

Policy Department External Policies



IMPROVING THE COHERENCE OF CRISIS MANAGEMENT: NEW TECHNOLOGIES FOR COMMAND AND CONTROL SYSTEMS

SECURITY AND DEFENCE

This study was requested by the European Parliament's Subcommittee on Security and Defence.

This study is published in the following language: English

Authors: **Kristiina Rintakoski** (Programme Director, Crisis Management) at Crisis Management Initiative (CMI) in Finland, and **Brigadier General Simo Alho** (ret.) Former EU Military Staff, Assistant Chief of Staff, Communications and Information Systems Division)
Study carried out within the framework agreement between **ISIS Europe** and the European Parliament

Responsible Official: **Dr Gerrard Quille**
Directorate-General for External Policies of the Union
Policy Department
WIB 06M081
rue Wiertz
B-1047 Brussels
E-mail: gerrard.quille@europarl.europa.eu

Publisher European Parliament

Manuscript completed on 29 February 2008.

The study is available on the Internet at
<http://www.europarl.europa.eu/activities/committees/studies.do?language=EN>

If you are unable to download the information you require, please request a paper copy by e-mail : xp-poldep@europarl.europa.eu

Brussels: European Parliament, 2008.

Any opinions expressed in this document are the sole responsibility of the author and do not necessarily represent the official position of the European Parliament.

© European Communities, 2008.

Reproduction and translation, except for commercial purposes, are authorised, provided the source is acknowledged and provided the publisher is given prior notice and supplied with a copy of the publication.

Contents

	Page
Executive Summary.....	iii
1 Introduction	1
2. EU Crisis Management Arrangements	2
2.1 Defining key concepts and terms	2
2.1.1. Command and Control, C4ISR	2
2.1.2 Operation Headquarters and Force Headquarters	4
2.1.3 Network Enabled Capability (NEC)	5
2.1.4 Interoperability	5
2.2 EU Command and Control options.....	6
2.3 Technologies for Command and Control	8
3. Crisis Management.....	11
3.1 ESDP Operations – Comprehensive Approach	11
3.2 Lessons from ESDP Operations.....	11
3.2.1 Civilian Crisis Management Operations	11
3.2.2 Military Crisis Management Operations.....	14
3.3 National Experiences in Military C2 Systems	17
4. Public Safety Communications and Emergency Response.....	21
4.1 Disaster Response and Civil Protection at the EU level	21
4.2 EU Emergency and Crisis Co-ordination Arrangements	22
4.3 Public authority networks for public safety communications	23
5. EU future needs and R&D.....	26
5.1 Priorities in crisis management in FP7	27
5.2 European Defence Agency	28
5.3 EU-funded research: public safety communications systems	29
5.4 NATO programmes on command and control systems	29
5.5 C2-related initiatives and research in the US.....	30
6. Crisis Management Markets	32
7. Improving the coherence of crisis management	34
8. Recommendations.....	37
9. Conclusions – role for European Parliament.....	38
Bibliography	39
Annex I: Examples of projects funded by the Preparatory Action on Security Research (PASR 2004-2006),	

Executive Summary

The European Union (EU) as a whole has to operate in a security environment where the division between external and internal security is becoming increasingly irrelevant. Societal changes related to scientific and technological developments as well as new types of vulnerabilities are challenging European societies. Global insecurity is now brought about primarily by various impacts of the networked political economy in a world where borders are highly permeable to flows of information, finance, goods and people.

The challenges to European Security and Defence Policy (ESDP) missions in the 21st Century have increased significantly. Today's missions are simultaneously more complex and more dynamic, requiring the collective capabilities and efforts of many organisations in order to succeed. This requirement for assembling a diverse set of capabilities and organisations into an effective operation is accompanied by shrinking opportunities to respond. New concepts of operations and approaches to 'command and control' (C2), as well as information sharing, are necessary to provide increased capabilities to deal with these challenges.

With the rapid development of communication technology over the last 50 years the model of communication has changed dramatically as has - or should have - our management model as well. However, in most of the military and civilian interventions today, participating organisations operate within their own individual communication/decision-making structures. Collaboration and information exchange are often governed through *ad hoc* and individual agreements among the partners – and approved at government level. The centralised and hierarchical communication structure – matching the traditional civilian and military command and control structures - has been in place in international and national regimes for centuries.

With the progress in communication technology a shift towards a more 'decentralised' operating model has been introduced. This has enabled the principles of responsibility, accountability and transparency to still be monitored and controlled according to existing civilian and military command and control structures. While technology offers 'speed' it still enables central decision making and intervention when necessary.

The 'distributed' model - basically introduced with the internet/web technology - enables individuals to collaborate and communities to work together independently of geographic or economic borders. This model imposes a new challenge to civilian and military command and control structures and to existing governance structures, both in the public and private sectors. Perhaps most importantly, to be effective, the distributed model requires a much better understanding of the 'end-to-end' process.

The aim of this study is to give an overview of the C2, as well as communication, arrangements in the EU and on the technologies used to support them. The study also discusses some key issues relevant to understanding the importance of command and control systems for the coherence of EU crisis management operations and public safety communications.

The study finds that decision-making and procedures supporting communication and information systems (CIS) arrangements in European Security and Defence Policy (ESDP) operations need to be improved to help to ensure interoperability and the interconnection of systems processing classified information. Member States should actively engage in these efforts within the European Defence Agency (EDA) framework to address the identified shortfalls in C2 systems and to develop interoperable systems.

The key recommendations of this study are:

- Member States should continue to address the gaps in the interoperability of communication and information systems between their armed forces.
- The EU should ensure that ESDP operations in complex and hostile environments have access to real-time situational awareness systems and ensure the safety and security of their personnel.
- Procedures are needed to enable the speedy accreditation of sensitive communication and information systems used in ESDP missions at all command levels.
- The exchange of information between different Member States should be based on a “need to share” principle rather than the traditional “need to know” principle.
- To ensure interoperability, Member States could use the Command and Control Information System to be established in the Operation Centre of the EU Military Staff as a guideline for the development and procurement of their own national headquarters (which they could subsequently make available for ESDP operations).
- The timely deployment of communication and information systems for ESDP civilian missions needs to be improved, both through streamlining organisational procedures and improving mission support structures.
- The Head of Mission should have more time (requiring faster decision-making at the Brussels level), enjoy greater flexibility and have stronger financial decision-making authority in procuring the necessary capabilities for a mission.
- The EU should ensure that the necessary framework contracts are established through tenders based on a scalable communications concept that could be based on the scenarios identified in CHG2008 and/or the CHG 2010 illustrative scenarios.
- A basic stock of critical equipment necessary for rapid mission start-up should be established.
- There is an urgent need to improve European and national inter-operability in public safety communications through the implementation of harmonized technologies and/or a gradual process bringing national legal rules closer together.
- In Security Research interaction with end users from the crisis management community is essential and there is need to ensure that it covers also the CIS requirements of ESDP civilian operations

Specifically in relation to the European Parliament, the study recognizes that the rapid growth in the number and type of ESDP civilian and military crisis management operations, as well as the complex nature of EU crisis management decision-making, represent growing challenges to parliamentary oversight.

The study, which has sought to provide a preliminary overview, contains a number of questions, suggestions and recommendations that could be taken up by the European Parliament, within the context of national or EU political institutions, or by the European

Parliament exercising its oversight role and drawing attention to command, control and communications issues that need to be addressed by the Commission and Council.

Improving the coherence of crisis management: new technologies for command and control systems

1 Introduction

The European Union (EU) as a whole has to operate in a security environment where the division between external and internal security is becoming increasingly irrelevant. Societal changes related to scientific and technological developments as well as new types of vulnerabilities are challenging European societies. Global insecurity is now brought about primarily by various impacts of the networked political economy in a world where borders are highly permeable to flows of information, finance, goods and people.

The characteristics of the current security risks and challenges, as laid out in the EU Security Strategy (ESS) of 2003, include their asymmetrical nature, lack of geographical constraint, inter-connectedness, and the fact that they are blurring the boundaries between internal and external security (1). A vision of the future nature and context of EU crisis management activities is essential to inform those near-term decisions that will determine Europe's long-term crisis management capabilities and capacities. Unless globalisation stops or goes into reverse, the world of 2025 is likely to be more diverse, more interdependent, and even more unequal. Globalisation will produce winners and losers, as between countries and regions, and within societies, whilst universal communication will make these disparities ever more apparent.

Crises are ever more complex; involving collapsed state institutions, humanitarian catastrophes, human rights violations, displacement and refugees. These developments underline the need to intensify co-operation between different sectors of national administrations and between governments, international and regional organisations. Therefore, in crisis management the EU will increasingly have to adopt a comprehensive approach; one that combines its 'hard' and 'soft' power instruments and that is able to coordinate civilian, military, governmental and non-governmental bodies collectively to achieve the necessary political effects. This calls for an integrated and comprehensive approach to the planning and conduct of interventions.

The mission challenges of the 21st Century have increased significantly. Today's missions are simultaneously more complex and more dynamic, requiring the collective capabilities and efforts of many organisations in order to succeed. This requirement for assembling a diverse set of capabilities and organisations into an effective operation is accompanied by shrinking opportunities to respond. New concepts of operations and approaches to 'command and control' (C2), as well as information sharing, are necessary to provide increased capabilities to deal with these challenges.

With the rapid development of communication technology over the last 50 years the model of communication has changed dramatically as has - or should have - our management model as well. However, in most of the military and civilian interventions today, participating organisations operate within their own individual communication/decision-making structures. Collaboration and information exchange are often governed through *ad hoc* and individual agreements among the partners – and approved at government level. The centralised and

¹ Solana, Javier, *A Secure Europe in a better world: European Security Strategy*, Brussels, December 2003.

hierarchical communication structure – matching the traditional civilian and military command and control structures - has been in place in international and national regimes for centuries. The network-centric concept of warfare is directly linked to the economic, technological and social developments advanced societies have experienced in the last twenty years. The emergence of information as the driving force behind the process has also had repercussions on military doctrines and the way operations are conducted.

With the progress in communication technology a shift towards a more ‘decentralised’ operating model has been introduced. This has enabled the principles of responsibility, accountability and transparency to still be monitored and controlled according to existing civilian and military command and control structures. While technology offers ‘speed’ it still enables central decision making and intervention when necessary.

The ‘distributed’ model - basically introduced with the internet/web technology - enables individuals to collaborate and communities to work together independently of geographic or economic borders. This model imposes a new challenge to civilian and military command and control structures and to existing governance structures, both in the public and private sectors. Perhaps most importantly, to be effective, the distributed model requires a much better understanding of the ‘end-to-end’ process.

The aim of this study is to give an overview of the command and control, as well as communication, arrangements in the EU and on the technologies used to support them. The study also discusses some key issues relevant to understanding the importance of command and control systems for the coherence of EU crisis management operations and public safety communications.

2. EU Crisis Management Arrangements

2.1 Defining key concepts and terms

2.1.1. Command and Control, C4ISR

Command and control can be defined as an exercise of authority and direction by a commander over assigned and attached forces in the accomplishment of a mission. Their functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission (2).

Some have defined C2 in terms of how it is conducted within a given organisation or collection of organisations. But such organisation-specific definitions are not helpful when the focus of the effort is on new concepts and approaches. For a C2 definition to be useful it needs to focus on why one conducts C2, and what functions an instantiation of C2 needs in order to achieve its purposes.

² This is the US definition of Command and Control (Joint Pub 0-2). According to the NATO glossary, Consultation, Command, and Control (C3) are “the responsibilities and activities of political, military and civil authorities in political consultation, including crisis management, nuclear consultation, and civil emergency planning. The term also applies to the authority, responsibilities and activities of military commanders in the direction and coordination of military forces and in the implementation of orders related to the execution of operations.”

The following are seen as essential C2 functions:

- Establishing intent
- Determining roles, responsibilities, and relationships
- Establishing rules and constraints
- Monitoring and assessing the situation and progress
- Inspiring, motivating, and engendering trust
- Training and education
- Making provision.

These functions are associated with 'mission' or 'enterprise' C2. They can be accomplished in very different ways. These differences boil down to how authority and relationships are determined, how decision rights are distributed, the nature of the processes involved, how information flows, and the distribution of awareness (3). The EU definition, based on the EUMS Glossary of Terms and Definitions, is the authority vested in an individual of the armed forces for the direction, co-ordination, and control of military forces. Control is the authority exercised by a commander over part of the activities of subordinate organisations (4). The Draft Guidelines for Command and Control Structure for EU Civilian Operations in Crisis Management seek to render the civilian command structure more comparable with the military levels of command structure, thereby facilitating civil/military coordination as well as mutual support and coherence (5). Both documents consider the C2 concept to be composed of three dimensions: command arrangements; continuous command process; and architecture i.e. systems supporting the C2 arrangements and process.

Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance (C4ISR) encompasses systems, procedures and techniques used to collect and disseminate information. It includes intelligence collection and dissemination networks, command and control networks and systems that provide the common operational/tactical picture. It also includes Information Assurance (IA) (6) products and services, as well as communications standards that support the secure exchange of information by C4ISR systems (7). C4ISR technologies are at the heart of modern crisis management operations. They act not only as force multipliers for the military platforms into which they are integrated, but also as the means to better link different types of forces (air, sea, land). Moreover, they can connect forces of different nationalities, enabling interoperability and the efficient use of military resources. Intelligence, Surveillance and Reconnaissance (ISR) is activity that synchronises and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of operations. It is an integrated intelligence and operations function.

Essentially, IA is the practice of managing information-related risks. It can be defined as measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and

³ Alberts, David S. and Hayes, Richard E., *Understanding Command and Control*, Command and Control Research Programme (CCRP), the United States Department of Defense, Washington D.C., 2006.

⁴ Council of the European Union, *EU Military C2 Concept*, 11096/03, Brussels, July 2003.

⁵ Council of the European Union, *The Draft Guidelines for Command and Control Structure for EU Civilian Operations in Crisis Management*, 9919/07, Brussels, May 2007.

⁶ Information Assurance is closely related to Information Security and the terms are sometimes used interchangeably.

⁷ US Defense Security Cooperation Agency (DSCA) Memorandum I-05/014306-STR/16.3.2006.

reaction capabilities. In other words, IA is the process of ensuring that the right people get the right information at the right time. IA products or technologies are those the primary purpose of which is to provide the security services (listed above) with correct information about known vulnerabilities, or to provide layered defence against various categories of non-authorized or malicious penetrations of information systems or networks. Examples include such products as data/network encryptors, firewalls, and intrusion detection devices (8).

Communications and information systems (CIS) is a general term and can be defined as an assembly - which may include personnel, equipment and procedures - organized to accomplish specific information conveyance and processing functions. CIS can, therefore, serve various functions as command, intelligence, and logistics - just to mention a few examples.

