Developing a C4I Architecture for the Netherlands Armed Forces

Dick Ooms & Tim Grant

Introduction

Motivation (1) – why an information architecture?

Why would someone want to develop an information architecture? Intuitively, we all know the purpose of an architecture when we think about it in the context of a building: it embodies the grand design, what it should look like when it is finished, how the different components contribute to the overall structure and form part of it, and how the components relate to each other. The architecture relates to the purpose of the building, the functionalities for its users, and expresses the vision of the architect about how these functionalities should be realised.

All of these attributes of the architecture of a building apply to an information (-systems, -services)[1] architecture as well. We can think about an information architecture as a composition of different components or building blocks, being information services, provided by information systems, supported by networks and communication systems, and supporting business processes. Unlike in the process of realising a building, these building blocks are usually not designed, developed and put into service in the same timeframe. On the contrary, they are developed, being used and ultimately being replaced in a continuous process. This is precisely why we need an information architecture: to improve coherence between new and existing building blocks, to provide guidance for new developments, and to ensure that the entire composition of building blocks supports the business processes by providing the information services required. To provide guidance for the development of new components, an information architecture usually depicts both the current situation (the *"ist"* situation) and the ideal situation in future (the *"soll"* situation), and provides guidance about the transition: how we should arrive from *ist* to *soll*.

Motivation (2) – why a C4I architecture and why is NLDA involved?

Development of information services, information systems and the ICT infrastructure for the Netherlands Armed Forces is guided by the Defence Information Architecture (*Defensie Informatie Voorzienings Architectuur,* DIVA). The Chief Director for Defence Information and Organisation (*Hoofddirecteur Informatie en Organisatie,* HDIO) is responsible for the development of DIVA, which is to be underpinned by a series of supporting architectures covering various architecture aspects[2] and defence policy areas[3].

[1] An information architecture defines organisational processes, the information flow required for these processes, services and systems which provide that information, and the technical means (ICT infrastructure: networks, communication systems, technical standards) required to support those systems. Such an architecture can be referred to as "information services architecture", "information systems architecture" or "ICT architecture", depending on which aspect prevails. In this chapter we will use the generic term "information architecture".

[2] DIVA Aspect Architectures cover aspects which are defence-wide and include information security and the ICT infrastructure (networks and communication systems).

[3] DIVA Sub Architectures cover policy areas such as operations (C4I), personnel, materiel, finance etc.

This is why a C4I architecture[1] is needed: it is one of the supporting architectures of DIVA. The business process it supports is the operational process. The C4I architecture defines the information flow required to support the operational process, information services that should be in place, and operational information systems which provide such services. The Commander in Chief of the Netherlands Armed Forces (*Commandant Der Strijdkrachten,* CDS) is responsible for operational policy and requirements, and for this reason also responsible for the development of the C4I architecture.

Why got NLDA involved? Since the creation of a new, amalgamated Defence Staff (*Defensie Staf,* DS) in 2005 as a follow-up of the separate staffs of the different services (navy, army, air force), various attempts have been made to create the C4I architecture, both by the DIO staff to assist CDS, and by the Netherlands Organisation for Applied Scientific Research (*Organisatie voor Technisch Natuurkundig Onderzoek,* TNO) as tasked by DIO. However, lack of capacity within DS halted further progress in this area. For this reason, CDS has requested the assistance of the NLDA to develop the first draft of the C4I architecture. It will be shown that this involvement will be beneficial for NLDA as well.

Theoretical context

The ISO-accepted *Recommended Practice for Architectural Description of Software-Intensive Systems* [ISO, 2007] defines a systems architecture as:

> *"the fundamental organisation of a (software-intensive) system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution".*

The intended purpose of developing a C4I architecture is essentially captured by *The Open Group Architecture Framework* [The Open Group, 2007]:

> *"an architecture description is a formal description of a system, organized in a way that supports reasoning about the structural properties of the system. It defines the (system) components or building blocks ... and provides a plan from which products can be procured, and systems developed, that will work together to implement the overall system. It thus enables you to manage ... investment in a way that meets (business) needs ..."*

This implies that for this research, the C4I facilities[2] of the Netherlands Armed Forces are collectively approached as one comprehensive system. This is a valid approach, since they collectively show the characteristics of a system as described in literature:

- they have a structure that is defined by its parts and processes;
- the Netherlands C4I system is a generalisation of reality;
- the various system parts have functional as well as structural relationships.

