Interoperable Sharing of Data with the Coalition Shared Data (CSD) Server

Barbara Essendorfer
Fraunhofer IITB, Fraunhoferstrasse 1, 76131 Karlsruhe, Germany

Barbara.Essendorfer@iitb.fraunhofer.de

Wilmuth Mueller
NATO Consultation, Command and Control (C3) Agency,
Oude Waalsdorperweg 61, 2597 AK The Hague, Netherlands

Wilmuth.Mueller@nc3a.nato.int

ABSTRACT

In crisis management quick and full situation awareness is essential to enable adequate countermeasures and reactions. Relevant information has to be distributed to agencies and decision makers. To overcome the limitations of today's stovepiped ISR systems, interoperable transnational systems, capable of including all relevant data sources and sharing them among law enforcement bodies, are needed.

To enforce the interoperability of ISR systems the multinational nine-nation intelligence and surveillance project MAJIIC (Multi-Sensor Aerospace-Ground Joint ISR Interoperability Coalition) developed standards, technologies and an architecture that allow commanders to instantly tap into real-time data from a number of NATO and national systems. Standardized data dissemination is the key in achieving interoperability. A Coalition Shared Data (CSD) server, which is based on STANAG 4559 is the core of that architecture and enables the dissemination and storage of data from heterogeneous sensors from different nations, as well as tasking information and sensor data exploitation results.

To make information available no matter where it is stored and where it is needed, the CSD concept envisions the near real-time synchronization of the metadata between different servers. The information about products in the CSD is available in the whole network, regardless of where those products are stored. Each user needs to know only one access point, his local CSD, but has access to the whole data in the network (under the provision of granted access rights by the owner of the data). If the product is of interest, it can be requested from the local CSD. Request forwarding for not locally stored data and delivery is handled by the interconnected and synchronized CSDs.

The CSD concept passed its first full-blown test during a major NATO exercise in Norway, Bold Avenger/Trial Quest 2007, which included real-time maneuvers by several thousand air and ground forces. In 2008 the concept was successfully tested during the Bundeswehr experiment Common Shield 2008. An adaptation of the concept has been tested in the project SOBCAH (Surveillance of borders, coastlines and harbours), partially funded by the European Commission under the Preparatory Action for Security Research (PASR) 2005 program.

The proven benefit of information sharing through the CSD at the NATO exercise Bold Avenger/Trial Quest 2007 and the Bundeswehr experiment Common Shield 2008, led to the planning of fielding the CSD in NATO and Bundeswehr in 2009 - 2010.

1.0 INTRODUCTION

In crisis management quick and full situation awareness is essential to enable adequate countermeasures and reactions. Relevant information has to be distributed to agencies and decision makers. Combining sensor information with intelligence data and sharing relevant information according to user requirements enhances the situation awareness of decision makers and enables them to act quickly and efficiently.

A crisis and emergency situation caused by terrorism – being it either in the phase of preventing terrorist attacks or crisis response after an attack has occurred – may be characterised as follows:

- Different security and crisis response organisations are involved, both military and civil
- The crisis response operations are very diverse in nature
- Each organisation or even entity employs its own surveillance and reconnaissance assets, which are heterogeneous in nature, designed and procured for different purposes and operating in a stovepiped manner.

This characterisation applies both to security forces within the European Union and NATO. Information that might be of interest for different members is not provided in time or even at all because information sharing capabilities are missing. Due to that, possibilities to avoid attacks or respond timely in an emergency situation are limited.

To overcome these limitations, interoperable transnational systems, capable of including all relevant data sources and sharing them among law enforcement bodies, are needed. In our paper we will present solutions for harmonising and integrating ISR data and information as well as access and dissemination mechanisms of integrated ISR which lead to enhanced situation awareness.

The remainder of this paper is organised as follows: In section 2 we motivate the need for situation awareness in crisis response operations and describe the mix of ISR systems needed to gain the necessary situation awareness for decision making and response actions in a large-scale crisis. Section 3 provides an architecture for integrated interoperable ISR systems and shows how the developed architecture leads to improved situation awareness in a crisis response operation. Section 4 gives an overview of the employment of the architecture in coalition exercises and the results of it. In section 5 conclusions are given.

2.0 SITUATION AWARENESS IN CRISIS RESPONSE OPERATIONS

In order to make the right decisions and initiate the adequate countermeasures and reactions in a large-scale crisis, the persons in charge must be fully aware of the current situation.

Situation awareness means that threats and suspicious behavior have to be perceived, the threat has to be understood and an appropriate reaction has to be performed [3]. To perceive threats, products from different sources (information systems, sensors, exploitation systems) have to be available. The data has to be accessible with respect to time and location of the product as well as to other decision-relevant (e.g. urgency) information. Relevant sources of knowledge should be incorporated. Situation awareness is achieved by developing a common operational picture. To support analysts, operators and commands it is important to integrate the correct i.e. temporally relevant information in this common picture in a user-friendly manner [4].

To enhance situation awareness by ISR (intelligence, surveillance, reconnaissance) it is necessary to use of a number of systems that detect threats and conspicuous behavior. The generated information has to be shared within the coalition of crisis response forces.