In order to develop Council activities in areas that require a degree of confidentiality, it was appropriate to establish a comprehensive security system. Therefore, in 2001 the Council decided to adopt security regulations (9) that lay down the basic principles and minimum standards of security involving the establishment of secure networks and communications that need to be adhered to by the Council, the General Secretariat of the Council (GSC), the Member States and the decentralised agencies of the EU. These secure communications networks assure all parties that a common standard of protection is established. These rules and regulations also have to be respected when preparing and conducting crisis management missions and implementing communication and information systems processing classified information. Typically, maximum classification levels of information in military missions have been CONFIDENTIEL UE and in civilian missions RESTREINT UE.

2.1.2 Operation Headquarters and Force Headquarters

According to the EU, the Military C2 Concept chain of command contains three levels of headquarters: an Operation Headquarters (OHQ), a Force Headquarters (FHQ) and Component Headquarters. One of the main responsibilities of the Operation Commander (OpCdr) and OHQ is to conduct operational planning at a military-strategic level i.e. Concept of Operations (CONOPS), Statement of Requirements (SOR), Operation Plan (OPLAN) and Rules Of Engagement (ROE).

The Operation Headquarters oversees the execution of an operation. It consists of the multinational military strategic staff. Usually OHQ is organised in divisions - personnel, intelligence, operations, logistics, plans, communications, training, finance, CIMIC (civil-military cooperation) and medical support – each of which is led by a senior officer responsible for a particular area of capability. Under the authority of the Operation Commander, they will conduct the necessary planning. One example of the role and tasks of an OHQ was set out by the Commander of the Response Forces Operations Command in Ulm, Germany, Lieutenant General Jan Oerding. He stated that the operational command level is responsible for translating the strategic objectives into practicable instructions for action for the tactical level. According to him this means that the operational command combines the elements and capabilities of the armed forces towards a stated goal (10).

⁸ US Army Regulation 25–2 Information Management, Information Assurance, Aug 2007, p 82.

⁹ Council of the European Union, *Council Decision adopting the Council's security regulations*, 5775/01, Brussels, February 2001.

¹⁰ Commander of the Response Forces Operations Command in Ulm, Lieutenant General Jan Oerding's interview "Absolutely professional and wholly committed" on 07.12.2006 and published on Bundeswehr website (<http://www.streitkraeftebasis.de/portal/a/streitkraeftebasis>).

FHQ, under the command of a Force Commander, functions as a base of operations and provides command and control over the troops. Typically FHQ, which are subordinate to the OHQ, operate within the Area of Operation of the force and therefore have to be deployable. The Force Commander (FCdr) and FHQ are responsible for providing developing the operational plan and issuing the respective Operation Orders. The role of the FHQ is to function as a kind of hinge between the military strategic level and the tactical level in theatre and as such is absolutely indispensable (11).

2.1.3 Network Enabled Capability (NEC)

The UK Ministry of Defence (MoD) states that Network Enabled Capability (NEC) aims to improve the ability to fight and win by enabling states to share and exploit information more efficiently and effectively. NEC is intended to bring together sensors, decision makers and weapon systems, along with support capabilities. It aims to ensure that information gets to where it is needed. A fundamental principle of the NEC is formulated thus:

“Full benefits from the NEC can only be realised with the addition of changes in organisation and individual behaviour. While NEC is not just about technology, it does pose major technology challenges.” (12)

NEC was developed in the US in the late 1990s under the name Network Centric Warfare (NCW) (13). NCW is characterized by the ability of geographically dispersed forces to create a high level of shared battle space awareness that can be exploited via self-synchronization and other network-centric operations to achieve a commander's intent. NCW is built around the concept of sharing information and assets. This new concept of “need to share” is also one of the cornerstones of the NEC and should be kept in mind when one studies the lessons learned from EU crisis management operations.

2.1.4 Interoperability

A common military understanding of interoperability is twofold: functional and technical. In the ESDP Headline Goal 2010 (HG2010) interoperability is defined as the ability of armed forces to work together and to interact with other civilian tools. It is an instrument to enhance the effective use of military capabilities as a key enabler in achieving the EU's ambitions in Crisis Management Operations (14). Just as equipment is only one element of capability, so the interoperability requirement relates to all other aspects of capability, from language to procedure to training. The European Defence Agency's ‘Long Term Vision’ (15) underlines the fact that interoperability needs to be at the heart of all European capability development work. Expeditionary, multinational operations, involving strong inter-action with civil instruments, require interoperability within national forces, between national forces, and with civilian actors.

For the sake of comparison, a US Department of Defence (DoD) definition covers both aspects well: (i) The ability of systems, units or forces to provide services to and accept services from other systems, units or forces and to use the services so exchanged to enable

¹¹ Lieutenant General Jan Oerding's interview on 7.12.2006.

¹² UK MOD Joint Services Publication (JSP 777)

¹³ Vice-Admiral Arthur K. Cebrowski, USN, and John J. Garstka, “Network Centric Warfare: Its Origin and Future,” Proceedings of the Naval Institute 124:1, January 1998

¹⁴ Council of the European Union, *Headline Goal 2010*, 6309/6/04/REV 6, Brussels, May 2006.

¹⁵ An Initial Long-Term Vision for European Defence Capability and Capacity Needs, Brussels, October 2006, page 21.

them to operate effectively together; (ii) The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users (16).

2.2 EU Command and Control options

Currently, the EU has three options available for arranging C2 for military crisis management operations. First option is, in a so-called autonomous operation, to make use of facilities provided by any of the five Operation Headquarters currently available in the European Member States i.e. the French, British, German, Italian and Greek OHQs. The latest EUFOR DR Congo military operation in 2006 employed the German OHQ in Potsdam. A second option is to exercise recourse to NATO capabilities and common assets under the so-called ‘Berlin Plus’ arrangements. The EU can make use of NATO’s command and control options such as the Operation Headquarters – that can be used for EU purposes under the Allied Command Transformation (ACT) mechanism – located at Supreme Headquarters, Allied Powers Europe (SHAPE) in Mons, with Deputy Supreme Allied Commander in Europe (DSACEUR) as the Operation Commander. This is the option currently used in the conduct of Operation Althea in Bosnia Herzegovina (BiH).

In theory at least, from 1 January 2007, the EU has had a third option for commanding operations of limited size (around 2,000 troops) from Brussels by using the EU Operations Centre within the EU Military Staff (EUMS). Using some EUMS core staff, as well as some extra double-hatted EUMS officers and augmentees from the Member States, the EU now has an increased capacity to respond to crisis management situations.

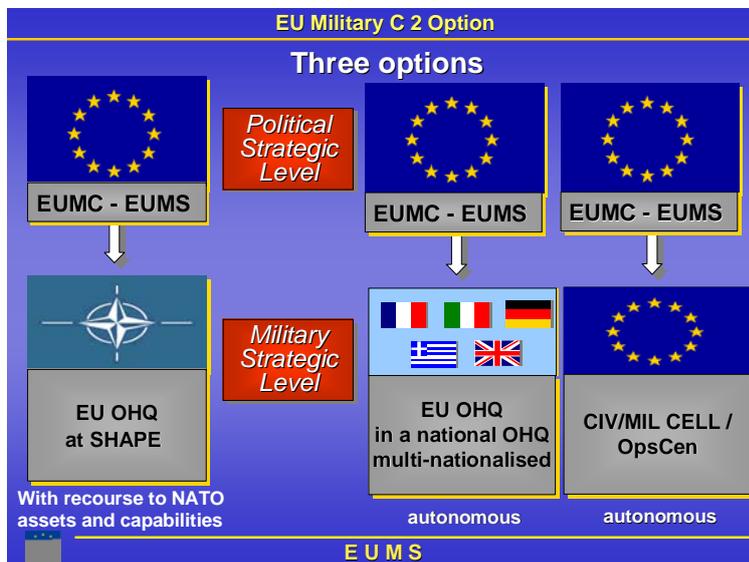


Figure 1: The EU Military C2 Options

Under the responsibility of the Council, the Political and Security Committee (PSC) exercises the political control and strategic direction of EU military operations, and the EU Military Committee (EUMC) monitors the proper execution of the operation. The Chairman of the EUMC (CEUMC) acts as the primary point of contact with the EU Operation Commander. In relation to operations, neither the Director General (currently Lieutenant General David Leakey) nor the EUMS are in the actual chain of command but continue to work primarily for

¹⁶ US DoD Joint Pub 1-02 Dictionary of Military and Associated Terms, June 1998, p. 231.

the CEUMC as a part of the Council General Secretariat. (The military planning process is depicted in detail below.)

On 18 June 2007, the EU Council of Ministers agreed on a new chain of command for civilian ESDP operations based on the establishment of a Civilian Planning and Conduct Capability (CPCC) within the Council General Secretariat. The CPCC will be headed by a Civilian Operation Commander (CivOpCdr) who, under the political control and strategic direction of the PSC and the overall authority of the Secretary-General/High Representative, will be responsible for the planning and conduct of civilian ESDP operations. The CPCC staff will support the CivOpCdr in exercising command and control at the strategic level of civilian ESDP operations.

The CPCC staff will be divided into an Operations Unit and a Mission Support Unit. The civilian-military (Civ-Mil) Cell within the EUMS will provide a joint civil-military planning capability, bringing together CPCC and military planners under the functional authority of the Civilian Commander and thus ensuring real civilian-military co-operation from the planning phase. The CPCC will draw on expertise and staff currently serving in the Council Secretariat civilian crisis-management directorate, DGE IX. The Head of Mission, who is directly responsible to the CivOpCdr, will exercise command and control at the theatre level. ESDP civilian crisis management missions can be deployed autonomously, jointly, or in close cooperation with military operations throughout all phases of the operation.

DGE IX, with the support of the CPCC, will continue to deal with horizontal issues (concepts, capabilities, training, etc.) of civilian ESDP and will also be in charge of the political-civilian aspects of crisis management, including the preparation of the Crisis Management Concept (CMC). It has been decided that the Civ-Mil Cell will provide a 'watch-keeping' capability in order to ensure continuous links with the various military and civilian ESDP operations and the Council Secretariat actors. This watch-keeping capability will be established within the Operations Centre (OpCen), will be activated using the facilities of the OpCen, and should be available during the preparation of each civilian operation.

The leading principle as to how to connect the different levels of command of an EU mission is from higher to lower. Therefore, the Council Secretariat establishes communications links from Brussels to the nominated OHQ. Then, when an operation has been launched, it is the responsibility of the Operation Commander to provide for the connectivity to the FHQ. In Operation Althea, DSACEUR (as the EU Operation Commander), can rely on NATO communications and information systems (CIS) assets to connect his headquarters with the FHQ in Sarajevo. However, the Council General Secretariat has established secure communications not only between Brussels and the EUSR in Sarajevo but between the different EU actors in BiH, including FHQ, in order to enable the EUSR to fulfil his role as a coordinator among the EU actors as required by the Joint Action (17).

Although the internet and the increased convergence of mobile telecommunications enable more information to be passed around the globe, these systems alone cannot be used to underpin the information exchanges and situational awareness required for all ESDP missions. Many missions require the passage of EU Classified Information (EUCI),

¹⁷ Council Joint Action 2004/570/CFSP of 12 July 2004 on the European Union Military Operation in Bosnia and Herzegovina.

especially those of a security, military or civil/military nature. Designing, assembling and maintaining the CIS to deliver the EUCI is a complex task, especially when networks have to be interconnected between personnel or military forces from different Member States. The EU Military Staff's CIS division, the primary task of which is to work on concepts and requirements for CIS for ESDP military and civil/military missions, seeks to coordinate efforts by the interested parties in Member States and the Council Secretariat.

One of the key challenges identified by the EUMS in Brussels is the lack of secure connections for the information exchange between the Council and the Commission. Even if the operations have secure connection to the EUMS, there are not yet sufficient secure connections inside the whole Council General Secretariat. These deficiencies have been identified and projects have been launched to develop a secure information infrastructure, starting with the Council General Secretariat. The aim in particular is to enable processing, distribution and storage of classified documents and files that are produced in the field of ESDP at Brussels.

In practice, to enable sufficient time for preparations and timely deployment, planning at the lower levels has to be conducted in parallel with that at the higher political-military level. This working method requires sufficient secure communications and information exchange capabilities, not only in Brussels but also between Brussels and OHQ and beyond to FHQ and Member States. This type of capability has yet to be fully implemented. There are a number of reasons for this. Apart from a variety of technical and procedural difficulties, it is difficult to realise a seamless flow of information during the planning and execution stages of an operation when OHQ and FHQ are provided by different Member States. Although efforts have been made to rectify this, the task is severely hampered by a lack of pre-defined command arrangements for OHQ and FHQ.

2.3 Technologies for Command and Control

Current C4ISR systems are based on Service-Oriented Architecture (SOA). The main objective is to establish network orientation i.e. the formation of networks of interconnected decision makers, effectors, information sources etc. The 'service' aspect of SOA refers to the functionality of a communication, piece of information or command and control system being made available as a service that can be accessed by any authorized user who is connected to the network (whether mobile or stationary). This concept is in line with the general trend within the information and communication industry.

The overall architecture of C4ISR solutions for network-oriented defence is depicted in Figure 3 below. The two main parts are 'Services' and 'Infrastructure'. The 'Services' part includes services for communication and collaboration, situation information, information operations, command & control, and engagement support. The 'Infrastructure' part includes a control layer, a convergence layer and a connectivity layer.

