Assembly of Western European Union
The Interparliamentary European Security and Defence Assembly

DOCUMENT A/1899 **14 June 2005**

FIFTY-FIRST SESSION

Network-centric operations: European capabilities

REPORT

submitted on behalf of the Defence Committee
by Klaus Werner Jonas, Rapporteur (Germany, Socialist Group)

ASSEMBLY OF WESTERN EUROPEAN UNION
THE INTERPARLIAMENTARY EUROPEAN SECURITY AND DEFENCE ASSEMBLY
43, avenue du Président-Wilson, 75775 Paris Cedex 16
Tel. 01.53.67.22.00 – Fax: 01.53.67.22.01
E-mail: info@assembly.weu.int
Internet: http://assembly.weu.int

Document A/1899 **14 June 2005**

Network-centric operations: European capabilities

REPORT[1]

submitted on behalf of the Defence Committee
by Klaus Werner Jonas, Rapporteur (Germany, Socialist Group)

TABLE OF CONTENTS

[1] Adopted unanimously by the Committee on 12 May 2005.

RECOMMENDATION 762[1]

on network-centric operations: European capabilities

The Assembly,

(i) Considering that the evolution of European defence is closely linked to development and enhancement of the national capabilities of the European states that are WEU, NATO and EU members;

(ii) Stressing the reforms and efforts to adapt undertaken by those states since the end of the cold war so as to be in a position to respond to the new security and defence challenges in Europe and worldwide;

(iii) Noting the progress achieved in the area of the EU's European Security and Defence Policy since the decisions taken by the European Council in Cologne and Helsinki in 1999, and welcoming in particular:

- the setting up of structures for political and military decision-making and for the conduct of operations;
- the achievement of the 1999 Headline Goal and the fact that a start has been made on the implementation of the Headline Goal 2010;
- the launch and revision of the European Capability Action Plan (ECAP);
- the creation of the European Defence Agency (EDA);
- the formation of battlegroups;
- the European Union operations in Africa (Artemis) in 2003 and in Bosnia and Herzegovina (Althea) in 2004;

(iv) Noting the reforms undertaken by NATO since 1990 the better to respond to post-cold war crises and conflicts and strengthen transatlantic ties;

(v) Concerned by the growing gulf between the military doctrines and defence-related technologies of Europe and the United States;

(vi) Stressing the need for European forces to maintain and increase their level of interoperability with US forces, necessary for NATO or coalition operations;

(vii) Emphasising the important role, in this context, of new information and communications technology (ICT) as applied to defence;

(viii) Considering that the concept of network-centric operations arising out of this development presents the defence capabilities of European nations with both an opportunity and a major challenge, at national level as in multinational institutional frameworks or in coalitions of the willing;

(ix) Taking the view that setting up national network-centric capabilities is a first essential step in that development process and in the transformation of the armed forces;

(x) Considering that European nations must work together on developing and implementing a common concept to increase their interoperability and the effectiveness of action taken under the ESDP or in NATO;

(xi) Considering that any European network-centric capability must be based from the outset on a process of identifying operational need and on the current state of play in European countries of RT&D (research, technology and development) in the relevant field;

1. Adopted by the Assembly on 14 June 2005 at the 3rd sitting.

(xii) Highlighting the significant contribution, past and present, made by WEAG (the Western European Armaments Group) and WEAO (the Western European Armaments Organisation) to the success of that process;

(xiii) Expecting the European Defence Agency, having inherited WEAG *acquis*, to be in a position to give more active encouragement to work on network-centric concepts in relation to operational command and control (C2) procedures and on associated communications and UAV technology;

(xiv) Taking the view that the gap, in terms of technology, doctrine and above all assets, between European and American forces is not conducive to the transposition of the US model to Europe;

(xv) Stressing the need to maintain a sufficient degree of European autonomy in network-centric capabilities to avoid increasing Europe's dependence on US concepts and technology, while at the same time seeking to reinforce the degree of transatlantic interoperability in that sphere;

(xvi) Considering that a substantial financial investment must be made in developing the technologies essential to the provision of national and European C4ISTAR[2] capabilities;

(xvii) Considering that resources must also be allocated proportionately to recruitment, training and to retaining within the armed forces the staff who operate, make use of and depend on those systems in the theatre of operations;

(xviii) Taking the view that the development of network-centric capabilities in Europe also depends on the general level of education, research and technological development in European societies, an area that falls within the field of action and responsibility of national parliaments,

RECOMMENDS THAT THE COUNCIL INVITE THE WEU MEMBER STATES AS MEMBERS OF THE EU TO:

1. Maintain and as far as possible increase defence RT&D investment, in particular in C4ISTAR technology;

2. Deepen the regular exchange of information and experience, bilaterally, in NATO and in the EU, and also through WEAO, on the state of play and technological development in regard to national projects on network-centric capabilities;

3. Cooperate with a view to developing and implementing concepts for shared or interoperable network-centric operations and capabilities, so as to maintain operational cohesion and coherency in multinational or coalition-based operations;

4. Seek, as a matter of priority, European solutions, technologies and products, so as to strengthen the defence industrial and technology base, both national and European, without which there will not be European autonomy in this sphere;

5. Cooperate with the United States at bilateral and multilateral levels in regard to network-centric capabilities and operations, so as to benefit from its experience and technology with a view to maintaining and strengthening transatlantic ties;

6. Seek, within the framework of transatlantic cooperation, to maintain a balance between the need for interoperability and the political requirement of strategic and operational autonomy that is the hallmark of the ESDP;

7. Engage more actively in the Alliance framework and in the EU, in particular through ECAP and EDA project groups, with the armed forces transformation process, leading to a shared European vision of the goals to be attained and the stages to be completed towards them;

8. Make the European Defence Agency (EDA) the framework for the definition of European network-centric technology required for ESDP missions and for interoperability with NATO, and provide the Agency with adequate funds to launch R&T programmes in that area;

[2] Command, Control, Communications, Computers, Intelligence, Surveillance Target Acquisition and Reconnaissance.

9. Support armed forces transformation with adequate spending at both national and multilateral level, paying particular attention to human resource management;

10. Keep the Assembly better informed about WEAO R&T work on C4ISTAR capabilities and activities undertaken by the EDA in conjunction with the Research Cell or based on work done by the latter.

EXPLANATORY MEMORANDUM

submitted by Klaus Werner Jonas, Rapporteur (Germany, Socialist Group)

I. Introduction

1. Network-centric warfare, network-centric capabilities and network-centric operations have become an integral part of the reforms of the armed forces now being introduced in many Atlantic Alliance and EU member states. Known as "transformation", the process concerns doctrines, force structures and weapons systems alike and is evolutionary rather than revolutionary in character. It is a process entered upon freely by those involved – from a known starting point and with clear short- and medium-term aims – but with little idea of its longer-term effects and where it might ultimately lead.

2. The key determinant in transformation is information, in the sense of strategic, operational and tactical intelligence. The widespread use of new Information Communication Technology (ICT) – its best-known practical application being the "network of networks", the Internet – is intended to make possible better exploitation and faster dissemination of intelligence in support of military operations so that political and military decision-making is more authoritative and practical outcomes more effective. Hence the description of these new forms of military action as "effects-based".

3. This is no mere passing "fad". Nor is it a straightforward, wholesale transposition of ICT and its various applications – already tried and tested in civilian walks of life such as commerce and public administration – to the defence sector. It represents an enormous challenge, with far-reaching consequences at military, industrial and technological levels as well as in the political and economic spheres. Network-centric forces are meant to be more coherent, more capable of joint working and more efficient because they are technologically superior. That superiority derives not only from the fact that better resources are available to them but also because they make better use of those resources.

4. Network-centric warfare has already moved on from the experimental stage. Its practical application began in March-April 2003 with "Operation Iraqi Freedom" led by the United States and the United Kingdom against Iraq. This field experiment, albeit undertaken against an immobilised adversary without adequate means of retaliation, meant that lessons were learned on a number of counts in regard to the implementation of the new concepts. It also provided an opportunity for testing the application of methods, originally developed in a national framework, in operations undertaken in a coalition.

5. It is on this last aspect that we propose to focus. For although transformation begins life first and foremost as a national undertaking, NATO or EU-led military operations are increasingly proving to be variable geometry coalitions. Some countries can cover all or a large part of the spectrum of requirements, others contribute highly specialised capabilities, numerically of lesser significance but which may be of considerable added value. Hence the importance of conceptualising, developing and applying joint or shared methods and standards to avoid the emergence of technology or operational "gaps" opening up between European forces.

6. While differences are inevitable, they need as far as possible to be ironed out, to maintain the coherence and efficiency of the whole. This much is clear already from combat operations involving a combination of American and European forces and assets. From a military point of view complementarity is an advantage, but may be experienced politically as giving rise to subordination or the loss of joint decision-making power. The capability to undertake network-centric operations is thus becoming as much a criterion for strategic autonomy as the defence industrial and technology base (DITB) that underpins it.

7. Transformation, whether national or achieved jointly through NATO and the EU, is now, in 2005, a strategic consideration, both for maintaining and seeking a better balance in regard to the transatlantic ties on which security and defence cooperation in both organisations is based and in order to enable European nations to deal more effectively with the challenges and threats of the 21st century. Technology is not an end in itself but rather a means of achieving that particular political objective.

Transformation at national level will be completely successful only if it extends to the European level. Alternative approaches are not ruled out but the outcome, at the end of the day, has to be a Europe "United in Diversity[3]" and able to act effectively in military terms.

II. Network-centric operations concepts and realities

8. Although the philosophies and objectives underlying their development vary from country to country, the network-centric capabilities that provide support in warfare and to other military operations have in common the crucial role they reserve for information. The gathering, exploitation and dissemination of intelligence are perhaps the most sensitive areas. Intelligence management is now no longer regarded as taking place in a closed arena but one open first to the different services whose forces are engaged in a particular operation, then extending outwards to allies and coalition partners, where it is shared between them where feasible, on "a need to know basis". Thus two indissociable aspects of the "network-centric" concept are its multi-service and, within certain limits, multinational character.

9. These processes are also now practically and economically feasible, thanks to a growing use of the information management technologies and systems, especially computerised networks, now available in civilian walks of life. The basic assumption is that the better integrated these technologies and their effects are into forces' structures, the greater will be their military effectiveness and consequently their strategic, operational and tactical superiority over potential adversaries. Information becomes a power multiplier, in the same way as projection capability or unrestricted access to air and extra-atmospheric space.

1. Information superiority

10. The network-centric concept is directly linked to the economic, technological and social developments advanced societies have undergone in the last twenty years. The emergence of information as the driving force behind the process has also had repercussions on military doctrines, particularly in the United States, currently engaged in its "Revolution in Military Affairs" (RAM)[4]. A simple definition of this concept would be the networking of command and control and weapons systems through new Information and Communications Technology (ICT). This would provide a continuous real-time link from political and military decision makers right down to the soldiers in the theatre of operations. All the different types of action (air, land, sea and space) would be covered. Traditional weapons systems – armoured vehicles, fighter aircraft and ships, for example – are connected up with one another at all times and exchange information as operational and tactical needs demand.