However, it should also be pointed out that, as laid down in the Netherlands Defence Doctrine (*Nederlandse Defensie Doctrine* (NDD), see [MOD NL, 2006]), deployed and

[1] Internationally, C4I has different meanings. Here we mean: Command & Control, Communications, Computers and Information / Intelligence.

[2] C4I facilities: these include operational information systems and mobile and deployable networks and communication systems.

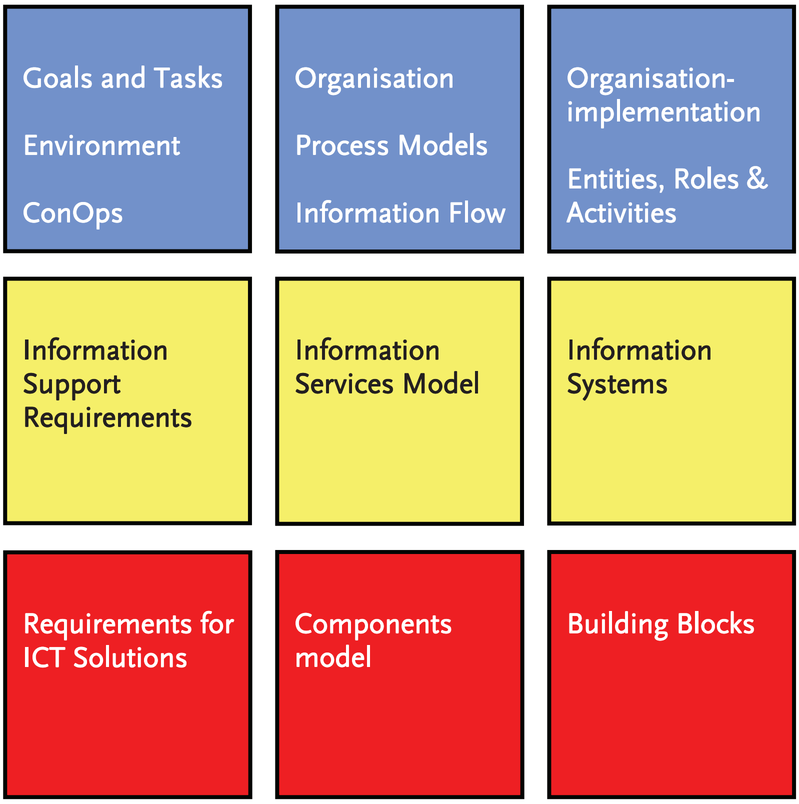
mobile operational staffs and units of the Netherlands Armed Forces assigned on a mission will in principle always be operating as building blocks in an international force. This implies that their C4I facilities should also be building blocks of an international C4I structure consisting of national contributions from participating nations. This international C4I environment points at the necessary international dimension of the C4I architecture. Indeed, the international environment defines to some degree what the national C4I architecture should look like.

There is a great variety of architectural styles in the scientific literature, such as client-server architectures, component-based architectures, blackboard systems, model-view-controller, modular plug-in architectures, layered architectures and peer-to-peer architectures. In selecting an architecture style and framework, the aforementioned international dimension of the C4I architecture should be taken into account. The C4I architecture will comply with the principles of third-generation C2/C4I system architectures, as implemented in the NATO Architecture Framework (NAF), see [NATO, 2004], the US DoD Architecture Framework (DoDAF), see [US DoD, 2004], and especially DIVA. In 2007 TNO has performed a comparative study of these and other architectures [Riemens et al., 2008], the findings of which will be used in the development of the C4I architecture. Specific tools, model views and methods developed for these architectures could be applied for the Netherlands C4I architecture and could be proposed as additions to DIVA.

DIVA has mandated the *Service-Oriented Architecture* (SOA), in which software systems are built from software services. Services are relatively large units of functionality that are not *a-priori* associated with one another, i.e., they have no calls to one another embedded in them. Examples of services in a military context are: geographical and oceanographical data support, prediction of acoustic propagation, advice on Rules of Engagements in force and related legal implications; computation of fire control solutions; analysis of large amounts of sensor data (e.g., pattern recognition); analysis of electromagnetic intercepts; advice on weapon and target selection; etc. Instead of embedding calls to one another in their source code, services define protocols that describe how the services talk to one another. Based on these protocols, services can be linked and sequenced automatically in a process known as *service composition*. Research issues in SOA include protocol standards and service composition methods. Additional research issues specific to C4I include how to adapt services and SOAs to real-time requirements; bandwidth limitations; joint, combined and civil-military interoperability; agility and reconfiguration on-the-fly; and international regulatory constraints.