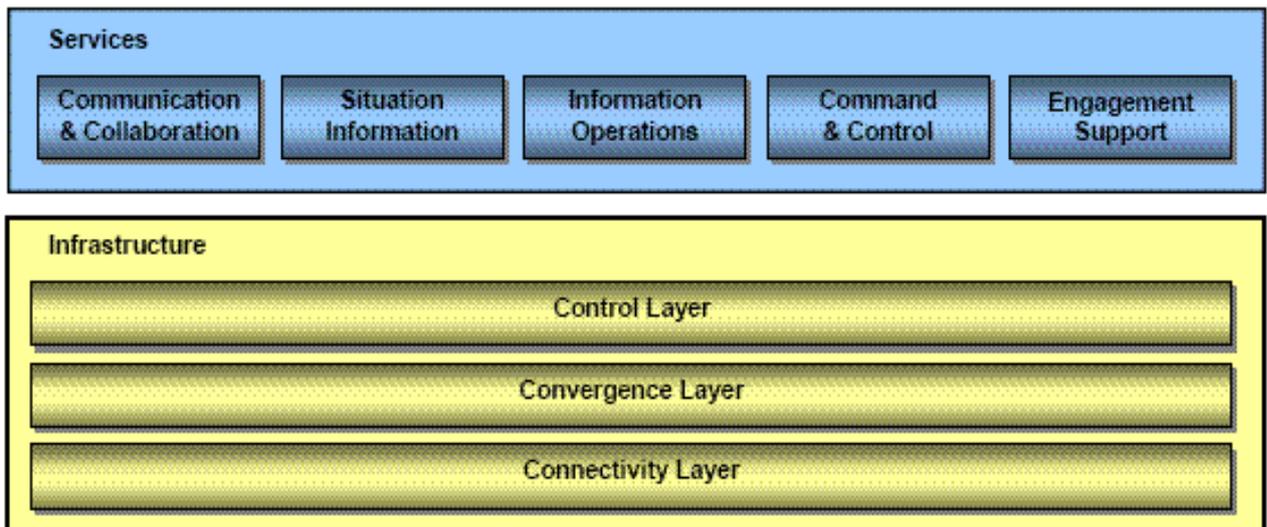


Figure 3: Service-oriented architecture for network-oriented defence (Source: C4ISR for Network-oriented Defence, White Paper, October 2006, Ericsson)

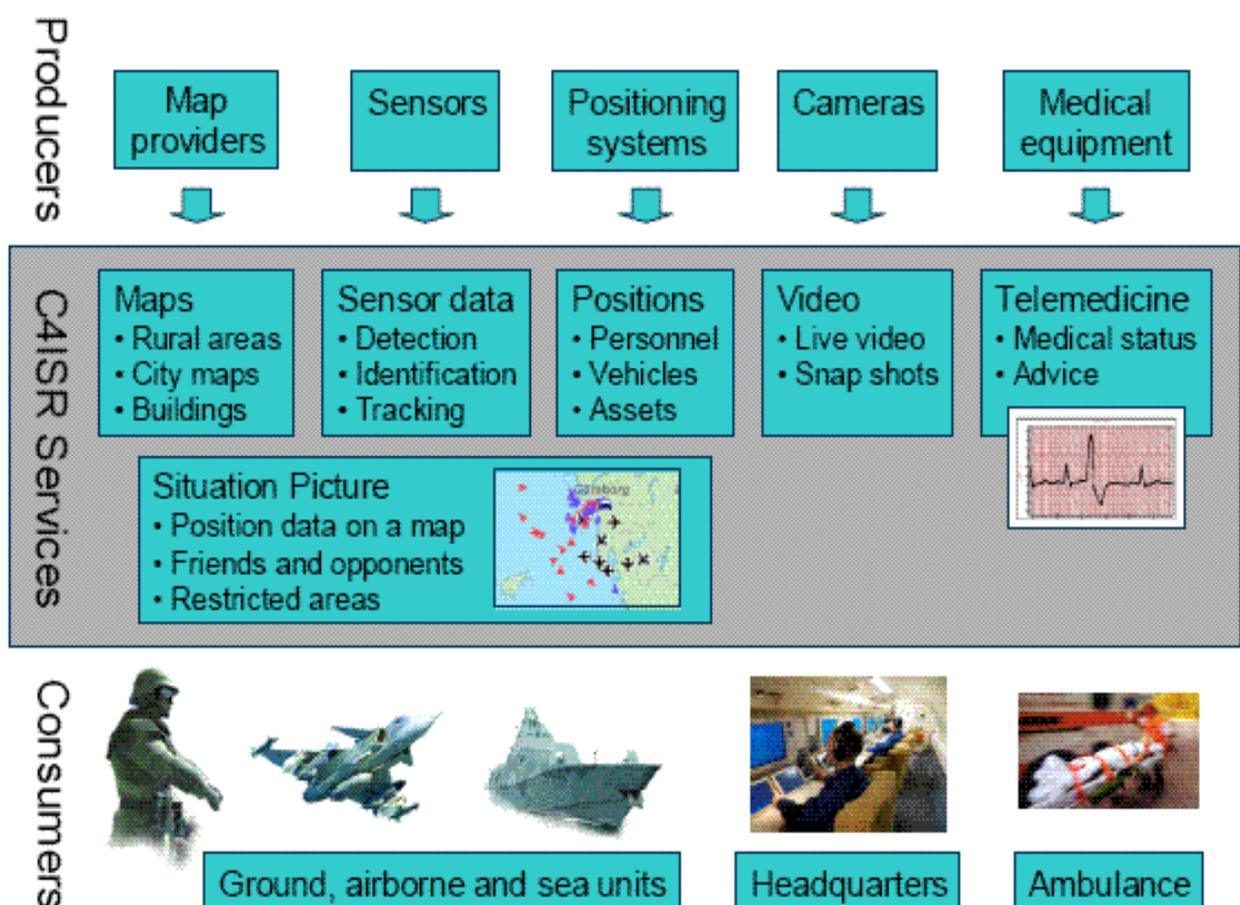


Figure 4: Examples of C4ISR services, their producers and consumers. (Source: C4ISR for Network-orientated Defence, White Paper, October 2006, Ericsson)

The services described in Figure 4 (above) create a number of improved capabilities for: communication and collaboration; situation information; information operations; command and control; engagement support. The key technologies for C4ISR systems are presented in

three categories; Command and Control, Communications and Intelligence, Reconnaissance and Surveillance (ISR).

Satellites are indispensable for modern ISR, navigation and communication systems. At the European level there is the Galileo satellite navigation system, the Global Monitoring for Environment and Security (GMES) initiative, and the European Union Satellite Centre (EUSC). Galileo is meant to be deployed by 2010, and is expected to be interoperable with GPS and the Russian GLONASS navigation network. GMES, designed to support the collection of environmental and security-related information, is expected to reach working capacity in 2008. The EUSC is dedicated to exploiting information based on space imagery from several European satellite systems in order to support EU decision-making in CFSP.

As many national systems are now designed to be interoperable with NATO systems, NATO is setting a *de facto* common standard of military CIS. To avoid duplication, this principle has also been generally accepted by the EU. However, this has created difficulties for the non-NATO EU Member States, and also for those who are members of the Partnership for Peace (PfP). Over the past few years the EU has also sought the release of NATO-sensitive standards, in particular those regulating secure communications and information technologies and arrangements. To this end, the recent release of TEMPEST standards [are these NATO standards?] for the INFOSEC authority of the Council General Secretariat represents progress. This will help the EU to revise its own relevant security regulations and arrangements to improve their compatibility with those of NATO, and will ease the required accreditation processes of secure CIS (thus enabling the processing of NATO classified information in the EU systems whenever close cooperation is required, and vice versa).

A study by the George Washington University about European C4ISR capabilities (18), based on the capabilities of seven countries, reached the following findings: The biggest constraint on European C4ISR investment is overall limitations on defence budgets, not the absence of adequate technology. Europeans also agree that interoperable C4ISR is essential to transatlantic coalition operations. The countries covered in the study expressed a strong desire for US cooperation both in terms of technology transfer and in designing US military systems that are interoperable with European ones. NATO provides the most up-to-date and complete framework for addressing transatlantic C4ISR technology and interoperability issues. C4ISR interoperability among the Europeans is most advanced in the area of space. The study concludes that while the EU is slowly becoming an important actor to facilitate the coordination of European policy, requirements and acquisition in the C4ISR arena, its military planning is still too preliminary to enable the resolution of interoperability problems. The trend toward a more common defence capability in Europe, autonomous of NATO, is likely to have major implications downstream for coalition military operations (19).

¹⁸ *Bridging the Gap, European C4ISR Capabilities and Transatlantic Interoperability*, Gordon Adams, Guy Ben-Ari, John Logsdon, Ray Williamson, the George Washington University, Washington D.C, October 2004. European countries investigated in the study are France, United Kingdom, Germany, Italy, the Netherlands, Spain and Sweden.

¹⁹ See Yves Boyer and Julian Lindley-French, *EU-interoperability: the effective military interoperability of European armed forces*, Policy Department external policies, European Parliament, Directorate-General for External Policies of the Union, November 2007.

3. Crisis Management

3.1 ESDP Operations – Comprehensive Approach

‘Comprehensive Approach’ is a term used in the context of EU crisis management. Briefly, it means bringing together and using all the instruments and capacities, civilian and military, to respond coherently to the whole spectrum of crisis management tasks - such as conflict prevention, peacekeeping, and the tasks of combat forces in crisis management - including peacemaking and post-conflict stabilization. NATO has introduced the terms ‘Effects-Based Approach to Operations’ and ‘Global Approach’. Lieutenant General Leakey, Director General of the EUMS, has stated that these terms mean the integration of lines of activity between the military, economic, political and judicial components, as well as the police (20).

General Bentegéat, Chairman of the EUMC, has said that the EU’s efforts must focus on enabling military and civilian personnel to work in intelligent synergy. This will require changing the culture as well as adapting the EU’s structures. The EU must be ready to deploy a Battlegroup (BG) and a civilian Crisis Response Team (CRT) rapidly and to direct their operations through clearly defined chains of command. This will require putting in place at each level the means of conducting ongoing, constructive and mutually supportive dialogue between civilian and military players, and to create full synergy between the EU’s civilian and military operations (21).

This approach can only be implemented effectively with the support of interoperable, secure communication and information systems between different command levels, and also horizontally between the military and civilian actors. Technology alone cannot solve all the challenges, but procedures and arrangements have to be in place to ensure that sensitive information can be distributed to all the actors regardless of which nation and/or organization they represent. Progress can be made only by making all the parties involved aware of the existing difficulties. Creation of a Lessons Learned database from the missions and the adoption of a systematic approach to remove the detected deficiencies would be beneficial. Key players that have to be fully aware of the current problems and look for improvements are the national security agencies of the nations concerned. Without their full collaboration procedures and arrangements cannot be revised.

3.2 Lessons from ESDP Operations

3.2.1 Civilian Crisis Management Operations

Aceh Monitoring Mission, Indonesia

The Aceh Monitoring Mission (AMM) in Indonesia was established to monitor the implementation of the peace agreement set out in the Memorandum of Understanding signed by the Indonesian Government and the Free Aceh Movement (GAM) on 15 August 2005. The mission was unique in many aspects, as it included rapid deployment, the pursuit of diverse tasks and cooperation with ASEAN countries. The AMM deployed into a post-conflict (30 years duration) environment - that had witnessed the collapse of previous

²⁰ NATO review Summer 2007 available at www.nato.int/docu/review/2007/issue2/english/main.html

²¹ Chairman of the EU Military Committee, General Henri Bentegéat’s statement in *Bulletin of the EU Military Staff IMPETUS*, Spring/Summer 2007, page 8.

ceasefire agreements – and which was still recovering from the tsunami disaster that had destroyed the local infrastructure nine months earlier.

The planning for the CIS for AMM began when international staff from the EU and ASEAN countries were sent to the area. Some individual monitors, particularly from Scandinavia, were equipped with hand-held satellite phones. Those were used in remote locations without any other functioning CIS. The British Embassy donated simple mobile phones and pre-paid phone cards to the monitors who were first deployed. This meant that some critical communications were handled with non-secure mobile phones and a few satellite phones.

As there was no concept for communications in civilian missions the system was planned on an *ad hoc* basis using what was available. With the exception of systems connecting mission headquarters in Banda-Aceh to Brussels, the procurement of CIS did not begin in a timely manner. There were insufficient funds available in the CFSP budget, and there was no ‘start-up’ fund. The local sources were limited, distances to Europe long, and the communications infrastructure in Aceh either non-existent or under repair. These drawbacks were overcome by the generous support of the Swedish Rescue Services Agency (SRSA) and its donation of elementary communication equipment - consisting of mobile phones, a few satellite phones and limited radio capability. The radio network was later extended by additional equipment.

The lack of means of communication was a limitation that affected the whole international community in its Tsunami relief work. No organisation was prepared to establish communication networks for aid and relief workers. In some cases the use of non-secure systems limited AMM operations and the ability to deal with sensitive questions.

The AMM studied the possibility of utilising the outcome of the Finnish Information Technology and Crisis Management project, in which inter-agency co-operation concepts and IT-tools were developed. The vision was to establish a CIS network that could have applications scaled from crisis management operations to wider generic benefits to the whole international community. The vision included the option of leaving the network in place as development aid – after the mission was completed - for the use of local public authorities. However, the EU was unable to finance the project and no other donor was found.

EUPOL Afghanistan

The EU launched an EU police mission (EUPOL) in Afghanistan in mid-June 2007. EUPOL Afghanistan is meant to consist of 160 personnel (possibly increasing to 190), with contributions from 17-18 EU Member States and perhaps with some personnel from third states, such as Canada, New Zealand and Norway. Again, this mission demonstrates the challenges involved in trying to establish adequate CIS arrangements for an ESDP civilian operation.

The planning for the CIS for EUPOL started (from zero) after the decision to deploy, and the work was strongly supported by the CIS Division of the EU Military Staff. In order to effectively support the planning of the CIS of EUPOL Afghanistan, the assessment mission conducted in November/December 2006 should have had a clearer mandate in relation to the mission support arrangements. But as details of the size of the mission and the field locations had not been decided at this stage, the CIS planning had to be conducted based on assumptions.

Because, at present, there is no concept for communications of civilian missions to cover different scenarios of operations, the communications systems are planned on a case-by-case basis without fully benefiting from the lessons identified in previous missions. This happened with EUPOL Afghanistan. Member States did not offer procurement and logistics officers for the mission in a timely manner. Therefore, except for those systems connecting mission headquarters in Kabul to Brussels (which were under the responsibility of the Council General Secretariat), procurement of the CIS could not be started early enough. The mission support officers should have been deployed first in order to prepare the mission for the deployment of the police and rule of law experts.

EUPOL co-operates closely with the International Security Assistance Force (ISAF) and its staff embedded in the Provisional Reconstruction Teams (PRTs) in Kabul and across Afghanistan. Therefore, the initial plan was to rely on the ISAF-wide area secure network through a special technical arrangement. Initially, one country blocked this arrangement but is now accepting it on condition that there is no formal agreement on paper. Although this enables the use of the network, it leaves the EU in a very weak position due to the lack of a firm, detailed written agreement. In the complex security environment of Afghanistan, a reliable communication system covering the whole operation is essential. It would also enable the use of the 'friendly force' tracking system necessary to ensure the safety and security of personnel - given that troops are operating in the same area as the civilian mission personnel. This is not happening because there is not a communications system that would be available for all actors.

The EUMS CIS division (22) has identified a number of possible actions to improve the current state of affairs of CIS in civilian missions. These are summarised in the following.

- Decision-making at the Brussels level should be speeded up in order to leave time for the Head of Mission to prepare a mission and enable timely procurement of equipment.
- The EU should also develop procedures that enable flexible support for the Head of Mission in procurement during the preparatory and launching phase of a mission.
- The financial decision-making authority of the Head of Mission should be increased.
- The EU should ensure that the necessary framework contracts exist, based on a 'scalable' communications concept. Scenarios identified in Civilian Headline Goal 2008 (CHG2008) would offer a good basis for the development of the concept.
- The possibility to set up a basic stock of critical equipment for rapid mission start-up could be considered - utilising, for example, the experience in the UN. The stock should include crypto devices for secure voice and data transfer, radios, GSM, satellite phones and dishes, equipment to connect to satellite systems, equipment to establish local area networks. This idea has not yet received wide support because of the maintenance and storage expenses. OpCen have deployable communications equipment, but these only enable the OpCen to connect FHQ to the OHQ in Brussels, and only for military missions. One solution to ensure interoperable CIS for a mission would be that one member state would provide the equipment.

