16th ICCRTS

"Collective C2 in Multinational Civil-Military Operations"

Improving Civil-Military Information Sharing in Peace Support Operations using a Service-Oriented Approach

Topic: (8) Architectures, Technologies, and Tools

Dick Ooms & Tim Grant

POC: Dick Ooms

Netherlands Defence Academy (NLDA)
P.O. Box 10000, 1780 CA Den Helder, The Netherlands
Tel: +31 223 657643 / +31 6 3814 8664
dm.ooms.02@nlda.nl

Improving Civil-Military Information Sharing in Peace Support Operations using a Service-Oriented Approach

Abstract

Peace Support Operations (PSO) involve inter-organizational cooperation between military actors and a wide range of civilian actors such as non-governmental organizations, referred to as Civil-Military Cooperation (CIMIC). Effective communication and information sharing in PSO is a prerequisite for effective CIMIC, but has proven to be problematic.
In a Service-Oriented Architecture (SOA), software resources are packaged as “services”, which are well-defined, self-contained modules that provide business functionality. Services communicate with each other, requesting execution of their operations in order to collectively support a common business task or process.
An analogy exists between the SOA approach and the requirements for information sharing and collaboration in the context of PSO and CIMIC. A wide range of military and civil partners cooperate loosely with one another, with each partner making its own specific contributions and collectively supporting the operation. This resembles the cooperation between a wide range of services in a SOA.
This paper outlines a study initiated to investigate whether a SOA approach could improve CIMIC information sharing. Initially, a process model of CIMIC operations will be developed, building on the experiences with our work on process modelling for a C4I architecture, as presented at the 14th ICCRTS.

1. Introduction

1.1 Problem background

Increasingly, the strategic aim of coalition operations is stabilisation and, in its wake, reconstruction, peace building, and/or conflict prevention. These types of operations are commonly referred to as Peace Support Operations (PSO). PSO involve inter-organizational cooperation between military actors and a wide range of civilian actors such as humanitarian international and non-governmental organizations (IOs and NGOs), referred to as Civil-Military Cooperation or CIMIC. Although military and civil actors might have different objectives, CIMIC can have many mutual benefits. From the military perspective, cooperation can prevent duplication of effort and waste of scarce resources, as well as building consent to the presence of a military force and therefore providing a means of protection. From a civil perspective, the military can guarantee a climate of security, and the skills, knowledge and assets of military actors could support the work of local parties and humanitarian organizations (Rietjens, 2006).

Effective communication and information sharing in PSO is a prerequisite for effective CIMIC, but has proven to be problematic (Rietjens et al, 2008). A purely military approach to this problem is prone to fail, since Command & Control arrangements for PSO are fundamentally different from traditional C2 arrangements, which are aimed at military war fighting operations, as observed by Alberts & Hayes (1995).

Initial investigation shows a number of technical challenges. The requirement to exchange information between a wide range of possible civil and military partners poses interoperability challenges for the supporting information systems. An additional challenge is the requirement to share real-time information, which is required to build and share a Common Operational Picture between cooperating partners. This requirement poses challenges for the information systems in use by the cooperating partners, as well as for the supporting ICT infrastructure. Finally, PSO are complex and uncertain, which drives the requirement for a robust and resilient information architecture, while at the same time the existing ICT infrastructure is often insufficient, unreliable or disrupted.

Other, non-technical factors play an important role in information sharing in dynamic coalitions, as investigated by G.G.A. van den Heuvel (2010), *inter alia* Perceived Information Shareability and Anticipated Reciprocity. Perceived Information Shareability relates to the specific security aspects of (military) information which may hamper or inhibit information exchange with civil partners. Any technical information exchange solution should take these security aspects into account. Van den Heuvel (2010) considers Anticipated Reciprocity as a significant determinant of information sharing, since individuals are motivated to share information with the anticipation that the same value of information will be received in return. Exchanging valuable information in such a way can be regarded as an information market (Grant & Van den Heuvel, 2010), and the technical solutions for information exchange should support this process. Moreover, research by Van den Heuvel (2010) was mainly performed on information sharing between military organizations and individuals. Information exchange for CIMIC could be much more problematic, since many humanitarian organizations solely focus on delivering humanitarian aid during ongoing conflict and see integration with military partners as deeply objectionable (Rietjens et al, 2008).

1.2. Research approach

In a Service Oriented Architecture (SOA), software resources are packaged as “services”, which are well defined, self-contained modules that provide business functionality. Services are described in a standard definition language, have a published interface, and communicate with each other requesting execution of their operations in order to collectively support a common business task or process (Papazoglou, 2008).

An analogy exists between the SOA approach and the requirements for information sharing in the context of PSO and CIMIC. A wide range of military and civil partners loosely cooperating with one another, with each partner making its own specific contribution(s) and collectively supporting the operation, rather than being centrally commanded, resembles the cooperation between a wide range of services in a SOA. Requirements for the supporting ICT infrastructure supporting peace operations and CIMIC could be compared to the Enterprise Service Bus (ESB) which serves as an integration platform in the SOA concept.

A PhD research proposal is being developed to conduct research into the problems of information sharing for CIMIC. This research could be based on the hypothesis that information sharing could be improved by using a service-oriented approach. Initially a comparison has been made between SOA elements and the characteristics of a CIMIC scenario. Current research issues in Service Oriented Computing (SOC) have been presented in a Research Roadmap for SOC by Papazoglou et al (2008). The relevance of these research issues with respect to the problems of information sharing for CIMIC has been investigated. W.J.A.M. van den Heuvel (2009) positions SOC in the wider concept of smart service networks. This concept and the related research issues have been investigated as well.