Information sharing in a coalition involves the need to adapt that information to the task an operator has to fulfil, to the level of command and to the overall situation where that data is needed. If data is needed for tactical ISR in operations it has to be provided in (near) real time and on often directly from the sensor. If data is needed for strategic ISR in the home country it is often not necessary to provide it immediately and exploited data is of interest. Due to that, information has to be provided in different granularity.

Depending on the command level and the AOR (Area of Responsibility) the degree of information has to be adaptable and has to be not only at the right place within the right time but also with the right granularity. The use of a mix of sensor and information systems is key to adequate situation awareness on the different command levels and to adequate response.

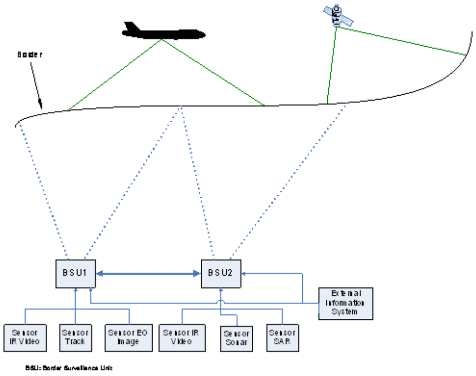


Figure 1: ISR with multiple surveillance systems on different levels

Within an integrated system, disparate technologies that complement one another are installed, the interaction of the data output is essential. An integrated system consists of sensors, exploitation systems (that might also be deployed as situational awareness displays) and external information systems.

In Figure 1 an area of responsibility is monitored by a range of different sensor types. Those sensors deliver data to command. However, the areas that are monitored intersect and data that is of interest for one command may also be of interest for adjacent commands. Thus it is necessary to share data and add information from external systems to be able to get enhanced situation awareness.

Sensor systems normally consist of the sensor and a ground station that does the primary data processing and possibly some exploitation. Combined sensor systems that consist of different sensors might use some sensors as triggers for others and only the secondary information is passed on to an “outside” exploitation system. Depending on the sensor type and the processing a proprietary (raw) data stream may be created. To observe land and sea borders it is necessary to make use of different sensor types with differing ranges and tasks [5].

Long-range border surveillance conducted by space borne and airborne systems is of interest for an all-weather and 24 hour detection of threats that harm a wide area (e.g. oil slicks that indicate an attack on the environment and/or on nations resource supply). These sensors can deliver all kinds of imagery such as IR (infrared), EO (electro optical) and SAR (synthetic aperture radar) as well as motion imagery (video), SIGINT (signal intelligence) or radar data.

Airborne sensors, including the use of balloons or zeppelins can be used for medium-range border surveillance.

Ground-based or seaborne sensors are mainly used for short-range surveillance. Real time information can be provided on critical areas, objects and people. Seaborne sensors can be installed above (cameras, radar) or under water (e.g. sonar, metal detection).

The display of sensor data in a common operational picture only makes sense if the operator/analyst is able to interpret that information correctly. Raw sensor data has to be interpreted by specialists. Therefore sensor data is only provided on system or liaison level.

Exploitation Systems are used for the exploitation of preproduced data. Exploitation can be done in different contexts and can be specific to the system, data type, area or task. For exploitation systems that work on products that are produced from multiple sensors it is important that the data is available in an inter-coordinated data format. Exploited data normally already contains more enhanced information. Similar to the sensor data it has to be integrated adequately into a common operational picture. This type of information is of interest for upper decision bodies. Still some special expertise is needed to read and decide upon it. If information is needed on a national legal level only the result of an analysis would be provided. The main effort on this level would be to fuse information from different sources.

Information systems are relevant for the rating/ evaluation of derived data and information. Weather data can give essential advice which product sources are of interest in certain circumstances can provide background information for all kinds of questions (provided it is understood that this is in general low grade intelligence).

Due to todays stovepiped systems information sharing is possible only with delay or not at all. This prevents provision of full situation awareness to decision makers. To overcome these shortfalls ISR systems has to be interoperable in order to be able to share information in a timely manner.

It has to be understood that information sharing between different nations and even within the nations is not only a technical challenge but also a challenge to the nations' security restrictions and the current processes that are used in ISR within nations. The processes that are currently used where not developed for the task of Defence against Terrorism (DAT) but for conflicts between nations and a clearly defined enemy.

Still, the first task to be solved is to ensure the interoperability of the ISR systems employed.

3.0 INTEGRATED INTEROPERABLE ISR SYSTEMS

To enforce the interoperability of ISR systems, the multinational nine-nation intelligence and surveillance project MAJIIC (Multi-Sensor Aerospace-Ground Joint ISR Interoperability Coalition) was set up [1]. The primary aim of the MAJIIC project is to improve the commanders' situation awareness through collaborative employment and use of interoperable ISR sensor and exploitation systems. To achieve this and to maximize military utility of ISTAR-systems, interoperability is addressed from three primary perspectives:

- Operational, including development and demonstration of concepts of employment (CONEMP) and tactics, techniques and procedures (TTP) for collaborative employment and use of coalition ISR assets in support of military missions.

- Architectural, including development of procedures and technology for sharing ISR data and information, system architecture design principles, tools and technology for collaboration and tools for managing coalition ISR assets.

- Technical, including definition and development of key data formats and protocols for the various sensor and data types.

The sensor platforms addressed by the MAJIIC project include space-based, airborne, ground-based or maritime as well as manned and unmanned subsets of these. The sensor platforms range from small tactical systems usually assigned to tactical commands and all the way up to highly capable strategic multi-user systems.

