ceis

March 2015

Toward a new generation of Communication and Information Systems in Europe

A harmonisation under NATO's influence

By Asinetta Serban
In collaboration with Gen. (Ret.) Christian Cosquer
And Axel Dyèvre

σtrategic notes

Intelligence
in decision-making

Les notes stratégiques

Policy Papers – Research Papers

The content of this study does not reflect the official opinion of CEIS. Responsibility for the information and views expressed in the study lies entirely with the author.

CEIS is a strategic consulting firm

Our mission is to assist our clients in defining their strategies and developing their activities in France and abroad. In order to achieve this goal, we combine foresight approach and operational business support with actionable information to support decision-making and action.

.

CEIS' Defence and Security activity gathers sector-specific expertise and involves more than twenty consultants and analysts who have access to an international network of hundreds of experts and organisations.

Based in Brussels, **CEIS - European Office** advises and assists European and national, public and private actors in the development of their European strategies, in particular in the fields of defence & security, transport, energy and maritime affairs. CEIS - European Office also takes part in European research projects in these areas. To carry out all of its missions, the team relies on an extensive European network of contacts, experts and partners.

The **DGA Lab (www.sia-lab.fr)** has been implemented and is led by CEIS, with Sopra Group. This innovative concept of the French Ministry of Defence aims to identify, test, and demonstrate off-the-shelf technological bricks stemming from innovative SMEs and industrial players.

The DGA Lab brings together end-users from the MoD and potential solution providers. It is also a space for brainstorming and discussion aimed at better understanding user needs and requirements as well as ensuring the suitability of the presented solutions.

Contact :
Axel Dyèvre
adyevre@ceis.eu

CEIS
280, boulevard St Germain
F-75007 Paris
+33 1 45 55 00 20

CEIS - European Office
Boulevard Charlemagne, 42
B-1000 Brussels
+32 2 646 70 43

www.ceis.eu

SIA Lab
40, rue d'Oradour-sur-Glâne
F-75015 Paris
+33 1 84 17 82 77

www.sia-lab.fr

Index

Executive Summary

In a dual context of shrinking defence budgets and modernisation and transformation of their national armed forces, European nations have taken forward the development of new Communication and Information Systems (CIS).

The objective of this Strategic Study is to present and compare the main Communication and Information Systems programmes currently undertaken by European countries. Although it covers a large number of countries, this panorama however does not claim to be exhaustive. It primarily serves the purpose of describing these programs and the ways in which they are being developed. The document also highlights the operational and normative influence exerted by the North Atlantic Treaty Organisation (NATO).

Country	CIS	Joint forces	Land	Sea	Air
Germany	FüinfoSysSK	✓	FüinfoSys H[1]	FüinfoSys Lw	FüinfoSys M
Spain	SMCM[2]	✓	BMS (SIMACET)	SMN[3]	SIMCA
France	SIA	✓	SICF	SIC21	SCCOA
Italy	Forza Nec	x	SIACCON SICCONA	LEONARDO	SICCAM
Sweden	SWECCIS	✓		9LV Mark 3E ou 9LV CETRIS	StriC 90 - Airforce 2000
United Kingdom	DII (FD) JOCS + JCS	✓	Bowman ComBAT Falcon	CSS[4]	CCIS[5]

Table 1 *- Overview of CIS in Europe*

[1]http://www.spacewar.com/reports/EADS_DS_Delivers_Army_Command_And_Control_Information_System_To_Franco_German_Brigade_999.html
[2]Sistema de Mando y Control Militar
[3]Sistema de Mando Naval
http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/La_Armada_Espanola.pdf (P176)
[4]Command Support System
[5] Command Control and Information System

The conditions under which these developments take place derive from a triple pre-requisite:

- Rationalise communication and information systems;
- Avoid duplications and save money;
- Acquire technologies to meet both national and operational needs and the requirements of network-centric operations.