1.3 Scope

Strictly speaking, CIMIC occurs as well in homeland defence operations in response to major emergencies, such as counter-insurgency, anti-terrorist and disaster relief operations. However, we intend to limit our research to CIMIC in the context of PSO, in order not to become entangled in ongoing discussions on the complex organization and division of responsibilities of different layers of government and public institutions in The Netherlands.

In addition, we limit the scope of PSO to “complex emergencies”, defined as “a humanitarian disaster that results from a political or ethnic conflict that causes massive population movements and a shortage of food and health care, and in which political authority and public services have deteriorated or completely collapsed”. This approach aligns well with the scope chosen by Rietjens in his PhD study on the phases and performance assessment of CIMIC processes (Rietjens, 2006) and with the case study by Rietjens et al (2008) on inter-organizational communication in CIMIC.

1.4 Related research

Investigation into problems with information sharing for CIMIC is closely related to ongoing research by the Netherlands Defence Academy (NLDA) into the development of an Operational Process Model (OPM). This is one of the architecture products of a service-oriented C4I architecture for the Netherlands Armed Forces, which is being developed. We initially reported on this work at the 14th ICCRTS (Ooms & Grant, 2009).

This relation is twofold. Firstly, CIMIC is one of the operational processes contained in the Hierarchical Process Diagram (HPD), which is one of the two components of the OPM. Individual processes of the HPD are to be modelled using the methods and views of the Information Flow Diagram (IFD), which is the other component of the OPM. Thus, modelling of the CIMIC process is a logical extension of the development of the OPM, and is as such an instantiation of the IFD.

Secondly, as shown in this paper, initial investigation reveals that an analogy exists between the cooperation of software services in a SOA and the way military and civil partners are cooperating in PSO. For this reason, it should be investigated whether a service-oriented approach could improve CIMIC information sharing. Since the C4I architecture is service-oriented, the methods and views of the OPM could be used to identify software services which support the CIMIC process. Thus, the results of our architecture development research could contribute to the proposed research into CIMIC information sharing.

1.5 Paper structure

This paper is structured as follows. This introduction is followed by a chapter on the research approach, which expands on the initial investigations on similarities between service oriented computing, SOA and information sharing for CIMIC, and on the applicability of SOA research issues for research on CIMIC. This chapter includes an investigation of the related concept of Smart Service Networks with respect to similarities and research issues. Chapter three is about related research and provides an overview of our work on an Operational Process Model for the C4I architecture of the Netherlands Armed forces. The results of this work could contribute to the proposed research into CIMIC information sharing, as discussed above. The final chapter provides conclusions and the intended future research.

2. Research approach: SOA and CIMIC

2.1 Similarities

In his textbook "Web Services: Principles and Technology", Papazoglou (2008) provides a comprehensive overview of conceptual and technical elements of service oriented computing and SOA. These elements have been compared with the characteristics and obstacles of information sharing for CIMIC in the context of PSO, as described by Rietjens et al (2008). As a result of this comparison, various CIMIC information sharing issues have been identified that could benefit from a service oriented computing approach. These issues are discussed below. Each issue starts with a quote from (Rietjens et al, 2008), with page number indicated, followed by a discussion how service oriented computing might alleviate the problem.

(1) Bridging the "principles gap". "Many humanitarian organizations solely focus on delivering humanitarian aid during ongoing conflict and see integration [with military actors] as deeply objectionable" (p.2). When information on capabilities, intentions, locations etc. is promulgated by each civil and military actor as web services on a common network, retrieval and processing of this information becomes an automated process which does not require specific point-to-point contact between military and civilian actors, and thus might become less objectionable. The loose coupling between the information systems of different partners, which is typical for service oriented computing could provide the necessary separation between parties that do not want to be associated with each other, thus providing a technical solution to alleviate or solve a non-technical problem.

(2) Preventing information overload. "During the deployments of ISAF III and IV approximately 650 humanitarian organizations were present in Kabul" (p.11). This number illustrates that just keeping track of the capabilities, intentions, locations and actual operations of all actors becomes an overwhelming task, let alone selection of suitable partners for specific operations, coordination and de-confliction. Web services are described in terms of a description language, which includes functional as well as non-functional characteristics, such as availability, scalability and security attributes. When this information of each civil and military actor is available as web services on a network, handling of this information (keeping track, selecting partners, coordination etc.) could be supported and/or (partially) performed automatically using service orchestration facilities.

(3) Providing structured information. "Due to a lack of expertise and analysis capacity, and to the large amounts of unstructured data and information, these information products [of the military CIMIC Coordination Center] were often not useful" (p.11). A similar problem was reported with IOs and NGOs: "Due to the large amounts of incoming information and the limited numbers of qualified personnel, the organizations lacked time to filter, analyse, assess and process all the information […] Disseminating information to external actors was thus seriously hampered"(p.13). Providing CIMIC-related information in a structured way by using web services, which are published and searchable in a web services registry, could ease, and partially automate information handling and presentation at the CIMIC Coordination

Center, as well as for other actors.

(4) Providing institutional memory. "The motivation of humanitarian personnel was seriously undermined by frustration with […] the fundamental lack of institutional memory of ISAF CIMIC" (p.15). Having current information about partners available on the network in a structured way, promulgated as web services in a web services registry, could partly provide the necessary functionality of an institutional memory.

(5) Reducing heterogeneity. "Within each ISAF rotation, level, military unit, nationality and even between individual staff members there were different […] interpretations of CIMIC and liaison. Humanitarian organizations differed significantly in working methods […]. For both ISAF and the humanitarian organizations the diversity in approaches produced problems in understanding the organizations, and prevented the realisation of agreements on information sharing" (p.16). Agreement on the use of web services as the standardised way for actors to promulgate information on their organization, capabilities etc. could reduce existing heterogeneity.