DIVA is a 3-level architecture (see Fig. 1), like NAF and DoDAF. The upper layer contains the business processes, the middle layer the information services which support the upper layer, and the bottom layer contains the technology required for the middle layer. For the C4I architecture, the business process is the operational process, for which the OODA Loop[1] will be adopted.

[1] As developed by Boyd. OODA: Observe, Orient, Decide, Act



Goals and Tasks Environment ConOps	Organisation Process Models Information Flow	Organisation-implementation Entities, Roles & Activities
Information Support Requirements	Information Services Model	Information Systems
Requirements for ICT Solutions	Components model	Building Blocks

Figure 1. The DIVA 3 layer framework

Purpose, scope and structure of this chapter

This purpose of this chapter is to provide an overview of the progress made to date in developing a C4I architecture for the Netherlands Armed Forces. It starts with a discussion on the intended purpose and scope of the C4I architecture, because as prescribed by DoDAF, purpose and scope are the first subjects one has to deal with when developing an architecture, as they provide direction for all further activities. Once these have been defined, we take a quick tour around the C4I world, defining some (potential) challenges. These relate to some research issues mentioned above: bandwidth limitations and interoperability. Subsequently, it is shown how the C4I architecture could assist in coping with those challenges. Finally, we address the research into the actual development of the C4I architecture: an overview on the method of work adopted to arrive at the intended C4I architecture for CDS, the progress to date, and how this effort will be beneficial for the NLDA as well.

Purpose and scope

Purpose

Definition of the purpose of an information architecture could help to avoid a common pitfall in the world of information architectures: their size and level of detail, as developed by (over)enthusiastic information architects, tend to grow out of proportion, compared with the actual application of the end product, and thus the architecture seems to become a goal in itself[1]. To avoid this trap, the practical purpose of the C4I architecture as viewed by the various stakeholders should be investigated from the outset[2]. The results of a first attempt are shown in Table 1. In addition to CDS and DIO, the following primary stakeholders have been identified: the Defence Materiel Organisation (*Defensie Materieels Organisatie,* DMO) which is responsible for the management and execution of C4I projects to realise C4I requirements as stated by CDS; the Centre for Automatisation of Mission Critical Systems (CAMS), which is responsible for the development of naval C2 systems, and its army-counterpart: the Command and Control Support Centre (C2SC), which is responsible for development of land-oriented C2 systems[3]. The major operational commands (maritime, land and air) are primary stakeholders as well, being the major users of C4I services and systems and as such involved in the identification of future C4I requirements. The required level of detail of the C4I architecture can thus be derived from its purpose, as viewed by its primary stakeholders.

Table 1. Primary stakeholders and purpose of C4I architecture as viewed by them

primary stakeholder	purpose of C4I architecture as viewed by stakeholder
CDS	supports the translation of C4I policy into C4I requirements, provides cohesion and priorities between C4I requirements
DIO	complements DIVA, provides specific requirements for the mobile and deployable ICT infrastructure[4] (DIO's responsibility)
DMO	provides guidance for C4I project architectures, specifies technical standards, provides coherence between C4I projects
CAMS & C2SC	provides priorities, guidance and coherence for development of new systems and services, specifies technical standards
major operational commands	provides a means to articulate information exchange requirements and insight in the realisation of these requirements

Although not considered primary stakeholders[5], NATO and operational partners could also be listed as stakeholders of the C4I architecture. They have an interest in the Netherlands C4I architecture as well, since it supports cohesion and interoperability in an international environment. Finally, even the C4I industry is to some extent a stakeholder, in view of the shift to more use of Commercial off-the-shelf (COTS) and Military off-the-shelf (MOTS) products, and the possibility of Public Private Partnerships.

[1] Personal experience of the first author, confirmed in the first round of interviews with stakeholders.

[2] This is in line with DoDAF, which mandates that as a first step in the development of the architecture, its intended use should be defined.