²² Interview with Ralf Persicke, EUMS CIS Division on 11 October 2007

In a more complex security environment like Afghanistan a functioning CIS is crucial for a civilian mission's security and operational activities. Naturally, the user requirements are also more extensive compared to smaller and "easier" operations. In a rather benign security environment, such as in Bosnia Herzegovina, the ESDP civilian missions mainly use mobile phones, satellite phones and the internet for basic communications. However, the same challenges with procurement and deployment are present there too. Furthermore, if civilian missions are using commercially available non-secure systems the civil-military information exchange and coherence is undermined.

3.2.2 Military Crisis Management Operations

Operation Artemis

Operation Artemis exposed certain shortcomings: the need for better and secure means of conducting long-distance communication, better information technology, the importance of intelligence sharing, and the need to improve the interoperability of European armed forces. Ideally, from the strategic level downwards, effective and secure communications and liaison for planning, as well as C2 and the passing of intelligence with the designated operational HQ should have been guaranteed. Having identified this shortfall in Operation Artemis, the EU has since taken the necessary action to resolve the problem by setting up secure data links with the five available OHQ and with SHAPE to enable collaborative planning and preparations for operations (23).

In a UN report (24) of Operation Artemis it was mentioned that MONUC had not been warned of the landing of the first Interim Emergency Multinational Force (IEMF) troops. The IEMF leadership made it clear that they did not trust the security of information in MONUC sufficiently to place their landing force 'at risk'. On the other hand, with two operations in the same theatre, there was a potential risk of confusion and lack of coordination.

EUFOR DR Congo

During the preparation and planning phase of EUFOR DR Congo, command arrangements were critical. Being an autonomous EU-led operation, the chain of command was determined in accordance with current procedures. As the EU does not have any standing command and control structure, the conduct of the operation was assigned to an operational command offered by Germany, while France offered the force command. The decisions at strategic level were made by the Council, according to the stipulations of relevant concept and planning documents - such as the Crisis Management Concept, Concept of Operations (CONOPS), and Operations Plan (OPLAN). Under the Council's responsibility, the PSC exercised political control of the operation and set the strategic directives. From the perspective of the EU internal procedures framework, the current chain of command has proved its functionality, having been successfully applied throughout several operations.

As a UN support mission, EUFOR DR Congo had to work closely with the other actors on the ground. Setting up the coordination and cooperation mechanisms with these different actors in the theatre (UN forces, National Congolese Armed Forces, existing EU missions – EUPOL and EUSEC, assigned to support the Congolese authorities in security sector reform

²³ Homan, Kees, 'Operation Artemis in the Democratic Republic of Congo', *Faster and More United? The debate about Europe's crisis response capacity*, European Commission, Brussels, May 2007.

²⁴ 'Operation Artemis: The Lessons of the Interim Emergency Multinational Force', UN HQ Peacekeeping Best Practises Unit, Military Division, New York, October 2004, page 11.

– governmental and non-governmental international agencies) was a real challenge. The basic principle that governed these relations was to maintain every participant’s decision-making autonomy. Thus, the deployed European multinational force acted throughout the mission under the strategic command and control of the Operation Commander and the political control of the PSC.

Within the lessons learned process several conclusions were made relating to C2, one of which related to the necessity to appoint the operation and force commanders and their commands at an early stage of the mission’s preparation, in order to start the parallel planning process as soon as possible. Other lessons are linked to the participation of the representatives of the force and operation commands in the fact-finding missions and in setting up coordination and cooperation mechanisms with different actors. During this preliminary phase, the involvement of various partners could lead to a better delineation of responsibilities and to a clearer definition of the chain of command.

General Bentégeat, based on his experiences in the Congo operation, has expressed his concerns about the possible difficulties derived from having a geographically long chain of command. He said that the planning of operations which the EU has conducted alone involved close cooperation between the EU Military Staff, OHQ and, as necessary, at FHQ. According to the General, such arrangements do not necessarily raise difficulties, but the geographical distance between the political decision-taking centre in Brussels, the military planners of OHQ, and the planners in the theatre of operations does not facilitate exchange (25).

Following a visit to the DRC, the Security and Defence Subcommittee (SEDE) of the European Parliament recommended that prior to future missions the EU should:

Carry out pre-deployment joint training for all troop contributing states taking part in ESDP Missions, in order to identify and remedy any interoperability or communication problems.
(26)

In February 2007, General Christian Damay, EUFOR DR Congo Force Commander, noted that the operation overall had been a success as well as a formidable test for the ESDP. Nevertheless, the lessons learned from Operation Artemis had not, in his view, been sufficiently taken on board, not least because of a missing ‘lessons management’ system. He hoped that better account would be taken for future EU operations of those learned from EUFOR DR Congo, namely:

- unwieldy and complex command structure;
- insufficient intelligence resources;
- disparate conditions for the deployment of the C-130 and C-160 tactical aircraft;
- excessive deployment time for the intervention units stationed in Gabon; and
- the need to include the deployment and re-deployment phases in the duration of the mandate.

²⁵ Chairman of the EU Military Committee, General Henri Bentégeat’s statement in the Bulletin of the EU Military Staff IMPETUS Spring/Summer 2007, page 7.

²⁶ ‘Visit of the ad hoc Delegation to Kinshasa (DRC), Chairman’s Report’, Committee on Foreign Affairs, Subcommittee on Security and Defence, Brussels, November 2006, page 7. Available via: http://www.europarl.europa.eu/meetdocs/2004_2009/organes/sede/sede_20061219_0900.htm

With regard to the chain of command, he wondered whether Brussels should not simply set up a permanent headquarters that would be in direct contact with the Force Commander(s) on the ground (27).

Lieutenant General Leakey, Director General of the EUMS, has stated that the other major lessons from the Congo - relevant to this study - are in the field of contracting, compatibility of communications, and availability of communications at the FHQ and levels below (always a problem in multinational operations). The European Defence Agency (EDA) is examining if and how the EU can improve such interoperability (28). Lack of interoperability (standards and equipment – including secure communications) was one of the findings of the *ad hoc* delegation of the Parliament that visited Kinshasa in November 2006. The report published by this delegation mentions that while theoretically the use of NATO standards avoids problems of interoperability, the practical reality in integrating different national contributions into the small EUFOR mission proved to be difficult (29).

EUFOR DR Congo has been a good example of the integrated approach to crisis management operations. Defining the features and functioning mechanisms of a joint civil-military chain of command is a way of improving civil-military cooperation. For the moment at least, however, cultural differences hinder a common approach to the issue (30).

Experiences from the Berlin Plus Arrangements

Under the Berlin Plus agreement, the EU has been given assured access to NATO assets, including planning capabilities, for EU-led military missions. This includes the availability of NATO assets such as AWACS (Airborne Warning and Control System). Exchange of classified information is governed by the NATO-EU security agreement.

Operation Althea, as the first operation to put the Berlin Plus arrangement to the test, has proved successful despite the limitations listed above. In his study (31), Leo Michel has listed some of the challenges for cooperation between NATO and the EU. First, the two organizations have to ensure that their procedures are very much in tune, if not identical, and their training is coherent. When it comes to doctrine, training and equipment interoperability, European military commanders understand that inconsistent practices could increase the inherent risk of military operations.

According to several informed accounts, effective NATO–EU cooperation on capabilities development is still lagging. The formal NATO–EU Capability Group has become a rather sterile forum and some nations have blocked the formation of sub-groups of technical experts

²⁷ Assembly of WEU, *Berlin Conference on European Security and Defence Policy* (6 and 7 February 2007), Press Release, February 2007.

²⁸ Director General of the EUMS, Lieutenant General David Leakey's interview on 13 June 2007 and published on the web-site <http://www.hybaskova.cz/hybaskova/EUDefence-EU-operation-planning-enters-a-new-era-General-Leakey-looks-at-where-we-go-from-here~.html>

²⁹ 'Visit of the ad hoc Delegation to Kinshasa (DRC), Chairman's Report', Committee on Foreign Affairs, Subcommittee on Security and Defence, Brussels, November 2006, page 4. Available via: http://www.europarl.europa.eu/meetdocs/2004_2009/organes/sede/sede_20061219_0900.htm

³⁰ Director General of the EUMS, Lieutenant General David Leakey's interview on 13 June 2007 and published on the web-site <http://www.hybaskova.cz/hybaskova/EUDefence-EU-operation-planning-enters-a-new-era-General-Leakey-looks-at-where-we-go-from-here~.htm>.

³¹ Leo Michel, Senior Research Fellow at the Institute for National Strategic Studies, formerly (June 2000 – July 2002) Director, NATO Policy Office in the Office of the Secretary of Defense. His study *NATO – EU Cooperation in Operations and Implications for Italy* is accessible at: www.comitatoatlantico.it/.

who could actually coordinate or propose joint solutions to specific capabilities development tasks.³² Similarly, a regular exchange of operational lessons learned between NATO and EU military staffs would be beneficial to a number of member states of both organizations.

Michel's findings about the recognised need to improve interoperability in the missions are supported by Professor Adrian Pop in his study of the evolving relationship between the EU and the Atlantic Alliance (33). One of the lessons from the Balkans for NATO and the EU is to focus on increasing interoperability and coordinating doctrine, planning, technology, equipment and training. He states that current acquisition and investment programmes do not meet the needs of today's multinational forces. The majority of ECAP Planning Groups have been amalgamated with the EDA, and eventually the remaining two or three will also be closed down or transferred to the EDA. Professor Pop also draws attention to the fact that today's terrorist groups and criminal networks operate internationally, benefiting from real-time communications, information sharing and relative freedom of travel.

Its comprehensive approach to crises is one of the factors that make the EU unique. Therefore, the early involvement of all EU bodies and other international participants in the decision-making and planning process is vital. The information exchange at all levels needs future improvement, taking into account the security of information, arrangements for sharing information between the actors involved and technical interoperability requirements for the CIS, and acceptance procedures for interconnections of the systems.

3.3 National Experiences in Military C2 Systems

In order to benefit from advanced information networking technology, modern armed forces are undergoing a rapid transformation and finding ways to improve the availability and management of information. Effective command and control systems are now allowing combat units to avoid dependence on slow and unreliable voice communication. Legacy airborne platforms are being upgraded and new ones built to exploit the power offered through integrated battle management computing and communications.

According to Gartner Industry Research (34), by 2011, more than 80 per cent of the defence establishments among NATO members and other aligned nations will adopt SOA as the dominant software framework for developing mission and administrative systems. On the other hand, by the same date, more than 70 per cent of them will have failed to develop and implement a SOA transition strategy that effectively addresses necessary elements of technology integration, change management, procurement and governance. According to Gartner, early initiatives such as the Finnish Defence Forces' iC4I command and control programme, the US Department of Defence's Net-Centric Enterprise Services (NCES) and Net-Enabled Command Capability (NECC), and Singapore's Military Service Portal have shown promise, and will prove helpful for future implementations.

Much progress has been made in Europe over the past decade. Many nations, most notably the UK, France, Germany, Spain, Italy, the Netherlands and Sweden, are researching,

³² Ibid. p.254.

³³ Professor Adrian Pop is Professor at the National School for Political Studies and Public Administration in Bucharest, Romania. His study *NATO and the European Union: Cooperation and Security* is accessible at: www.nato.int/docu/review/2007/issue2/.

³⁴ Planning the Shift to SOA in Defense Establishments Involves More Than Technology, Herbert Strauss, Gartner Industry Research, 21 November 2006

developing, procuring, and deploying significant transformational capabilities, and the trend is accelerating. Many countries are investing in and deploying unified digital communications infrastructures, cross-service command and control systems, and various types of ISR platforms - manned, unmanned and space-based - and they are able to rely on the European defence industrial base to provide them. Below some examples of the efforts underway in certain European countries and in the US are explained (see further details on national C4ISR capabilities in Annex I).

Sweden

Based on a decision of the Swedish Parliament in 2001, the Swedish armed forces are currently conducting a profound transformation to a Networked-Based Defence (NBD). The technical part of the NBD transformation starts with the development of a C4ISR functions environment, named LedsystT, which was initiated following pre-studies in the late 1990s, and which aims to achieve operative systems between 2010 and 2020. The LedsystT project is governed by the Swedish Defence Materiel Administration and is performed in close collaboration with industry contractors and other partners. The functional design of the operative systems has begun and will be further elaborated in a following procurement phase aimed at system implementation.

Finland

The main objective of the work to develop C2 systems in Finland is to integrate the planning, command and control, and intelligence systems of all the services into one secure joint system. Just a few years ago the Finnish Defence Forces tried to map all communication and information systems being used in Finland alone. It was impossible. They found over 5,500 applications and more than 300 information systems that did not communicate with each other. Therefore, the first objective is to rationalise current C4I systems. The same applies also to interagency co-operation where the situation is even worse. The typical operational environment, in which there is usually a mixture of nations and non-governmental organizations, multiplies these problems.

The second main goal is to create a joint and common platform for future operations. The national information grid will link sensors, decision makers and 'shooters' to create shared situational awareness and enable faster decision making. This same principle is also guiding the development of network and services for inter-agency collaboration. A similar platform is also necessary for operating in multinational and multicultural environments.

The TETRA-network and the Deployable Commercial-Off-The-Shelf, COTS Network-System have been operational since 2003, and were deployed in Kosovo Force (KFOR) for MNB(C) Multinational Brigade (Centre). Since then the system has been used by many nations both in Kosovo and Bosnia. The basic idea was to use proven COTS products and solutions in an innovative way that is acceptable to most users in a static crisis management operation – to meet the minimum information exchange requirements. For national purposes, the Finnish model was successfully implemented in Crisis Response Operations in Kosovo and Bosnia and Herzegovina..

The next step is to develop an information exchange 'gateway' that enables multiple national applications and systems from different generations to connect securely with inter-agency partner systems. This Co-operative Integrated Interoperability Solution (CIIS) project was initiated in December 2006 by the Finnish Defence Forces in partnership with commercial companies ASCOM and IBM. Any interested nation has been invited to take part in the

project. Testing of the concept and solution is planned for the Coalition Interoperability Demonstrator in 2007.

The Finnish Defence Forces are also taking part in the development of civilian crisis management capabilities. Between 2001 and 2004 they took part in an Information Technology and Crisis Management project in which inter-agency co-operation concepts and IT-tools were developed. These solutions have been fielded in Kosovo, but they still need further development. The next step in this area will involve the Multinational Experiment 5 (MNE5), a US-led series of exercises. Finland leads one of the MNE5 Focus Areas named Shared Information Framework and Technology (SHIFT). SHIFT seeks to replace the current practice of building on bilateral or *ad hoc* information exchange connections and relationships between governmental, non-governmental, private and local actors in conflict regions. As a technological solution SHIFT would integrate information sharing and management, online collaboration and situational awareness/picture tools via a portal on the Internet.