11. Increased computerisation and automation means that traditional platforms can be linked up to "future" systems such as UAVs and robots, even in combat operations, and may sometimes be used to replace them. This concept is based on a modular approach combining different assets adapted to the effect it is sought to produce – the opponent is seen as a whole, comprising networked subsystems that have to be isolated from one another, damaged and destroyed. These are what are described as "effects-based" operations. In such a concept, information plays a leading part. ICTs are integrated and applied intensively across the fighting force. Data gathering, input, analysis and interpretation and dissemination make it possible to achieve a common perception of a situation, thus providing essential command support, at the political/strategic and the tactical/operational levels. Spaced-based communication and navigation are of special relevance in network-centric architectures.

[3] Treaty establishing a Constitution for Europe: Part I, Title 1 "Definition of the Objectives of the Union", Article I-8, The symbols of the Union: European Union, 2004, http://europa.eu.int.

[4] "Arising from fundamental changes in American society and business, military operations increasingly will capitalise on the advances and advantages of information technology"; "Network-Centric Warfare: Its origin and future", Vice Admiral Arthur K. Cebrowski et John J. Garska, *Proceedings magazine*, United States Naval Institute, January 1998; www.usni.org. From 2001-2005, Vice-Admiral Cebrowski (Reserve Officer) was responsible for the transformation of the US armed forces (Director, Force Transformation) directly answerable to the US Secretary of State for Defense (Donald Rumsfeld). John Garska is Deputy Director, Concepts and Operations, Office of Force Transformation; www.oft.osd.mil.

(a) Information gathering and dissemination

12. The widest and most comprehensive information provided in the shortest possible time, or in real time if possible, is the key to a firm overall understanding of the situation in a theatre of military operations. That information must include data both about the adversary and the environment in which the latter moves as well as on the totality of national and allied assets engaged, thus making it possible, via the strategic and operational chain of command that has been set up, to concentrate the main force of the attack against the opponent's weakest points, while responding rapidly to the way the latter reacts. The process is described as follows, in an article published by the United States Naval Institute in its "Proceedings Magazine" in 1998, which is still today one of the seminal reference works on the topic:

> "(1) The force achieves information superiority, having a dramatically better awareness or understanding of the battle space rather than simply mere raw data. Technologically, this will require excellent sensors, fast and powerful networks, display technology, and sophisticated modelling and simulation capabilities.
>
> (2) Forces acting with speed, precision and reach achieve the massing of effects versus the massing of forces.
>
> (3) The results that follow are the rapid foreclosure of enemy courses of action and the shock of closely coupled events. This disrupts the enemy's strategy and, it is hoped, stops something before it starts. One of the strengths of network-centric warfare is its potential, within limits, to offset a disadvantage in numbers, technology, or position[5]".

13. The three essential phases in the successful functioning of a network-centric system are information collection, exploitation and dissemination. Twenty years ago, information was based fundamentally on written documents, maps and photos from various sources, particularly aerial photos. High resolution satellite images and electronic information (signals intelligence or SIGINT) played an important part in the conduct of operations undertaken against Iraq by the international coalition in the 1991 Gulf War. In operation "Allied Force" against the Federal Republic of Yugoslavia during the Kosovo crisis of March-June 1999, video imagery gathered by observation UAVs was used to direct bombing raids. Since then, in Afghanistan and Iraq, information has been expanded and enhanced by combining a whole range of media: text, high resolution photographic and video imagery, sound and computerised data.

14. In addition to this wealth of diverse information, there has been a significant development in ways of processing it. It is now handled with a view to shared, rather than compartmentalised use by all the various components of an operation, at the strategic, operational and tactical levels, thus reinforcing the trend, already underway since the 1991 Gulf war, towards joint action. Information superiority, including denying the same degree of control to the adversary, is becoming almost synonymous with victory. In a coalition situation, a country that knows how and is able to handle every aspect of this area in detail is *de facto* the leader. It alone is in a position to have a full Common Operational Picture (COP) and the ability to concentrate combat effort on the enemy's areas of vulnerability by making use of the full range of available national and allied resources.

15. Networking of information goes hand in hand with the networking of platforms. The one best placed for action is used, whether it is land, air or sea-based. During "Enduring Freedom" in Afghanistan, in 2001, US forces linked sensors and shooters, satellites and unpiloted armed aerial vehicles and special mounted forces armed with recent high-tech Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) equipment in this way[6]. As well as the improvement in

[5] "Network-Centric Warfare: Its origin and future", Vice-Admiral Arthur K. Cebrowski et John J. Garska, *Proceedings magazine*, United States Naval Institute, January 1998 ; www.usni.org.

[6] "Special Operations Forces become network-centric – Afghanistan proves the worth of total battlefield awareness"; Robert K. Ackerman, *SIGNAL Magazine*, March 2003; AFCEA (Armed Forces Communications and Electronics Association); www.afcea.org. AFCEA is an international body, founded in the United States in 1946, "dedicated to supporting global security by providing an ethical environment that encourages a close cooperative relationship among civil government agencies, the military and industry".

quality of the information gathered in space, from the air and on land, it could be distributed quickly, thus considerably reducing response times – from hours to only a few minutes[7].

16. Thus seamless, real-time integrated and verified information led to increased accuracy of fire, in spite of difficult geographic and climatic conditions. In the war against Iraq, in 2003, the lessons learned in Afghanistan helped dispel even further the "fog of war", and at the same time, to an extent, deprived the Iraqi forces of their advantage of knowledge of the terrain and their ability to exploit local topographical and meteorological conditions (heat, sandstorms)[8]. In both operations, information-sharing between the various levels of command and its joint dissemination to all services played a crucial part in their successful outcome and in validating a network-centric concept of the battle field.

17. Even so, information superiority is not in itself a decisive factor. It is how the available data is managed and used that determines the outcome. The fact that in both of these cases, the opponents, Afghans or Iraqis, unable in this domain either to defend themselves or to attack, were nevertheless at times able to counter-attack or avoid being neutralised, shows that network-centric warfare, despite its proven record, still has its weak points.

(b) Effects-based operations (EBOs)

18. The first phase of a network-centric operation is information control. Once the sensors have been placed and connected, the huge mass of information available in different formats needs processing in order to build up a Common Operational Picture (COP) (or CROP – Common Relevant Operational Picture) and then identify targets. These are defined in terms of strategic, operational or tactical priorities and divided into "grids" to be dealt with depending on the desired effect, with the aim right from the very first strikes of reducing the opponent to a position from which recovery is impossible.

19. The EBO concept does not only apply to the military aspects of an operation: it also includes, for example, the political, economic, psychological aspects. The aim is, on the one hand, to downgrade the adversary's military potential, or even to eliminate the leadership (as in the war against Iraq) while at the same time trying to avoid an excessive amount of material damage and loss of life, so as to facilitate the post-conflict stabilisation and reconstruction phase. To that end, interaction between military and civilian players (non-governmental or humanitarian organisations for example) has to be built into the equation from the start of operations.

20. This does not rule out large-scale action involving massive use of force in strategic locations, as in the bombing of Baghdad on 21-22 March 2003 or the successive attacks on Iraqi Republican Guard units or installations. Effects-based operations depend on the quality of information and the speed at which it can be disseminated and presuppose joint and coalition-based action, as necessary, and coordination between other national and international players ("friendly" armed resistance groups, international organisations and NGOs) in the theatre of operations, as well as an arsenal of (so-called) "precision" weapons to disable or destroy the opponent's nerve-centres to a point short of total annihilation and reduce to a minimum the virtually inevitable collateral damage involved.

21. Guided weapons thus represented two thirds of the airborne assets used (68% of the total)[9]. Added to this was the combined effect of coordinated strikes from air, land and sea, so as to deal more quickly and to maximum effect with large numbers of targets simultaneously. Effects-based operations

[7] Examples of such interaction, occurring prior to the network-centric war on Iraq, can be found in Assembly Document 1783 adopted on 3 June 2002: "European military capabilities in the context of the fight against international terrorism", submitted on behalf of the Defence Committee by John Wilkinson, Rapporteur (United Kingdom, Federated Group) paragraphs 33-45;
http://www.assembly-weu.org/en/documents/sessions_ordinaires/rpt/2002/1783.pdf .

[8] "Iraq war operations validate hotly debated theories – Investments and innovations pay off as new capabilities give a glimpse of the future"; Robert K. Ackerman, *SIGNAL Magazine*, July 2003; AFCEA (Armed Forces Communications and Electronics Association); www.afcea.org

[9] "Operation Iraqi Freedom – By The Numbers"; United States Central Command Air Forces (CENTAF), Assessment and Analysis Division, 30 April 2003; www.centaf.af.mil

depend on this kind of synchronisation and on the ability to keep up unremitting pressure on the adversary without ever giving ground. Strikes are pursued relentlessly, round the clock, in all weathers, to prevent the enemy from gaining the initiative, with the avowed aim of demoralising him and forcing surrender. Otherwise, in the event of protracted resistance or his being forced to break cover, elimination is virtually certain.

22. Also characteristic of effects-based operations is the ability to react and adapt quickly to developments on the battlefield – through a manoeuvre known as auto-synchronisation. The various players, who are in principle autonomous, with their own chain of command and differing operational and material specificities, interact at the various strategic, operational and tactical levels to produce coordinated, coherent "bottom-up" action. Information is no longer the privilege of decision-makers at the top but is accessible at every level. It is in constant circulation and constantly being added to. The fact of its being networked and disseminated rapidly leads to continual redefinition of the aims in the field, demanding high levels of responsiveness from the command structure.

2. C4ISR capabilities

(Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance)

23. Information control and effects-based operations are both key concepts in network-centric operations, which have already been implemented in Afghanistan and Iraq and are central to US and Allied armed forces transformation. However, for them to work, a suitable, dedicated decision-making and material infrastructure is needed. The latter hinges on C4ISR, a group of procedures and modular systems that can be used either as a whole or piecemeal, without reduction in overall effectiveness. The power to access and use such capabilities to the full is a central aspect of the information control process, and for guaranteeing information superiority in this sphere.

(a) Command, Control, Communications, Computers (C4): the core of the system

24. The move, from the traditional C3I (Command, Control, Communications and Intelligence) combination, designed, implemented and developed in the member states of the Atlantic Alliance during the cold-war period, to the C4ISR concept, took place in the last decade of the 20th century. This was due mainly to three factors: the growing number of external interventions, the need for greater coordination between services and across nations and technical developments, particularly in the field of the new Information Communications Technology (ICT).

25. The war in Iraq in 1991 provided an illustration of these three trends which became more marked throughout the 1990s, in a long sequence of military interventions of a "humanitarian" nature, culminating in the NATO operation in Kosovo, from March to June 1999. The requirements for force and power projection over distances of hundreds, even thousands of kilometres from national bases and the deployment of personnel and assets, the recourse to multinational coalitions between countries within that Alliance and, additionally, the involvement and inclusion of third countries, required new, more flexible modular C2 structures. Communications and intelligence requirements increased and changed qualitatively as well as in quantity.