This trend is reinforced by the fact that operations are increasingly led in coalition, particularly in the NATO framework. Many European countries have thus adopted an approach summarised by the concept of "NATO-First policy" which identifies the Alliance as the privileged framework of cooperation.

The influence of the NNEC concept (NATO Network-Enabled Capability), its implementation in the national doctrines, the systematisation of coalition-led operations and, as a corollary, the increased requirements for interoperability, have been instrumental in influencing the development of the European Allies' CIS programmes. Further, the Bi-SC AIS (Bi-Strategic Command Automated Information System) programme, launched by NATO for use in NATO operations, has significantly contributed to the harmonisation and convergence of European CIS programmes towards a specific model with precise characteristics: a common Services Oriented Architecture, a fleet of software applications bought off the shelf, and the networking of all actors around a joint approach.

Ensuring interoperability with NATO is also of a paramount importance for the Allied Nations. Yet, the development of their respective CIS also remains largely dependent on both national use and national operational requirements. If the convergence of those CIS programmes towards a single model is justified by the need for interoperability, to date the connection between national CIS and the NATO Bi-SC AIS programme remains unclear. Furthermore, the acquisition of off-the-shelf software and applications, both at national and NATO levels, is also largely reliant on

economic, industrial and political competition. Regarding the software acquired in the framework of NATO, the question of its re-use in a national context is not yet fully resolved.

Modernisation and transformation of the Armed Forces: NCW and NEC

The Challenge of information control

The concept of "Network Centric Warfare" (NCW), pioneered in the United States in the 1990s, describes a way of conducting military operations based on the use of information and network systems. It seeks to gain information advantage enabled by new information and communication technologies. One of the main changes that this doctrine introduced is the new strategic prevailing of information sharing. The NCW indeed aims to:

- Enhance the ability to link the different armies (Land forces, Navy, Air force) and the armies of Allied Nations;
- Retrieve information thanks to UAVs, sensors and satellites;
- Disseminate the information in real time to deployed units to enable them to strike faster and more accurately.

To preserve the dominance of its defence system, the transformation launched by the United States is a process of "continuous and active" development and integration of innovative concepts, doctrines and capabilities designed to improve the efficiency and the interoperability of the armed forces. This approach has been largely taken-up among European countries.

The challenge of accessing and sharing information

The concept of net centricity is not merely limited to the sharing of information among the various branches of the armed forces using modern communication and

information technologies. The benefit of this capability is also that it creates added value by providing all battle space entities with real time access to the information exchange system thus significantly reducing the "fog of war"[6].

This new concept has led to a paradigm shift in how communication and information systems are designed. Many European countries consider those systems as a priority in their endeavours to transform their armed forces and subsequently launched ambitious programmes to modernise their command and control systems.

For example, tactical data exchanges enabling a common operational picture have proven to have a multiplier effect on the armed forces. Real-time blue force tracking and friendly force tracking combined with the automatic transmission of orders have also allowed for a technological revolution that shortens the OODA loop[7] and ultimately accelerates the action on the ground.

The challenge of interoperability

The orientation of European countries towards the modernisation and transformation of their information and communication systems is also motivated by three main principles:

- the necessity to benefit from the adequate technology to participate in coalition-led missions in the context of network-centric operations,
- the ability to connect to Allied Nations' networks,
- the need to streamline and optimise existing systems and avoid costly duplications in a context of budget constraints and limited financial resources.

Network-centric operations render command and control capabilities and, as a corollary, interoperability, essential - particularly in the context of coalition-led operations. NATO's orientation towards increasingly network-centric operations also

[6]http://www.nato-pa.int/default.asp?SHORTCUT=1176
[7]Observe, orient, decide, and act

implies greater cooperation between Allied Nations making interoperability a necessity.

NATO NNEC – Network enabled capability concept

In November 2003, nine NATO Allied Nations (Canada, France, Germany, Italy, the Netherlands, Norway, Spain, the United Kingdom and the United States) signed an agreement to fund a feasibility study on a NATO Network-enabled Capability (NNEC). The study was conducted by the NATO C3 Agency (NC3A, which has since become NCIA).