[3] This would seem to leave out the development of air force C2 systems. A software development centre for air force C2 systems does not exist in The Netherlands for two reasons: firstly, the air force is using NATO C2 systems and proprietary C2 systems embedded in aircraft, which means less requirements for own C2 software development; secondly, some systems developed by C2SC are also in use by the air force, such as TITAAN (a deployable ICT infrastructure for deployed army and air force units).

[4] The deployed and mobile ICT infrastructure is comprised of deployable **networks** to support deployed operational staffs and units, and deployed and mobile **communication systems** to create networks among mobile units and to link deployed and mobile networks into larger networks and into the static ICT infrastructure.

[5] They are not listed as primary stakeholders because they do not define the required level of detail of the Netherlands C4I architecture.

Scope

The definition of the intended scope of the C4I architecture is closely related to discussion and even controversy about the responsibility for the armed forces deployable and mobile ICT infrastructure[1]. This is a sensitive issue in the operational world, because the deployable and mobile part of the ICT infrastructure is considered to be essential for deployed and mobile operational forces. This discussion can be traced back to the creation of DIO. At that time this caused discussion about the remaining responsibilities of the staffs of the various services (navy, army, air force). Since its inception, DIO has been responsible for the defence-wide information architecture, but the staffs of the services retained their responsibility to state, fund and realise requirements for their own mobile and deployable ICT infrastructure. When in 2005 the separate staffs of the services amalgamated into the new Defence Staff, the topic of discussion turned into the delineation of responsibilities between DIO and DS. A remaining responsibility for CDS was identified to state requirements for the deployable and mobile ICT infrastructure, while DIO retains the overall responsibility for the defence-wide ICT infrastructure: fixed, deployable and mobile.

Translated into architecture terms, this means that DIO is responsible for the DIVA aspect architecture of ICT Infrastructure, referred to as the Communications and Networks (aspect) architecture. CDS is responsible for the C4I architecture (a DIVA sub-architecture), which will articulate specific requirements, from an operational point of view, for the deployed and mobile ICT infrastructure. These requirements feed into DIO's Communications and Networks (aspect) architecture. Similarly, the C4I architecture will formulate specific requirements for information security systems and services, which feed into the Information Security (aspect-) architecture[2], and other requirements e.g., regarding operational logistics, which are catered for by other sub-architectures.

The discussion about scope is more than the reflection of old "territorial battles", which have by now been settled. It reflects a broader development: from "stovepipes", i.e. different specific ICT infrastructures for different services and different policy areas such as operations and logistics, into a common ICT infrastructure which supports all deployed and mobile staffs and units, and provides services for all policy areas.

C4I challenges

First we list some C4I challenges, both generic and specific for the Netherlands C4I situation. Subsequently we will show how a C4I architecture could help to cope with these challenges.

[1] The following information about internal discussion on scope and responsibilities is derived from personal author inside knowledge (from the first author), who served at the time as department head in the Naval staff and in the Defence staff. It provides useful contextual information and illustrates the shift from separate to common, from service-specific to joint systems and infrastructure.

[2] The Information Security architecture is a DIVA aspect architecture which is the responsibility of the Netherlands Defence Security Authority (*Beveiligings Authoriteit, BA*).

Common C4I challenges

In general, C4I systems have the following characteristics in common, which set them apart from "ordinary", i.e., non-operational information systems and which pose a challenge both for their design and for the supporting ICT infrastructure:

- **unique real-time requirements:** C4I systems supporting the C2 process are often real-time systems (e.g., supporting weapon engagements and providing the air picture) as opposed to most business-oriented processes[1], which generates specific requirements for processing speed and bandwidth;
- **bandwidth-limited environment:** C4I systems often have to operate in a bandwidth-limited environment[2] (mobile military communications and networks), which generates specific requirements for bandwidth-efficiency and -management;
- **interoperability and agility:** C4I systems and the supporting ICT infrastructure often operate in a dynamic environment with ad hoc arrangements, and a varying composition of partners: different forces, nationalities, non-governmental organizations, etc. The configuration of military units often changes on-the-fly during an operation, and the C4I system must itself change configuration accordingly. This generates requirements for interoperability (joint, combined, civil-military) and agility;
- **international architecture dialogue:** the international military C4I community is very much involved in the development of C2 concepts, C4I systems, the supporting ICT infrastructure, and in the choices to be made in the architectural development, which evolve in an ongoing international dialogue. For non-operational information systems used by the armed forces, one can and must conform to international standards that cannot be influenced, or even COTS;
- **unique security requirements[3]:** operating in an international coalition involves sharing of sensitive information and transport of information between national networks. At the same time, these networks carry highly classified national information that cannot be shared. Technical solutions should be accredited by all parties participating in the coalition.