26. Also, unlike the scenario of all-out war in Europe where, in all likelihood, the civilian political power would have only an indirect influence on the conduct of military operations, in "humanitarian" interventions it is all-pervasive, including in the process of identifying targets, and even down to the level of tactical action.

27. The progressive incorporation of ICTs into the process means that different aspects of a military operation can be connected up with one another. Thus this will give rise to the idea of a C4ISR architecture, first in the United States, then extending via the Atlantic Alliance – and as a result of individual countries' pursuing the same lines of thinking – to the allied nations. Network-centric operations are in part the product of this ICT-led sequential development. The increasing automation of command and control processes means they are more responsive to developments on the battlefield.

28. Broadband communications, satellite data transmission and reception and recourse to computer simulations are major achievements in this field and are helping to improve substantially the

COP/CROP essential for successful effects-based operations. The nature of communications has also changed. The traditional forms: the written and spoken word, are being supplemented by photographic and video imagery, including image streaming and video-conferencing, instant messaging and chat rooms – already familiar to Internet users.

29. In a multinational, multi-service context, such technologies are essential to the coordination of operations as they make possible the real-time involvement of government. This last aspect is likely to lead to major changes in military operations through shorter response times and hence deadlines for decisions – possibly something of a mixed blessing. There is a need not to lose sight of the human, non-automatic face of decision-making, based not just on knowledge (i.e. information) but also on instinct and intuition.

30. In the "see first-decide-act" triad that is the characteristic (although not exclusive) model for network-centric operations, automation and the use of information technology reduce the time-lag between observing and acting while continuing to allow time for decision-making, or indeed extending it, with the consequent advantage this affords. The lessons learned in Afghanistan and Iraq and, on a smaller scale, Kosovo, showed that the fully automated model often in practice led to collateral damage or "friendly fire" incidents which are increasingly unacceptable, politically and in the eyes of the general public.

(b) The ISTAR concept: "sensor to shooter"

31. While C4 methods and procedures are obviously capable of generalisation and standardisation, ISR (intelligence, surveillance and reconnaissance) capabilities and the target acquisition capability normally associated with them (ISTAR stands for Intelligence, Surveillance, Target Acquisition and Reconnaissance) are not accessible to all the allies to the same extent. This is true of space-based intelligence, the control of communications and navigation/positioning satellite constellations, MALE and HALE UAVs[10] and autonomous UCAVs and even guided munitions (in terms of both quality and quantity) and to rapid response and special forces. In joint or multinational operations, intelligence is perhaps the most difficult area to deal with: several levels of security are needed, and there are also the difficulties of overcoming the hurdle of bureaucratic inertia or reconciling the discrepant situation analyses reached by the various armed forces branches or countries involved in an operation.

32. An even more highly controversial and sensitive subject than acquisition – achieved through a combination of space-, air-, land- and sea-based assets – at both the political and technical levels is the networking of intelligence. Both closed (Intranet) and open systems (Internet) with gateways as required are able to coexist and currently do exist, but are difficult to manage on a shared basis when operating at the level of a coalition rather than nationally. While tactical intelligence (gathered by special forces or observation UAVs, for example) should logically be shared by units in a given sector of a theatre of operations, strategic and operational intelligence is also a response to political imperatives and subject to political constraints: independent decision-making, tighter control over the use of national forces, protection of technologies and human sources.

33. While it is possible to resolve such difficulties with network-centric capabilities within national defence forces, they acquire a different order of magnitude within a coalition situation, as they offer the opportunity for an adversary to exploit the weaknesses inherent in differences between its member nations in terms of technology standards or levels of technical attainment in this domain. This is a point that can be equally validly made at national level (where each armed forces' branch has its own dedicated systems and forms of protection) and explains the emphasis on joint architectures and procedures for networking, disseminating, exploiting and, last but not least, protecting intelligence.

34. In surveillance and reconnaissance, below space-based means come traditional air assets (piloted aircraft and helicopters), supplemented in recent years by growing numbers of unmanned

[10] Medium altitude long endurance; high altitude long endurance; on this topic see Assembly Document 1884 adopted on 30 November 2004: "Unmanned combat air vehicles and military aeronautics of the future", submitted on behalf of the Technological and Aerospace Committee by Antonio Braga, Rapporteur (Socialist, Portugal); http://www.assembly-weu.org/en/documents/sessions_ordinaires/rpt/2004/1884.pdf .

craft, equipped with different sensors and weapons systems. There are dozens if not hundreds of different models available: micro-drones, strategic and autonomous attack capability UAVs, guided or deployed from networks managed from the ground or air, capable of three forms of action: observation, electronic warfare and – a recent development – attack[11]. Here too, only a limited number of countries have, and can handle all the existing capabilities in this field. Drones and piloted platforms in combination and ground deployment of robots are opening up new vistas in the conduct and execution of military operations and are therefore a key element of network-centric capabilities and operations (UAVs and robots can also serve as nodes or gateways for data-networks).

35. In target acquisition, the above devices are used for firing systems, mainly for guided munitions: bombs, shells and what are now "traditional" cruise missiles. These munitions have GPS-type satellite-assisted navigation systems, to increase their precision. Their guidance systems are able to draw on data captured by and transmitted virtually in real time from other space, air, land or sea-based platforms, thanks to advanced computerised data-networks based on wireless or wireless fidelity (wi-fi) technologies commonly available in non-defence markets for mobile telephone and Inter- and Intranet uses. Modern guidance systems also benefit from developments in electronic miniaturisation since, in many cases, the addition to existing munitions of a simple kit is all that is needed to give them that capability, with no loss of performance (in terms of payload or range, for example). Munitions can be adapted in this way, without the need to have recourse to expensive replacements, in view of the amount of older equipment still in circulation.

36. Another type of "matériel" in the process of evolving towards the network-centric model is the soldier. Special forces offer a typical example of armed forces transformation, particularly after the intensive use made of them in Afghanistan and Iraq. With their high-tech gear, they have also been able to test out new concepts and equipment, the use of which could then be extended by stages to the whole of a country's armed forces. Special forces' members today each, individually, represent a concentration of ISTAR capabilities, with their own sensors and target acquisition capabilities, an enhanced round the clock action capability, constantly in touch with a network that may consist of no more than a group of 5-6 soldiers. Several such groups provide the links in a much more extensive network that can cover a very wide area, the components of which are able to converge very swiftly on areas of weakness in the adversary's defence or political structures, and prepare the way for more conventional reinforcements. This is what happened in Afghanistan in the first phase of the war against the Taliban.

III. Network-centric operations and their implications: transformation of European military capabilities

37. The thinking on the subject and the testing and application of network-centric methods and elements has also come about because of the process of adapting national defence forces to the new international geostrategic environment which emerged in the post-cold war period. Forces and power projection requirements intensified in the last decade of the 20th century with the Gulf War (1991) followed by variously led "humanitarian" military operations, culminating in NATO's intervention against the Federal Republic of Yugoslavia in Kosovo in 1999.

38. Networking and real-time processing of information at every level, coordination of deployed assets and a rapid response (adaptation) to developments in the theatre of operation became, and still are today, the driving-force behind the transformation of European and American armed forces. In this context, network-centric operations could be said to be just one of a number of means of carrying forward the process. However, the pull exerted by their increasing importance in American military thinking and practice has made them reference criteria for European Allies seeking to maintain and develop an external intervention capability interoperable with that of the United States.

[11] *Idem.*

1. National approaches: United in Diversity

39. The attempt to develop a capability for network-centric operations has provided the impetus behind the move to reform the armed forces of the EU and NATO European states, especially now the United States has demonstrated the validity of this new concept in Afghanistan and Iraq. By the close of the 20th century, thinking on the subject was already in progress. The countries involved have now moved forward to the experimental stage pending partial implementation. Transformation has two major objectives: strengthening, improving and developing national and joint force and power projection capabilities and being able to integrate with a multinational and especially a coalition environment, so as to be interoperable with allies and partners, foremost among them the United States.

40. In Europe, the approach of four countries – France, Germany, Sweden and the United Kingdom – to transformation represents an attempt to cover virtually all of the required capabilities in an overt bid for autonomy. Other states like Spain, Italy, Norway, and the Netherlands for example are seeking to acquire more targeted network-centric capabilities, although not yet with a view to wholesale transformation of their military systems into these new models of organisation and action.

(a) Germany

41. The concept of network-centric operations (Netzwerkgestützte Operationsführung (NetOpFü) is tied in closely with reforming German armed forces' capabilities to make them better adapted to today's operational requirements and constraints. The development of a national concept has therefore become a determining factor in the success of that country's current forces restructuring process. This independent project is being pursued simultaneously with the discussion on inter-allied interoperability in regard to the concept of network-centric capabilities being developed within NATO (NATO Network Enabled Capabilities – NNEC) and also takes account of the possibility of forms of bilateral and multilateral cooperation at the European and transatlantic levels.

42. The aim of transformation in the case of the Bundeswehr is to develop its expeditionary and forces projection capability, preferably in a joint multinational context. The present reform envisages the setting up of three joint forces by 2010: an intervention force, a stabilisation force and a force providing support to land forces (some 250 000 troops in total, 105 000 for the land army). Six major essential capabilities have been identified in the process, the first two of which are basic to network-centric operations. They are:

- "Command and Control;
- Intelligence collection and reconnaissance;
- Mobility;
- Effective engagement;
- Support and sustainability;
- Survivability and [force] protection[12]".

43. Defence policy guidelines adopted in 2003 state: "Considering the security situation, there is no requirement to furnish all sub-capabilities with state-of-the-art, high quality material, nor are there the financial resources". Priority is to be given to capabilities that as yet do not exist, in particular "global reconnaissance" and "efficient interoperable command and control systems and means". These are two essential network-centric capabilities for setting up ISTAR groups around which Germany is to develop its NetOpFü capabilities.

44. Battalion-size ISTAR groups concentrate within them the range of intelligence-gathering and reconnaissance resources required to secure a COP more rapidly and efficiently than in the past: UAVs with optical observation and SIGINT systems, human intelligence and combat/reconnaissance

[12] Defence Policy Guidelines for the area of responsibility of the Federal Minister of Defence; Berlin, 21 May 2003; www.bundeswehr.de.

vehicles with modern networked communications systems (Dingo, Fennek and Luchs vehicles). The use of SAR-LUPE satellite radar imagery will significantly strengthen those units by increasing their range of observation of the theatre of operations.

45. In terms of C2 structures, current reforms envisage the setting up of "HERKULES", a wired and wireless communications system that will eventually integrate and connect up existing networks: the army's HEROS and FAUST systems; the navy's MHQ and MCCIS and the Luftwaffe's (air force) EIFEL/GAFCCIS (German Air Force Command and Control Information System) and the German Defence Ministry's RUBIN systems. Negotiations for undertaking the project, estimated to be worth over 6.5 billion euros over a 10-year period[13] are in progress between the German Government and a consortium comprising Deutsche Telekom, AG, Siemens and IBM.