France

France has deployed C2 systems in all services. The army has the Force Command and Information System (Système d'Information et de Commandement des Forces, or SICF) for division-level C2 (including C2 for overseas task forces), the Regimental Information System (Système d'Information Régimentaire, or SIR) originally for regimental-level C2, but redirected to company level in 2001 (450 command post vehicles will have this system installed), and the Final Information System (Système d'Information Terminal, or SIT) for tactical-level C2. SICF and SIR are both compliant with NATO Standardization Agreements (STANAGs).

Other existing C2 systems are Martha for air defence, the air force's Aerial Operations Command and Control System (Système de Commandement et de Contrôle des Opérations Aériennes, or SCCOA), the artillery corps' Atlas, and the navy's Naval Tactical Information Exploitation System (Système d'Exploitation Navale des Informations Tactiques, or SENIT) installed on frigates and aircraft carriers. The interoperability of these systems among themselves and with allied systems is currently far from complete, although SCCOA is planned to be interoperable with the NATO Air Command and Control System (ACCS), and Atlas is currently interoperable with US, UK, Italian and German surface-to-surface firing systems as well as with SIR (35).

The French Navy has also deployed Cooperative Engagement Capability (CEC) systems on several vessels. Ships equipped with it can operate as a single, distributed anti-aircraft system. This system is also deployed on US and UK ships, which enables interoperability in naval air defence between the forces of these countries.

France is in the initial stages of deploying its next generation of C2 systems in the form of a strategic-level system called the Joint Information and Command System (Système d'Information et de Commandement des Armées, or SICA). Additionally, there are plans for the development of a next-generation C2 system for the navy (project SIC21) in 2004, and a heliborne C2 system for the air force's helicopters is being considered under project C2H. The Navy SIC21 system will come into use between 2007 and 2009.

³⁵ *Bridging the Gap, European C4ISR Capabilities and Transatlantic Interoperability*, Gordon Adams, Guy Ben-Ari, John Logsdon, Ray Williamson, the George Washington University, Washington D.C, October 2004. page 18.

United States

Formerly known as the Joint Command and Control Capability, the Net-Enabled Command Capability (NECC) (36) will serve as the DoD's principal command and control information technology. NECC integrates databases, servers, client workstations, local area networks, and computer software into an open, scaleable, network-centric single architecture. It will support force-level planning, execution, monitoring, and assessment of joint and multinational operations. It will use Net-Centric Enterprise Services (NCES) Core Enterprise Services (CES) and will be able to exchange data across multiple security domains.

The NECC mission space is defined as the C2 area encompassing the National Military Command System (NMCS) through unit-level commanders executing or supporting C2 functions that support Joint Task Force or military commands. Traditionally, war-fighting C2 is divided into three stratified levels: strategic, operational, and tactical. In today's environment, these demarcation lines are no longer separable. NECC will eliminate these traditional vertical and horizontal C2 boundaries. NECC customers will include both political and military leaders, Joint Force Commanders (JFC), component commanders, and coalition forces.

Conclusions

Operations in Afghanistan and Iraq have demonstrated the need for interoperability between national forces. Most nations, particularly those in NATO, recognize the value and the necessity of deploying in multinational contingents, to mitigate the decreasing size of land forces and to leverage the many niche capabilities being developed by certain smaller nations. If these countries are going to deploy successfully together, battlefield digitisation programmes will need to be compatible. While interoperability between different national networks continues to be addressed through the Multilateral Interoperability Programme (MIP)⁽³⁷⁾, effective interoperability will only be accomplished through the diffusion of software-defined radio (SDR) across NATO and the EU⁽³⁸⁾.

A number of European countries already possess or are seriously exploring elements of modern C4ISR capabilities. However, the approach is not uniform across Europe and there continues to be major interoperability gaps both within and between European countries. Interestingly, countries tend to place higher emphasis of achieving interoperability with NATO and the US rather than at European level. In conclusion, there is not a significant technology gap between EU Member States and the US in C4ISR technologies. Europe possesses information technologies, communications equipment and sensor platforms (both in the defence and commercial sectors) to compete with US technology.

³⁶ <http://www.disa.mil/pao/fs/necc.html>

³⁷ <http://www.mip-site.org/>

³⁸ See Stephen Pullinger, *Software Defined Radio*, Policy Department external policies, European Parliament, Directorate-General for External Policies of the Union Study for the European Parliament, October 2007.

4. Public Safety Communications and Emergency Response

4.1 Disaster Response and Civil Protection at the EU level

Some crises are likely to demand some form of civil protection assistance and the Community Civil Protection Mechanism, established on 23 October 2001, is of special relevance (39). This links national authorities of 30 countries (40) to the Monitoring and Information Centre (MIC), which, through the network, can forward a request for assistance from one state to all national contact points.

It is important to note that the Mechanism applies to disaster relief both inside and outside the EU. Past operations include those mounted after: the forest fires in France and Portugal; the floods in central Europe in 2003 and 2005; the Prestige oil tanker accident off Galicia in 2002; and the major earthquakes in Algeria and in Bam, Iran, in 2003. Most recently, European civil protection resources were used following the south-east Asian tsunami in 2004, Hurricane Katrina and the earthquake in northern Pakistan in 2005, the Java earthquake and Lebanon crisis in 2006 (41).

There have been important lessons learned through these operations. The particular gaps that were identified after the tsunami, include:

- working effectively with the military is a challenge for MIC – lack of effective coordination of civilian and military assets
- lack of transport capability
- more EU assessment and coordination experts were needed on the site
- communications with the headquarters sometimes proved problematic
- Member States had differing conceptions on the role of European coordination

The MIC mechanism will be improved in two major ways. First, a secure general rapid alert system (ARGUS) will be created that will link the MIC to the six other rapid response systems within the community, ranging from the ECURIE system (radiological emergency) and BICHAT (biological and chemical threats), over EWRS (communicable diseases) to ADNS (animal health) (42). The Commission will enhance its ability to coordinate efforts and lead the assistance in emergencies. To this end, a communication and information system (CESIS) has been created for the MIC. Moreover, a new Central Crisis Centre, bringing together representatives of all relevant Commission services during an emergency, is being established. The Commission's role has thereby expanded from mere contingency planning to the running of operational centres in the event of an emergency. However, it is too early to evaluate whether these new measures have helped to bring coherence to the Community response.

The responsibility and mechanisms in Civil Protection are divided between the Council and the Commission, with some overlapping elements. Rapid and coherent coordination and

³⁹ Council of the European Union Decision, *Establishing a Community mechanism to facilitate reinforced cooperation in civil protection assistance interventions* (2001/792/EC, Euratom), Brussels, October 2001.

⁴⁰ EU-27, Iceland, Liechtenstein and Norway.

⁴¹ Bucella, Pia, 'Enhancing the civil protection capacity of the EU', *Faster and More United? The debate about Europe's crisis response capacity*, European Commission, Brussels, May 2007.

⁴² European Commission, Communication from the Commission to the Council and the European Parliament on 'Preparedness and consequence management in the fight against terrorism, COM (2004) 701 final, p.10, Brussels, October 2004.

decision-making is at the core of an effective response. Steps have been taken to improve the effectiveness of the political coordination process in Brussels and the mechanisms for calling on available assets (the Commission is linked to the Council through COREPER 2). Following the Hague Programme and the JHA Council Declaration of July 2005, the Council has taken steps to ensure that the EU will improve the effectiveness of assistance provision when major emergencies occur in future.

4.2 EU Emergency and Crisis Co-ordination Arrangements

The manual on EU emergency and Crisis Coordination Arrangements (CCA) (43) was submitted to the Council in June 2006. The CCA sets out how EU Institutions and affected Member States interact in Brussels in a crisis mode. Not all the emergencies require a coordinated EU response at a political level and, therefore, CCA is only applied to a few of the most severe emergencies.

The Council had on several occasions requested the setting up of integrated EU arrangements for crisis management with cross-border effects. The manual is built on the key principle of subsidiarity. Member States are still primarily responsible for the management of crises within their territory, and the manual does not impose any obligations, nor does it change existing competencies. Nevertheless, the manual is cross-pillar and relevant both to external crises and crises within the EU, and aims to assist Member States during emergencies. Once an emergency has arisen it is up to the affected Member State to evaluate whether the response can be handled without external help.

In the most severe cases where political EU level coordination is required, the information will be conveyed to the SitCen immediately and the procedures of the interim CCA will be triggered. The Director of SitCen shall then relay the information to the Presidency, the Directors of the Private Offices of both the High Representative/Secretary General (HR/SG) of the Council and President of the Commission. The Presidency will confer with the Council Secretariat and the Commission, as well as the Permanent Representatives of the affected Member States to determine whether the emergency or imminent crisis warrants triggering the CCA. The decision to activate the CCA will be taken by the Presidency, in agreement with those Member States directly affected. The Presidency may then decide to convene a Crisis Steering Group, comprising the Council Presidency, affected Member States, CGS, the Commission and the European Parliament.

The Crisis Steering Group would assess the situation and take an initial view on the EU's response; ensure a common understanding of the situation is shared; offer advice to Member States on collective action; develop options for the Committee of Permanent Representatives (COREPER) and the Council; ensure appropriate follow-up; act as a channel through which Member States may communicate needs not covered by existing arrangements and ensure that a common communication strategy is deployed vis-à-vis the media. The Crisis Steering Group would be supported by the services of affected Member States, the CGS, the Commission and the Presidency. An *ad hoc* Support Group of senior officials with relevant expertise would be convened. The composition of this group would reflect the expertise and analysis needed to meet the particular circumstances of each emergency.

⁴³ The manual on EU emergency and Crisis Coordination Arrangements (CC) (10011/1/07 REV 1 ANNEX)

COREPER would be the central body for coordination decisions. It would need to receive assessments of the situation and information on the measures taken by affected Member States and EU institutions. COREPER would also promote coordination and coherence of action, and identify any decision that might need to be taken by the Council.

These arrangements were tested in CCAEX06 in October 2006 and CCAEX07 in September 2007. The main aim of the latter exercise was to test the arrangements to respond quickly and efficiently to a crisis at EU level and the capacity of the Council and the Commission jointly to support Member States' crisis response efforts (⁴⁴).

According to the CCAEX07 Final Evaluation Report (⁴⁵), the exercise showed a significant improvement over the previous exercise. However, further work needs to be done to prepare the Union's response in a real life situation, where events develop at a faster pace and unexpectedly. Nevertheless, the exercise did highlight the fact that the CCA is a workable model, that information can flow at a reasonable rate, that the mechanical aspects of the arrangements work, and that the right people can be brought together in a realistic timeframe to evaluate the situation and to develop ideas for a strategic EU level response. The division of labour among the support machinery, the Support Group, the Steering Group, and COREPER, in a CCA context, could be further clarified. To this end, a more detailed proposal of roles and responsibilities will be elaborated in the ambit of the revision of the Crisis Coordination Arrangements' Standard Operating Procedures (CCA SOPs).

The use of the CCA webpage was an important innovation introduced in this second CCA exercise. The page kept track of all relevant messages and events immediately before and during the active phase of the exercise, and it allowed all Member States to follow the situation's evolution in real time. It significantly reduced the dependence on SMS messaging and e-mail communication, providing all those with access an opportunity to be remotely informed of all relevant aspects of the exercise, both in terms of its logistics and its scenario.

The current encryption software and procedures for the exchange of information classified RESTREINT UE has been worked out, but with some limitations. Before a more efficient solution can be found, the Chiasmus COCCA (encryption software) key, used for CCAEX07 on a temporary basis, should be made permanent, for use by all Member States' Permanent Representations, as well as relevant Council services and the Commission. According to the evaluation report, consideration should also be given to the creation of means by which classified information can be communicated to relevant national entities, previously identified by Member States' Permanent Representations.

4.3 Public authority networks for public safety communications

Responses to many major disasters are adversely affected by the lack of compatibility and interoperability between responding emergency services. The need for secure and fully meshed communication between agencies is evolving as a key strategic requirement for all public safety organisations. Many international responders to major disasters (e.g. tsunami or

⁴⁴ The exercise was based on a totally fictitious scenario. It assumed a simultaneous terrorist attack in certain EU Member States perpetrated with a single bio-agent. It focussed on managing the consequences of such an attack at EU level.

⁴⁵ Emergency and crisis coordination arrangements-CCA exercise (CCAEX07) Final Evaluation Report, 14650/07; Brussels; 5 November 2007

earthquake) require international coordination. Requirements for public safety and homeland security mobile communications systems are rapidly evolving as a direct result of recent world events.

User requirements are also changing as technological innovations open up new communication possibilities, applications and services. Law enforcement agencies at the federal, state, and local level have, over time, employed a range of independent and sometimes proprietary systems. These systems' differences have often precluded fast and easy sharing of information between departments or even limited, basic inter-departmental communications. The transition from analogue to digital in both fixed and wireless communication networks is well underway, creating new challenges for co-operation and interoperability among different public safety organisations. The ease with which people can communicate globally and access vast amounts of information has an impact on security organisations in their fight against crime, terrorism and their need to maintain public safety. In this rapidly changing world the need for standardised technology solutions that can be upgraded, adapted or newly created to meet evolving user requirements becomes more important.

When looking at the coherence of crisis response and management at the national level one cannot really talk about command and control systems but rather about communication systems that bring together the various first responders. Standardised and interoperable equipment for first responders is essential. Communication systems are of vital importance to first responders which must be able to seamlessly and dynamically interconnect multiple agency users, who have multiple functions, and multiple information and communications technology systems.

In public safety communications the diversity of technologies used by different European Member States and user groups creates serious interoperability problems at different levels, starting from the level of equipment up to the level of applications and user/system requirements. The lack of interoperability dramatically reduces the efficiency of emergency responses, especially in complex situations and /or those requiring coordinated international efforts.

For many years now, land mobile radio (LMR), based on analogue voice communications over locally-dedicated radio frequencies and transmission facilities, has been the mainstay of public safety agencies. The lack of interoperability between emergency response organisations has supported the attempts to deploy systems that enable coordinated operations on a wide scale and give access to critical data in real time.

In Europe, many countries have already deployed or are currently deploying nationwide coverage with PMR narrowband systems. They are based on TETRA (46) or TETRAPOL digital radio network. For example Belgium (47), Finland (48), Sweden (49), France (50),

⁴⁶ Terrestrial Trunked Radio, open standard by ETSI which defines a digital system for land mobile radio communication, Private Mobile Radio (PMR). This has created a basis for a multi-vendor market and TETRA products from several manufacturers are being introduced. Interoperability aims to guarantee that TETRA products - especially TETRA terminals - can be used in any vendor's network.

⁴⁷ ASTRID (All-round Semi-cellular Trunked Radio communication network with Integrated Dispatching)

⁴⁸ VIRVE official network

⁴⁹ The public authority network in Sweden is called RAKEL, which is an acronym for "Radiokommunikation för Effektiv Ledning", an attempt to integrate all the different radio systems in the different blue-light organisations so they have the possibility to exchange data between the different organisations via radio.

