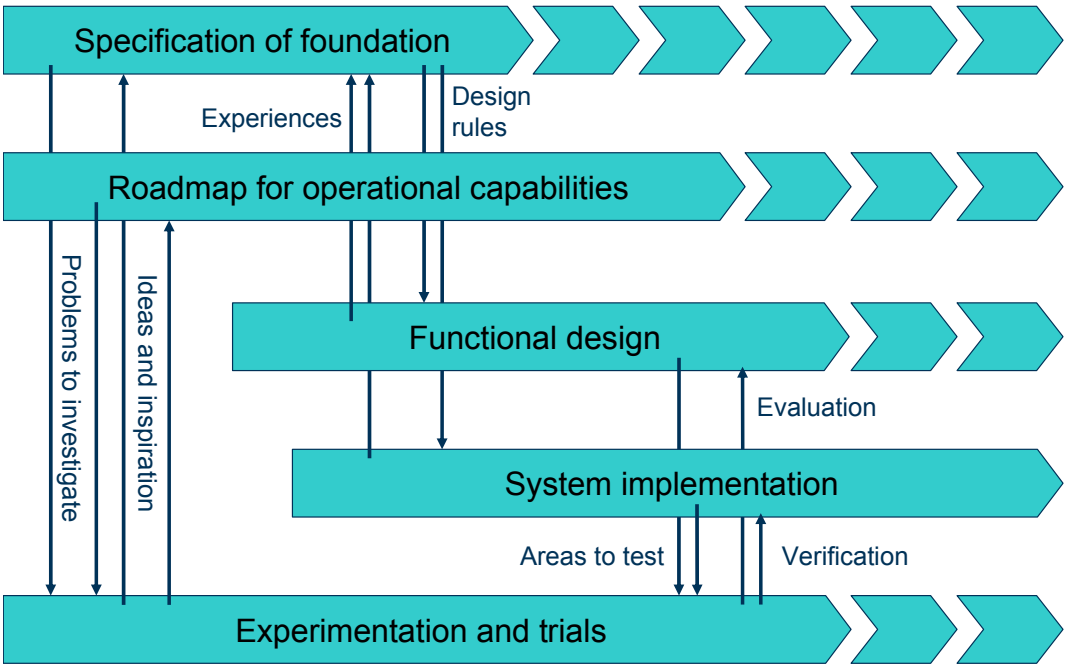

Figure 6: The proposed implementation activities and some examples of their interrelations. The dashed arrows indicate that an activity continues at a lower intensity throughout the continuous evolution.

Suitable technology and solutions for implementing service-based C4ISR solutions for network-oriented defense exist. Several organizations have already started their development, and as one example the development in Sweden is briefly described below.

Based on a decision of the Swedish parliament in 2001, the Swedish Armed Forces are currently conducting a profound transformation to a Networked-Based Defense (NBD). The technical part of the NBD transformation starts with the development of a C4ISR functions environment, named LedsystT, which was initiated with prestudies in the late 1990s and which has the objective of realizing operative systems during the time frame between 2010 and 2020.

The LedsystT project is governed by the Swedish Defence Materiel Administration (FMV) and is performed in close collaboration with industry contractors and other partners. The currently ongoing phase, that started in the autumn of 2003 and will continue until the end of 2006, has emphasis on the foundation and demonstrators. The work on foundation in particular involves design rules and architecture. The demonstrators are intended to be national test-beds for creative interaction between technology and methods development. Furthermore, functional design of the operative systems is initiated and will be further elaborated in a following procurement phase aiming at system implementation.

Interesting examples of ongoing development programs in the USA are the Warfighter Information Network-Tactical (WIN-T) and the Future Combat Systems (FCS). WIN-T is intended to be the U.S. Army's next-generation battlefield network backbone and will provide battlefield soldiers with voice, data, and video through wireless communications. FCS is the U.S. Army's modernization program consisting of a family of manned and unmanned systems, connected to a common network e.g. WIN-T. The FCS program enables a modular force, and provides soldiers and commanders with leading-edge techniques and capabilities allowing them to dominate in complex environments.