(6) Optimise use of limited available communications. "Since technological channels such as telephone and e-mail often did not function properly, information was frequently exchanged by face-to-face contact" (p.14). However: "[an] issue negatively influencing the information sharing process was the lack of time available to staff to share information with all actors in the field". An unreliable ICT infrastructure renders a more technical approach for information sharing impractical at first sight. However, the use of web services to promulgate information could support a more efficient use of the network than the use of telephone and e-mails. Moreover, the minimum infrastructure required by the web services paradigm is purposefully low.

2.2 Research issues

Papazoglou et al (2008) provide a Research Roadmap for Service Oriented Computing which identifies four pivotal, inherently related, research themes to Service Oriented Computing: (1) service foundations, (2) service-composition, (3) service-management & -monitoring and (4) service-oriented engineering. These themes are related to the concept of the Extended SOA, which was proposed earlier by Papazoglou (2005). For each theme they identify the state of the art, including ongoing research activities, and the major research challenges. A first analysis reveals the following research topics which are relevant to civil-military information sharing.

With respect to the theme of service foundations:

- Improving service discovery, publication, and notification mechanisms across distributed, heterogeneous, dynamic organizations using an open, modular, extensible framework;
- Improving the description of services using Semantic Web concepts, providing richer semantic descriptions of web-services that describe properties and capabilities in a computer-interpretable form.

With respect to the themes of service-composition and service-management & -monitoring:

- Improving service composition allowing more ad-hoc and dynamic service composition using lightweight and adaptive workflow methodologies, including advanced forms of coordination and less structured process models;

- Improving service-composition and service-management & -monitoring by autonomic composition of services, including management services, e.g. services which are self-configuring, self-adapting, self-optimizing, self-healing and self-protecting.

With respect to the theme of service-oriented engineering (design and development):

- Development of novel techniques that allow engineering decisions to be postponed at run-time, with highly distributed control and stakeholders with possibly conflicting business needs;
- Associating a services engineering methodology with business process modelling techniques; are emerging business modelling notations such as BPMN suitable to model CIMIC processes?

We add to these SOA related issues the following research issues from a C2 systems perspective. With respect to interfacing client applications (especially military Command & Control (C2) systems) to underlying services:

- Investigating the conceptual relationship between network theory, networked applications (e.g. networks of C2 systems from different nations, services, and organizations), and SOA;
- Investigating the conceptual relationship between multi-agent systems (MAS) – often used to implement C2 systems - and SOA.

Existing research into information exchange issues in the context of PSO and CIMIC seems to take mostly a less technical but more of a social / organizational / information management approach. A reason could be that information exchange problems are diverse and complex, because different participants might have different missions, different requirements for cooperation, C2 is more complicated, and the supporting ICT infrastructure is problematic at best. These circumstances render a more technical approach impractical at first sight, reducing information exchange to periodical meetings between actors (Rietjens et al, 2008). However, current rapid worldwide adoption and improvements in ICT infrastructure could change the setting in the near future, allowing a SOA approach to improve information exchange for CIMIC. Research efforts should anticipate this development.

2.3 Smart Service Networks

In his inaugural address "Changing the Face of the Global Digital Economy", W.J.A.M. van den Heuvel (2009) introduces the concept of Smart Service Networks. These are systems of systems, composed of smart service systems. What makes these networks and systems "smart" is the interweaving of smart physical devices, tagged objects and sensors with the software services. In this way, smart service systems and networks support processes that can monitor their own performance, and repair, upgrade or replace themselves in a pro-active manner. Resources in smart service systems may include people, software systems, computing devices and sensor networks, organizations and shared information. As we have done with service oriented computing and SOA, we will first investigate the similarities between this concept and the information exchange issues related to CIMIC. Subsequently we investigate to what extent Smart Service Network research issues, as identified by Van den Heuvel (2009), are applicable to the problems with information sharing for CIMIC.

The wide variety of military and civil actors (government, IOs, NGOs, local authorities) collaborating in PSO could be regarded as a smart service network since they share some of the distinguishing characteristics (Van den Heuvel, 2009 p.34):

- global resource dependencies: participants need to cooperate and need mutual in-theatre support, while at the same time they rely on logistic support from their parent organizations or national home base, and in addition benefit from support and cooperation from local authorities;
- actor-network relationships: participating parties often share the same mission goals and their cooperation in-theatre could be viewed as value co-creation for the local community and government. In this complex environment they have typical polyadic relationships with all parties involved;
- smart: collaborating parties in peace support operations could benefit from capabilities sensing their internal working and the environment, providing feed-back on their efforts. This should allow improvements of their effectiveness and efficiency.

Like the study of service systems, the CIMIC sector could take advantage of cross-disciplinary research efforts (Van den Heuvel, 2009 p.33). Current CIMIC research efforts are lacking an information systems approach. Such an approach could be complementary to, and unified with existing approaches, and could benefit from the results of existing socio-economic science approaches.

Van den Heuvel (2009, p.53) proposes a Smart Service Network lifecycle model in which research issues can be positioned which are aimed at empowering (networked) enterprises. As we have shown above, CIMIC partners could be regarded as such. CIMIC research issues could be positioned in the different phases of this model as follows:

- phase 1, networkability analysis: since CIMIC involves a variety of partners (government departments, NGO's, local authorities), process maps and possibly collaborative Key Performance Indicators could be developed;
- phase 2, configuring generic processes: available research results such as (Rietjens et al, 2008) reveal many deficiencies in the current CIMIC process, and could be used as start of a multi-dimensional gap analysis;
- phase 3, rationalization, simulation and optimization: the resulting smart service network blueprint should be simulated in a test bed environment, involving CIMIC practitioners.