C4I and NEC

C4I systems and the supporting deployable and mobile ICT infrastructure are an essential requirement for the realisation of the concept of Network Enabled Capabilities (NEC). The planned, phased realisation of this concept is laid down in the NEC Action

[1] Some non-military information systems have real-time requirements as well, such as Air Traffic Control and bank transactions. However, this is not true for the non-operational information systems used in the armed forces, which are non real-time. So, within the military context the distinction is valid. Moreover, non-military real-time systems do not require the same mobility and bandwidth as C4I systems. So, the combination of listed characteristics set C4I systems apart from military non-operational systems and from non-military systems.

[2] Some non-military information systems operate wireless as well, but mostly operate within commercial broadband coverage, which is not true for mobile operational units.

[3] Some non-military information systems also have special security requirements, but these are accommodated by commercially available products. C4I systems require specific non-commercial security solutions, which are to be certified at the national government level, and if necessary by NATO or partners.

Plan[1] which provides goals and milestones. C4I developments have to be synchronised with the planned realisation of NEC.

A specific requirement for Netherlands operational staffs and units is to become "*net ready*", i.e., to be able to make their weapon, sensor and C2 capabilities available to cooperating staffs and units, and vice versa: to be able to make use of such capabilities offered by cooperating staffs and units. While this requirement is recognised in general, translation into specific C4I requirements proves to be difficult.

C4I stovepipes

The term "stovepipe" refers to a C4I system which is dedicated to a specific service (navy, army, air force) or to a specific transmission channel, or a specific discipline or specialisation, or in another way shows a shortfall in the characteristics which are nowadays required in a network enabled battle space. These requirements are relatively new, which explains why many in-service C4I systems still show some stovepipe-characteristics. Until as recent as 2005, in the Netherlands Armed Forces each of the three main services developed its own C4I systems and supporting deployable and mobile ICT infrastructure, without much coordination with the other services. For many years, being interoperable with international partners was of far more importance than being interoperable within the Netherlands Armed Forces.

Of course not all stovepipes are bad. The different forces operate in different environments and this sometimes leads to other requirements and different choices. Examples are:

- restrictions in weight and space on board of military aircraft which leads to other choices for tactical datalink systems (i.e., only Link 16) than in the maritime environment, where coverage is the driver for continuation of use of HF datalink systems such as Link 11 and its successor Link 22, in addition to Link 16 for major units;
- interoperability at unit-level required for maritime operations, which has lead to extensive standardisation for communications equipment and operational information systems (i.e., MCCIS)[2], unlike in the land environment, where national internal interoperability prevailed in the past, and the approach now is to make use of national systems, linked by a common interface;
- the use of VLF radio specifically for submarine broadcasts, because these low frequencies can penetrate the water, allowing the submarine to stay submerged while copying the broadcast.

However, many current differences cannot be explained in this way and are simply caused in the past by a lack of coordination.

[1] NEC Action Plan: a yearly updated plan, developed by the Defence Staff, which governs the implementation of the NEC concept in the Netherlands Armed Forces.

[2] MCCIS: NATO's Maritime Command & Control Information System, initially intended for NATO command posts, now also widely implemented in national maritime headquarters and on board frigates and above.

Interoperability

This important aspect was already mentioned as one of the common C4I challenges. In an ideal situation, operational staffs and units in any mix of different services and nationalities should be able to interoperate seamlessly, and technical solutions to this aim should be transparent to the user. However, reality is still a far cry from this ideal end state. This means that from a national perspective, sometimes choices have to be made with which partners achieving interoperability has the highest priority, and whether national (joint) or international (combined) interoperability should prevail.

Solutions: the C4I architecture

Solutions for common C4I challenges

The fact that these challenges are common can be considered a blessing in disguise: it means that we can take a close look at NATO and partner nations to see how they cope with them. Having a Netherlands C4I architecture provides a means to implement possible solutions as embodied in e.g., NAF and DoDAF, by translating them into the Netherlands C4I architecture.