46. Another ongoing project is Standard-Anwendungs-Software-Produktfamilien (SASPF)[14] a range of products, software and standardised computer applications for the armed forces being developed by the German group SAP (Systeme Anwendungen, Produkte in der Datenverarbeitung). SASPF is intended to replace current systems (networks, software and applications) that are now either obsolescent or incompatible. Investment in excess of 1 billion euro over 10 years has been earmarked for the SASPF.

47. Training in joint formation constitutes a priority in developing the German armed forces network-centric capabilities. From 15-26 November 2004, an initial joint exercise took place at the Wilhelmshaven Naval Base, for verifying the capacity to produce and exploit a CROP (Common Relevant Operational Picture). The "Common Arrangement 04" exercise[15] brought together naval, air force and land force units to validate concepts evolved by the Bundeswehr's Transformation Centre (Zentrum für Transformation der Bundeswehr [16]). A further exercise "Common Umbrella 05" is to be held in 2005. The aim is ultimately to end up with an autonomous German capacity to produce and exploit a CROP by 2010 (CROP Vision 2010).

(b) France

48. As a nuclear and a space power, France keeps a close watch on developments in network-centric capabilities with an eye to all three of the following: forces and power projection, multinational interoperability and the maintenance of strategic autonomy and independence characteristic of its foreign and defence policy. The Bulle Opérationnelle Aéroterrestre (Armée) (BOA) project, due for completion in 2025, is a demonstrator of France's new military technology capabilities present and future, with a three-pronged research and investment strategy focusing on information control, space-based assets and observation UAVs and UCAVs[17].

49. The BOA is based on the "combined action of a number of factors (manpower, vehicles, robots and UAVs) that can simultaneously communicate, observe, provide information and act both through existing technologies and new technologies yet to be developed"[18]. It is essentially a reorganisation of France's (land) army based on the idea of "battlefield digitisation" but joint cooperation remains a possibility in the event of there not being total integration (although that would seem to be the aim in the American project through the Cooperative engagement and Global Information Grid concepts).

[13] "New group seeks big German military IT contract"; 18 January 2005; www.itworld.com.

[14] *"Effizienter werden – SASPF in der Bundeswehr"*, German Federal Defence Ministry, 25 March 2003; www.buvg.de.

[15] **"***Bundeswehr erprobt Vernetzte Operationsführung"* Luftwaffe (German Air Force), 17 November 2004; http://www.luftwaffe.de.

[16] The ZTB was established in 2004 to replace the Zentrum für Analysen und Studien der Bundeswehr (Bundeswehr Centre for Studies and Analyses); Zentrum für Transformation, 30 June 2004, German Federal Defence Ministry. www.bmvg.de .

[17] See Assembly Document 1884 adopted on 30 November 2004: "Unmanned combat air vehicles and military aeronautics of the future", submitted on behalf of the Technological and Aerospace Committee by Antonio Braga, Rapporteur (Portugal, Socialist Group);
http://www.assembly-weu.org/en/documents/sessions_ordinaires/rpt/2004/1884.pdf

[18] BOA – Bulle Opérationnelle Aéroterrestre (Armée) (BOA) – project, Press file: French Ministry of Defence, 2002; www.defense.gouv.fr

The BOA is based on a range of assets: those existing (communications, aircraft, radar, satellites), currently being developed (UAVs, robots, the "soldier of the future") and to be defined in the near future (Directed Energy Weapons (DEW), such as, for example, Electromagnetic Pulse (EMP) and High Powered Microwave (HMP) Weapons).

50. Man-machine interaction is central to BOA, of which the first elements of the "Félin" solder system programme come on stream in 2006-07. France will be the first European country to deploy a network-centric solider, to meet national requirements and those of the NATO Response Force and European Union battlegroups. From 2015-25, BOA designers will also work on a concept for use, HOBOT, involving autonomous robots and human soldiers employed in close coordination. "Félin" consists of three principal systems:[19] individual, specific and collective. The first has six different elements: clothes and other forms of protection, the portable electronic platform, individual energy sources, weapons, headgear and the "Félin" information network. The other two systems are concerned with means of communications/ navigation/positioning and of observation, and with batteries.

51. BOA is highly dependent on a space-based defence system made up of observation (Helios 1 or Helios 2), communication and navigation satellites (necessary for locating national, allied or enemy forces and for guided and precision munitions) and the capability to deploy UAVs and multi-mission robots, as sensors or for active or passive reconnaissance or defence. All of these systems, down to the vehicles and the "soldier of the future" will be linked via the high band-width communications networks necessary for transmitting all forms of real time data essential in building up the COP that any nation aspiring to lead a multinational or coalition operation must now have at its disposal.

52. The Helios 2A optical observation satellite, which was put into orbit in December 2004 and declared operational in April 2005, is one of the centrepieces of the whole system. Supplementing and enhancing the capabilities already provided by the Helios I satellites, its presence means that areas such as intelligence, preparation of missions and drawing maps of hitherto uncharted or imprecisely charted areas can now be covered. These three aspects, taken together, constitute ISTAR capabilities from which France's partners, Belgium and Spain[20], are able to benefit by means of this satellite. This approach has confirmed France's "umbrella" role in Europe in regard to the development of network-centric capabilities, also in evidence in the Franco-German "Tigre/Tiger" attack helicopter programme, designed from the outset to integrate with the BOA.

(c) The United Kingdom

53. The objective of the British concept of "Network Enabled Capability" (NEC) is "to enhance military capability by the better exploitation of information[21]". Information is a power multiplier and NEC has been designed in that optic around four key notions: "sense, understand, develop intent, synchronise effects", or in other words around information sensors, COP, C2 networking and auto-synchronisation to achieve an optimum EBO on the theatre of operations. NEC is one of the main thrusts of the reform (transformation) of the British armed forces described in the "Defence White Paper 2003", and the "Defence Command Paper 2004", where it is stated that:

> "NEC is about the coherent integration of sensors, decision-makers and weapon systems along with support capabilities. NEC will enable us to operate more effectively in the future strategic environment through the more efficient sharing and exploitation of information within the UK Armed Forces and with our coalition partners. This will lead to better situational awareness across the board, facilitating improved decision-making, and bringing to bear the right military capabilities at the right time to achieve the desired military effect. This enhanced capability is about more than equipment; we will exploit the benefits to be obtained from transformed doctrine and training and optimised command and control structures. The ability to respond

[19] "Félin": technical data sheet; Direction générale de l'armement (DGA), France 2004 www.defense.gouv.fr.
[20] France's partners for Helios 1 were Spain and Italy.
[21] "Network Enabled Capability"; United Kingdom Ministry of Defence, 2003. www.mod.uk.

more quickly and precisely will act as a force multiplier enabling our forces to achieve the desired effect through a smaller number of more capable linked assets [22]".

54. The UK's network-centric capabilities are thus being developed via a raft of major programmes, either still in their initial phases or already being implemented by the armed forces. This is being done in three stages: initial (2007), transition (2015) and maturity (2020-30) which together form part of whole project known as "Network Integration Test and Experimentation Works" or NITEWorks, under the leadership of BAE Systems.

- Cooperative Engagement Capability: in cooperation with the United States. This is a naval air and missile defence project "combining and distributing sensor measurement data from all CEC equipped ships, aircraft and land sites" to achieve "an integrated, netted, air defence system that greatly enhances detection, tracking and identification of air targets, as well as providing engagement coordination[23]";
- Skynet 5: military and communications satellites;
- Cormorant, Falcon and Bowman: strategic (link between satellites and forces) operational and tactical communications systems;
- Defence Information Infrastructure: INTRANET/INTERNET information infrastructure covering all defence sites and operations;
- ASTOR, Watchkeeper, Soothsayer: airborne radar surveillance, observation UAVs and tactical electronic warfare equipment;
- Future Offensive Air Systems (FOAS): a combination of classic air and robotic systems (drones and missiles), coordinated and networked in a C4ISR system. The FOAS centre-piece is the Joint Strike Fighter/F-35 currently being developed by the United States and several Allies.
- Future Integrated Soldier Technology (FIST): a tri-service project (Army, Royal Marines and the Royal Air Force). FIST is an integrated fighting system for troops that have to fight on foot at close quarters with the enemy. The programme in fact began in 1994 as the Future Fighting Soldier System but its initial operating capability is not scheduled to come on stream until 2009.

55. The United Kingdom is the only country to date to have experience of a network-centric operation under actual coalition conditions. This was Operation Telic, which formed part of the American Operation "Iraqi Freedom" carried out in March 2003. The first evaluations of this joint undertaking were published in 2004 and reviewed in 2005 in a report: "US/UK Coalition Combat Operations during Operation Iraqi Freedom" published by the US Defense Department's Office of Force Transformation in conjunction with the UK Ministry of Defence[24].

56. In order to be able to operate with the United States, British forces had to be equipped with American kit and were partially connected to the US network. They thus had access for the first time to the Force XXI Battle Command Brigade and Below (FBCB2)/Blue Force Tracker (BFT) systems[25],

[22] "Delivering Security in a Changing World – Future Capabilities" Chapter 2 – *Force Structure Changes, Network Enabled Capability*; UK MoD, July 2004. www.mod.uk.

[23] "UK Co-Operative Engagement Capability (UKCEC); Defence Procurement Agency, United Kingdom, December 2004. www.mod.uk.

[24] "A Network-Centric Operations Case Study: US/UK Coalition Combat Operations during Operation Iraqi Freedom"; Office of Force Transformation, 2 March 2005; www.oft.osd.mil.

[25] "The Force XXI Battle Command Brigade & Below system (FBCB2) is the principal digital command and control (C2) system for the US Army at brigade level and below. The system is an automated, network-enabled command and control system, which provides brigade and below elements with a seamless battle command capability. It comprises a personal lightweight GPS receiver (PLGR) and a data terminal that links to a satellite hub to create and maintain a method of tracking and communicating with other FBCB2/BFT systems. The system automatically updates its position every 5 minutes or if the platform has moved 800m. The system provides the following major capabilities: positional information and navigation support, tactical messaging,

thanks to a loan of 47 kits (as against approximately 1 000 in service in US land army, Marine Corps and air force units). Communications were strengthened by the deployment of the Joint Operational Command System, of British origin, but which does not have the same capability as equivalent US systems.

57. In order to facilitate coordination and better integrate the British force into the US environment, a specific information system for the coalition – CENTRICS-X – was set up, but the UK's dependence in intelligence terms became obvious from the fact that the SIPRNET[26] system was operated in the British units under extremely strict procedural constraints imposed by US (Foreign Disclosure) officers.

58. Coordination between the two forces was effected generally without much difficulty, notwithstanding the short period of training the British troops had in working in coalition in a network-centric environment. So the BFT kits were not integrated into deployed assets until February. However, in some instances the two forces were unable to communicate and act in coordinated fashion[27] and the "gap" in terms of technology, doctrine, training and profile of staff involved in so far as systems operators were concerned, served to illustrate the problems Europeans have to deal with if they want to interact with US forces in the near future.