Other research issues related to Smart Service Networks, as identified by Van den Heuvel (2009, p.46), are aimed at empowering end-users. The following issues are applicable to CIMIC information research:

- in the highly agile and distributed PSO environment, CIMIC workers could benefit from the rapid development of enterprise mash-ups to support their specific mission requirements;
- mobile applications, smart devices and sensor networks could provide rapid feed-back to supporting organizations to adjust local requirements and support for CIMIC workers;
- CIMIC workers need robust, mobile solutions that operate reliable under adverse conditions including a bandwidth-limited environment, and provide them with customised information.

3. Related research: process modelling for C4I architecture

3.1 Developing a C4I architecture[1]
Since 2008 the NLDA has been involved in the development of a C4I architecture for the Netherlands Armed Forces, in close cooperation with the Netherlands Organization for Applied Scientific Research (TNO), as requested by the Netherlands Defence Staff. We reported on the research approach and the first results of our architecture work at the 14th ICCRTS (Ooms & Grant, 2009). The C4I architecture should provide coherence and guidance for the evolution of our C2 processes, the required operational information support and the underpinning ICT infrastructure.

The C4I architecture being developed is a sub-architecture of the corporate Information Architecture of the Netherlands Ministry of Defence, called DIVA.[2] DIVA includes a nine-segment architecture framework (a 3 x 3 matrix: three layers and three columns), a set of high-level architectural principles, the definition of a series of architectural products and some methods for the development of the products, which have been published separately. Its three layers from top down contain the Business Architecture, Information Architecture and ICT Architecture, respectively. As such, DIVA resembles the US Department of Defense Architecture Framework DoDAF (US DoD, 2009) and the NATO Architecture Framework NAF (NATO, 2007). The Operational View(point), Systems (and Services) View(point) and Technical (Standards) View(point) of DoDAF and NAF correspond with the Business Architecture, Information Architecture and ICT Architecture of DIVA, respectively. Like DoDAF and NAF, DIVA takes a service-oriented approach. The DIVA nine-segment framework is depicted in figure 1.

3.2 Developing an Operational Process Diagram
Various C4I architecture products are currently being developed. NLDA, together with TNO, is developing an Operational Process Model (OPM), which is part of the Operational View(point). The purpose of the OPM is:

- to derive operational information services for the Information Services Model;
- to provide guidance for the implementation of (changes in) operational processes;
- to identify the requirements for the supporting ICT infrastructure;
- to allow the positioning of C4I projects in relation to other processes and projects.

The OPM and the Information Services Model are closely related. The Information Services is being developed by TNO, in cooperation with NLDA. The OPM consists of 2 views:

- Hierarchical Process Diagram (HPD): an comprehensive overview of all business processes and their relations. As a guiding principle for HPD design, the output of each process should contribute to the output of the related process one hierarchical level higher. The HPD provides process descriptions and serves as a common reference model for operational services.
- Information Flow Diagram (IFD): a description of the relations between different processes within one process at one hierarchical level higher. This should include interactions (information flows) between the processes. The IFD is used to model a specific operational process. The process is decomposed in process steps. Process actors are identified with their Information Exchange Requirements (IERs), in order to specify the information flow that is required for the process.

[1] C4I: Command & Control, Communications- and Computer-systems and Information
[2] DIVA: in Dutch: *Defensie Informatie Voorzienings Architectuur*