The sensor data types addressed in MAJIIC include GMTI (Ground Moving Target Indicator) radar, synthetic aperture radar (SAR), electro-optical (EO) and infra-red (IR) imaging and video sensors, artillery locating radar, and electronic warfare support measures (ESM) sensors.

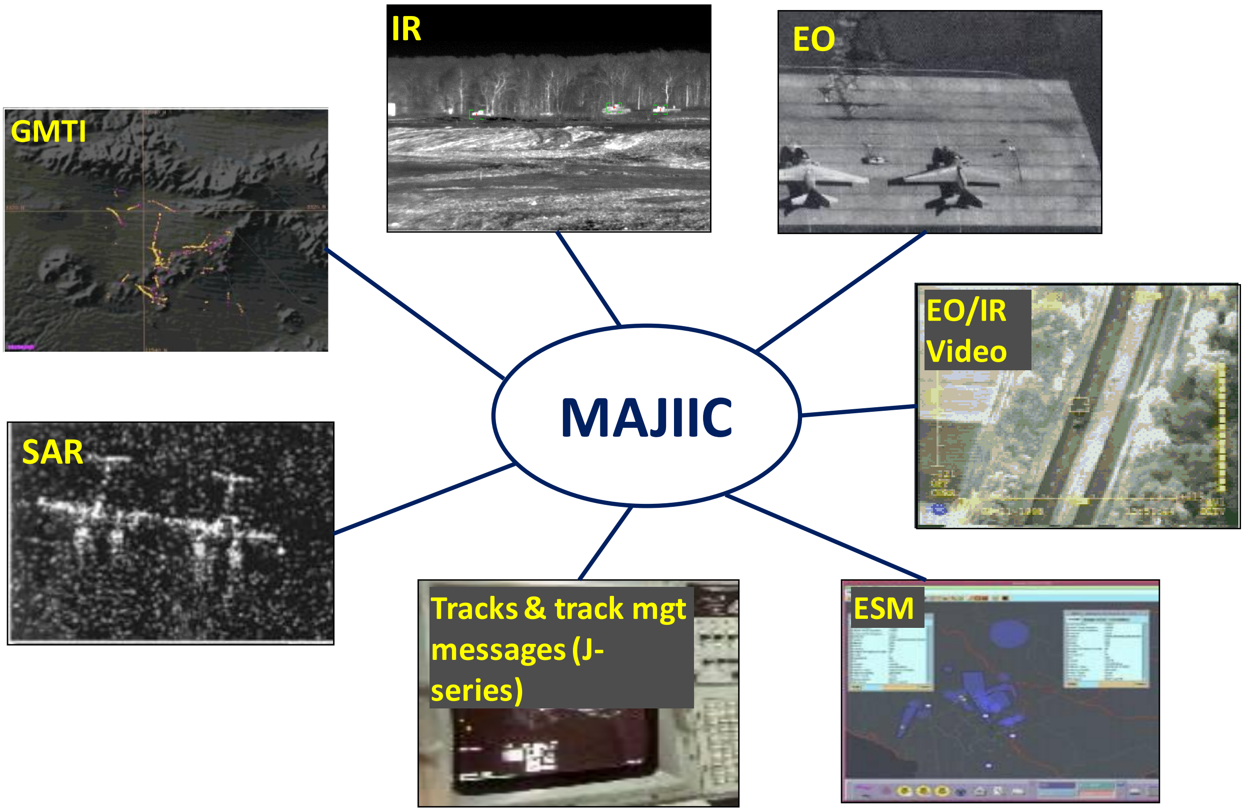


Figure 2: Sensor data types addressed by the MAJIIC project

3.1 An Architecture for interoperable ISR systems

In order to achieve the aim to improve the commanders' situation awareness, an appropriate architecture for integrating all the ISR assets and sensor data and to enable interoperability between ISR and C2 systems is necessary.

Crisis response operations require the co-ordination across the whole spectrum of command levels, each with their own personnel, systems, assets and equipment. It is required to collect, manage, and exploit data from numerous sources including NATO and National, military and non-military, governmental and non-governmental sources; and make the data and the results of the exploitation available in such a way that the right information is available to the right people at the right time in the right format.

The task of information sharing in a crisis response domain places requirements on the architecture. To be able to share data and information three main aspects have to be taken into account:

Information has to be provided according to user needs and requirements: As data has to be provided to users according to their task (analyst, decision maker in multinational operations or for forensic analysis), data access has to be linked to predefined user roles. Information is gathered at different locations, so distributed data access has to be enabled. To integrate information systems with different semantics, intelligent methods of information retrieval have to be established.

Information has to be provided in time and at the right place: An adequate data transmission network is required (i.e. distributed architecture and standardized mechanisms to access data). Databases at different locations have to be able to synchronize their information, without synchronizing all of the data as this would mean shifting unnecessary data loads through the network.

Information has to be reliable and secure: To be able to make the right decisions and react appropriately, information has to be reliable. Access to classified data has to be limited to entitled agencies and persons. Data transfer has to be secure and protected against cyber attacks.

Taking into account the requirements and aspects stated above, an architecture was developed in which standardized data dissemination is the key to achieve the stated aim.

