Coalition Network Defence Common Operational Picture
(CNET-D COP)

Josef Kaderka
josef.kaderka@unob.cz
University of Defence
Kounicova 65
617 00 Brno, The Czech Republic

Abstract
This paper shortly describes selected examples of the prepared or existing systems for coalition collaboration. It deals also with the Coalition Network Defence Common Operational Picture (also called Coalition Information Assurance Common Operational Picture), which is momentarily investigated by the NATO RTO Exploratory Team.

Keywords: NEC, COP

1 Introduction
The way to reach the information superiority, which is a necessity for the successes of future coalition operations, is a concept of NATO Network Enabled Capability (NNEC). This concept is based on coherent integration of sensors, commanders and weapon systems along with support capabilities to create superior decision-making. Such combined structure will enable military forces to operate more effectively in the future strategic environment through the more efficient sharing and using of information. This way will lead to the better situational awareness across the board, facilitating improved decision-making, and bringing to bear the right military capabilities at the right time to achieve the desired military effect [1].

This enhanced capability will also exploit the benefits to be obtained from transformed doctrine and training and optimized command and control structures, moreover - the ability to respond more quickly and precisely will act as a force multiplier enabling forces to achieve the desired effect through a smaller number of more capable linked assets. NEC warfighting force elements will have the ability to operate at a higher level and pace. Intelligence gathered from multiple sources will be fused and presented to those who need it anytime, any place and anywhere in the theatre environment [2].

Information assurance constitutes the basis for confidence that the security measures work as intended to protect the system and the information it processes.

All kind of NEC activities naturally need reliable communication, which will be carried out purely using computer networks in the future conditions. Those networks will turn into viable important means for successive combat activity and therefore they can be seen as a new kind of fighting activity. Simply spoken, they can convert to the new battle space; moreover - networks will become a battle space, which will need to be defended. They will also come with increased vulnerability to attacks given the growing complexity of Information Technology (IT).

Several projects exist both on national and multinational levels, like US Network Centric Warfare (NCW) and NNEC conceptions. It is important to understand that some important differences occur between them. The goal of NCW is better collaboration among US branches of service to improve effectiveness of their joined operations. The NNEC is rather targeted to reach better interoperability among individual countries, i.e. it is slightly less ambitious, but realistic. A crucial principle is that every national force will have to share, actively and passively, some information resources. It exposes national control, command, information and other systems to the increased threats. Of course, many delicate and sensitive questions to solve are here; not only technical, but also (primarily) political.
It is suitable to mention herein already existing NATO Multilateral Interoperability Program (MIP), which among others encompasses:

- Objective to share
- Situational Awareness
- Plans and Orders
- NBC alerts and critical messages
- Common Interface Specification
- Message Exchange Mechanisms (MEM - AdapP-3)
- Data Exchange automatic push (Data Exchange Mechanisms - DEM)
- LC2IEDM (Land Command and Control Information Exchange Data Model) = semantic meaning
- Nations interface on a secure LAN
- LC2IEDM Data Model

2 Examples of Secure Coalition Collaboration Systems

2.1 TTCP

Several nations or group of nations (including non-NATO) intensely work on secure collaboration tasks for longer time period. The Technical Cooperation Program (TTCP), whose members are Australia, Canada, New Zealand, UK and USA is an example. Information exchange regarding potential or real threats and incidents among mentioned nations was organized on manual procedures in past. It brought into significant delays: hours – but even days! Moreover, personal mutual trust built up between members internationally was feasible on the strategic level and under relatively invariable conditions. The multinational combat operations constitute entirely different environment.

The Domain Approach [3] as an approach to security architecture capture developed for the UK Ministry of Defence, initially by Defence Evaluation and Research Agency (DERA) and after it’s splitting was partially adopted by QinetiQ [4] (the Defence Science and Technology Laboratory - DSTL - is the second successor). Its focus is the data exchanges between discrete, classified information systems.

The basic idea of the Domain Approach is that people who collaborate closely and share the same IT facilities on a daily basis work together in a domain. Domains can be described as logical places within an information system, where people can perform their work by means of software, acting on their behalf. People who work in the same domain are given the authority, and have the need, to freely exchange data. The only information security controls are who may work in the domain, the nature of the data handled in the domain, and the IT tools and applications that can be used in the domain. Of course, some other similar national projects already exist. They were realized primarily in the USA and later by some of their coalition partners to solve operational problem [5], see next paragraphs.