59. One conclusion of the report states that:

> "The UK land forces have largely used paper charts and voice communications as their primary means of gaining situational awareness for many years – the existing combat net radio having been deployed for around 30 years. As a result, their tactics, techniques and procedures (TTPs) have been thoroughly optimised for this environment and everyone is well trained and experienced in war-fighting this way. Consequently there is little incentive to change and indeed a fear that new and unproven systems may reduce combat effectiveness – at least in the short-term while its intricacies are mastered.
>
> In contrast, the US land forces deployed in OIF had more familiarity with computer-based systems – having already used tactical intranets, such as SIPRNET, to provide some INTEL and situational awareness for some time. Therefore, their TTPs are likely to have evolved somewhat towards those needed for digital situational awareness. This is likely to have made them more amenable to adapting to using FBCB2/BFT for a significant proportion of their situational awareness needs during OIF.
>
> (...)
>
> Due to their earlier exposure to the next technology wave (i.e. digital information that supports SA [situation awareness], such as tactical intranet and FBCB2/BFT) a larger proportion of the US forces are happy to migrate to this technology. By comparison, the bulk of the UK forces are still happiest with their proven technology and it is only a relatively small number who are prepared to try the new technology – largely in a tentative and experimental way"[28].

(d) Sweden

60. In the late 1990s, Sweden introduced a process of reform and adaptation of its armed forces to take place over a period of at least 15 to 20 years. The main aim is to create a Network Based Defence (NBD) system. This is regarded as the means of "developing a new kind of defence [by] transforming today's force structure into a defence based on flexible, rapid and controlled engagement

---

graphical overlay creation and transmission, the production and dissemination of reports and returns, limited terrain analysis". *Idem.*

[26] SIPRNET – Secret Internet Protocol Router Network; an encrypted intelligence transmission and messaging system used by the US armed forces. *Idem.*

[27] The same thing occurred between some US units, in particular between Marine Corps and land army units. *Idem.*

[28] "A Network-Centric Operations Case Study: US/UK Coalition Combat Operations during Operation Iraqi Freedom"; Office of Force Transformation, 2 March 2005"; www.oft.osd.mil.

capabilities[29]". As an EU, but not a NATO member state, Sweden also wants to be able to act as a lead/framework nation within the ambit of the European Security and Defence Policy, particularly in the Nordic region. It has a leading-edge industrial and technology base upheld by such industrial giants as SAAB and Ericsson.

61. In October 2004, the Swedish Government introduced a bill on the development of Sweden's defence capabilities over the period 2005-07[30]. This states that: "The Swedish Armed Forces shall develop a modern, flexible and highly accessible operational defence. The emphasis should be on rapid operational capability. We shall increase our capability as regards international operations both quantitatively and qualitatively". The means identified for achieving this is implementation of the NBD concept. Networking information is seen as the way to speed up the decision-making process at the strategic, operational and tactical level and make it more effective, at national level, when acting in coalition systems or in multinational operations.

62. Defence research and technology is one of the main planks of the NBD project. "All systems and platforms are to be made 'net ready' (i.e. adapted or replaced) step by step, to enable them to function smoothly when integrated". To achieve economy and efficiency the Swedish authorities are also proposing to have recourse widely to dual/civilian technologies. Here, three broad development guidelines have been adopted: "short development cycles"; "components and modules [to] form exchangeable parts in complex systems" and "the development of methods, organisation, personnel and technology to be done jointly with all Services represented and with support from both industry and the academic institutions".

63. In October 2003, the technical side of the NBD project, for which the guidelines and priorities are together defined by the Armed Forces, the Swedish Defence Material Administration (FMV), la Defence Research Agency (FOI) and the National Defence College (FHS), was awarded to a consortium comprising SAAB and Ericsson with input from Boeing and IBM. Priority areas for development identified are:

- "network-based command and control systems;
- aircraft;
- combat vehicle systems;
- short-range combat systems;
- unjammable telecommunication systems; (...)
- interfunctional sensor and data fusion; (...)
- signature, protection and system design[31]".

64. International cooperation is also integrated in the NBD project, either with other European partners[32] or with the United States. Sweden's active involvement in the technology demonstrator programme for the autonomous European combat UAF "Neuron[33]" and in the research on future air combat systems within the ETAP (European Technology Acquisition Programme) is part and parcel of the same thinking, shared by France and Germany, about the development of national and European

[29] "A Network Based Defence"; Swedish Armed Forces, Ministry of Defence 2004. www.mil.se.
[30] "Our future defence – the focus of Swedish Defence policy, 2005-2007" Swedish Ministry of Defence, October 2004. www.sweden.se .
[31] *Idem*, "Military Equipment Issues – National Niches".
[32] In particular, with the states parties to the Framework Agreement on the restructuring of the defence industry/Letter of Intent (France Germany, Italy, Spain, Sweden and the United Kingdom) and also by taking up opportunities offered by the establishment of the European Defence Agency (EDA).
[33] The Neuron project involves France, Sweden and Greece. Negotiations with Italy, Belgium and Switzerland are in progress. The French aeronautics firm Dassault Aviation is the lead contractor in partnership with EADS; see Assembly Document 1884 adopted on 30 November 2004: "Unmanned combat air vehicles and military aeronautics of the future" submitted on behalf of the Technological and Aerospace Committee by Antonio Braga, Rapporteur (Portugal, Socialist Group);
http://www.assembly-weu.org/en/documents/sessions_ordinaires/rpt/2004/1884.pdf

network-centric capabilities which are autonomous, but possibly interoperable as necessary with US systems.

2. NATO and the EU – the search for a joint European capability

65. Network-centric operations are not only combined and/or joint operations. They also have to be conceived from the outset in a multinational context (within a pre-established cooperation structure) or in a coalition (two or more countries that form a partnership to conduct a military operation). This makes it possible for states that do not have the resources (in terms of finance or organisation) or the capacities (industry and technology) necessary to embark on a long and costly process of transformation and adaptation to benefit from progress in those areas and exploit their national strengths and areas of excellence. In this way, multinational operational coherency can be secured through generalised procedures and common standards intended to facilitate forces' interoperability in-theatre.

66. In Europe, the primary competent organisation in this area is NATO, with its 50 years' experience in pooling resources and defining common or harmonised standards. Two structures are responsible for concepts and harmonisation of network-centric capabilities: they are, respectively, the Allied Command Transformation (ACT) and the NATO Consultation, Command and Control Agency (NC3A). On the forces side, the NATO Response Force and Allied Ground Surveillance (AGS) programme represent the closest embodiment of NATO's endeavours in terms of information control.

67. The European Union too is adapting its military structures and capabilities in line with this development. The vehicles for Europe's transformation are the European Capability Action Plan (ECAP) groups dealing with C4ISR and ISTAR, which can also take advantage of the relevant NATO structures, particularly through the Capability Development Mechanism. Given its structure and mandate, the European Defence Agency, is likely to have a central role in this particular process, directed towards those countries with fewer resources or that have just acceded to the European Union.

(a) NATO and Transformation

68. On 12 June 2003, the Defence Ministers of NATO members, meeting in Brussels, decided to reform the Alliance military command structure. This now consists of an Allied Command Operations (ACO), based at SHAPE in Mons, Belgium, and an Allied Command Transformation (ACT) based in Norfolk, Virginia, United States. The latter has a key role in developing and implementing network-centric capabilities in NATO and in the member states.

69. ACT's brief is the transformation of NATO, according to the following five priorities:

- "Transform NATO's military capabilities.
- Prepare, support and sustain Alliance operations.
- Implement NATO Response Force and other deployable capabilities.
- Achieve ACT full operational capability.
- Assist transformation of partner capabilities[34]".

ACT cooperates closely with ACO and the United States Joint Forces Command (USJFCOM). USJFCOM has been described as the US armed forces "transformation laboratory[35]". Its role is similar to ACT's own.

70. ACT has three major divisions, each responsible for a particular area, with support structures in different Alliance countries as follows:

- "Strategic concepts, policy and requirements identification – ACT Staff Element (Mons, Brussels) Capabilities Planning and Implementation;

[34] NATO's Allied Command Transformation (ACT), Standing Priorities. www.act.nato.int.
[35] USJFCOM, About us. www.jfcom.mil.

– Joint Concept Development – Joint Warfare Centre (Stavanger, Norway), Joint Force Training Centre (Bydgoszcz, Poland), Joint Analysis and Lessons Learned (Monsanto, Portugal);

– Future capabilities, Research and Technology – Undersea Research Centre (La Spezia, Italy)".

The various NATO Schools – the NATO Defence College (Rome, Italy), the NATO Communications and Information Systems School (Latina, Italy) and the NATO School (Oberammergau, Germany) are also involved with ACT activities. The national/multinational "Centres of Excellence" in the service of NATO are another important factor in relation to its work. These eight centres, funded by one or more countries, constitute a tool for experimentation and for the validation of concepts, available to the Alliance, its member states and to other countries involved in the Partnership for Peace Programme (PfP). Their areas of specialisation are as follows: Nuclear, Biological and Chemical Defence (NBC) (Czech Republic), Cold Weather (Norway), Demining (Spain), Tactical Air (Turkey), Counter-terrorism (Turkey), PfP Training (Turkey), Joint Air Power Competence[36] (Germany: this is the first fully multinational NATO Centre of Excellence, set up in December 2004), Command and Control (C2) Support (Netherlands).

71. The NATO Technical Agencies: the NATO Consultation, Command and Control Agency (NC3A) and the Research Technology Organisation (RTO) also contribute to the work of ACT, while remaining independent. Their roles are as follows:

– The NC3A, based in The Hague, Netherlands is central to the process within the Alliance for developing the C41SR capabilities essential for network-centric operations. Its five main areas of activity are: C3 (Command, Control, Communications), Policy Concept and Architecture, Operations Research, Communication and Information Systems, Command and Control Systems and Acquisition[37]. NC3A works directly on the elaboration and development of the NATO Network Enabled Capability (NNEC) concept defined as "linking sensors, decision-makers and weapon systems so that information can be translated into synchronised and overwhelming military effect at optimum tempo. (...) It emphasises provision of data to a wide community of users in a data pull rather than data push environment, the provision of a high bandwidth Web-based intranet and the use of Web Services technology[38]".

– The RTO is answerable to the North Atlantic Council/NATO Military Committee and the Conference of National Armaments Directors. It has a technical support unit, the Research and Technology Agency (RTA) based in Paris, France. The RTO's mission is to "conduct and promote cooperative research and information exchange to support the development and effective use of national defence research and technology to meet the military needs of the Alliance; to maintain a technological lead; and to provide advice to NATO decision makers[39]". The RTO is heavily involved in developing Alliance network-centric capabilities: On 15-18 November 2004, it carried out the first ever "NATO-wide area networked real-time simulation of Combined Air Operations" (First WAVE – War fighter Alliance in a Virtual Environment) involving simulated air units from seven NATO states (Canada, France, Germany, Italy, the Netherlands, the United States and the United Kingdom) [40].