The architecture foresees the use of common interfaces for data formats and exchange mechanisms. The inner workings of each employed system are left untouched and only minor external interface modifications are required. The common formats and exchange mechanisms employed in MAJIIC are based on NATO standardisation agreements (STANAGs).

As the employed sensor systems normally do not deliver the data in the standard formats, converters have to be developed that translate the incoming data into a common data format. As can be seen in Figure 3 different proprietary data formats are converted into a standardized one, so that inquirers do not have to know the type of source (e.g. sonar, radar or infrared) the information is coming from, but can focus on the information itself.

For example imagery is transferred to STANAG 4545 [6], motion imagery to 4609 [7], GMTI data to STANAG 4607 [12], and tracks to STANAG 5516 [8].

The standardized data is then transferred over the network to a local data server. Figure 3 shows an example of a regional network with (via converters) connected information suppliers such as sensor stations, criminal registers, etc. Connected to the same network are exploitation systems taking in a filtered set of the provided information (depending on the tasking). By fusion and analysis they generate new additional information (e.g. reports) that is also stored in the data server(s). Situational awareness systems are able to display selected intelligence and can ask for additional information from sensors, exploitation or information systems to support decision makers.

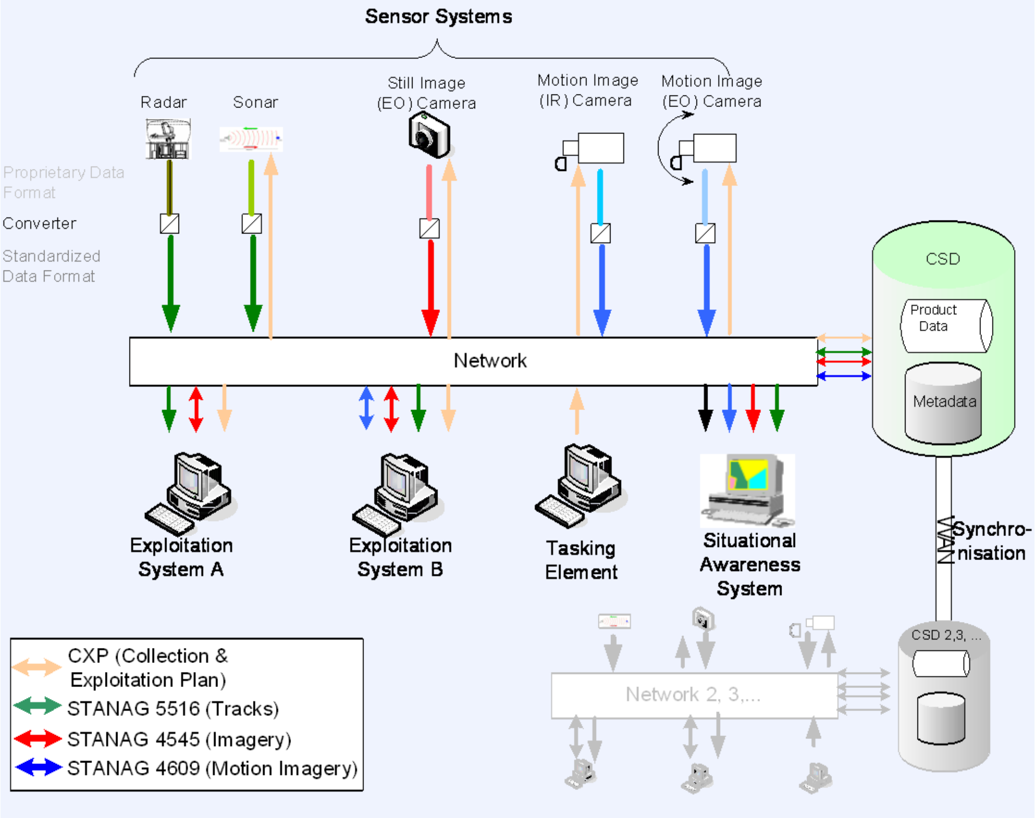


Figure 3: Information sharing in a local network and synchronization

3.2 The Coalition Shared Data (CSD) Server

The key component of that architecture is the data server. The server concept developed under MAJIIC as a Coalition Shared Data (CSD) server, is based on STANAG 4559 [2] and provides a mechanism for distributed, searchable, persistent storage and retrieval of Joint ISR sensor data as well as exploited data and information, such as tracks and exploitation reports and tasking information.

Data in the common format is stored in the CSD and can be accessed by clients via the access mechanisms provided by STANAG 4559. The stored data consists of the actual ISR-data and a set of metadata that describes it. The metadata is defined within the STANAG and gives information about the geo-location and the time when a product (e.g. an image) was acquired, the source of the data, security settings or product specific information (e.g. resolution). Based on this metadata, a user has the ability to query and subscribe to information that is of interest for him. Over the standardized interfaces he can retrieve the information he needs depending on his role.

To retrieve a product a client (working on a system) asks for the metadata and is able to order the product if it is of interest to the user. Within the metadata all (for the domain) relevant aspects of the product are defined and queryable. Those parameters could be for example: location, time, speed, friend/foe, weather condition, certainty/quality of the info, product type.

The user can either use an interactive query where the database is searched once or a subscription method where the data query is transferred to the server once and continues running for a set time interval whereby the client is automatically notified whenever new incoming data sets fit the query parameters.