2.2 CENTRIXS

Coalition Commanders need to stand up the Task Force quickly, assume roles, conduct planning, and monitor execution through all stages of coalition operations (planning, deployment, execution, and redeployment). Therefore, separate Combined Enterprise Regional Information Exchange System (CENTRIXS) [6] networks are required for each coalition domain. The CENTRIXS network is both network-centric and web-centric, using a combination of readily available Commercial-Off-The-Shelf (COTS) and Government-Off-The-Shelf (GOTS) solutions to reduce implementation costs while providing a robust, innovative approach to warfighting communications.
CENTRIXS implementation first focused on fielding core collaboration services (i.e., e-mail with and without attachments, web-browser-based data access, and file sharing). Other required services to include tactical, near-real-time data access, have been enabled as the network has matured. To the extent possible, CENTRIXS will subsume and consolidate existing coalition networks as part of a single, unified system.

The basic mission of CENTRIXS is to support the secure, sharing and exchanging of intelligence and operations information through reliable communications connectivity, data manipulation, and automated processes. CENTRIXS services provide Combatant Command (COCOM) commanders with:

- Common and consistent situational awareness of the battlefield Common Operational Picture (COP)
- Common Intelligence Picture (CIP)
- Electronic mail (Email) with attachments
- Web-enabled services, office automation, bulletin boards, and chat service (collaboration services)
- Voice over Secure Internet Protocol (VoIP)

However, separate CENTRIXS domains, incompatible data models and multi-national composition usually limit coalition communications to text messages and manual data entry. Text messages, typically have used, are slow (often due to manual processing), inaccurate (possible typographical errors), and require translation in exchanges between coalition partners that do not share a common language.

### 2.3 COSMOS

The Coalition Secure Management and Operations System (COSMOS) project is currently under development and testing by countries mentioned above. Some information regarding COSMOS project can be found also in [7], from where were next items taken over.

1. **Capability**
   - Application-independent (indigenous) Coalition C2 Systems ("Come as you are")
   - Collapse multiple CENTRIXS networks into a single IP network
   - Role-Based Release

2. **Function**
   - Machine-to-machine data sharing
   - Improved information sharing
   - Reduced footprint (hardware, software, power, air conditioning, operators, support, etc.)
   - Share information on the basis of nation's functional roles in the coalition, and in accordance with the originator's assigned sensitivity and other values

3. **Technology**
   - Command and Control Information Exchange Data Model (C2IEDM)
   - Virtual Private Networks
   - Data Management
   - Multi-Level Security
   - Data Management
   - Multi-Level Security
   - Multiple Security Levels
Shared Vision and Purpose High Level Operational Requirements (COSMOS Management Plan):

- Enable protected lateral communication across a collapsed CENTRIXS environment.
- Enable machine-to-machine exchange of command and control information between MIP-compliant systems and applications.
- Reduce the number of coalition networks required to support Coalition Task Force operations within a theatre of operations.
- Enable coalition members to share information with other coalition members based upon roles.
- Enable coalition members without a MIP-compliant system to receive command and control information.
- Enable any MIP compliant partner to engage with, or disengage from, the coalition without disrupting the information sharing capability of the network.

COSMOS is

- Focused on high tactical and operational level coalition information sharing among coalition partners known to each other to be participating in combined operations.
- About taking advantage of a well defined and internationally agreed to “information language set” designed for C2 interoperability and using it to.
- Enforce the discrete dissemination (Protected Sharing) of released information to those coalition partners who have a need to know based on role.
- Focused toward a single Secret High Releasable to Coalition network.

COSMOS is NOT

- About generating a first instantiation of a complete MNIS Protection Profile (Draft)-compliant network environment.
- A Cross-Domain capability between national networks (e.g., SIPRNET) and CENTRIXS.

2.4 FGAN/FKIE

Another interesting research is conducted in Germany at FGAN/FKIE (Forschungsgesellschaft für Angewandte Naturwissenschaften, Forschungsinstitut für Kommunikation, Informationsverarbeitung und Ergonomie) institutes [8]. Their effort is focused on the Intrusion Detection Systems. Despite of rather neutral/civilian designation, the authors take into account special military requisites (MITE - MANET Intrusion Detection for Tactical Environments) in their projects. Other security targeted research and projects take place there [9], [12].