NATO NNEC concept is defined as the ability to collect, process, and disseminate an uninterrupted flow of information in order to gain operational advantage through information superiority. NNEC can thus be considered as the ability to effectively federate capabilities in coalition operations, by addressing not only networks and systems, but also the information to be shared, the process employed to handle it, and the policy and doctrine that allow the sharing of information and services[8].

This vision has also implied that the acquisition of a capacity for a specific force (e.g. the Air Force) must take into account, from the beginning, its necessary integration with other branches, in a joint forces manner, in order to not only avoid duplication of acquisitions but also to allow the realisation of a common operational picture.

Moreover, the NNEC is more services-oriented (i.e. IT services) rather than technology-oriented. The concept also implies a paradigm shift by focusing on "Services Oriented Architecture" (SOA) and on the acquisition and integration of services using an incremental and modular approach to avoid duplications and to leverage existing services. The NNEC also relies more heavily on commercial off-the-self products and software. Finally, the NNEC concept advocates the adoption of common norms and standards to promote interoperability among Allies.

[8]http://www.act.nato.int/nnec

The impact of NATO on the development of Allied Nations' CIS

Since military interventions are increasingly taking place in coalition-led missions and military budgets are continuously more constrained, many Allied Nations are turning more and more towards NATO as a normative organisation.

NATO's normative influence

This normative function exercised by the Alliance was widely emphasized at the Chicago Summit in 2012: "*NATO has a role to play through the* ***harmonisation of national and multinational capability requirements***".

The establishment of norms, standards and common protocols - such as STANAG - led the Allied Nations to harmonise their own systems and align them with the NATO model, in order to address the need for interoperability. The development of Information Exchange Gateways (IEG) to converge to a more comprehensive level of interoperability also demonstrates NATO's increasing influence on the development of national concepts and capabilities in the field of information systems.

The appropriation of the NEC concept by European Allies

The Allied Nations' endeavours to pursue battlefield digitisation combined with NATO NNEC initiative have led to a doctrinal evolution: from "need to know" to "need to share", which in turn also steered the capabilities acquisition process towards a new direction.

Country	Concept	Documents
Germany	Vernetzte Operationsführung - NetOpFuBw	Teilkonzeption Vernetzte Operationsführung, BMVg, Novembre 2006
Spain	Información en red	Concepto de información en Red (NEC) del JEMAD, juillet 2007
France	Numérisation de l'espace de bataille (NEB)	Concept exploratoire des opérations en réseaux, CICDE, 2007
Italy	Net-centric	Il Concetto Strategico del Capo di Stato Maggiore della Difesa, 2005
Sweden	Network-based Defence	Rekkedal, N.M. Vad är militärteori idag. Krigsvetenskaplig årsbok. 2002. Stockholm. Försvarshögskolan, 2003
United Kingdom	Network-enabled capability (NEC)	Network enabled capability, JSP 777 EDN 1

***Table 2** - Overview of NEC doctrines*

Operational and economic streamlining

The new capabilities acquisition strategy is driven by the need to rationalise the armed forces' communication and information systems in a context of spending cuts. The approach also aims at preventing technological gaps and system obsolescence by purchasing commercial off-the-shelf products. As such, it draws more heavily from the civilian market (dual-use, shorter time-to-market products).

This new approach is also reflected by:

- The adoption of shorter development cycles;
- The adoption of an incremental approach;
- The introduction of the spiral model;
- The focus on user requirements.

This approach has also been largely driven by economic and budget constraints. Some Allied Nations have chosen to develop common capabilities through the NATO Smart Defence[9] initiative. However, in this economic context, NATO programmes - funded by contributions from Allied Nations to NATO's Security Investment Programme (NSIP) - are also subjected to questioning, especially when it comes to national use and/or reuse of software systems developed in the framework of NATO[10]. These programmes are also subjected to strong political and industrial competition, each Allied Nation pushing for its own national champions.