72. ACT and the NATO technical agencies are where the concepts and technologies on which the network-centric capabilities of the Alliance are worked out and developed. Two major projects currently under way are representative of the practical implementation by stages of those capabilities

[36] "NATO takes steps toward creating first multinational centre of excellence", 13 December 2004. www.act.nato.int.
[37] NATO Consultation, Command and Control Agency (NC3A). www.nc3a.nato.int.
[38] NATO C3 Technical Architecture; Volume 2, Chapter 5 "NATO Network Enabled C3 Architecture Concepts"; December 2003. www.nato.int
[39] The NATO Research and Technology Organisation. www.rta.nato.int.
[40] NATO RTO First WAVE Collaborative Simulation. www.rta.nato.int.

so as to make it possible for NATO to lead and execute network-centric operations. They are the NATO Response Force and the Allied Ground Surveillance Programme.

– The NATO Response Force[41] is a joint, multinational force equipped to the highest technology standards, which will provide a demonstration over the coming years of the Alliance's capability to undertake a wide spectrum of missions – from peacekeeping to medium and high intensity operations. It is also the ideal test-bench for the setting up of a network-centric force, fully interoperable internally and externally, particularly with United States forces. The three main contributor nations to the NRF are France, the United Kingdom and Germany which provide more than half of the 21 000 troops planned for the force. Those three countries, along with Sweden, are at the leading edge of developments in network-centric capabilities in Europe (NATO and the European Union). The force's initial operational capability (of 17 000 troops) was reached in 2004 and it should be fully operational by 2006.

– The Allied Ground Surveillance Project, developed jointly by the two companies EADS (Europe) and Northrop Grumman (United States) with the involvement of General Dynamics (Canada), Indra (Spain), Galileo Avionica (Italy) and the European firm Thales, is also a major development in technological and network-centric capabilities in the service of the Alliance and its members. Envisaged as early as 1989, the AGS did not really "take off" until 2001, with implementation starting in 2003. Its mission is to provide the Alliance with a real joint air-ground surveillance capability with military and defence as well as security applications such as civilian protection, counter-terrorism, internal security, border surveillance, humanitarian operations and assistance in the event of major natural or industrial disasters. It is also a (real-time interoperable) network-centric system comprising an airborne (satellites, aircraft and UAVs) and a ground segment (fixed and mobile stations). Technical production has been awarded to an industrial consortium, the Transatlantic Industrial Proposed Solution (TIPS) made up of six leading companies and over 130 firms from the 24 NATO European nations and Canada. The system is intended to be operational in 2010-11.

(b) The European Union: innovation and duplication

73. Since 1999 the European Union has been acting autonomously to strengthen European security and defence. From the Headline Goal defined at the Helsinki European Council in December 1999 as the capacity to deploy over 60 000 troops in 60 days, with full logistic support, in the framework of the Petersberg tasks, things have now moved on to the 2010 Headline Goal, centred around increased responsiveness and a new multinational battlegroup structure, underpinned by an industrial and technological base whose development is being managed through the European Defence Agency. In parallel, military cooperation with NATO is being deepened to avoid pointless duplication, given that the armed forces of the various nations in most cases serve within both organisations.

74. As far as network-centric capabilities go, the work of the ECAP (European Capability Action Plan) project groups responsible for ISTAR and interoperability is crucial. Indeed the battlegroup is proving to be the ideal vehicle for developing and testing out the new force doctrines, structures and forms of organisation that are emerging as part of the transformation of European armed forces within both national and multinational contexts, including the work being done in NATO (the NNEC, NRF and the AGS project, for example). The battlegroups, scheduled to become operational between 2007 and 2009 are, by definition, joint multinational forces that are virtually fully interoperable. Network-centric concepts are the key to their success.

75. The EU Defence Ministers, meeting in Brussels on 22 November 2004 in the framework of the Military Capability Commitment Conference, adopted a series of decisions of the utmost importance

[41] On the origins, missions and capabilities of the NRF, see Assembly Document 1825 adopted on 3 June 2003: "The EU Headline Goal and the NATO Response Force (NRF) – reply to the annual report of the Council" submitted on behalf of the Defence Committee by Dario Rivolta, Rapporteur (Italy, Federated Group); http://www.assembly-weu.org/en/documents/sessions_ordinaires/rpt/2003/1825.pdf .

for the development of EU military and civilian crisis-management capabilities over the next five years: "Interoperability, deployability and sustainability will be at the core of Member States' efforts to improve military capabilities. The Union will thus need forces which are more flexible, mobile and interoperable, making better use of available resources by pooling and sharing assets where appropriate and increasing the responsiveness of international forces[42]". In that Declaration are to be found the basic elements that contribute to the concept of network-centric capabilities and operations, in particular interoperability, the pooling of resources and information, speed of response, flexibility/adaptation (auto-synchronisation).

76. Like the NATO Response Force, the battlegroups, in view of their size (1 500 soldiers) and specific capability (rapid response) can be more easily transformed into a network-centric force than traditional armed forces units. "The battlegroup is a specific form of rapid response. It is the minimum military effective, credible, rapidly deployable, coherent force package capable of stand-alone operations, or for the initial phase of larger operations. The battlegroup is based on a combined arms, battalion-sized force and reinforced with Combat Support and Combat Service Support elements. A battlegroup could be formed by a Framework Nation or by a multinational coalition of Member States. In all cases, interoperability and military effectiveness will be key criteria[43]". At the 22 November 2004 meeting, EU member states agreed on the formation of 13 battlegroups, at least one of which would be operational by 2005 and two ready for deployment by 2006-07.

77. Battlegroup capabilities are directly related to work currently being done on a shared basis by the ECAP project groups and the new European Defence Agency[44], as well as that being done at national level and in NATO. Indeed, the battlegroup concept has from the outset been associated with the development of the NRF, to ensure complementarity and global strengthening of European capabilities while remaining respectful of each organisation's specificity. The European Capability Action Plan, launched in 2001 and revised for the first time in 2003, encompasses areas specifically concerned with network-centric capabilities: combat search and rescue, C2, special operations forces, theatre ballistic missile defence, unmanned aerial vehicles, space assets, ISTAR/ground surveillance. All these areas have in common the control and dissemination of networked information.

78. However, results obtained through ECAP are less positive than were originally hoped for. Structural problems and difficulties in organising the work, differing national priorities and assessments and chronic underfunding have had an adverse effect which was explicitly acknowledged by the Ministers: "The Single Progress Report of May 2004 noted that marginal progress had been made since the Helsinki Progress Catalogue 2003. It also stated that Member States had to give considerable extra impetus to the development of capabilities in order to realise the ambitions expressed in the ongoing work on the Headline Goal 2010, including the EU Battlegroups Concept. The Headline Goal 2010, adopted in May 2004, recognises that existing shortfalls still need to be addressed". This state of affairs is clearly evident from the Capabilities Improvement Chart II/2004 (period 2002-2004) showing progress made on ECAP projects. There has been little significant movement in terms of: Reconnaissance and Liaison helicopter battalions; Surveillance and Target Acquisition (STA)/Unmanned Aerial Vehicles, Combat Search and Rescue (CSAR), Cruise missiles and Precision Guided Munitions, ISTAR and Tactical Ballistic Missile Defence".

79. To inject new life into ECAP, the European Council decided to re-evaluate the role and functioning of the project groups and at the same time give the European Defence Agency a central part to play in the EU's defence capabilities enhancement process, looking to the 2010 Headline Goal. "The newly established European Defence Agency (EDA) will play a crucial role in this improved framework for capability development. Its mission is to assist Member States' efforts to improve their

[42] Military Capabilities Commitment Conference – Declaration on European Military Capabilities; Council of the European Union, Brussels, 22 November 2004. http://ue.eu.int.
[43] *Idem.*
[44] For information on the origins and functions of the AED see Assembly Document 1856 adopted on 3 June 2004: "The European Defence Agency – reply to the annual report of the Council" submitted on behalf of the Technological and Aerospace Committee by Antonio Braga, Rapporteur (Portugal, Socialist Group); http://www.assembly-weu.org/en/documents/sessions_ordinaires/rpt/2004/1856.pdf .

military capabilities to sustain ESDP as it stands now and develops in the future. Its tasks in the field of capability development include :

- coordinating the implementation of ECAP, an enhanced ECAP or any successor plan;
- scrutinising, assessing and evaluating against criteria to be agreed by the Member States the capability commitments given by the Member States through the ECAP process, and utilising the Capability Development Mechanism (CDM);
- promoting and coordinating harmonisation of military requirements;
- identifying and proposing collaborative activities in the operational domain[45]".

80. The EDA with its four directorates for Capabilities, Research and Technology, Armaments and Industry/Market, is ideally positioned at the centre of, and to act as a catalyst for, capabilities development and possibly forces transformation at EU level and within the member states. Its recent establishment provides an opportunity for the introduction of new approaches and concepts, drawing in particular on network-centric capabilities and net warfare, leaving older "legacy projects" to existing structures (ECAP and the Western European Armaments Organisation (WEAO) for example).

81. The EDA's working relationship with the European Commission over security research and dual technology is also helpful in the development of network-centric capabilities, many of which draw on technologies and equipment for information management and distribution, reconnaissance and surveillance and on software available on the open market. The tie-in between the EDA and the Commission could make for greater permeability between technologies whose development and adaptation rates in the civil and military sectors are "out of sync".

82. This aspect is discussed in the EDA's initial work programme for 2005, approved by the Steering Board at its second meeting[46]:

"A. As early priorities, the Steering Board expects the following to have been achieved:

(...)

6. The Agency to have identified and engaged with urgent agendas ('departing trains'), bringing proposals to the Steering Board as necessary. Examples include:

- Capability issues relevant to urgent operational needs;
- HLG 2010 and battlegroups development;
- Ongoing Commission initiatives:
  - Green Paper on Defence Procurement;
  - Future ESRP;
  - Space policy;
  - DTIB Monitoring;

(...)

B. By the end of the year, the Steering Board expects the following to have been achieved:

(...)

2. The Agency to be leading (or managing as *ad hoc* projects) initiatives in as many as possible of the following areas:

[45] Military Capabilities Commitment Conference – Declaration on European Military Capabilities; Council of the European Union, Brussels, 22 November 2004 ; http://ue.eu.int.

[46] Second Meeting of the European Defence Agency's Steering Board, chaired by Javier Solana; Brussels, 22 November 2004, Press Release. http://ue.eu.int.

– UAVs/ISTAR. Technology demonstration work on long-endurance UAVs, in the context of development of a wider ISTAR architecture, taking account of relevant work in other multinational fora;

– Advanced European Jet Pilot Training;

– Command, Control and Communication. Work to find solutions to current ESDP operational shortfalls, and to develop capacity and interoperability for the future;

– Defence Test and Evaluation Base Rationalisation. Development of proposals for budgetary savings by elimination of duplication/redundancy of facilities in Europe;

– Armoured Fighting Vehicles. Based on review of future requirements and the relevant technological and industrial base, development of proposals for collaborative technology development and/or procurement programmes, potentially facilitating industrial restructuring;

– COTS/MOTS. Work to develop proposals for a European market in Commercial/Military Off-the-Shelf equipment, including feasibility study of an "electronic market place"."