3 NATO RESEARCH

Among others, the NATO RTO Exploratory Team (ET) on Coalition Information Assurance Common Operational Picture (CIA COP) has been established in 2005. One of its missions was a debate over important aspects of coalition information assurance in future warfare. Next and more concretely, to decide regarding following steps in that area; to suggest a Technical Activity Proposal or not; and eventually prepare supporting and other materials. The Exploratory Team preliminary decision is to propose establishing of the NATO Research Task Group (RTG) for the next consideration. The ET also has decided to use new designation Coalition Network Defence Common Operational Picture (CNet-D COP) instead of CIA COP and it has prepared some groundwork. The term Common Operational (sometimes Operation) Picture can be defined like “A single identical display of relevant information shared by more than one command. A common operational picture facilitates collaborative planning and assists all echelons to achieve situational awareness.” [10]
After discussion and adjustments, the ET also preliminarily agreed on a data model, based on previous Canadian research. There is a Computer Network Defence Situational Awareness term (CND SA) widely discussed. It is interpreted as a superset of Common Operational Picture, because it encompasses not only information referring to the combat activity (which is rudimentary important for the Force Commander), but also computer network security-related business.

When dealing with CND SA from the battlefield point of view, the usual Observe – Orient – Decide – Act cycle can be used. The logical network environment can be divided into following elements: IT Services, IT Infrastructure (Vulnerabilities, Safeguards). CND SA must provide feedback to the Force Command concerning defensive posture, risk, and impact using statements of potential and real reductions in these IT Services.

For example, new areas for new research exist [11]:

- The semantics and syntax for describing IT Services required by the Force Command to support operations is an area for further research. It is envisioned that the semantics will include value statements for confidentiality, integrity and availability. Of these three qualities, availability seems to be understood the best.

- A simple mathematics for defining relative requirements is needed. This mathematics will likely be tied into the semantic values for each of the three qualities of service. The relationships between Quality of Protection (QoP) values cannot be finalized until the value semantics is defined.

- When defining IT Services, some definition of a QoP that must be maintained will be defined. In the model mentioned above, impact is also defined as the lack of providing an agreed set of IT Services at some defined QoP. The notion of how impact changes over time with respect to the IT Service definition is not well understood and requires further research.

The NATO Research Task Group (RTG) on Coalition Network Defence Common Operational Picture, if its setting up will be agreed, will be open for every NATO nation. It could be a good opportunity both for scientific collaboration and effectual activity.

CNet-D COP is composed of two aspects of information assurance: secure information sharing in a coalition environment and the computer network situational awareness. This task group will focus on the latter as it pertains to a coalition network environment. A representative Computer Network Defence Situational Awareness Model and a Data Exchange Model should be developed and made available to a NATO Standards Panel for coordination between the NATO nations.

4 Conclusion

Network defence command and control requires the merging of IA, Network Management, and Command and Control. The task group can help to enhance the understanding and awareness of network and security management with in the Coalition NETOPS environment. The objectives of that NATO group is to advance research and technology in computer network defence situational awareness, as a step towards defining a common data model for the network defence command and control; as a potential base for future standardisation efforts. Next steps could be as follows:

- Recommend CnET-D WG (C2 of IA):
  - Clear definition of Information Assurance
  - Define coherent IA Data Model
  - Define coalition required IA Data Model interchanges
  - Influence MIP Baseline 4/5 development
  - Collaborate in defining MIP extensions for IA
• Consider C COP Security WG (IA of C2):
  • Boundary Controller (BC) Research
  • Complexity of MIP data model
  • Release/Security policy reflects commander intent
  • Sufficient trust in BC
  • Distributed & dynamic coalition communications

Coalition interoperability is of key importance to NATO and Coalition Network Defence Common Operational Picture is a future requirement to support network-enabled operations. There is momentum in NATO for increased Coalition information sharing, such as the use of Multilateral Interoperability Program (MIP) and its information exchange data model, to facilitate the establishment of Coalition Common Operating Pictures (CCOP). Computer Network Defence plays a vital part in operations and needs to be represented within the overall CCOP. There is no international endeavour incorporating CNet-D COP into the overall CCOP and it is necessary to initiate it at this time.

Several supporting nations have started developing their own Network Defence COPs, which would support the development of a common Coalition Net-D data model. The recommending of creation new RTO Task Group to address the related research and technological issues appears desirable. The experts in Computer Network Defence, Cyber Situational Awareness and Command and Control for network-enabled operations coming from participating countries will be needed.

References