[9] http://www.nato.int/cps/fr/natolive/78125.htm

[10] "Conditions for Allied Nations to use NATO software", Strategic Note CEIS, June 2014, http://ceis.eu/en/european-office/news/strategic-study-conditions-allied-nations-use-nato-software

Technologies to meet the challenge of information control

These new technological needs must meet the requirements arising from battlefield digitisation and are thus common to most European countries.

These technologies should help accelerate the decision making process and shorten the OODA loop by enabling:

- Accelerated flow of information;
- Shortened processing times;
- Collaborative work.

These capabilities should thus allow for the acquisition, processing, and sharing of information while complying with the need for information fluidity and rapidity, and security of exchanges. These capabilities are as follows:

- SOA (Service Oriented Architecture);
- Communication satellites (data link communication)
- Recognition systems;
- Global positioning system;
- Geographical and spatial representation systems;
- Visualisation interfaces (3D, simulation, virtualisation);
- Messaging and communication systems;
- Information storage (cloud);
- Information security (technologies to avoid intrusions and interceptions, technologies enabling encryption, traceability).

Major CIS programmes in Europe

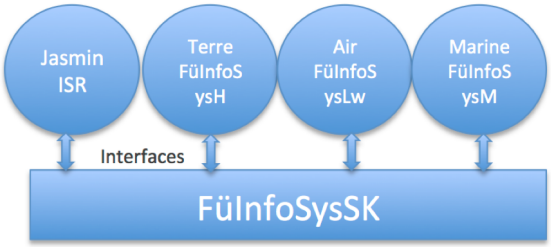
GERMANY

FuInfoSysSK is considered as the German Forces' most important IT system project. It forms an integral part of the German Forces' network-centric operations concept (*NetOpFuBw*) both in the context of national defence and in connection with international assignments, where it will ensure network-centric operations between different services of the armed forces[11].

This command and control information system has been developed incrementally: new features and new components on the system are added gradually as soon as they reach maturity. This incremental method will allow users to use the system and its features as soon as they are ready.

The medium-term goal of the FuInfoSysSK project is to harmonise the Forces' command and control information systems with the objective to establish end-to-end interoperability. The objective is to obtain a single unified system, accessible by all users - from defence ministry headquarters to troops serving overseas - that enables mission-relevant data to be exchanged between armed services (on joint operations) and between German forces and the systems operated by NATO, the EU and Allied Partners (in operations led in coalition).

This will create a comprehensive, seamless information resource for use throughout all areas of the organisation and all levels of command[12].

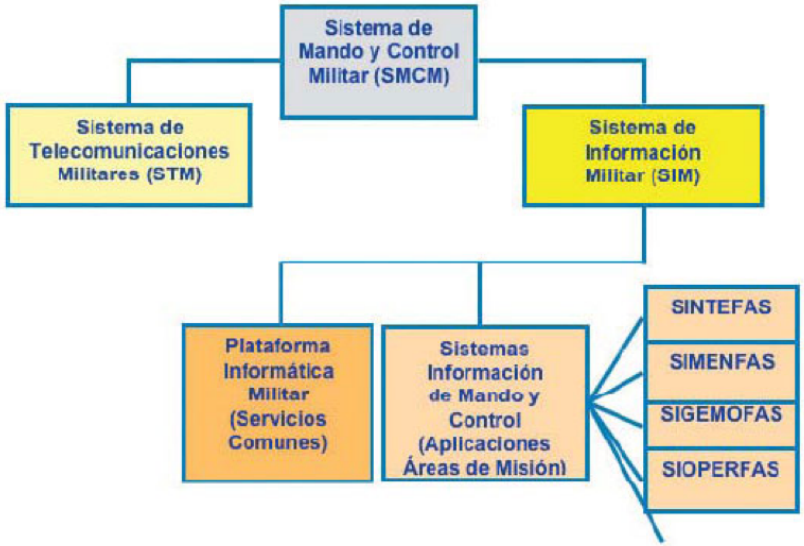


[11]http://www.asdnews.com/news-14199/ESG_Awarded_Contract_for_C2_Information_System__FuInfoSysSK_.htm
[12]http://www.afcea.org/events/augusta/13/documents/130912.pdf