An implementation as sketched above is possible to initiate today and there are various examples of ongoing programs around the world, e.g. in the USA, UK and Sweden [6].

8 Conclusions

A coherent overall view on service-based C4ISR solutions for network-oriented defense is presented above. These solutions aim to improve and extend operational capabilities, i.e. fulfill the prime objective of the network-oriented defense concept.

The approach gives the possibility to interconnect and utilize new and existing systems in a cost efficient way, making the functionality of these systems generally available as “services on the net”. Widely used civilian technology can be utilized whenever it meets the requirements relevant in each application. One example is the GSM and WCDMA communication technologies that already bring new advanced services to millions of consumers and also can be used for solutions for network-oriented defense.

Service-based solutions for network-oriented defense are as a whole superior to solutions based on traditional stovepiped systems and a so-called platform-centric defense. The C4ISR solutions can be adapted to the needs of different situations and allow units to operate across organizational as well as technological borders. Furthermore, the solutions lead to cost efficiency and the possibility to give the desired information and functionality to anyone authorized, anytime, anywhere.

The introduction of service-based C4ISR solutions for network-oriented defense will increase operational capabilities by allowing all personnel and technical systems used in an operation, for instance decision makers, information systems and effectors, to cooperate as needed by using common networks-of-networks. In this way, forces can act as a joint and combined networked force with access to all relevant information and functionality.

Suitable technology and solutions for implementing service-based C4ISR solutions for network-oriented defense exist and an implementation is possible to initiate today. Realization of the C4ISR solutions can be effected through an evolutionary process starting with networking of existing systems.

9 Glossary

C4ISR: Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance.

EBO: Effects-Based Operations; a concept involving use of a broader and more strategic perspective in all actions in a conflict. This means consideration of the full range of direct and indirect effects of the actions that may occur in military, diplomatic, psychological, and economic areas.

GSM: Global System for Mobile Communications; second generation (2G) mobile telecommunication technology standard.

IP: Internet Protocol (version 4 and 6); a data-oriented protocol used by source and destination hosts for communicating data across a packet-switched network.

JC3IEDM: Joint Command, Control and Consultation Exchange Data Model; information exchange data model for C4ISR systems developed by the Multilateral Interoperability Programme (MIP) supported by NATO Data Administration Group.

NBD: Network-Based Defense

NCW: Network-Centric Warfare

NEC: Network Enabled Capability

SOA: Service-Oriented Architecture

WCDMA: Wideband Code Division Multiple Access; wideband spread-spectrum third generation (3G) mobile telecommunication technology standard.

XML: Extensible Markup Language; a general-purpose markup language for sharing of data across different systems.

10 References

[1] *The Implementation of Network-Centric Warfare*. The Office of Force Transformation, US Department of Defense.
http://www.oft.osd.mil

[2] *Network Enabled Capability Handbook*. Joint Services Publication 777, UK Ministry of Defence.
http://www.mod.uk

[3] Per Nilsson, *Opportunities and risks in a Network-Based Defence*, Swedish Journal of Military Technology, #3 2003.
http://www.militartekniska.se/mtt

[4] Edward A. Smith, *Effects Based Operations: Applying Network Centric Warfare in Peace, Crisis, and War*. Command and Control Research Program (CCRP), US Department of Defense.
http://www.dodccrp.org

[5] *Communication and Information Services for National Security and Public Safety*. Ericsson White Paper.
http://www.ericsson.com/technology/whitepapers

[6] Franklin D. Kramer and John C. Cittadino, *Sweden's Use of Commercial Information Technology for Military Applications*, Defense Horizon, October 2005, Center for Technology and National Security Policy.
http://www.ndu.edu/ctnsp/defense_horizons.htm