Considering the security of the data user roles should be supported, i.e. clients need an account specifying their access rights and statuses. For restricted information a login and user password have to be supplied before each connection to guarantee the authenticity and the right of access. The users should be supported by single sign on procedures. Additionally, the usage of certificates raises the security of the system to a satisfactory level.

To make information available no matter where it is stored and where it is needed, the CSD concept envisions the near real-time synchronization of the metadata between different servers. The information about products in the CSD is available in the whole network, regardless of where those products are stored. Each user needs to know only one access point, his local CSD, but has access to the whole data in the network (under the provision of granted access rights by the owner of the data). If the product is of interest, it can be requested from the local CSD. Request forwarding for not locally stored data and delivery is handled by the interconnected and synchronized CSDs.

3.3 Improved situation awareness with integrated interoperable ISR systems

With the described architecture a timely delivery of the needed information to decision makers is enabled, which leads to their improved situation awareness.

With the CSD ISR systems can publish and retrieve the information which is needed. A sensor system has the ability to retrieve its tasking and information about the operational architecture and publish the sensor data it produces. An exploitation system can receive sensor products and tasking information and publish the exploitation results it produces, e.g. annotated imagery, relevant video clips, MTI tracks or exploitation reports. A situation awareness system has the ability to only retrieve information that is of relevance for command and control.

An example: Based on information requirements a C2 system generates tasks that are stored in the CSD combined with metadata (creator, time, status etc.). In a next step, a sensor system gets the relevant tasks either automatically (subscription) or on demand (query) by querying the metadata database using a CSD client. Based on the task the sensor system plans its mission and generates sensor data which is stored in the CSD. The sensor data can be associated with the task - by that the relation task/sensor product can be reconstructed later on.

An exploitation system has been given the task to produce information regarding a specific area of interest. The analyst queries for specific (sensor) products which lie in his tasked area and analyses them. As a result, reports are generated and associated with the task and the sensor data. By that the whole reconnaissance cycle can be retraced and exploited data can be contextualized within forensic analysis. Sensor products of different sensor types (GMTI, images and videos) can be reviewed, combined and thoroughly analyzed.

4.0 DEPLOYMENT OF THE ARCHITECTURE IN COALITION EXERCISES

The CSD concept passed its first full-blown test during a major NATO exercise in Norway, Bold Avenger/Trial Quest 2007 [9], which included real-time manoeuvres by several thousand air and ground forces. During the exercise joint ISR interoperability was demonstrated in a ‘Live’ environment with a multi-sensor, multi-service geographically dispersed set-up (see Figure 4).