SPAIN

Sistema de Mando Militar y Control (SMCM) is the command and control system of the General Staff of the Spanish Forces. It consists of two parts: the Military Communications System (*Sistema de telecomunicaciones Militares* - STM) and the Military Information System (*Sistema de Información Militar* - SIM).

The SMCM forms a set incorporating features and tools for the planning and conduct of operations. It is structured in several stages: upper, middle and lower. The system allows the connection between these stages and the different levels responsible for conducting operations: strategic, operational and tactical[13].



Source : Revista Dintel n°10, May 2007

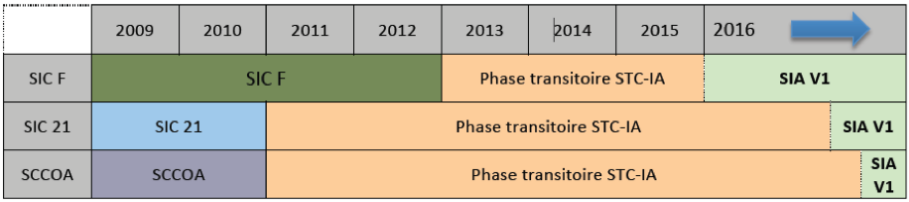
[13]http://www.belt.es/expertos/HOME2_experto.asp?id=3670

FRANCE

The Information System of the Armed Forces (**Système d'Information des Armées - SIA**) is a programme launched in 2010, which aims at replacing gradually - between 2012 and 2017 – the CIS of all forces. Most CIS used within the different branches of the forces had been scheduled to expire between 2015 and 2020, with no identified successor. The 2008 French White Paper on National Defence and Security already highlighted the efforts needed to streamline costs and resources. The constrained budget of the 2014 Military Programming Law confirmed this trend and the need for rationalisation.

The growing involvement of information systems in the action of the French Armed forces stressed a critical need for the General Staff of the Armed Forces: the rationalisation of the CIS landscape. The SIA aims to provide a common CIS to each branch of the armed forces. Users, policy makers, sensors and weapons systems will all be connected.

The SIA will eventually replace 17 existing information systems. This requires the establishment of a coherent system, agile, and modular. The convergence of all existing systems will go through a transitional phase during which the various systems will be transferred to a joint common technical base (STC-IA).



Source : Strategic Note, CEIS

The development of the SIA began in 2012. The components – constituting the SIA V1 - will gradually be integrated into the architecture of the SIA. The SIA will be delivered in 2017 and will evolve through 2030. In 2014, the first modules were delivered in order to be integrated into the structure of the SIA.

The SIA will allow the digitisation of battle-space operations and ensure the overall functioning of CIS. It will aim at providing the strategic and operational levels with means to:

- control information (passing of information up from the lowest levels, synthesis of tactical situations, sending of orders, collaborative work);
- manage and exploit the gathered information and intelligence (processing requests for information);
- monitor logistics.

The SIA will have to ensure the operability of these different elements together. But it will also have to ensure the interoperability with other nations' networks as well as with NATO and the EU.

The SIA aims to network all users together and structure the chain of command, from strategic to operational level.

ITALY

Forza NEC programme was launched to carry out the concept of Network Enabled Capability. This project has benefited from a spiral development between 2007 and 2031. The total cost of this project is estimated at 22 billion euros.

Forza NEC programme aims to digitise middle level brigades of the Italian army. The first brigade should be made operational in 2018[14].