83. Through the Headline Goal 2010, the setting up of the battlegroups, the reform of ECAP and the advent of the EDA, together with enhanced cooperation/coordination between it and NATO, the European Union is, by stages, moving into a position as the main player in the development of a common European concept for network-centric capabilities and operations. This is complementary to NATO's concept, which, although there is a degree of duplication, hinges to a greater extent on transatlantic interoperability with developments as regards EU military structures being progressively brought in; the only thing missing now is a permanent operations HQ.

IV. Challenges and prospects for network-centric capabilities

84. Net warfare and network-centric capabilities and operations constitute a new phase in warfare development. These new concepts and their technological consequences go further than their mere application in the theatre of operations. There is a major industrial, technological and economic challenge involved with this new conceptual approach. Thus the increasing integration of new information and communication technologies in command and control and weapons systems, right down to the combatant in the field, are leading to changes in doctrine, structures and organisation and in the management of material and human resources. The use of force and the rules of engagement are also profoundly affected. The fact of being able to strike quickly and accurately from a distance is already a reality today, with the perverse effect of creating an at times exaggerated feeling of overriding superiority – a weakness that would undoubtedly be exploited by current or potential adversaries.

85. From a concept based on the introduction of new technologies in the armed forces things have progressed to virtually total transformation, in depth, of national defence forces. Such a project has very important economic and technical implications, particularly in the defence electronics sector and for systems integrators, consultancy firms and manufacturers of traditional platforms, which now find themselves having constantly to modernise and update as the technology moves forward. All the major American and European firms are actively involved in the area of network-centric capabilities in a "transformation market" worth billions of dollars or euros.

86. The Network Centric Operations Industry Consortium (NCOIC) was established on 27 August 2004 in the United States, to coordinate the industrial side and facilitate the necessary interoperability/connectivity between the national or common systems being developed in the United States and Europe. The NCOIC, which is NATO's Allied Command Transformation (ACT)'s main industry contact, states that its mission is[47]:

[47] NCOIC – Mission and Vision. www.ncoic.org.

> "to help accelerate the achievement of increased levels of interoperability in a network-centric environment within, and amongst, all levels of government of the United States and its allies involved in Joint, Interagency and Multinational operations.
>
> We will achieve this mission through the creation of an international industry body, whose membership is open to all interested parties sharing a common vision of facilitating Network Centric Operations, and whose efforts are directed in support of the respective members' customers".

The NCOIC is made up of four main bodies: the Executive Council, the Advisory Council and the Business and Technical Councils. The NCOIC's founder members are the major national and international firms in the defence/electronics/information technology sectors with a preponderance of US-based companies (over 20 of the 30 identified by the consortium). Among the European representatives are the likes of Alcatel, BAe Systems, EADS, Ericsson, Finmeccanica, Rheinmetall, SAAB and Thales. Participants have different rights according to the financial and technological contribution they make to NCOIC activities. As of April 2005, 62 companies belonged to the organisation, divided into three categories of membership with differing rights according to contributions.

87. The Consortium aims to assist transformation of the armed forces of the US and its allies. However, representation from Europe is lower than would be desirable if a fair balance is to be struck in what might be viewed a 'friendly' takeover bid by US network-centric concepts and solutions for the work ongoing at national level in Europe, in NATO and in the European Union. For example, of the 17 members of the Advisory Council, set up in February 2005, only two are drawn from European countries (Netherlands and Sweden). Yet, this Council will have a crucial role in the way the NCOIC evolves, its task being to "ensure that the NCOIC remains focused on its objectives and that it is accessible to all stakeholders. The role of the Advisory Council is to represent the needs of government agencies in the identification and development of the open, consensus-based approaches necessary to support transformation to network-centric operations throughout the Department of Defense, the Department of Homeland Security and other agencies[48]".

88. Unless NATO, the EU and European countries are included in the "other agency" category, NCOIC seems likely to have a very limited international dimension. However, the NATO technical agencies and the European Defence Agency and even the European Commission (in the field of Homeland Security research) should be represented on the Affiliate Members Council, which is open to:

> "Members of industry associations, standards bodies, specification working groups and others whose work will impact upon, or be impacted by, Network Centric transformation activities.
>
> Others, such as academia or advisory bodies, as deemed appropriate by the Executive Council".

89. The NCOIC is still too recent an arrival to be truly influential in the transatlantic debate on network-centric capabilities. If, through it, joint solutions and technologies can be developed, the NCOIC could prove to be a crucial instrument for transatlantic cooperation, allowing the United States and its Canadian and European allies, who are members of the Atlantic Alliance to achieve an optimal level of interoperability for operational coherence in NATO and coalition operations. However, Europe's presence, in terms of its industries and governments, needs to be bolstered, if only to create a heightened awareness of European industrial and technological capabilities and European solutions and concepts to meet the challenges of transforming the allied armed forces.

90. The transition from platform-based action (equipment, personnel, land-sea-air divide) to another based on networked systems involves a cultural revolution that impacts on command structures, forces, logistic support/management and procurement. A number of different military models and traditions exist side by side in Europe and there is also a very wide variation in materials and systems which are non-interoperable and, in terms of technical or technological development, may even be obsolete. To replace the legacy of decades of national planning over a short space of time is virtually

[48] NCOIC – Advisory Council Charter; www.ncoic.org.

impossible. Hence the more gradual approaches, by stages (in terms of quantity, tempo or types of forces involved) and by category of materials and systems (heavy, light, electronic, information technology).

91. However, the rhythms of transformation in the United States and Europe are already too dissimilar[49] and will have detrimental consequences in the medium term for interoperability in the Atlantic Alliance and in terms of a better balance in transatlantic relations. The rate of transformation in the US also gives American firms a considerable edge when competing internationally to provide solutions and new network-centric weapons systems. Hence Europe's interest in becoming actively involved at the industrial level and also in military and political terms, both as (European members of) NATO and as the EU, in organisations like the NCOIC, so that all parties concerned can exchange information and monitor and guide, if not control completely, the direction of the research being carried out into network-centric capabilities.

92. The report on "US/UK Coalition Combat Operations during Operation Iraqi Freedom" already referred to provides an illustration of the gap that has opened up and not just in terms of technology. There is also a "generation gap", as far as staffing goes. A comparison between the establishment tables of American and British communications personnel before and during operations "Iraqi Freedom" and "Telic" shows the kind of difficulties Europeans have to deal with over the coming years if they want to become interoperable with the United States. While the United Kingdom deploys in accordance with the traditional vertical ("stovepipe") structure set out in all the NATO manuals, US forces already have a simple or enhanced network-centric structure as depicted by the diamond-shaped diagrams, where all the corner nodes are in virtually simultaneous communication[50].

UK Forces before and during operations (with tactical communications by satellite and Blue Force Tracker (supplied by the United States) :

US Forces before and during operations (partially networked and robustly networked):

93. Technology is the backbone of the concept of network-centricity. Without it, the subject would be purely of academic interest. However, technology is never neutral in its effect. It creates dependency and forces changes of method and organisation. European states, the European Union and NATO together represent a major technological capability with internationally recognised expertise. However, that capability is fragmented and widely distributed. There is no masterplan or common vision giving a clear lead as to the direction to follow – towards cooperation and integration – to the benefit of all concerned, countries and institutions alike. Each country develops concepts that will give

[49] The same is true in the case of civilian technologies with military applications but which are making few inroads because of the length and slow tempo of defence programming and procurement schedules.

[50] "A Network-Centric Operations Case Study: US/UK Coalition Combat Operations during Operation Iraqi Freedom"; Office of Force Transformation, 2 March 2005; www.oft.osd.mil.

its own "national" companies (EADS France and Germany, Thales UK and SAAB) the edge in those areas where it has a dominant or influential position

94. With funding limited and different priorities, any attempt to standardise becomes risky. Participants sign up to projects and then withdraw according to swings in the political mood and changing priorities at home. The risk is of eventually having a range of European technology demonstrators, simulation laboratories, concepts and systems which are only partially compatible or interoperable and not adequately linked or coordinated.

95. For medium and small countries the question arises as to the choice of model and type of cooperation. This is a strategic challenge given that, in the face of European fragmentation, the United States has the attraction of coherency (Joint Vision) and concepts and technologies tested out under field conditions in the course of recent military operations (Afghanistan and Iraq). Europe's strategic autonomy is not only a matter of having high performance aircraft or decision-making structures in Brussels, but also, in the years to come, the vision and technologies that will provide the basis for network-centric concepts and capabilities.

96. Another very important aspect of the transformation set in train by network-centric concepts is human resource management, issues connected with recruitment and the way those employed are treated. Information superiority is a complex process and is underpinned by a range of sources, automated and human (HUMINT). The management, selection, distribution and network uploading of information can all be done using automated computer systems. However, information selection and analysis are tasks that must be done by people, and likewise the management and upkeep of the automated network and sensors on which information control depends – down to the soldier in the theatre of operations linked at C2 level through his Personal Data Assistant (PDA). Combined joint multinational horizontal networking of systems and people requires well-qualified staff who are properly trained and equipped, as only they can derive maximum benefit from the advantages that network-centric concepts can offer.

97. This is a key issue for the years to come. In the United States, investment in technology and human beings, with priority given to the former, showed, during the 21-day campaign in Iraq, that a force of modest size was capable of beating a numerically far greater adversary on its own ground. Technological superiority compensates for lack of numbers. However, in the stabilisation phase that followed, those fighting on the other side were also able to take advantage of the new technologies (particularly mobile telephones, the Internet and wireless communication networks) to plan and carry out operations against a coalition force which, although of superior standard, was inadequate numerically (notwithstanding local and international assistance) to secure the whole of the territory occupied. This is a lesson to be borne in mind by European armed forces, many of them still in the transitional stage from conscript to professional army (along British or American lines depending on national priorities).

98. Things are becoming more complicated for Europeans, given that budgets are decidedly inadequate to make good all national shortcomings and that medium/high-technology equipment programmes, on which efficiency and interoperability depend, consume a major part of the resources allocated. The trend towards power and forces projection goes hand in hand with substantial volume reductions in equipment and manpower. This produces a drive towards increased cooperation, a beneficial effect manifest in increasing numbers of exercises and manoeuvres of a multinational nature, more cross-country exchanges of experience and officers and the training being developed in such institutions as the NATO College and the EU's new Security and Defence College which opened its doors in September 2004.

99. However, the introduction of network-centric concepts and systems will boost the demand for qualified specialist staff, trained in the use of the new information and communication technologies and able to develop in that field, since already in modern societies there is a "digital divide" between those with access to, and the ability to use computers, the Internet, PDAs, the latest generation mobile telephones and so on (not to mention the specialists in computerised systems, network administrators, systems engineers), and the many others unaffected by or unsuited to join that trend.

100. Network-centric forces in which the traditional "fighter" still has pride of place are extremely dependent on the above types of staff and on many others: intelligence analysts, linguists and even "hackers", the information warfare troopers of the present and future. This highly specialised resource is one also coveted by the private sector of the economy where new ICT/electronic/systems integration, consultancy and economic and technology monitoring firms are a major driving force.