The C4I architecture could serve another purpose in relation to two of the listed challenges. Real-time requirements and bandwidth limitations could be considered a paradox: C4I systems pose high demands on bandwidth, while at the same time they have to operate in an environment that is characterised by its bandwidth limitations. This paradox will become even more apparent with the advent of many remote sensing systems, operated from satellites and UAVs. The C4I architecture could provide insight into the cumulative bandwidth requirements by various existing, planned and required C4I services and systems. This would reveal the total impact of these bandwidth requirements on the mobile and deployed ICT infrastructure. To put it the other way around, this could help in setting boundaries to unrestricted bandwidth claims. Rather than discussing bandwidth requirements ad hoc, each time when a new requirement pops up, the C4I architecture would allow a more structural approach.

Solutions with respect to NEC

The C4I architecture should describe both the current situation with respect to C4I services and systems *("ist")* and the situation required in future *("soll")*. The transition from *ist* to *soll* is to be specified in phases or *architecture stages*, which should be aligned with the different NEC maturity levels as specified in the NEC Action Plan. Admittedly, this could be a challenge, since the description of NEC maturity levels is non-specific as to C4I requirements. This would require that the NEC maturity levels are translated into specific C4I requirements, which then collectively can be depicted as C4I architecture stages. This translation should be performed in the context of the development of the C4I architecture.

With respect to the other challenge related to NEC: the C4I architecture could also be used to find a solution for the problem to define what it means to make units *net ready*. As mentioned in the previous paragraph, it could be used as a means to translate possible solutions by NATO and partners into the Netherlands C4I architecture.

Solutions for C4I stovepipes

Developing a common C4I architecture for the armed forces is probably a prerequisite to get rid of unnecessary stovepipes in a coherent and planned way. While investigating the *ist* situation, it should be questioned whether current differences are justified by differences in environment and deliberate choices. If they are not, they should probably no longer exist in the *soll* situation. The process of arriving at a shared view within the armed forces on what should be the *soll* situation, as part of the development of the C4I architecture, could prove to be very valuable in itself. Once the *soll* situation is agreed upon, a transition plan should be developed to arrive from *ist* to *soll*, and this coincides with the transition mentioned in the previous paragraph.

Solutions for interoperability

This aspect should be an essential feature of any C4I architecture. By investigating the information exchange requirements in different scenarios, the C4I architecture should support logical choices for setting interoperability priorities. At the systems and technical level, the applicability of different solutions should be investigated and principal choices should be made, such as the implementation of internationally agreed standards (e.g., NATO datalinks and waveforms) or implementing internationally agreed gateway solutions such as developed by the Multilateral Interoperability Programme (MIP). MIP developed a “common semantic core”, which provides interoperability at the semantic level between nationally developed operational information systems (see [Chaum and Lee, 2008]).

Research into the development of the C4I architecture

Method of work

From a theoretical point of view, the research approach is *formulative* with *descriptive* and *evaluative* elements:

- it is formulative because the C4I architecture document formulates what the architecture should look like at a specific point in time to achieve the goals and milestones of the NEC Action Plan;
- it contains descriptive and evaluative elements because it describes the baseline, being the C4I components currently available, planned and being realised, and evaluates these components against the requirements defined in the C4I architecture.

Research methods include interviews, literature review, operational case studies and conceptual analysis of current C4I systems and projects.

The first phase of research consists of identifying stakeholders, defining purpose and scope, and ensuring leadership support. In the past years various C4I architecture efforts have been made as mentioned earlier in this chapter, the results of which are to be examined and used to the maximum extent possible, to avoid duplication of effort. It will also be investigated to what extent methods, tools and views from other architectures can be used for the development of the C4I architecture (see “theoretical context” above), and to what extent TNO will be involved.

The second phase of research consists of the collection of information to create the upper and middle layers of the C4I architecture. The upper layer describes the operational process and its information exchange requirements in various typical scenarios. The middle layer describes the information services and systems required to support the upper layer. To build the upper layer, interviews will be held with representatives from the operational commands, augmented with case studies and literature study. To build the middle layer, interviews will be held with representatives from the C2 development centres CAMS and C2SC and from the Defence Materiel Command (DMO)[1], augmented with conceptual analysis of current C4I systems and projects.

Building the upper layer should provide insight into the information exchange requirements in a number of standard operational scenarios. This should include whether these are currently being supported by available information services and systems, what is still missing and which deficiencies should be rectified first. Building the middle layer should result in the definition of a set of common operational information services which can be used both by CAMS and C2SC[2]. It should also provide an overview of information services currently being provided by C2 systems and being developed and planned. Comparing the information from the upper and middle layers could show discrepancies between what is required (upper layer) and what is being developed (middle layer), and could help setting priorities for further development of services.