Forza NEC aims to integrate, under a single and comprehensive umbrella, other systems and programmes such as: the Army Command and Control System (*Sistema di Comando e Controllo dello Stato Maggiore dell'Esercito* - SIACCON); the Command, Control and Navigation System for the digitisation of combat platforms (*Sistema di Comando, Controllo e Navigazione* - SICCONA); the Future Soldier (*Soldato Futuro*) programme; the Blue Force Situational Awareness (BFSA), a system to identify friendly units; the Software Defined Radio (SDR), a new type of communication equipment[15].

The programme will be interfaced with the C2 of the General Staff of the Armed Forces. If the Forza NEC programme should ensure interoperability and the connection between land and naval C2 through a gateway, it seems however that there will not be any migration of all C2 systems on a common platform.

[14]http://www.spindlerconsult.fr/index.php?option=com_content&task=view&id=44&Itemid=41
[15]http://www.iai.it/sites/default/files/iairp_05.pdf

SWEDEN

SWECCIS is the information and communication system of the Swedish Armed Forces for tactical and operational levels. It is used for the planning and the conduct of operations. The SWECCIS system is certified to handle classified information up to “Secret” level.

The system includes a number of features including:

- a mapping system,
- a geographic information system,
- logistical support system,
- an information exchange portal.

SWECCIS was used in the European operation Atalanta[16]. It has also been used in Afghanistan and was connected to the Afghan Mission Network (AMN) in 2013[17].

The ROLF-2010 System is a C2 project that began in 1995 and was embodied in a first prototype, ROLF MARK I. The project then led to a second version Mark II, which was a first version of the "future command post" for Swedish armies. MARK II has been used in the Swedish National Defence College since 1998, particularly in the context of exercises and experiments. Another version, MARK III is currently being developed[18].

[16]http://www.army-technology.com/contractors/data_management/systematic/press7.html
[17]http://www.ncia.nato.int/news/Pages/130313---Sweden---AMN.aspx
[18]Berndt Brehmer, « Rolf 2010: A Swedish Command Post of the Future », in Malcom James Cook, Jan Noyes et Yvonne Masakowski, Decision Making in Complex Environments, Ashgate, 2007, p 129

UNITED KINGDOM

The Joint Operational Command System (JOCS) was commissioned in 1999. This system was designed to exchange information between the Permanent Headquarters (PJHQ), the Joint Forces Headquarters (JFHQ) and the Joint Rapid Reaction Forces (JRRF). This system, combined with ATacCS, has set the standard for future applications for battlefield information system to achieve the digitisation of the battle space of the 21st century[19].

The DII system (FD) - Defence Information Infrastructure System – aims at replacing JOCS, though JOCS will remain in use in Afghanistan[20]. The DII System is a restricted "Secret" and above network. It is used by all branches of the British armed forces (Army, Royal Navy, Royal Air Force) and its objective is to streamline all the CIS previously existing in the UK. This system was developed incrementally by the ATLAS Consortium[21] and will eventually connect 300,000 users in nearly 2000 location sites. The project began in 2005 and the last increment was implemented in the summer of 2014.

[19]http://www.armedforces.co.uk/army/listings/l0105.html
[20]http://www.army.mod.uk/signals/25247.aspx
[21]http://www.computerweekly.com/news/1280091904/MoD-awards-890m-DII-contract-to-Atlas-consortium

National programmes converging gradually towards NATO's Bi-SC AIS programme

NATO has launched a development programme for an information and communication system to align with its NNEC concept. This programme called **Bi-Strategic Command Automated Information System (Bi-SC AIS)**[22] is intended to harmonise the communication and information systems of the Alliance and to support interoperability efforts within the Alliance.

Bi-SC AIS is one of the most important programmes funded under NATO's common fund. The launching of this programme is the result of the Washington Summit in 1999. Bi-SC AIS has been strengthened by the Prague Summit in 2002 and designated as a critical capacity and priority respectively during the NATO summits in Lisbon in 2010 and Chicago in 2012[23].