101. European professional and conscript or mixed armies are thus faced with the difficulty of providing enough specialists to service the fighters, in the knowledge that the latter, if they are to be able to use the new systems properly, need to understand them thoroughly and be able to repair them in the event of failure in the field. The "future soldier", at the kernel of a network, is also a manager and administrator. The issue of contract renewal thus becomes a strategic matter, since high-level staff with armed forces training become a favourite target for civilian head hunters, leading to too rapid a turnover of staff (once the initial contract period has ended) or a salary race which the defence sector, pitted against a much more integrated, globalised, networked civilian sector, cannot hope to win.

102. The human factor is thus central to the thinking on the concept of network-centric operations. Absolute confidence in computerised systems and in the automatic responses generated by them is making human beings increasingly dependent on machines, which can prove to be a dangerous choice in an environment where there is an information overload and wide differences over the interpretation of that information that could have direct implications for decision making. Incorrect or wrongly interpreted information, not recognised as such, will inevitably produce "path-dependent" results possibly with extremely serious consequences at every level ("friendly" fire, collateral damage, pointless destruction, tactical and operational failure, for example).

103. European countries, the European Union and NATO, either of their own volition or impelled by the need for interoperability with the United States, are today firmly locked into a process of out and out transformation where network-centric capabilities have a vital role to play. If one thinks of the NATO Response Force or the 2010 Headline Goal, the Allied Command Transformation or the European Defence Agency, the aims are invariably the same: to strengthen and develop European military capabilities in order, either autonomously or in partnership with the United States, to cover the entire range of possible engagements, from peacekeeping to medium and high-intensity conflict. Collective defence, as it exists in NATO or in WEU will soon also be the responsibility of the European Union. Coherence, cohesion and interoperability among Europeans are essential if they are to take that mission upon themselves.

104. Transformation holds out a future that is bright, provided it does not simply boil down to a matter of technology, much of which is not accessible to the majority, is as yet untested and is not currently available even in the United States. It is not technology *per se* that confers superiority, but the use made of it and the exploitation of its potential adds value. It is necessary for the military at large to throw their weight behind these new concepts and to some extent get rid of the divisions between the various armed force branches (air, land and sea) and between national forces. This leads on directly to the importance of the human factor in the whole process. Use of UAVs and robot armies, on land and at sea, is emerging as a multiplier of military power in a network-centric environment, but invariably it is a human being who takes the decision about the timing and the arrangements under which they are deployed.

105. Europe (the European countries of the Alliance and the European Union) is, in its diversity, an almost perfect example of the network-centric concept: decentralised, autonomous, interdependent, interoperable, auto-synchronised, effects-based, and on that account vulnerable. And it is this awareness of its own vulnerability that provides it with its strongest argument for the pursuit of transformation: to make it "a Secure Europe in a better world", while remaining "United in Diversity".

ANNEX

Glossary

1. **Allied Ground Surveillance (AGS):** NATO R&D programme currently still in the design phase, which will provide the Alliance with an aerial battlefield surveillance capability through radar and the fusing of information gathered by other sensors. Initially, the system was to be deployed on manned aircraft only; in a more recent development, the system is being redesigned for deployment on both manned and unmanned aircraft.

2. **Bandwidth**: rate at which data can be transmitted over a given communications circuit – usually expressed in either kilobits or megabits per second.

3. **Bits (bps)**: stands for bits per second, the measure of transmission speed used in relation to networks and communication lines and representing the basic unit of measure.

4. **Bulle Opérationnelle Aéroterrestre (BOA):** the first practical application of network-centric warfare defined by France's Direction Général de l'Armement, consisting of networked foot-soldiers, tanks, terrestrial robots and unmanned aerial vehicles, working together to develop tactical situations, protect one another, cover ground and optimise fire.

5. **Command and Control (C2):** exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the 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.

6. **Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR):** technologies at the heart of modern warfighting. 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.

7. **Common Operational Picture (COP):** single identical display of relevant information shared by more than one command. A common operational picture facilitates collaborative planning and assists all echelons to achieve situational awareness.

8. **Database**: collection of information organised in such a way that a computer program can quickly select desired pieces of data. A database can be thought of as an electronic filing system.

9. **Effects-Based Operations (EBO):** methodology for planning, executing and assessing military operations to attain the effects required to achieve desired national security objectives. It offers an approach to modelling the enemy as a system, or more specifically as a System-of-Systems.

10. **Fibre optic cable**: form of network cabling that transmits signals optically, rather than electrically as coaxial and twisted-pair cables do. Fibre optic cable can transmit clean signals at speeds as high as 2 Gbps and as it transmits light, not electricity, it is also immune to eavesdropping.

11. **Force Transformation**: a process involving large-scale, discontinuous, and possibly disruptive changes in military weapons, organisation, and concepts of operations that are prompted by significant changes in technology or the emergence of new and different international security challenges.

12. **Global Command and Control System (GCCS):** a highly mobile, deployable command and control system supporting forces for joint and multinational operations across the range of military operations, any time and anywhere in the world with compatible, interoperable, and integrated command, control, communications, computers, and intelligence systems.

13. **Global Information Grid (GIG) Infrastructure**: globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and

services, software, data, security services and other associated services necessary to achieve information superiority.

14. **Global Positioning System (GPS):** satellite constellation that provides highly accurate position, velocity, and time navigation information to users.

15. **Grid**: **permits** the identification of ground locations with respect to other locations and the computation of direction and distance to other points when superimposed on maps, charts and other similar representations of the Earth's surface.

16. **Hacker**: one of NCW's greatest threats – a skilful programmer who enjoys the challenge of breaking into other computers with a view to destroying information or introducing a virus.

17. **Imagery**: collectively, the representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media.

18. **Information Technology (IT): a**ny equipment or interconnected system or subsystem of **equipment**, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

19. **Intelligence, Surveillance and Reconnaissance (ISR):** activity that synchronises and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function.

20. **Internet**: An interconnected system of networks that connects computers around the world via the TCP/IP protocol.

21. **Internet Protocol (IP):** protocol governing the routing of data messages, which are transmitted in smaller components called packets.

22. **IP version 6:** one of the transport protocols for digital communications use by the US military that will replace the IPv4 by 2008. This will become the new standard for all transmission through the GIG and for all systems that are part of the Defense Information System Network (DISN) that will interoperate with the GIG enabling to quadruples the size of the address field from 32 bits to 128 bits.

23. **Interoperability**: ability of Alliance forces, and when appropriate, forces of partner and other nations, to train, exercise and operate effectively together in the execution of assigned missions and tasks.[51]

24. **Intranet:** private network based on Internet technologies but confined to use within an organisation, such as a corporation (As opposed to extranet).

25. **Link-16**: a relatively new tactical data link being employed by the United States Navy, the Joint Services, some North Atlantic Treaty Organisation (NATO) nations and Japan. It provides certain technical and operational improvements to existing tactical data link capabilities and some data exchange elements which the other data links lack. It also offers significant improvements, such as jam resistance; improved security; increased data rate (throughput); increased amounts/granularity of information exchange; reduced data terminal size, which allows installation in fighter and attack aircraft; digitised, jam-resistant, secure voice capability; relative navigation; precise participant location and identification and increased numbers of participants.

26. **Link-22:** the next-generation NATO Tactical Data Link, is also referred to as the NATO Improved Link Eleven (NILE). The NILE collaborative project will design a system consisting of a computer-to-computer digital data link for Tactical Data Systems (TDS) equipped ships, submarines, aircraft and shore sites which meet the requirements of the NATO Staff Requirement. The goal of the system is to increase the timeliness of the tactical information transfer and transmission of high priority warning and force orders in a dense and hostile communications environment.

[51] www.nato.int

27. **Modem:** device that enables computer-to-computer communication over a telephone line. When transmitting, the modem transforms (modulates) signals from the digital form required by the computer to the analogue form required by the phone line. When receiving, the modem reverses the action, demodulating the signal from analogue back to digital form.

28. **NATO Response Force (NRF):** its purpose is to provide NATO with a robust and credible high readiness capability, fully trained and certified as a joint and combined arms force able to deploy quickly to participate in the full spectrum of NATO missions wherever required, expeditionary in character and design.

29. **Network:** system that transmits any combination of voice, video and/or data between users. The network includes the network operating system in the client and server machines, the cables connecting them and all supporting hardware in between such as bridges, routers and switches. In wireless systems, antennas and towers are also part of the network.

30. **Network Centric Warfare (NCW):** refers to the combination of emerging tactics, techniques, and technologies that a networked force employs to create a decisive warfighting advantage. It accelerates the ability to know, decide, and act, linking sensors, communications systems, and weapons systems in an interconnected grid.[52]

31. **Node**: location in a mobility system where a movement requirement is originated, processed for onward movement, or terminated.

32. **Octet**: unit of information equal to 8 bytes.

33. **Personal Digital Assistants (PDAs):** portable computers that are designed to act as organisers, note takers and/or communication devices. Due to the small physical size of these devices they often possess the latest and most compact user interfaces such as touch screens, hand writing recognition, or miniature keyboards

34. **Revolution in Military Affairs (RMA):** Dramatic changes in the art of warfare precipitated by rapid technological advances. Exploiting the RMA means not only acquiring fully new systems based on advanced technology but also developing the concepts, doctrine and organisations to utilise the new technologies in a way to dominate the battlefield.

35. **Router**: network device that transmits message packets, routing them over the best prescribed course from one point of origin to a specific destination (route) available at the time. Routers are used to connect multiple network segments, including those based on differing architectures and protocols.

36. **Self-synchronisation:** a form of organisation contributing to dissolve the inflexible hierarchy of the traditional defence. It is of special importance in complex, high tempo situations. Educated and trained mission-assigned units complying with fundamental rules of engagement have therefore the possibility, in the network, to organise themselves in the best way, depending on the situation.

37. **Signals intelligence (SIGINT)**: category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted.

38. **Swarm tactic:** one advantage of NCW is that networked forces consist of smaller units that can travel faster and lighter. All units know the others' locations and if one runs into trouble, other independent units nearby can quickly come to its aid, "swarming" to attack the enemy from all directions at once.

39. **Switch**: network device capable of forwarding packets directly to the ports associated with particular network addresses.

40. **Unmanned Aerial Vehicle (UAV):** powered, aerial vehicle that does not carry a human operator, uses aerodynamic forces to provide vehicle lift, can fly autonomously or be piloted remotely, can be expendable or recoverable, and can carry a lethal or non-lethal payload. Ballistic or semi-ballistic vehicles, cruise missiles, and artillery projectiles are not considered unmanned aerial vehicles.

[52] Department of Defense

41. **Virus**: manmade programme or piece of code, loaded onto a computer without its knowledge, which runs against the user's wishes. Viruses are dangerous because, by duplicating themselves, they quickly use up all the available memory, bringing systems to a halt. Some types of virus are capable of transmitting themselves across networks and bypassing security systems.