Spain (51) and Czech Republic (52) have deployed public authority networks that provide local and national authorities and agencies with a safe and reliable management and communications system. Using the same network enables the relevant authorities and agencies to respond more flexibly and in a more coordinated way when dealing with major accidents. These networks have made it possible to introduce new forms of cooperation between different services and agencies, and have added a new dimension to national security. Despite being a common system, such networks, such as VIRVE in Finland, provide their users - such as the police, fire brigades and ambulance service - with all the services of dedicated networks. Particular emphasis has been given to guaranteeing data protection and ensuring high-speed data and speech throughput. The network in Belgium, called ASTRID, is based on two technological advances: a digital radio network and computer-aided control rooms. Numerous new applications enhance operational efficiency, including data and image transmission, message encryption, GPS and high-volume remote use of databases.

Project status in nationwide authority networks in European area

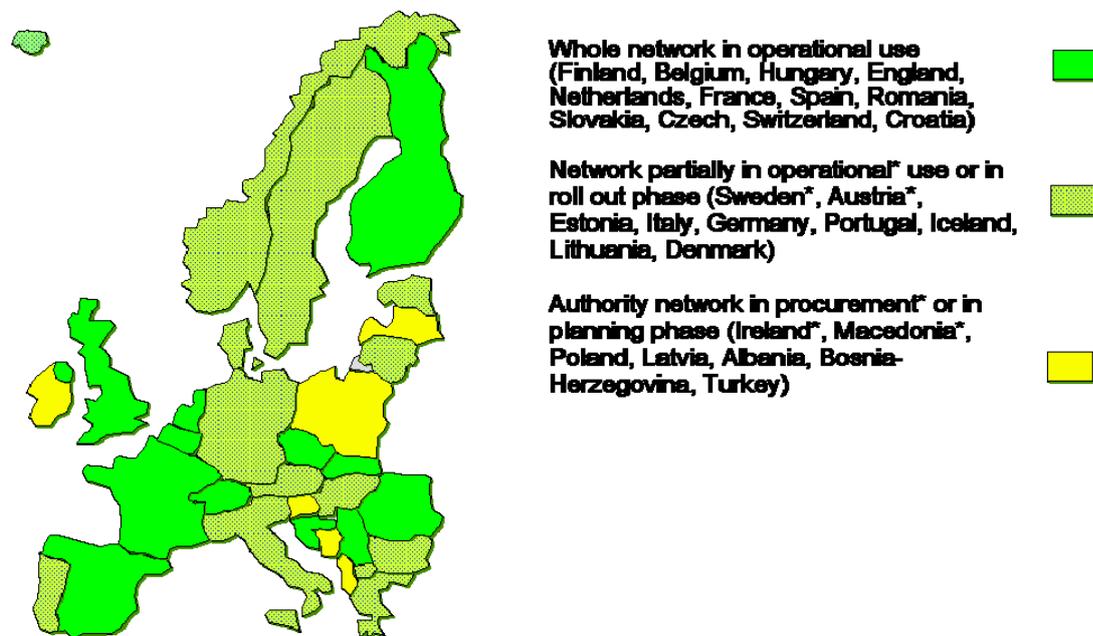


Figure 5: Public Authority Networks project status in Europe, Source: EADS marketing department, October 2007

⁵⁰ In France ACROPOL and ANTARES networks for French national police and fire brigades are recent initiatives aimed at improving public safety communications.

⁵¹ SIRDEE network (Sistema de Radiocomunicaciones Digitales de Emergencia del Estado)

⁵² PEGAS is a full digital cellular system, with integrated voice and data services.

Summary of the public authority networks

Country	Network	Users	Technology
Finland	VIRVE	Emergency and rescue services, police, frontier guard, social and health services, the customs authority and the defence forces. Totally 30.000 users.	TETRA digital radio network
Sweden	RAKEL	Police, coast guard, customs services, local rescue services, emergency healthcare and ambulance services and armed forces.	TETRA digital radio network
Belgium	ASTRID	Local police forces, federal police, fire services, ambulance services, civil defence, state security police, customs. More than 20000 users.	TETRA digital radio network, and computer aided control rooms
Czech Republic	PEGAS	National police, fire brigade, military police, civil security. 27000 users.	TETRAPOL digital radio network: 380-400 MHz. Speed transfer for voice communication is 8 kbps, whereas for data communication speed transfer is 3.6 kbps
France	ANTARES and ACROPOL	French National Police and Fire Brigades. ACROPOL: 1,150 Base Stations, 200 switches, total of 130,000 users ANTARES: will serve over 150,000 members of fire and rescue services	TETRAPOL digital radio network
Spain	SIRDEE	Spain's National Police and the Guardia Civil: 52,000 terminals, 186 switches and 1,450 base stations. 60,000 users.	TETRAPOL digital radio network

The major future evolution in the TETRA and TETRAPOL networks will be wideband data service. TETRA Enhanced Data Service (TEDS) wideband data will provide high speed data for authorities where capacity is same level as General Packet Radio Service (GPRS) / Enhanced Data rates for GSM Evolution (EDGE).

5. EU future needs and R&D

One of the keys to effective action will be policy and investment at the European level in research and development (R&D). There are several parallel processes mapping the EU's future needs in crisis management, in both capabilities and technologies. The following provides a short overview of these efforts and presents the projects that are relevant to command and control systems.

5.1 Priorities in crisis management in FP7

The current European Security Research Programme was preceded by the Preparatory Action on Security Research (PASR 2004-2006), which provided limited funding for exploratory, 'agenda setting' actions with rather short projects. It covered all R&D fields of international and national security with a particular focus on Chemical Biological Radiological Nuclear and Explosive (CBRNE) issues, border protection, infrastructure protection and emergency management. In 2004-6 PASR funded 39 projects overall with a total value of around €75m. Most relevant of the funded PASR projects for the scope of this study are presented in the table in Annex I).

The European Security Research Advisory Board (ESRAB), at its meeting to consider the European Security Research Agenda in September 2006, identified command and control, information management and communications as key functions in crisis response that had to be addressed by the European Security Research Programme under the Framework Programme 7 (FP7).

A report from ESRAB further identified as key functionalities:

- Develop a common operational picture between departments, states, first responders etc.
- Warning, alerting and response coordination: communication, message and information exchange at all levels (local, regional, national, international, EC)
- Intelligent decision support
- Robust and reliable (secure when necessary) communication and message exchange at all levels
- Interoperability of data, systems, tools and equipment
- Public information: Develop a media strategy for dealing with large scale incidents utilizing the full spectra of media coverage.

Major technologies for development identified included:

- Communications network management and control equipment, network supervisor
- Optimisation, planning & decision support systems
- Human factors in the decision process
- Infrastructure to support information management & dissemination
- Web and language technologies

The overall budget for Security Research in 2007-2013 is around €1.4Bn. The Work Programme for the next two years is around €170m (comprising about €150m for Security Research Call 1 and €20m for Security and ICT).

One of the seven mission areas identified under the Security Research agenda is "Restoring security and safety in case of crisis", which covers C2 as well as public safety communication issues. Its priorities are at the level of integration projects: network enabled command and control systems; integrated specialist search and rescue system; post-incident basic service restoration system; and wireless communication for EU crisis management. Within capability projects the priorities are: situation awareness (developing a common operational picture between regional and national authorities, first responders etc.); C2 (intelligent decision support); and incident response (personal equipment, neutralisation of devices/effects).

5.2 European Defence Agency

The EDA will aim to develop defence capabilities in the field of crisis management, promote and enhance European armaments cooperation, strengthen the European defence technological and industrial base (EDTIB) and create a competitive European defence equipment market⁽⁵³⁾. In liaison with the Community's research activities, it will also promote research aimed at leadership in strategic technologies for future defence and security capabilities. In particular the EDA aims to work in liaison with the Commission to maximise 'complementarity' and synergy between defence and civil or security-related research programmes⁽⁵⁴⁾, for example, on the development of (SDR)⁽⁵⁵⁾.

Following the publication of its Long-Term Vision document⁽⁵⁶⁾, the EDA has continued the work on preparing a Capability Development Plan (CDP) aimed at making the Vision's capability guidance more specific. Knowledge exploitation has been identified as one of the key issues. Dominance in the area of knowledge management is not built upon computers or CIS architectures, sensors or innovative training alone, but upon all these and much more – all welded together by an agreed doctrine and common standards.

Network-Enabled Capability (NEC) must be a fundamental development priority for ESDP operations and will be essential to ensure interoperability with the US in this area, interpreted through NATO. Interoperability needs to be at the heart of all European capability development work. Expeditionary, multi-national operations, with strong inter-action with civil instruments, require interoperability within national forces, between national forces and with civilian actors⁽⁵⁷⁾.

In February 2007, a methodology for identifying Information Exchange Requirements (IER) was noted by the PSC. This work aims at defining operational requirements for exchanging information between all entities, both civilian and military, that may interact in support of ESDP operations with a view to a comprehensive approach. The establishment of an agreed IER will provide a reference point from which the EU NEC activities can be built.

In autumn 2006 Finland, France, Italy, Spain and Sweden proposed, and the Steering Board accepted, a €100m study on a European Secured Software Defined Radio Referential (ESSOR). This ambitious study aims at enhancing interoperability (in Europe and with the US) of medium-term national SDR projects and at promoting a truly European technological and industrial capacity of strategic importance. The ESSOR study, planned to be a 'Category B' programme under the auspices of the EDA, will address the following main objectives in order to give European industry the capability to develop interoperable SDR in the period 2010-2015:

- In relationship with the US, developing the normative referential required for development and production of software radios in Europe;
- Setting up a common security basis to increase interoperability between European forces as well as with the US; and
- Stimulating a balanced transatlantic relationship on SDR.

⁵³ Michael Brzoska, *Protection of the European Defence Technological and Industrial Base*, Policy Department external policies, European Parliament, Directorate-General for External Policies of the Union, October 2007.

⁵⁴ Council Joint Action 2004/551/CFSP of 12 July 2004 on the establishment of the European Defence Agency.

⁵⁵ Stephen Pullinger, *op. cit.*

⁵⁶ This is available on the EDA website at: <http://www.eda.europa.eu/genericitem.aspx?id=146>

⁵⁷ Head of the European Defence Agency's report to the Council – 14 May 2007.

The Agency is playing a key role to ensure coordination and complementarity between this project, its own SDR activities, and the Commission initiatives (⁵⁸).

5.3 EU-funded research on public safety communications systems

In order to facilitate consensus building in the area of public safety communication and information management systems, and with the support of the European Commission, a 'Forum for Public Safety Communication Europe' was launched in June 2006 for an initial period of three years. This Forum invites users and policy makers, industrialists (technology and service providers), research organizations and standard-making authorities to reach consensus on:

- Consolidated user requirements;
- Solutions for interoperability of communication systems among users;
- An R&D road map for future activities;
- Guidelines for policy makers and regulators;
- Indicating ways for the improvement of global, European or national inter-operability through implementation of harmonized technologies and/or approximation of legal environments.

The European Commission has funded a number of projects relevant to public safety communications, including the examples from PASR explained in Annex I. Other relevant projects include, for example: OASIS, Open Advanced System for disaster and emergency management (<http://www.oasis-fp6.org/>); CHORIST, Integrating Communications for enHanced enviroNmental RiSk management and citizens SafeTy (<http://www.chorist.eu>); DeHiGate, Deployable High Capacity Gateway for Emergency Services (<http://www.celtic-dehigate.org/>); LIAISON, Location based Services for the Enhancement of Working Environment (<http://liaison.newapplication.it/>); and many others (59).

In addition, several standard-related projects relevant for public safety communications have been launched. For instance: EMTEL addresses standardization issues in the field of emergency telecommunications (<http://www.emtel.etsi.org/>); Project MESA is an international partnership producing globally applicable technical specifications for digital mobile broadband technology, aimed initially at the sectors of public safety and disaster response (<http://www.projectmesa.org/>); TETRA (Terrestrial Trunked Radio) is a digital trunked mobile radio standard developed by the European Telecommunications Standards Institute (ETSI). The purpose of the TETRA standard is to meet the needs of traditional Professional Mobile Radio (PMR) user organisations including Public Safety users (<http://www.tetramou.com/>).

5.4 NATO programmes on command and control systems

The NATO C3 Agency (NC3A) is developing, procuring and implementing state of the art C3 capabilities for NATO. The Agency's core competencies are organised into functional areas and co-ordinated by integrated programme teams. Those functional areas are: C3 Policy

⁵⁸ See Stephen Pullinger, *Software Defined Radio*, Policy Department external policies, European Parliament, Directorate-General for External Policies of the Union Study for the European Parliament, October 2007.

⁵⁹ See further information about the funded projects at Forum for Public Safety Communication Europe - <http://www.publicsafetycommunication.eu/index.php?id=97>,

Concept & Architecture, Operations Research and Functional Services, Communication and Information Systems, Command and Control Systems and Acquisition Project management.

The NATO C3 Board started the NATO Network-Enabled Capability (NNEC) initiative to elaborate new doctrinal, structural and architectural concepts for the Allies to successfully inter-operate in the network-centric environment. The new NATO structure should be robust and flexible, capable of sharing high volumes of information almost instantaneously. NNEC, when developed, is expected to change the way of doing business within NATO by speeding up the decision-making process in NATO Headquarters.

The future NATO Air Command & Control System (ACCS) is a very significant programme and a good example of NATO interoperability activities. ACCS is designed to support the planning, tasking and execution of NATO defensive, offensive and support air operations. The basic tasks of ACCS are force management, air C2 resource management, airspace management, air mission control, air traffic control and surveillance. In addition, ACCS supports such necessary features as deployability, information exchange, communications and comprehensive land and maritime interface capabilities. ACCS will replace legacy air C2 systems and will interface with a number of existing automated and semi-automated systems currently employed by NATO and the NATO nations.

The NATO Research and Technology Organisation (RTO) conducts and promotes co-operative scientific research and exchange of technical information amongst 26 NATO nations and 38 NATO partners. The RTO Studies, Analysis, and Simulation Panel Working Group SAS-050 have produced a comprehensive C2 Conceptual Reference Model.

5.5 C2-related initiatives and research in the US

In the US there is a wealth of research related to C2 and communications systems. Below are a small number of examples of the current research programmes and their focus areas.

The Department of Homeland Security (DHS) established the Office for Interoperability and Compatibility (OIC) in 2004 to strengthen and integrate interoperability and compatibility efforts in order to improve local, tribal, state, and Federal emergency preparedness and response. Managed by the Science and Technology Directorate, OIC is assisting in the coordination of interoperability efforts across DHS. OIC programmes and initiatives address critical interoperability and compatibility issues. Priority areas include communications, equipment, and training.

OIC programmes address both voice and data interoperability. OIC is creating the capacity for increased levels of interoperability by developing tools, best practices, technologies, and methodologies that emergency response agencies can immediately put into effect. OIC is also improving incident response and recovery by developing tools, technologies, and messaging standards that help emergency responders manage incidents and exchange information in real time.