Programme Overview

The objective of Bi-SC AIS is to provide NATO commands (Strategic Command, Operational Command and Component Command) with integrated core applications (common to all users) and functional services (specific to staff functions) for command and control[24] both in static and dynamic phases of NATO operations.

The logic behind the development of the Bi-SC AIS programme is twofold: first is the greater need for interoperability and, second is the economic and industrial decision to integrate commercial off-the-shelf software.

[22]http://www.act.nato.int/article-16a
[23]http://www.nato.int/cps/en/natolive/opinions_82646.htm
[24]https://www.ncia.nato.int/Our-Work/Pages/Airc2/Concept--Capabilities.aspx

The objective is to create a ready-to-use architecture on which Allied Nations can plug onto their own systems[25].

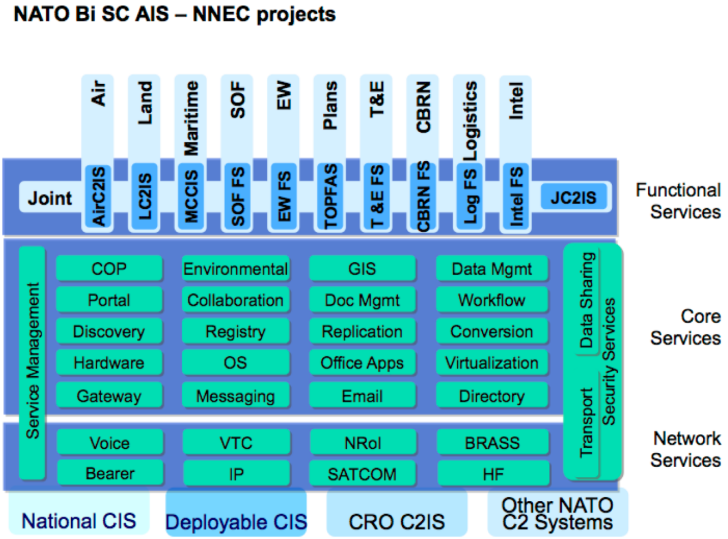
The Bi-SC AIS programme is managed by the NATO Information and Communication Agency (NCIA) and consists of a hundred projects, funded by Capability Packages, for a total budget of about 1 billion euros.

The Bi -SC AIS logic: core and functional services

The range of functional services to support the operational commanders includes command and control capabilities (C2) for land, air and naval forces. Functional services also include intelligence and logistics[26].

The diagram below shows an overview of the Bi-SC AIS project:

Source: Atlantic Council of Canada



[25]Gordon Adams, Guy Ben-Ari, Transforming European Militaries: Coalition Operations and the Technology Gap, Routledge, 2006 p 87

[26]http://www.defensa.gob.es/Galerias/info/servicios/concursos/2012/01/LOG-FAS-Industry-Day-10-02.pdf

ceis

Société Anonyme au capital de 150 510 €
SIREN : 414 881 821 – APE : 7022 Z
Tour Montparnasse - 33, avenue du Maine - BP 36
75 755 Paris Cedex 15
Tél. +33 1 45 55 00 20 / Fax +33 1 45 55 00 60 / **contact@ceis.eu**

Recent publications

Download on www.sia-lab.fr or www.ceis.eu
These Strategic Notes are also available in French

Intelligence, the Human Factor and Cognitive Biases - June 2015

SIA Lab : Fostering Defence Innovation and Transformation. Overview of two years in activity – June. 2015

MRO of military helicopter engines: Innovative solutions for a critical asset in military operations– June 2015

Towards a new generation of Communication and Information Systems in Europe – April 2015

Aerospace MRO: A key issue of capability-based planning of the Armed Forces – February 2015

Conditions for Allied Nations to use NATO software – June 2014

A new approach to Terrorism - A better understanding of profiles of terrorist groups and their members – May 2013

ceis