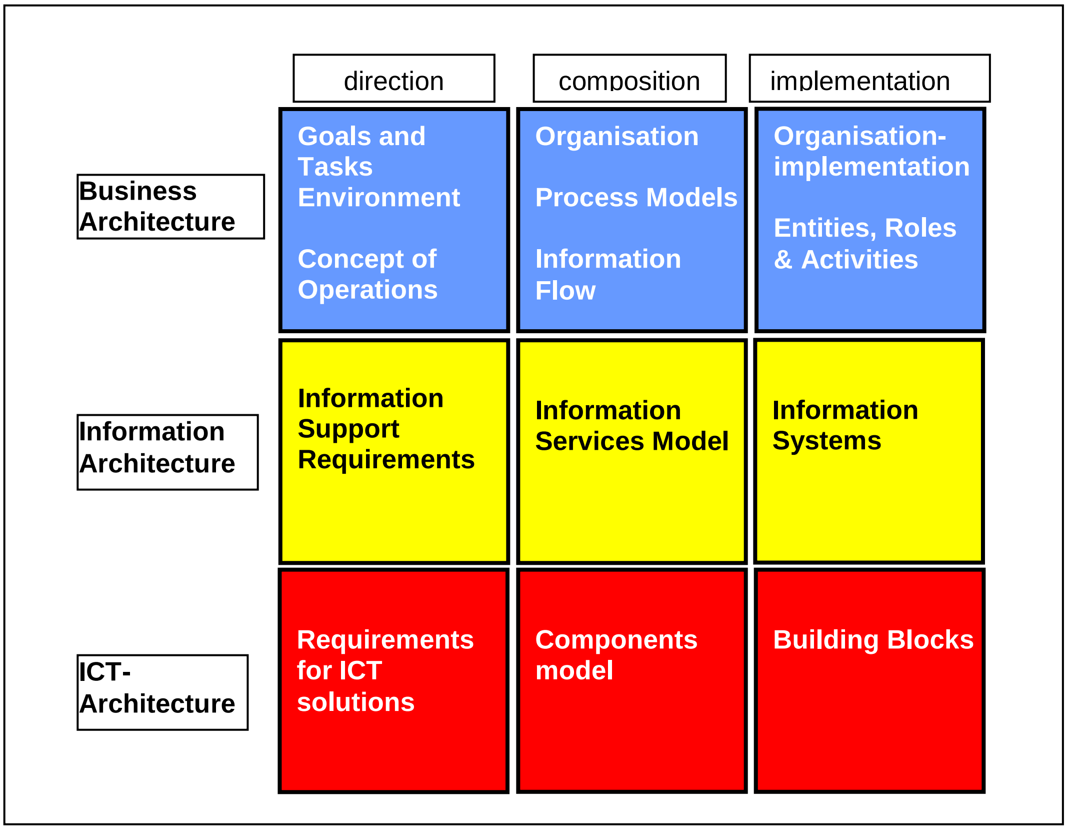

Figure 1: DIVA nine-segment framework

The HPD includes CIMIC as a process and could be used to identify CIMIC-related processes. The definition of an IFD implies that IFDs can be developed as required, contrary to the HPD which is developed only once and aims at completeness. An operational process such as CIMIC can be selected to be modelled with an IFD, to support concept development, to identify shortfalls which translate into requirements, or to support a specific project. An IFD could be a building block in the development of requirements for new information services, information systems or ICT components that support the modelled process.

3.3 Designing a method for IFD development

The IFD characteristics mentioned above imply that we had to design a method for IFD development, rather than developing a model of a specific operational process. However, to be able to validate the design, in consultation with stakeholders we chose a specific operational process to be modelled initially, being Joint Air Defence (JAD). The IFD development method was thus designed in iterations, while applying it for the actual development of the IFD of the JAD process.
As a result, the output of our research is twofold:

- a validated method for the development of IFDs;
- the IFD of the JAD process, developed with this method.

The IFD of the JAD process is being validated by actual process actors and other subject matter experts. They should recognise the model as a realistic representation of the operational reality. However, this validation does not guarantee that the IFD fulfils its requirements in the context of the C4I architecture, i.e. to identify operational services. This can only be tested in relation with other architecture products, once the C4I architecture will actually be used, e.g. to support the generation and specification of requirements. This test could thus be regarded a second stage of validation. This development and validation process is depicted in figure 2.

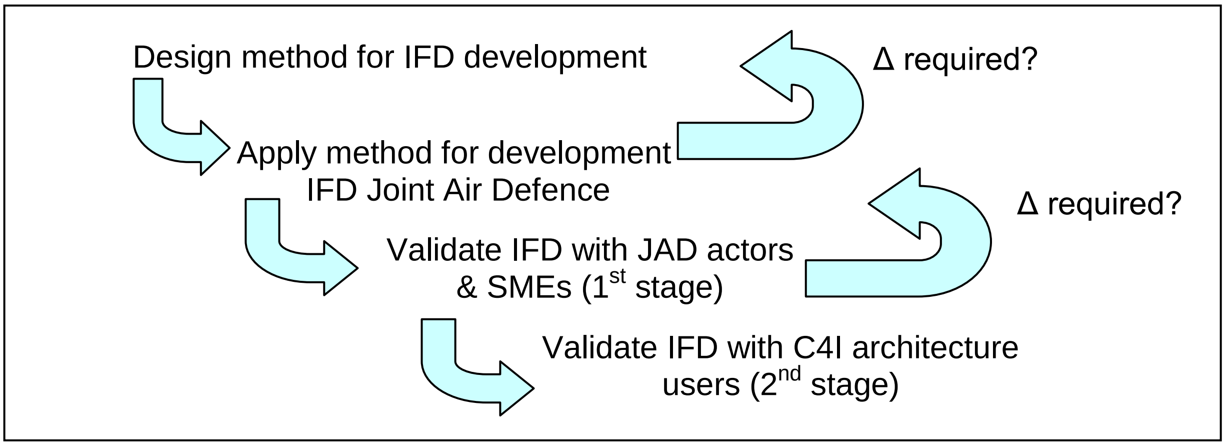

Figure 2: IFD development & validation

3.4 Developing an internal and external process view

We decided to develop the IFD with two views: an internal and external process view. The internal view models the processes internal to an actor, and the external view models the interactions between actors. This approach could be compared with the modelling of arcs and nodes of a network. For the development of both views we use a generic joint and combined scenario, which is broken down in events. Each event should require activities by process actors and interactions between process actors. The sum of all events should provide a complete view of the interactions between process actors. Table 1 provides an example of the event list for the JAD process.

The external process view consists of a network diagram and IERs tables and should provide a complete picture of the interactions between process actors. The network diagram depicts the process actors and links between them. Figure 3 is a simplified example of the network diagram for the JAD process. The boxed text below the figure provides an explanation of the scenario and the actors. The aggregated information flow between process actors via these links is modelled as Information Exchange Requirements (IERs), presented in tables with attributes like maximum time late, data type and classification. IERs tables are compiled in brainstorm sessions with subject matter experts, during which the course of actions caused by events is discussed. The external process view serves to identify requirements for the supporting ICT infrastructure, and can be used to identify operational services[3].

The internal process view is used to model the internal processes of process actors. Process actors could be individuals, such as a fighter pilot, or teams such as the team in the opsroom of an air defence ship. In this case we don't model team interactions; the team is regarded as one of the process actors. Both the fighter aircraft and the air defence ship are entities in the air defence process, regardless of the number of individuals involved. For the development of the internal process view we decided to use Boyd's (1996) OODA loop as modified by Grant

[3] For the identification of operational services from IERs, the Services Architecture Method (SAM, 2007) is used as developed by TNO for the Netherlands Defence. A description of SAM falls outside the scope of this paper.

(2005), i.e. the Rationally Reconstructed OODA model (OODA-RR), as described in the next section.