SAFECOM, a communications programme of the OIC, with its Federal partners, provides research, development, testing and evaluation, guidance, tools, and templates on communications-related issues to local, tribal, state, and Federal emergency response agencies. OIC is managed by the Science and Technology Directorate. As an emergency responder-driven programme, SAFECOM is working with existing Federal

communications initiatives and key emergency response stakeholders to address the need to develop better technologies and processes for the multi-jurisdictional and cross-disciplinary coordination of existing systems and future networks. SAFECOM harnesses diverse Federal resources in service of the emergency response community.

The US DoD Command and Control Research Programme (60) (CCRP) has the task of improving the DoD's understanding of the national security implications of the information age. Focusing upon improving both the 'state of the art' and the 'state of the practice' of C2, the CCRP helps the DoD take full advantage of the opportunities afforded by emerging technologies. The CCRP pursues a broad programme of research and analysis in information superiority, information operations, C2 theory, and associated operational concepts that enable us to leverage shared awareness to improve the effectiveness and efficiency of assigned missions.

An important aspect of the CCRP programme is its ability to serve as a bridge between the operational, technical, analytical, and educational communities. The CCRP provides leadership for the C2 research community by:

- articulating critical research issues;
- working to strengthen C2 research infrastructure;
- sponsoring a series of workshops and symposia;
- serving as a clearing house for C2-related research funding; and
- disseminating outreach initiatives that include the CCRP Publication Series.

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

The Institute for Defense Analyses (61) is a non-profit corporation that administers three federally-funded research and development centres to assist the US Government in addressing important national security issues, particularly those requiring scientific and technical expertise. IDA's research on C2 has concentrated on several different stands; strategy, capability requirements, acquisition management, technology development, systems assessments, testing and evaluation, and operations. In the strategy and capabilities area a key task is the Joint Battle Management Command and Control Roadmap. This effort focuses on providing logical methods for synchronizing interdependent C2-related programmes into a coherent approach that is aligned to a unified strategy. The complexity of this task is compounded by the large number of programmes and organizations that are developing, managing, and overseeing the work. Systems and acquisition management are particularly busy areas for IDA's researchers in C2 networking. The work includes innovative research on C4ISR systems that addresses the complexities and nuances associated with providing a meaningful cost estimate of systems that include intensive software, hardware, services, and information technology infrastructure.

⁶⁰ See further at <http://www.dodccrp.org/>

⁶¹ See further information at <http://www.ida.org/researchareas/idaresearchnotes.php>

The technology development and testing areas are best exemplified by IDA's work on the Command Post of the Future (CPOF) and the Deployable Joint Command and Control (DJC2) system. These tasks focus on providing pragmatic tools for operational and tactical commanders. The CPOF system was accelerated through the development cycle and deployed to Operation Iraqi Freedom (OIF) so that it could be used to gain valuable experience and data in a live operational environment. Similarly, the DJC2 is being tested through training exercises in several commands. IDA's analyses on the operational aspect of C2-networking through the OIF Bandwidth Studies were the first of its kind and provided a holistic look at the in-theatre networks and the associated performance relative to the command structure down to the last tactical mile.

6. Crisis Management Markets

The market for security products is vast and fragmented – with private customers, national, regional and sometimes local public services, all with their own requirements. As funding is often provided by government authorities, the rate of enhancement is determined by the level of assigned public budgets. In 2001 the total revenues for the C4ISR market in Europe were \$6.98Bn (€4.75Bn). The market has a compound annual growth rate of 4.7 per cent; and strong growth is likely to continue, mainly due to technology advances and changes in military doctrine (62).

The success of network-centric warfare in recent military operations and substantial growth in the quantity of information available to military commanders has underlined the critical importance of C2 systems for all European land forces. According to Frost and Sullivan, the ability of C2 systems to act as a force multiplier for armed forces looking to project more military power with limited assets has opened up new market opportunities. They found that the European land-based C2 markets will grow to \$5.43Bn (€3.7Bn) between 2005 and 2014. A substantial portion of the market is driven by large, comprehensive and often incremental programmes in places of traditionally high European military spending including France, the UK, Spain, Italy, Germany, the Netherlands and Greece. Analysts said many other smaller European nations, particularly in Eastern Europe, have articulated long-term plans for the development of C2 systems, although on a more moderate scale.

⁶² Frost and Sullivan, *European Command, Control, Communications, Computers and Information, Surveillance and Reconnaissance (C4ISR) markets*, B055-16, Texas, 2002, page 1.

Figure 1-1 and Chart 1.1 illustrates the 2001 revenues for the total market.

FIGURE 1-1

Total C4ISR Market: Revenue Forecasts (Europe), 1999-2008

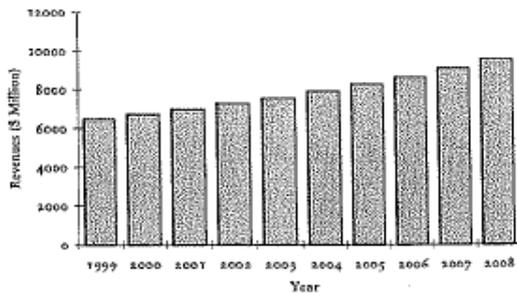
Year	Revenues (\$ million)	Revenue Growth Rate (%)
1999	6,504	---
2000	6,730	3.5
2001	6,976	3.7
2002	7,245	3.9
2003	7,550	4.2
2004	7,896	4.6
2005	8,246	4.4
2006	8,627	4.6
2007	9,085	5.3
2008	9,569	5.3

Compound Annual Growth rate (1999-2008): 4.7%

Note: All figures are rounded. Source: Frost & Sullivan

CHART 1.1

Total C4ISR Market: Revenue Forecasts (Europe), 1999-2008



Note: All figures are rounded. Source: Frost & Sullivan

The major trends affecting the C4ISR market are: defence budgets; military lessons learned from recent operations; and the adoption of network-centric warfare doctrine by European militaries. The markets can be split into three according to the major technology segments: reconnaissance and surveillance; C2; and communications systems. The growth of the reconnaissance and surveillance technologies is strong compared to the other two segments. Procurement of strategic surveillance and reconnaissance (ISR) platforms and ISR unmanned aerial vehicles (UAVs) will be the main drivers in this market. Systems will increasingly be more mobile and able to take part in rapid reaction forces. According to Frost and Sullivan, land reconnaissance will also experience strong growth as communications bandwidth improves to allow greater data feeds. The key drivers in the market include the need for information superiority and time critical information in the recent conflicts (63).

⁶³ Frost and Sullivan, *op. cit.*, page 4.

The C2 market produced revenues of \$1.86Bn (€1.27Bn) in 2002 but overall growth might be relatively low in the future, since the market is now moving from purely strategic systems to operational and tactical systems. Interoperability of systems is going to be a major factor as European militaries attempt to develop interoperable forces. Mobility and survivability will be a key factor in this market as European military doctrine continues to shift towards rapidly deployable forces.

Communications systems markets produced revenues of \$2.25Bn (€1.53Bn) in 2001 and overall growth in the future is expected to be rather high. Militaries have begun to focus on network-enabled systems and platforms. The move from fixed systems to mobile systems and the impact of commercial advances in communications technology have revolutionised areas of this market and created numerous sub-markets.

In France, the UK, Spain, Italy and Germany, major global defence contractors like General Dynamics Corporation, Thales, EADS and Lockheed Martin Corporation, the Finmeccanica Inc., group of companies and Amper Programas serve as leaders of large, multi-year C4I projects. Smaller companies like DRS Technologies Inc., are providing displays for the General Dynamics Corporation in the UK, and other important hardware elements for large-scale battlefield digitisation projects led by the major companies. The Baltic States and several other Eastern European states have seen a significant degree of US-based industrial penetration, most notably Northrop Grumman Corporation, through government-to-government aid. Government-to-government programmes generally favour sole-source suppliers. Other smaller European nations have capable indigenous defence electronics industries that have met their countries' C2 needs, particularly in software that drives C4I systems. Poland, the Czech Republic, Slovakia, Denmark, Norway, Sweden and Greece in particular have so far used domestic industry to source C4I requirements.

7. Improving the coherence of crisis management

Efforts are being made to improve the coherence of crisis management, both in EU operations as well as in public safety communications in EU Member States. There is also a growing understanding that new technologies can support more co-operative and interoperable practices in crisis management. However, it is important to note that technology cannot help if command and control relationships, decision-making authority and procedures are not adapted to operational crisis management. Currently, a large majority of key challenges in creating interoperability in crisis management at various levels are not technological or related to the availability of systems, but procedural in nature. Technical interoperability is still a problem because ESDP operations as well as cross-border crisis management is heavily dependent on national systems that have been procured on the basis on national considerations and not of interoperability with other EU Member States.

The ability to make decisions rapidly in crisis management needs to be enhanced. The role of the Presidency and the input of Member States are crucial in determining whether or not the EU should intervene in a timely fashion. Existing crisis management procedures are rather cumbersome with consultations between different groups and committees taking up a lot of time and resources. While not altering the planning sequence, practical ways should be identified to streamline the procedure, including more parallel planning. Urgent operational decisions can also pose a problem. Crisis management bodies must be able to respond rapidly

to emergencies on the ground, and decision-making by a committee of 27 is not best suited for that.

Important steps in strengthening the civilian chain of command have been the adoption of the Guidelines for Command and Control Structure for EU Civilian Operations in Crisis Management and the creation of the position of a Civilian Operation Commander for the civilian missions. The main importance of these guidelines is that they set out the functions, roles and responsibilities of the Civilian Operation Commander, who will have command and control of those assets put at the disposal of civilian ESDP operations by Member States. The Guidelines also render the civilian command structure more compatible with the military levels of command, thereby facilitating improved civil/military coordination and coherence. Evolving operational requirements clearly demand further civil-military synergy, both for planning and conducting ESDP operations. Steps need to be taken to enhance civil-military coordination throughout crisis management procedures.

A case study and recommendations on Civil-Military Coordination (CMCO) in the EU supporting action to the AU in Darfur was noted by the PSC on 29 May 2007. This has fed into an overall compilation of practical recommendations on CMCO in theatre on the basis of experiences in BiH, Darfur and DRC – again, to be noted by the PSC

However, clear gaps still exist in the CIS mission support arrangements both in terms of capacity and procedures. CIS planning in civilian operations is usually challenged from the start. For instance, user requirements are often poorly articulated and a scalable communications concept is lacking. There is no adequate civilian planning capacity in the Council General Secretariat and the EUMS CIS Division is supporting CIS planning on an *ad hoc* basis. The Council Secretariat cannot easily procure the necessary equipment for the mission for budgetary reasons: the process can only be started at the behest of the Head of Mission as soon as s/he has the funds available. The Head of Mission is usually nominated just before the launch of the mission, and acquisition usually takes weeks or even months. Therefore, CIS services are not available for the mission when they are needed. At worst this state of affairs may put the safety of the personnel in jeopardy.

A lack of rapidly available financing has been identified as a problem for the operational capacity of civilian crisis management operations in the start-up phase. This is also a particular problem for the planning and deployment of CIS. In accordance with the remit following the informal meeting of Heads of State/Government at Hampton Court in December 2005, work has been taken forward to find practical solutions to this problem in order for the EU to be able to launch civilian ESDP operations more rapidly and effectively. Accordingly, the Financial Regulation and its implementing rules have been amended to provide for possibilities for financing of preparatory measures agreed by the Council. These are, *inter alia*, to assess the operational requirements, to provide for rapid initial deployment of resources or to establish the conditions on the ground for the launching of civilian crisis management operations.

In the field of procurement, technical work has been started for the establishment of framework contracts to acquire essential mission equipment and services for civilian ESDP. The first contracts to be concluded will cover health and high-risk insurance, financial liability insurance and strategic transportation, followed by communications and IT equipment and vehicles.

Drawing on the operational conclusions from EUFOR mission in the DR Congo, the EU needs to further improve its planning and command capabilities for autonomous ESDP operations in terms of efficiency, speed and clarity. On the military ESDP side, a positive development has been the establishment of the EU Operations Centre within the EU Military Staff. Also the work started to procure Command and Control Information System for the Operation Centre and the latest improvements in the secure connections to the OHQs and deployable CIS packages for the OpCen support effective planning and conduct of operations.

A key challenge for consolidating interoperability is in finding unanimity on arrangements between 27 Member States and other contributors, particularly in the force generation phase where governments may attach caveats for the use of their resources. EU Member States are developing technologies and systems to meet their national needs and requirements, EDA is just a facilitator. Member States are not always as motivated to co-operate under the EDA umbrella to ensure interoperable CIS for operations, and often it is bilateral and NATO-related projects that receive priority.

Increased mission complexity places a premium on coherence: both at intra-EU and inter-state level. The Commission's new Stability Instrument could be a potential vehicle to further facilitate cross-pillar coherence in crisis management. The Commission currently finances a lot of research relating to crisis management under the FP7 security research. Coherence needs to be fostered between different EU instruments in the field, including the civil-civil dimension.

The new EU Emergency and Crisis Co-ordination Arrangements are a positive step forward in improving co-operation in emergencies. The arrangements were tested in CCAEX06 exercise in October 2006 which noted the adequacy of the CCA structures, the good level of knowledge among participants of the CCA structures and procedures, as well as on the importance of close cooperation between the Council and the Commission, and the need for improvement in the use of communication technology.

There is a positive trend in public safety communications in investing in country-wide public authority networks that all first responders are using. However, these networks do not normally guarantee civil-military interoperability in emergencies as the military does not usually have these technologies.

In public safety communications, the diversity of technologies used by different European Member States and user groups creates serious interoperability problems at different levels, starting from the level of equipment and going to the level of applications and user/system requirements. The interoperability problem dramatically reduces the efficiency of emergency response, especially in complex situations and /or requiring coordinated international efforts.

Currently there are a large number of diverse technology systems that either cannot inter-operate, or, if they can, the interoperability is very limited in scope. In the interests of effective and consistent levels of service delivery across Europe, the communication within authorities, from authorities to citizens and from citizens to authorities needs to be internationally harmonized. Among the obstacles presently hindering the building of an internationally integrated system is, for example multiple languages and the difficulty of localization of emergency calls. Also, the networks enabling the communication between the

authorities and from authorities to the citizens are difficult to implement as harmonized systems due to different structures, cultures and policies of the various authorities.

The market for security products is vast and fragmented – with private customers, national, regional and sometimes local public services all with their own requirements. As funding is often provided by government authorities, the rate of enhancement is determined by the level of assigned public budgets.