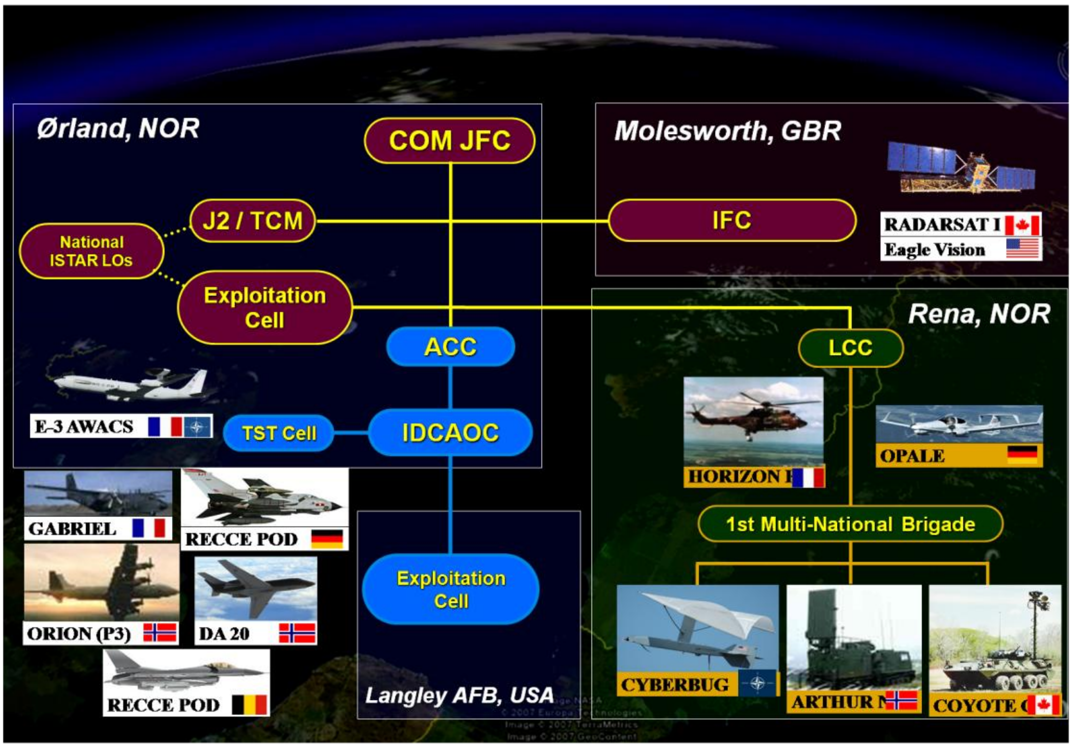
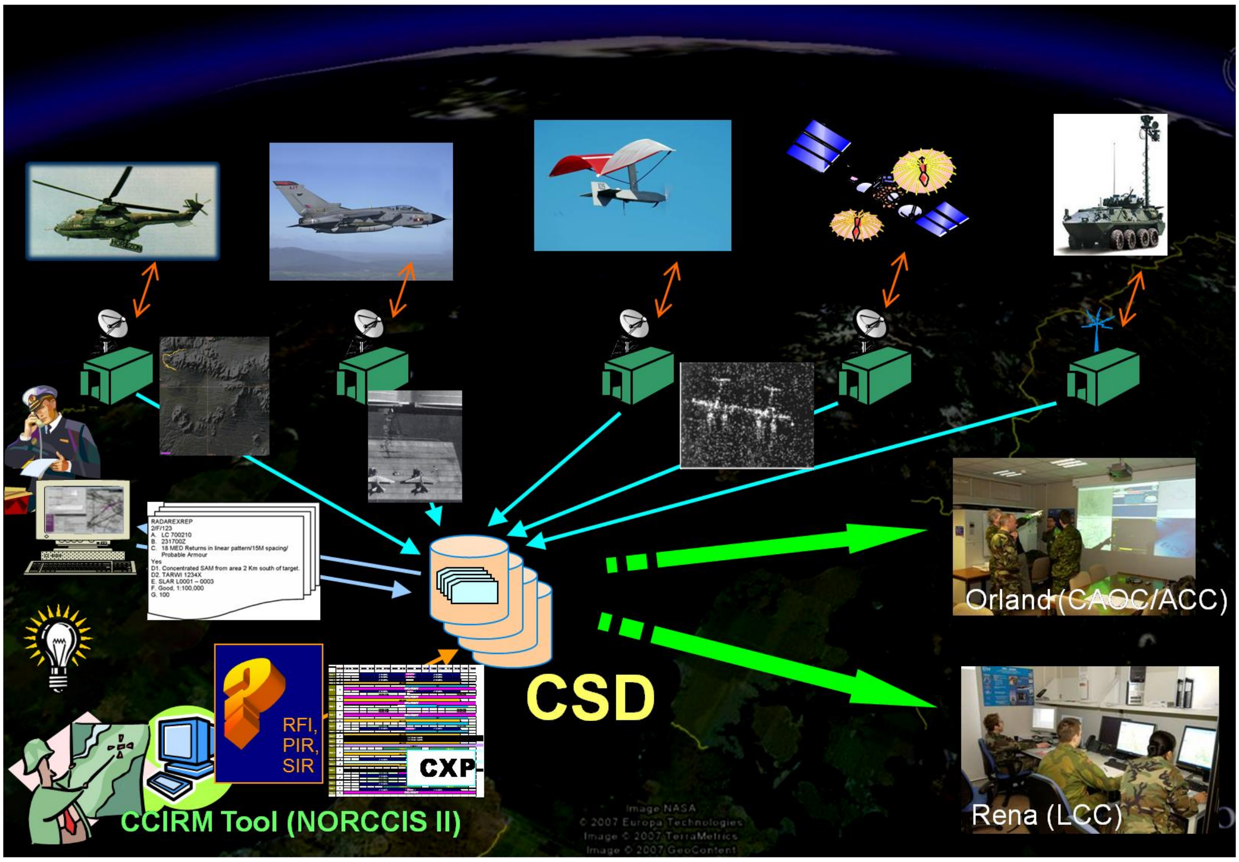


Figure 4: Trial Quest operational architecture

During TQ the operational processes were supported by the designed architecture and CSD concept (see Figure 5): The ACC and LCC respectively its collection manager receives RFIs (request for information), details them into PIRs (prioritized information requirements) and SIRs (specialized information requirements), generates collection and exploitation tasks, allocates those tasks to the available assets and compiles the Collection and Exploitation Plan (CXP). The CXP is published together with the associated PIRs and SIRs on the CSD. The collection asset commander, which has subscribed to the CSD for CXPs receives the newest CXP automatically, plans it mission and starts the collection according to the task defined in the CXP. As soon as sensor data is available, the data is posted to the CSD from where it is available to all users with the appropriate access rights. Users may either query for sensor data or subscribe to it for automatic delivery. Sensor data analysts query or subscribe to sensor data according to their exploitation task – which they receive via the CXP – retrieve the sensor data, perform the analysis and exploitation, produce the exploitation results and post it to the CSD. From there the information is available to all commands interested on the information and may be retrieved. The collection manager retrieves the exploitation results as well and closes the answered RFIs and with that the CCIRM loop.



RADAREXREP
2/F/123
A. LC 700210
B. 231700Z
C. 18 MED Returns in linear pattern/15M spacing/
Probable Armour
Yes
D1. Concentrated SAM from area 2 Km south of target.
D2. TARWI 1234X
E. SLAR L0001 – 0003
F. Good, 1:100,000
G. 100

Figure 5: Operational processes in Trial Quest

In 2008 the concept was successfully tested during the common Bundeswehr experiment Common Shield 2008 and NATO DAT (Defence against terrorism) experiments Technology of ISTAR against Terrorism, Critical Infrastructure Protection, and Harbour Protection Trial [10]. The aim of the Common Shield exercise was to test C2 processes in a NEC (network enabled capability) environment with integrated ISR and C2 systems. The Common Shield architecture integrated sensor systems, exploitation capabilities, situation awareness tools and common operational picture displays, and C2 systems provided by 27 different producers. Amongst the collection assets there were airborne imaging sensors like the Bundeswehr Recce Tornado with Recce Pod and RecceLite pod, the OPALE UAV with infrared video sensor, the Condor UAV with high resolution electro-optical video sensor; ground based imaging sensors; but also ground based radar systems providing MTI and chemical sensors capable to detect explosives as well as sea-based surface and sub-surface sensors. Exploitation systems provided capabilities to exploit still and motion imagery, MTI data, to fuse alarms generated by the chemical explosive detection sensors with imagery, and to fuse alarms and tracks generated by the sea-borne sensors with imagery. The overall system is depicted in Figure 6.