EVENT / ACTIVITY	INFORMATION EXCHANGE
PREPARATION	
Planning	AD Plan, OPGEN, OPTASK, OPSTAT UNIT reports, OPDEFs, ACO
Tasking	ATO
TRANSIT / DEPLOYMENT	
Threat evaluation	re-assess plans
	(re-)positioning AD units
	sitrep
Fighter control	Positioning, fuel state, weapon state, alert state, AAR planning/execution
Evaluate RAP	Sitrep
Picture compilation	Track reports
Joiners / leavers	Re-assess plans
	(re-) positioning AD units
ACTION	
Detection enemy	Position / activity, threat evaluation, sitrep
Pre-Planned Response trigger	Codewords, manoeuvring orders
Engagement	Weapon assignment, damage assessment

Table 1: example event list Joint Air Defence process

3.5 Using the OODA-RR model

The OODA-RR model (Grant, 2005) addresses most of the shortcomings of Boyd's (1996) OODA loop, as identified by Grant & Kooter (2005) and Brehmer (2005). Of particular importance for the IFD, it allows both rational and naturalistic decision making. Operational process modelling reveals that both decision making models are being used by process actors. For deliberate decision making, such as for planning and tasking, rational decision making is applied, while for urgent decisions an actor reverts to naturalistic decision making. The latter has been extensively researched by Gary Klein, who developed the Recognition-Primed Decision Making (RPDM) model (Klein, 1998). According to the RPDM model, mental modelling is used to match a specific situation with a prototype situation, rather than evaluating different options. Once a match has been found, the corresponding actions will be executed. If a match is incomplete, in the RPDM model more information is collected with a separate process step "more information". The OODA-RR model allows for naturalistic decision making by including a repository of prototype situations as "knowledge representation" and describing the process steps in accordance with the RPDM model.

Our research indicates that the Joint Air Defence process seems an excellent example of the use of both decision making models. Air planning and tasking prove to be elaborate processes for which rational decision making is employed. In the execution phase however, the air defence process is characterised as being highly reactive with short reaction times. For this reason, Pre-Planned Responses (PPRs) are being used, which specify a set of reactions which are executed automatically if the actual operational situation is matching a set of predefined conditions. Sets of predefined conditions, together with the corresponding set of reactions (the PPR) can be regarded as the prototypes of the RPDM model. It should be noted however that Klein's prototypes appear to be tacit knowledge of experienced process actors, whereas the

PPRs are formally promulgated as the result of air defence planning, and thus represent explicit knowledge.