8. Recommendations

Decision-making and procedures supporting CIS arrangements in ESDP operations need to be improved to help to ensure interoperability and the interconnection of systems processing classified information. Member States should actively engage in these efforts within the EDA framework to address the identified shortfalls in C2 systems and to develop interoperable systems. The key recommendations of this study are that:

- Member States - within the EDA and in close co-operation with NATO - should continue to address the gaps in the interoperability of communication and information systems between their armed forces. To this end, they should actively participate in the EDA's work in developing common EU crypto-algorithms and devices to ensure interconnection of systems processing classified information, in close cooperation with NATO.
- The EU should ensure that ESDP operations in complex and hostile environments have access to real-time situational awareness systems and – via the use of interoperable Friendly Force Tracking Systems - ensure the safety and security of their personnel.
- There is a need to ensure that procedures are put in place to enable the speedy accreditation of those sensitive communication and information systems to be used in ESDP missions on all command levels.
- The exchange of information between different Member States should be based on a “need to share” principle rather than the traditional “need to know” principle.
- To ensure interoperability, Member States could use the CCIS (Command and Control Information System) to be established in the OpCen of the EUMS as a guideline for the development and procurement of their own national OHQ and FHQ (which they could subsequently make available for ESDP operations).
- The timely deployment of communication and information systems for ESDP civilian missions needs to be improved, both through streamlining organisational procedures and improving mission support structures.
- The Head of Mission should have more time (requiring faster decision-making at the Brussels level), enjoy greater flexibility and have stronger financial decision-making authority in procuring the necessary capabilities for a mission.
- The EU should ensure that the necessary framework contracts are established through tenders based on a scalable communications concept that could be based on the scenarios identified in CHG2008 and/or the CHG 2010 illustrative scenarios.
- A basic stock of critical equipment necessary for rapid mission start-up should be established.

- There is an urgent need to improve European and national inter-operability in public safety communications through the implementation of harmonized technologies and/or a gradual process bringing national legal rules closer together.
- In Security Research interaction with end users from the crisis management community is essential. There is need to ensure that the Security Research under the 7th Framework Programme covers also the CIS requirements of ESDP civilian operations

9. Conclusions – a Role for European Parliament

The rapid growth in the number and type of ESDP civilian and military crisis management operations, as well as the complex nature of EU crisis management decision-making, represent growing challenges to parliamentary oversight. The issue is further highlighted because of the need to link the work on crisis response and management under Community instruments with those carried out in the ESDP framework. The requirements of both these sectors should be effectively addressed under the EU research programmes.

The European Parliament plays a key role in ensuring coherence across the pillars (especially in relation to civil-military coordination) and in the oversight of those aspects of CFSP and crisis management which the Commission implements. It has important co-decision rights with regards the budget for civilian crisis management under the first pillar, and has a more limited ability to scrutinise the CFSP budget (used to support second pillar activities - excluding those with defence implications) under the Inter-Institutional Agreement between the EP, Council and Commission that was agreed in 1999. This states that the Presidency will consult the EP on a yearly basis and provide it with a document on the financial implications of CFSP for the Community budget.

The European Parliament has an important role to play in overseeing decisions, promoting transparency and accountability. Its existing budgetary powers are an important means by which it can enhance its influence. The link between civilian and military elements of crisis management and the need to further combine cross-pillar resources for effective external action might strengthen the EP's role in the future and contribute to making it a more influential player in ESDP.

This study, which has sought to provide a preliminary overview, contains a number of questions, suggestions and recommendations that could be taken up by the European Parliament, within the context of national or EU political institutions, or by the European Parliament exercising its oversight role and drawing attention to command, control and communications issues that need to be addressed by the Commission and Council.

Bibliography

Adams, Gordon, Ben-Ari, Guy, Logsdon, John and Williamson, Ray, Bridging the Gap, European C4ISR Capabilities and Transatlantic Interoperability, the George Washington University, Washington D.C, October 2004.

Alberts, David S. and Hayes, Richard E., Understanding Command and Control, Command and Control Research Programme (CCRP), the United States Department of Defense, Washington D.C., 2006.

Assembly of WEU, Berlin Conference on European Security and Defence Policy (6 and 7 February 2007), Press Release, February 2007.

ASTRID (All-round Semicellular Trunked Radio communication network with Integrated Dispatching)
http://www.astrid.be/_uk/html/frameset.htm

Bucella, Pia, 'Enhancing the civil protection capacity of the EU', Faster and More United? The debate about Europe's crisis response capacity, European Commission, Brussels, May 2007.

Committee on Foreign Affairs, Subcommittee on Security and Defence, 'Visit of the ad hoc Delegation to Kinshasa (DRC), Chairman's Report', Brussels, November 2006.

Council Joint Action 2004/551/CFSP of 12 July 2004 on the establishment of the European Defence Agency

Council Joint Action 2004/570/CFSP of 12 July 2004 on the European Union Military Operation in Bosnia and Herzegovina.

Council of the European Union, *Council Decision adopting the Council's security regulations*, 5775/01, Brussels, February 2001.

Council of the European Union Decision, Establishing a Community mechanism to facilitate reinforced cooperation in civil protection assistance interventions (2001/792/EC, Euratom), Brussels, October 2001.

Council of the European Union, EU Military C2 Concept, 11096/03, Brussels, July 2003.

Council of the European Union, Headline Goal 2010, 6309/6/04/REV 6, Brussels, May 2006.

Council of the European Union, Manual on EU Emergency and Crisis Coordination, 9919/07 Brussels, 2007.

Council of the European Union, Presidency Report on ESDP, 10910/07, Brussels, June 2007.

Council of the European Union, Reinforcing the European Union's emergency and crisis response capacities, 16642/06, CAB 72, PROCIV 259, JAI 701, PESC 1266, COCON 38, Brussels, December 2006.

Council of the European Union, The Draft Guidelines for Command and Control Structure for EU Civilian Operations in Crisis Management, 9919/07, Brussels, May 2007.

Director General of the EUMS, Lieutenant General David Leakey's interview on 13 June 2007 and published on the web-site <http://www.hybaskova.cz/hybaskova/EUDefence-EU-operation-planning-enters-a-new-era--General-Leakey-looks-at-where-we-go-from-here~.html>

Emergency and crisis coordination arrangements-CCA exercise (CCAEX07) Final Evaluation Report, 14650/07; Brussels; 5 November 2007

European Commission, Communication from the Commission to the Council and the European Parliament on 'Preparedness and consequence management in the fight against terrorism, COM (2004) 701 final, p.10, Brussels, October 2004.

European Defence Agency (EDA), An Initial Long-Term Vision for European Defence Capability and Capacity Needs, Brussels, October 2006, p. 27.

European Union Council Secretariat, Factsheet, EU Battlegroups, February 2007.

European Union Operations Centre,
http://consilium.europa.eu/cms3_fo/showPage.asp?id=1211&lang=FI&mode=g

Forum for Public Safety Communication Europe
<http://www.publicsafetycommunication.eu/index.php?id=97>

Frost and Sullivan, European Command, Control, Communications, Computers and Information, Surveillance and Reconnaissance (C4ISR) markets, B055-16, Texas, 2002.

General Henri Bentégeat's, Chairman of the EU Military Committee, statement in the Bulletin of the EU Military Staff IMPETUS Spring/Summer 2007.

Gnesotto, Nicole and Grevi, Giovanni, The New Global Puzzle. What World for the EU in 2025?, Institute for Strategic Studies, Paris, 2006.

Homan, Kees, 'Operation Artemis in the Democratic Republic of Congo', Faster and More United? The debate about Europe's crisis response capacity, European Commission, Brussels, May 2007.

Interregional response to natural and man-made catastrophes – SIPROCI -
<http://www.siproci.net/>

Interview with Ralf Persicke, EUMS CIS Division on 11 October 2007.

Johansson, Björn, Joint control in dynamic situations, Dissertation No. 972, Linköping Studies in Science and Technology, Department of Computer and Information Science, Linköpings universitet, SE-581 83 Linköping, Sweden, Linköping 2005.

Lieutenant General Jan Oerding's interview 'Absolutely professional and wholly committed' on 07.12.2006 and published on Bundeswehr web-site (<http://www.streitkraeftebasis.de/portal/a/streitkraeftebasis>).

Lieutenant General Leakey's interview published in NATO Review Summer 2007, accessible at www.nato.int/docs/review/2007/issue2/English/main.htm.

Michel, Leo, NATO – EU Cooperation in Operations and Implications for Italy, is accessible at: www.comitatoatlantico.it/.

Pop, Adrian, NATO and the European Union: Cooperation and Security, is accessible at: www.nato.int/docu/review/2007/issue2/.

Solana, Javier, A Secure Europe in a better world: European Security Strategy, Brussels, December 2003.

UK MOD Joint Services Publication (JSP 777)

United Nations Peacekeeping Best Practices Unit, Military Division, "Operation Artemis: The Lessons of the Interim Emergency Multinational Force", New York, October 2004.

US Army Regulation 25–2 Information Management, Information Assurance, Aug 2007.

US Defense Security Cooperation Agency (DSCA) Memorandum I-05/014306-STR/16.3.2006.

US DoD Joint Pub 1-02 Dictionary of Military and Associated Terms, June 1998.

Vice-Admiral Arthur K. Cebrowski, USN, and John J. Garstka, "Network Centric Warfare: Its Origin and Future," Proceedings of the Naval Institute 124:1, January 1998

List of Figures:

Figure 1: The EU Military C2 Options

Figure 2: Service-orientated architecture for network orientated defence (Source: C4ISR for Network-orientated Defence, White Paper, October 2006, Ericsson)

Figure 3: Examples of C4ISR services, their producers and consumers. (Source: C4ISR for Network-oriented Defense, White Paper, October 2006, Ericsson)

Figure 4: Public Authority Networks project status in Europe, (Source: EADS marketing department)

Annex I: Examples of projects* funded by the Preparatory Action on Security Research (PASR 2004-2006)

Project	Objective	Costs	Duration	Partners
Crisis Simulation System (CRIMSON) http://crimson.c-s.fr	To research, develop and validate an innovative system using the latest Virtual Reality technologies for the interorganisational preparation, rehearsal and management of security missions in response to urban crisis (terror attacks, seizure of hostages, NBCR crisis, etc.).	Total Cost : € 2,933,610 EU Contribution : € 1,520,000	Starting Date : 1/12/2004 Duration: 28 months	CS Systèmes d'Information (FR), Consiglio Nazionale delle Ricerche (IT), Crisis Research Center – University of Leiden, Centre for Advanced Studies (NL), Research and Development in Sardinia (IT), Mathématiques Appliquées SA (FR), Estonian Rescue Board (EE)
Advanced Space Technologies to Support Security Operations (ASTRO+)	To study and illustrate how space capabilities - Earth Observation and Reconnaissance, Navigation, Telecommunication and their integration and implementation into services and infrastructures can contribute in the short and long term to the equipment of Europe in security facilities supporting in particular the improvement of foreign operations.	Total Cost : € 2,946,866 EU Contribution : € 2,200,000	Starting Date : 1/1/2005 Duration : 15 months	Partners: EADS Astrium Limited (UK), EADS Astrium GmbH (DE), Alcatel Space (FR), Alenia Spazio (IT), Telespazio (IT), Centre National d'Etudes Spatiales (FR), Deutsches Zentrum für Luft- und Raumfahrt (DE), Alcatel ETCA (BE), Ecole Royale Militaire de Belgique (BE), Fondation pour la Recherche stratégique (FR), Istituto Affari Internazionali (IT), Indra Espacio (ES), Landmåteriet Metria (SE), Infoterra Limited (UK), Nottingham Scientific Limited (UK), Space Research Centre Polish Academy of Science (PL), QinetiQ (UK), Royal United Services Institute for Defence & Security Studies (UK), SkySoft Portugal (PT), European Union Satellite Centre (ES) and Infoterra GmbH (DE)
Highway to Security: Interoperability for Situation Awareness and Crisis Management (HiTS/ISAC)	To enable information analysis and fusion from many different sources, through secure cross-border on-line group cooperation between authorities, in order to detect and provide	Total Cost : € 1,739,093 EU Contribution : € 1,132,895	Starting Date : 1/6/2006 Duration : 18 months	EADS Defence and Security Systems SA (FR), TeliaSonera (FI), Swedish Defence Research Agency (SE), EADS Secure Networks (FI), TietoEnator ALISE (LV), Denodo

	early warnings for suspicious activities, be it communication between suspected criminals, or anomalous movement of persons, goods or money, etc. HiTS/ISAC will develop a Problem Solving Environment and demonstrate it in a Virtual Operations Room which can be established anywhere, at any time.			Technologies S.L. ES), Hugin Expert A/S (DK), Cybernetica AS (EE), UAB "ERP" (LT), Military University of Technology (PL)
Mobile Autonomous Reactive Information System for Urgency Situations (MARIUS)	To develop a pre-operational autonomous Command Post which can be deployed very quickly to monitor every type of crisis management operations. It will be equipped with its own sensors, information and communications systems and focuses on improving Crisis Management efficiency: deployment rapidity, inter-agency co-operation, situation assessment and decision-making. The project will also address situation awareness and interoperability issues through the analysis of the operational scenarios and of the pre-normative aspects. The MARIUS Demonstrator will be deployable by helicopter and will incorporate open scalable IT infrastructure, generic gateways, decision support and crisis communication support.	Total Cost : € 1,915,905 EU Contribution : € 1,431,988	Starting Date : 1/3/2006 Duration : 18 months	THALES Communications SA (FR), SELEX Communications SpA (IT), SELEX Sistemi Integrati SpA (IT), THALES Research and Technology (FR), AMPER PROGRAMAS DE ELECTRONICA Y COMUNICACIONES SA (ES), EUROCOPTER SAS (FR), BAE Systems (UK), Immobiliser Central Europe Ltd (CZ), CRANFIELD University (UK), Universidad Politécnica de Valencia (ES), Commissariat à l'Energie Atomique (FR), SWAPCOM (FR)
Wireless Interoperability for Security (WINTSEC)	To overcome the barriers for wireless interoperability across different security agencies, taking into account the constraints of the security services and the legacy base. WINTSEC studies the	Total Cost : € 3,600,000 EU Contribution : € 2,700,000	Starting Date : 02/01/2007 Duration : 24 months	ETHERSTACK (UK), SAGEM (FR), The UNIVERSITY of SURREY (UK), EADS SECURE NETWORKS (FR), ELEKTROBIT LTD (FI), ERICSSON (SE), ROHDE & SCHWARZ (DE), Universität

	<p>deployment of standardised Internetworking layer at Core Network level and Software Defined Radio (SDR) added value for Base Station and Terminal. WINTSEC addresses Information Assurance, elaborates the European “SDR Architectural Framework” and the concepts for the “SDR Certification Environment”, explores the impacts of flexible spectrum management for security applications, and illustrates the interoperability concepts elaborated through tangible proof-of-concept demonstrations.</p>			<p>KARLSRUHE (DE), SELEX COMMUNICATIONS (IT), ACORDE (ES), INDRA SISTEMAS S.A. (ES), SKYSOFT Portugal (PT), RADMOR S.A. (PL), INTRACOM DEFENSE ELECTRONICS (GR), TNO (NL), PRISMTECH (UK), FOI (SE), JRC Joint Research Center / IPSC – ISPRA (EU), GMV (ES), AMPER PROGRAMAS (ES), FEE CTU (CZ)</p>
--	---	--	--	--

* see further information about the projects at http://ec.europa.eu/enterprise/security/articles/article_2007-02-23_en.htm