The seamless data and information exchange of all the sensor data and exploitation products with an real-time update of the common operational picture was enabled by the employment of a series of CSDs with the capability of storage, query, subscribe and retrieve, and automatic real-time synchronisation of metadata.

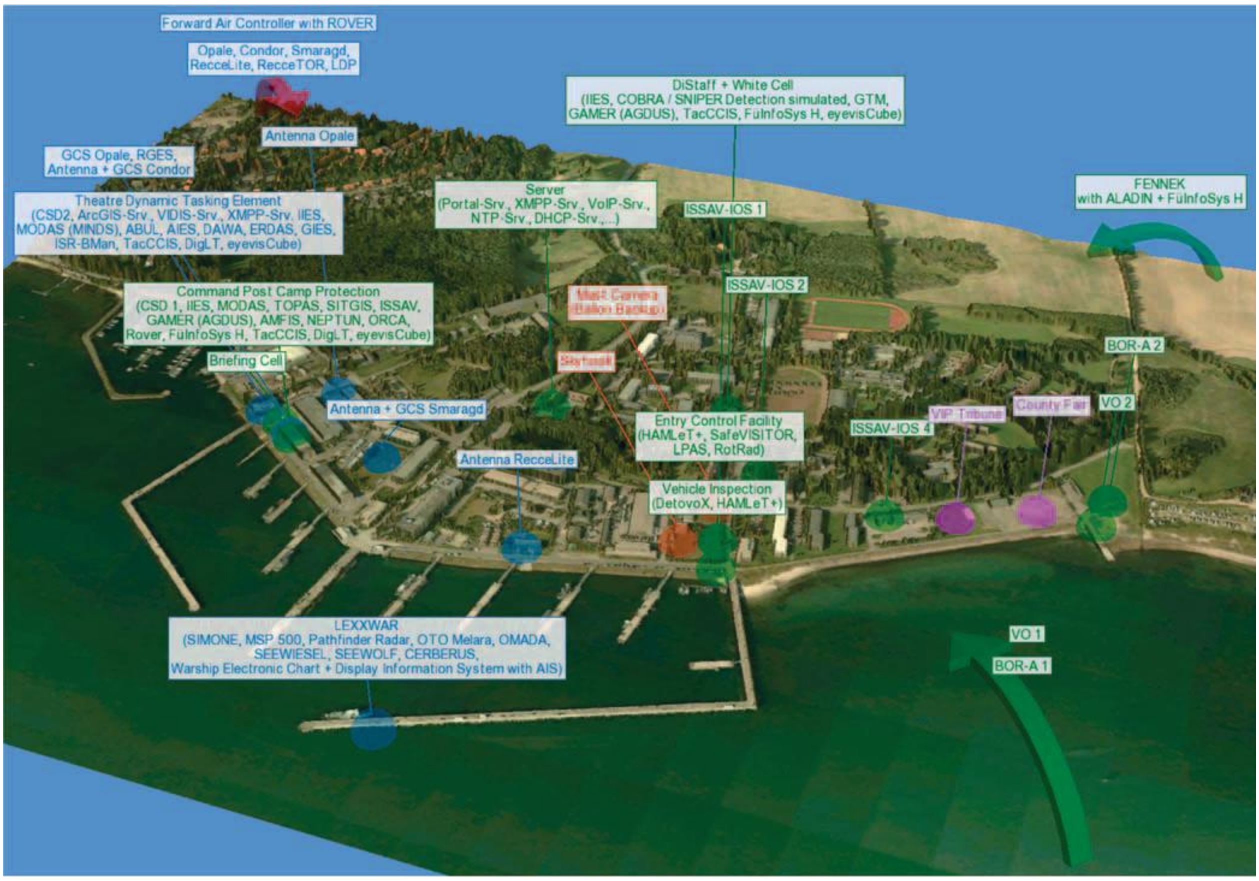

Forward Air Controller with ROVER
Opale, Condor, Smaragd, RecceLite, RecceTOR, LDP
Antenna Opale
GCS Opale, RGES, Antenna + GCS Condor
Theatre Dynamic Tasking Element (CSD2, ArcGIS-Srv., VIDIS-Srv., XMPP-Srv. IIES, MODAS (MINDS), ABUL, AIES, DAWA, ERDAS, GIES, ISR-BMan, TacCCIS, DigLT, eyevisCube)
DiStaff + White Cell (IIES, COBRA / SNIPER Detection simulated, GTM, GAMER (AGDUS), TacCCIS, FüInfoSys H, eyevisCube)
Server (Portal-Srv., XMPP-Srv., VoIP-Srv., NTP-Srv., DHCP-Srv.,...)
ISSAV-IOS 1
FENNEK with ALADIN + FüInfoSys H
Command Post Camp Protection (CSD 1, IIES, MODAS, TOPAS, SITGIS, ISSAV, GAMER (AGDUS), AMFIS, NEPTUN, ORCA, Rover, FüInfoSys H, TacCCIS, DigLT, eyevisCube)
Mast Camera (Ballon Backup)
ISSAV-IOS 2
BOR-A 2
Briefing Cell
Antenna + GCS Smaragd
Entry Control Facility (HAMLeT+, SafeVISITOR, LPAS, RotRad)
ISSAV-IOS 4
VIP Tribune
County Fair
VO 2
Antenna RecceLite
Vehicle Inspection (DetovoX, HAMLeT+)
LEXXWAR (SIMONE, MSP 500, Pathfinder Radar, OTO Melara, OMADA, SEEWIESEL, SEEWOLF, CERBERUS, Warship Electronic Chart + Display Information System with AIS)
VO 1
BOR-A 1

Figure 6: Common Shield exercise layout (Source: Politik&Sicherheit – Nr. 6 / Dezember 2008)

As the concept is of use for the management of crisis and enables the adaptation of off-the-shelf sensors it is of special interest in CIMIC (Civil Military Cooperation) operations. An adaptation of the concept has been tested in the project SOBCAH (Surveillance of borders, coastlines and harbours) [11], partially funded by the European Commission under the Preparatory Action for Security Research (PASR) 2005 program. The aim was to integrate systems that are already used for civil surveillance tasks (like radars at harbours/airports or CCTV cameras) with innovative technologies and show the benefit of it within a technical demonstration. Within a DAT (Defence Against Terrorism) and harbour protection scenario, an adapted CSD disseminated alarms, tracking information and videos from sensors to a situation awareness system. For tracks and alarms a common data format was developed. The data generated by the sensor systems was transmitted to the SSD (SOBCAH Shared Database). Through subscription to the SSD server, all systems connected to the network were able to retrieve those data. The situation awareness system used it to generate the operational picture and support the decision makers on actions to be taken, whereas e.g. video sensor systems used especially track and alarm data to decide on sensor cross cueing and direct the video sensor to an alarm location.

5.0 CONCLUSION