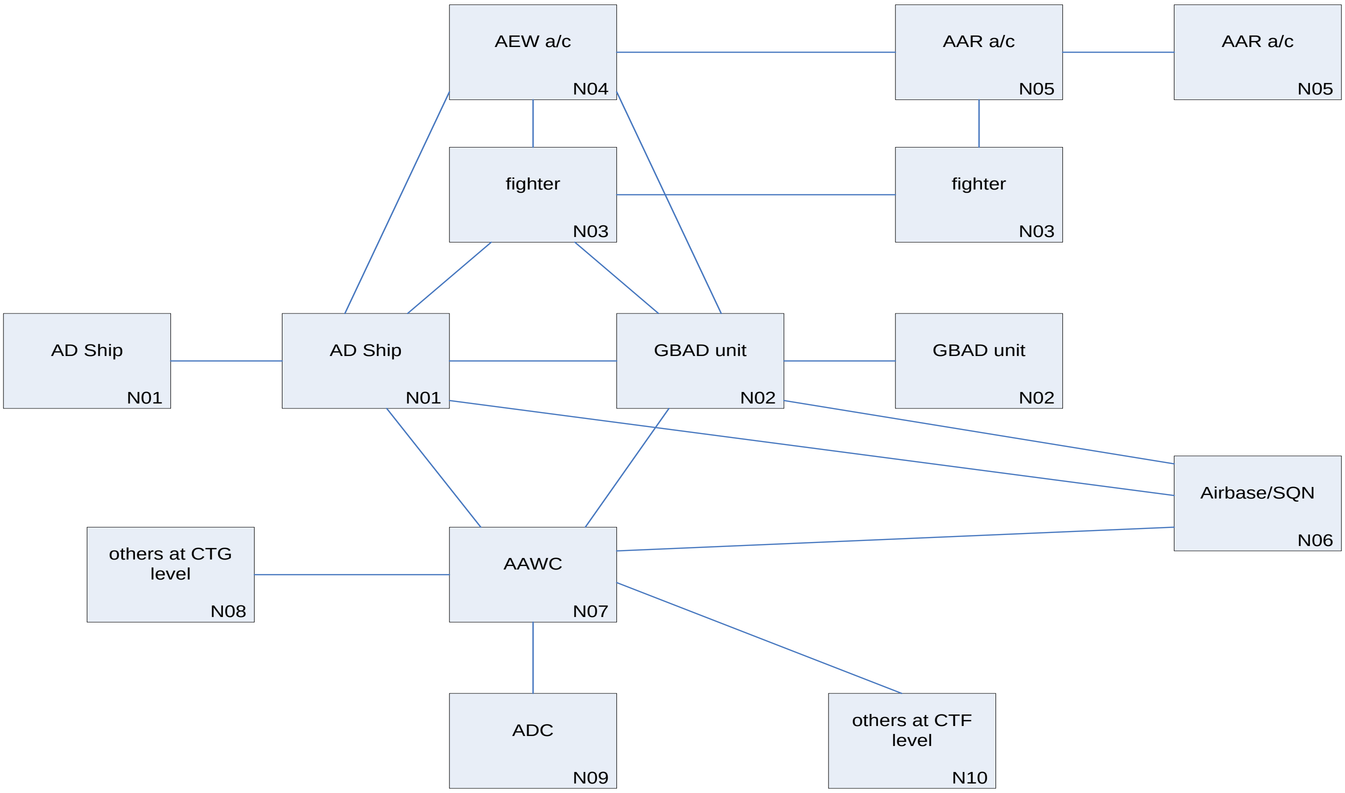

Figure 3: network diagram Joint Air Defence process

Figure 3 depicts the actors in a Joint Air Defence (JAD) scenario and the links for information exchange between them. The diagram serves as an example and is not necessarily correct or complete. Each actor is depicted only once, unless information exchange between similar actors is possible and should be modelled. From all possible actors in the scenario, only those which could be instantiated by Netherlands operational staffs or units (i.e. *Netherlands* actors) are modelled, and those *non-Netherlands* actors with whom they could exchange information. The following JAD actors are depicted:

- ADC – the Air Defence Commander, in charge of JAD on behalf of the Joint Force Commander (JFC, not depicted);
- AAWC – Anti-Air-Warfare Commander, a maritime warfare commander in charge of the air defence of a Task Group (group of maritime units), reporting to the Commander Task Group (CTG, not depicted) and to the ADC and if necessary to other (component) commanders at the force level. The AAWC exchanges information with other warfare commanders at the task group level. The AAWC coordinates primarily the employment of the following air defence units of (or attached to) the task group:
- AD ships: ships with air defence capabilities (sensors, weapons, C2);
- GBAD units: Ground Based Air Defence units ashore, which could be Army or Air Force units, equipped with sensors and/or ground-to-air missile systems. In this scenario a ground-based C2 structure has not yet been deployed, so the deployed GBAD units ashore are being coordinated by the AAWC at sea;
- Fighters: Air Defence aircraft attached to the force, being directed by AD ships or by:
- AEW a/c: Airborne Early Warning aircraft, providing the air picture to the force and capable of directing fighters;
- AAR a/c: Air-to-Air Refuelling aircraft, capable of providing fuel to fighters in-flight;
- Airbases and squadrons from where the fighters, AEW, and AAR aircraft deploy.

Figure 4 shows the internal process view of the JAD process, using the OODA-RR model with IDEF0 diagrams for each process step. The Orient process is decomposed in three steps. Initially the actual situation is compared with the sets of predefined conditions in the prototype repository (the PPRs). If a match occurs, it triggers the corresponding set of actions, to be executed by the Act process, and the Decide process will be bypassed. If the match is not complete, the Orient process could initiate an adjustment of the sensor settings. This is the equivalent of the RPDM step "more information", and corresponds with the feed-back loop from Orient to Observe as specified by Boyd (1996).

Our research indicates that the OODA-RR model is probably not suitable for modelling all operational processes because, like OODA, it is specific to C2. Work has just started on the IFD for the Intelligence process, for which decomposition into INTEL sub-processes seems more suitable than into OODA-RR steps. C2 and Intelligence are closely related, of course, with the outputs of Intelligence forming part of the inputs to C2, with intelligence reports being ingested as a part of the Observe process. We expect to see this relationship in the developed IFD.

4. Conclusions and future research

4.1 Conclusions

A preliminary investigation into service oriented computing and on CIMIC information exchange processes using literature study shows a number of similarities. Various research issues identified in the literature for service oriented computing seem as well applicable to the problems with information sharing for CIMIC. This conclusion applies as well to the related area of Smart Service Networks.

Recent work by NLDA and TNO on the C4I architecture for the Netherlands Armed Forces has taken a service oriented approach. For this reason its initial results, *inter alia* an Operational Process Model including a method for the development of Information Flow Diagrams, could provide a suitable starting point for the investigation and modelling of CIMIC processes.

4.2 Future research

After finalizing the work on operational process modelling for the C4I architecture using Joint Air Defence and Intelligence as test applications, work will be extended to the existing shortfalls in information sharing between cooperating civil and military actors (CIMIC) in peace support operations. It is intended to start a PhD project for this purpose. Based on the similarities between CIMIC information exchange and service oriented computing as shown in this paper, the preliminary research question could be: *Could information sharing between civil and military partners in Peace Support Operations be improved by applying the principles and technologies of Service Oriented Computing?*