The third phase of research will be aimed at providing the bottom layer, which completes the C4I architecture. This layer will define technical standards for C4I services and systems, and technical requirements for the supporting ICT infrastructure, e.g., the cumulated capacity requirements for communication links (see "solutions for common C4I challenges" above). This development effort is a logical follow-up of the building of the middle layer, and will use the same information sources mentioned above.

The C4I architecture covers a vast area. To keep the development efforts manageable, initially the scenarios to be studied will be kept as simple as possible, covering standard situations. As follow-on, more complex scenarios should be examined, up to the maximum level of ambition for deployment of the Netherlands Armed Forces[3], using the experience from the first architecture efforts.

Progress to date

Phase one has been largely completed. Working arrangements have been established with DS, in close coordination with DIO. This has resulted in a first definition of purpose and scope, an outline of the method of work, and an initial framework for the C4I architecture document ([Ooms, 2008]). This version has been discussed with DS and DIO. The report

[1] Although only national players in the C4I field will be interviewed, this should not imply a primarily national focus. As a rule, Netherlands C4I projects are embedded in international developments, which is strongly promoted by Netherlands C4I professionals.

[2] DIVA already contains operational information services, which will be used as a starting point. As a first impression, a finer granularity seems required.

[3] As politically agreed, this is for the army a deployed brigade, and for navy and air force the equivalent.

of the comparative study conducted by TNO ([Riemens et al., 2008], see "theoretical context" above) is being studied, and the possible use of methods, tools and views from other architectures will be discussed with TNO. Involvement of TNO in architecture work in 2008 has been agreed in principle with DS and TNO and will be formalised in the near future. Leadership support is being ensured at two-star level within DS and DIO.

Phase two has been initiated. For the middle layer, initial contact with C2SC has been made and information provided on architecture efforts and C4I projects is being studied. CAMS will be contacted at short notice. For the upper layer, the staff officer C4I of the Defence Staff Operations Center (DOPS/J6) has been interviewed and as follow-on his counterparts in the operational commands (maritime, land and air) will be approached at short notice.

Benefits for NLDA

The information derived from the involvement in the C4I architecture can directly be integrated into the study material for the Bachelor CICS course and various C2/C4I related subjects of the Bachelor MS&T course, such as computer networks, C2 architecture, military communications, and subjects within the C4I profile. Furthermore, the C4I architecture document could provide a starting point for various BSc thesis projects. From a wider perspective, the architecture research efforts will increase the visibility of NLDA defence-wide and will show how its scientific know-how can be applied for the armed forces.

References

ISO (2007) *Recommended Practice for Architectural Description of Software-Intensive Systems,* ANSI/IEEE standard 1471-2000, in 2007 accepted by the International Standards Organisation (ISO) JTC1 as ISO/IEC DIS 42010:2007. ANSI: American National Standards Institute, IEEE: (US) Institute of Electrical & Electronics Engineers.

The Open Group (2007) *The Open Group Architecture Framework* (TOGAF), developed by the Architecture Forum of The Open Group, continuously evolved since mid-90's. Current version is 8.1.1.

MOD NL (2006) *Netherlands Defence Doctrine (Nederlandse Defensie Doctrine)* (NDD), first edition, Netherlands Ministry of Defence (MOD NL), 2006

NATO (2004) *NATO C3 System Architecture Framework* (NAF) version 2, AC/322-D(2004)0041.

US DoD (2004) *DoD Architecture Framework* (DoDAF), version 1.0, Vol I-III, US Department of Defense, February 2004.

Riemens, J.M.J., Hekken, M.C. van, Lasschuyt, E. and Niet, M. de (2008) *Een architectuurmetamodel voor Defensie; meer samenhang en herkenbaarheid,* TNO-DV 2007 A117, 30 January 2008 (in Dutch).

Chaum, E. and Lee, R., (2008) *Command and Control Common Semantic Core Required to Enable Net-centric Operations,* Proceedings of AFCEA – GMU C4I Center symposium "Critical issues in C4I".

Ooms, D. (2008) *DIVA Deelarchitectuur operationele informatie voorziening,* (in Dutch), in preparation.