In crisis management quick and full situation awareness is essential to enable adequate countermeasures and reactions. Relevant information has to be distributed to agencies and decision makers. Combining sensor information with intelligence data and sharing relevant information according to user requirements enhances the situation awareness of decision makers and enables them to act quickly and efficiently.

An architecture integrating ISR systems for crisis response in an interoperable way was developed. Interoperability was addressed from three primary perspectives: operational, architectural, and technical. The architecture foresees the use of common interfaces for data formats and exchange mechanisms. The inner workings of each employed system are left untouched and only minor external interface modifications are required. The common formats and exchange mechanisms are based on NATO standardisation agreements (STANAGs).

The key component of that architecture is the Coalition Shared Data (CSD) server, which is based on STANAG 4559 [2] and provides a mechanism for distributed, searchable, persistent storage and retrieval of Joint ISR sensor data as well as exploited data and information, such as tracks and exploitation reports and tasking information. The real-time synchronisation mechanism for metadata between multiple CSDs employed at geographically dispersed locations ensures that at any node in the network knowledge about the available ISR information is available and the information itself is accessible.

The proven benefit of information sharing through the CSD at the NATO exercise Bold Avenger/Trial Quest 2007 and the Bundeswehr experiment Common Shield 2008, led to the planning of fielding the CSD in NATO and Bundeswehr. The Capability is scheduled for IOC (Initial Operational Capability) in ISAF in mid-2009 and FOC (Final Operational Capability) in early 2010.

REFERENCES

[1] www.nato.int/docu/update/2007/pdf/majiic.pdf

[2] STANAG 4559 NATO Standard ISR Library Interface. Edition 2. http://www.nato.int/structur/AC/224/standard/4575/ag4_4575_E_ed2_nu.pdf

[3] Endsley, M. R. Situation awareness global assessment technique (SAGAT). Proceedings of the National Aerospace and Electronics Conference (NAECON). (New York: IEEE), 789-795. 1998

[4] Endsley, M.R., Garland, D.J. Situation Awareness Analysis and Management. Lawrence Erlbaum Associates. 2000

[5] Peterson, J.K. Understanding surveillance technologies: spy devices, privacy, history & applications. Auerbach Publications. 2007

[6] STANAG 4545: NATO Secondary Imagery Format (NSIF). http://www.nato.int/structur/AC/224/standard/4545/4545_documents/4545_ed1_amd1.pdf

[7] STANAG 4609: NATO Digital Motion Imagery Format. http://www.nato.int/structur/AC/224/standard/4609/4609_documents/4609Eed01.pdf

[8] STANAG 5516: Tactical Data Exchange- Link 16.

[9] www.nato.int/docu/update/2007/12-december/e1210d.html

[10] Common Shield 2008. Strategie & Technik, October 2008

[11] http://ec.europa.eu/enterprise/security/doc/project_flyers_2006/766-06_sobcah.pdf

[12] STANAG 4607: NATO Ground Moving Target Indicator Format (GMTIF). http://www.nato.int/structur/AC/224/standard/4607/4607.htm