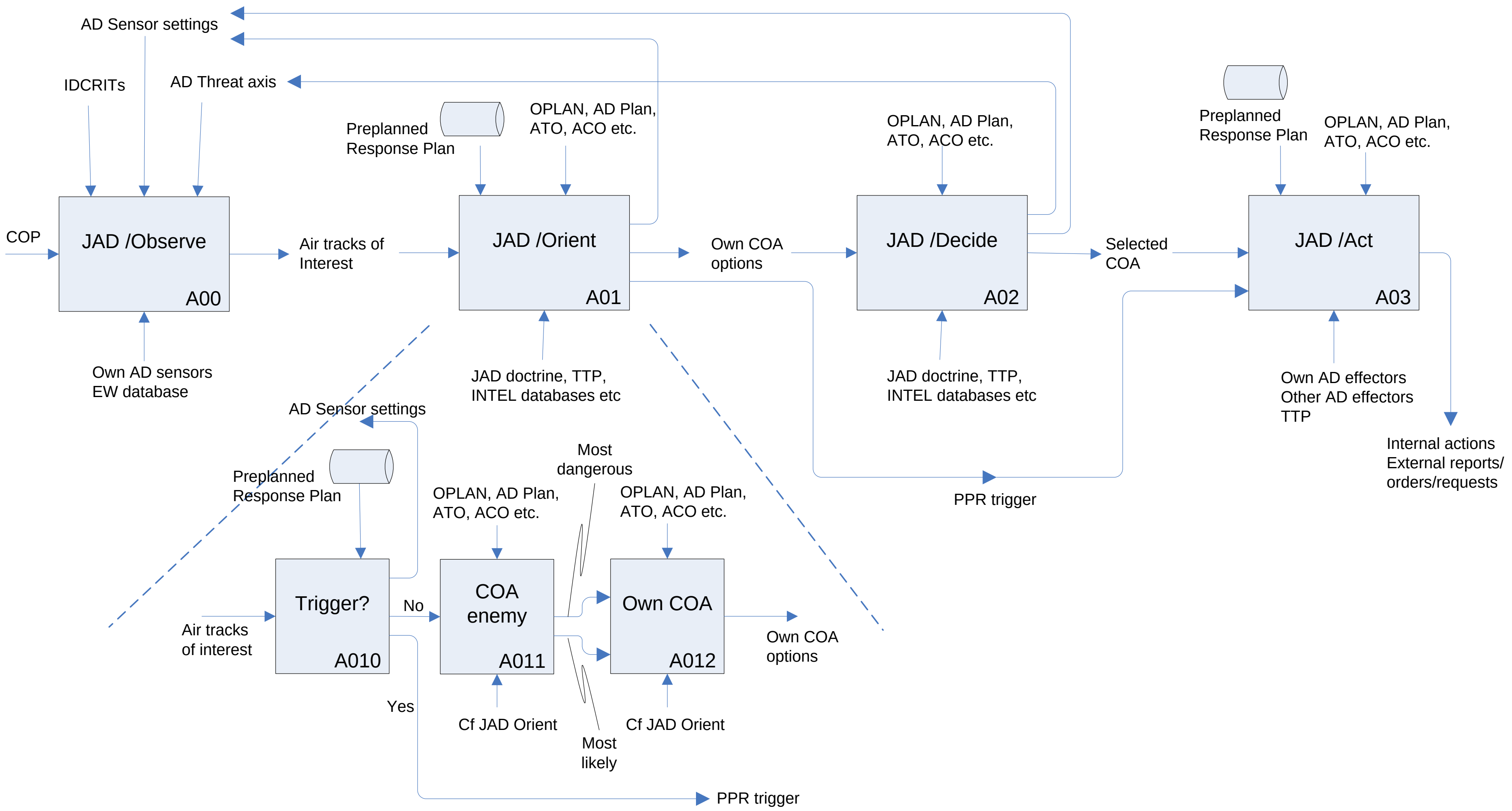

Figure 4: internal process view Joint Air Defence process

References

Alberts, D.S., and Hayes, R.E.(1995). *Command Arrangements for Peace Operations*. US DoD Command & Control Research Program, Washington DC, USA

Boyd, J.R. (1996) *The Essence of Winning and Losing*, unpublished lecture notes

Brehmer, B. (2005) *The Dynamic OODA Loop: Amalgamating Boyd's OODA loop and the cybernetic approach to Command & Control*, in Proceedings of the 10th ICCRTS, June 2005

Grant, T.J. (2005) *Unifying Planning and Control using an OODA-based Architecture*, Proceedings of SAICSIT 2005 p. 111 – 122

Grant, T.J., and Kooter, B.M. (2005) *Comparing OODA & Other Models as Operational View C2 Architectures,* in Proceedings of the 10th ICCRTS, June 2005

Grant, T.J., and Van den Heuvel, G.G.A. (2010). *Identifying C2 Tools for Bridging Cultural Gaps in Coalition Information Sharing.* Proceedings, 7th International Conference in Information Systems for Crisis Response And Management (ISCRAM 2010), 2-5 May 2010, Seattle, WA, USA, paper 236

Klein, G. (1998) *Sources of Power: How people make decisions*, MIT Press, Cambridge, Mass., USA, 1998

NATO (2007) *NATO Architecture Framework (NAF),* version 3, 2007

Ooms, D.M. & Grant, T.J. (2009). *Developing a C4I Architecture for the Netherlands Armed Forces,* Proceedings of 14th ICCRTS, June 2009

Papazoglou, M.P. (2005). *Extending the service oriented architecture*. Business Integration Journal, February 2005

Papazoglou, M.P. (2008). *Web Services: Principles and Technology*. Pearson Education Limited, Harlow, Essex, UK, 2008

Papazoglou, M.P., Traverso, P., Dustdar, S. and Leymann, F. (2008). *Service-Oriented Computing: A Research Roadmap*. International Journal of Cooperative Information Systems Vol. 17, No. 2 (2008).

Rietjens, S.J.H. (2006). *Civil-Military Cooperation in Response to a Complex Emergency: Just Another drill?* Dissertation at University of Twente, NL, 23 March 2006

Rietjens, S.J.H., Verlaan, K., Brocades Zaalberg, T.W. and De Boer, S.J. (2008). *Inter-organizational communication in civil-military cooperation during complex emergencies: a case study in Afghanistan*. Blackwell Publishing, Oxford, UK

SAM (2007) *Services Architectuur Methode (PAM) Defensie IV Architectuur (DIVA) (DIVA Services Architecture Method),* version 2.2, 8 May 2007

US DoD (2009) *DoD Architecture Framework* version 2.0, May 2009

Van den Heuvel, W.J.A.M. (2009). *Changing the face of the Global Digital Economy*. Inaugural speech at Tilburg University, NL, 30 November 2009

Van den Heuvel, G.G.A. (2010). *Share to win: Unravelling information sharing in dynamic coalitions.* Proceedings, 2010 European Conference on Information Systems (ECIS 2010), University of Pretoria, South Africa, 7-9 June 2010, paper 0309