SCIENCE AND TECHNOLOGY

175 STC 07 E
Original: English

NATO Parliamentary Assembly

TRANSFORMING THE FUTURE OF WARFARE: NETWORK-ENABLED CAPABILITIES AND UNMANNED SYSTEMS

DRAFT GENERAL REPORT

PIERRE CLAUDE NOLIN (CANADA)
GENERAL RAPPORTEUR*

International Secretariat 14 August 2007

* Until this document has been approved by the Science and Technology Committee, it represents only the views of the Rapporteur.

TABLE OF CONTENTS

I. INTRODUCTION

1. Military transformation and the Revolution in Military Affairs is not as forthright a process as it was perceived only several years ago. The globalisation and the boom of information, computing, networking, satellite and precision technologies all have tremendous implications for the defence and security sector. The extensive use of modern technologies in the offensive campaigns in Kosovo, Afghanistan and Iraq enabled the military to achieve an unprecedented operational tempo and precision, and to win wars in the course of several weeks, instead of years, as was the case in the not too distant past. The high-tech side of military transformation proved to be enormously promising, prompting a number of states to assign a significant part of their military budget to programmes such as Network-Enabled Capability (NEC)[1].

2. The recent experience of allied forces in Afghanistan and Iraq demonstrated, however, that high-tech is not an answer to everything. While new technologies are critical to winning wars, they seem to be ill-equipped to winning peace. These technologies, although helpful in some cases, are not the ultimate answer when it comes to fighting small groups of insurgents or maintaining order in post-conflict areas. Thus, there is an increasing understanding that the process of military transformation should incorporate not only cutting-edge technologies but also focus on counter-insurgency and peacekeeping capabilities. This understanding is expressed in the latest US 2006 Quadrennial Defense Review. These two trends of transformation sometimes can be mutually contradicting. For example, network-enabled and unmanned capabilities can be expected to significantly reduce the need for manpower to be deployed in the areas of conflict, whereas counter-insurgency missions would imply the opposite.

3. While bearing in mind this two-fold nature of military transformation, in this report, the Rapporteur will address the topic of advanced military technology, which is a natural subject for the Science and Technology Committee. This report will particularly focus on two most prominent nascent capabilities – network-enabled and unmanned systems – that promise to revolutionise the way military operations are carried out in the 21st century. The new technologies raise a number of issues of vital importance for policy-makers: how the increased importance of information security will affect the functioning of military alliances? Will these developments lead to a greater synergy of efforts or will they result in an unprecedented technology divide? Will NATO maintain its relevance or will the focus shift towards coalitions of several most trusted partners? Should technology transfer policies become more flexible or tougher? Should the Alliance develop its own network-enabled and unmanned systems, or should it be the exclusive responsibility of member states? Are the new sophisticated technologies instrumental when it comes to fighting terrorism, or do these technologies provide yet another tool for terrorists? How will these technologies alter the military decision-making hierarchy: will decision-making be more effective or more chaotic? Will human control of autonomous war-fighting systems be maintained? Should there be an international convention to address possible proliferation of these technologies? All these questions are of paramount political relevance, and therefore it is crucial that legislators systematically follow the developments of network-enabled and unmanned technologies and do not disregard the issue as a merely technical one.

1. In this report, we use the official NATO term 'Network-Enabled Capability' (NEC), which is also the title of the respective UK programme. Other countries use different names for the same phenomenon: 'net-centricity', 'Network-Centric Warfare', 'Network-Based Defence', 'Network-Centric Operations', etc.

II. NETWORK-ENABLED CAPABILITY

A. THE PROMISE AND CHALLENGES OF NET-CENTRICITY

4. Net-centricity, the military expression of the Information Age, is a relatively new concept, coined and introduced by US Navy Vice Admiral Arthur K. Cebrowski and John J. Garstka, Assistant Director of the US Office of Force Transformation, in their article “Network-Centric Warfare: Its Origins and Future” in 1998. Net-centricity is not merely about sharing information between different branches of the armed forces using modern technology. The virtue of network-enabled capability (NEC) is that it creates an added value by providing all battlespace entities with real- or near-to-real time access to the information exchange system and thus dramatically reduces the ‘fog of war’. The three most prominent experts of NEC, David S. Alberts, John J. Garstka and Frederick P. Stein defined net-centricity as:

> "An information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision-makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronisation. In essence, [network-centric warfare] translates information superiority into combat power".[2]

5. Thus, NEC is about fundamentally improving sensor-to-shooter capabilities (C4ISTAR – command, control, communications, computers, intelligence, surveillance, target acquisition and reconnaissance) that become a critical, rather than supplementary, element of military capabilities. Just like in business, new technologies and better co-ordination of efforts generate “mass-effects” and maximise the efficiency of armed forces. In the Information Age, information is redefining the concepts of mass, manoeuvre, firepower and logistics.

6. The rudiments of NEC have already been tested in Operation Enduring Freedom in Afghanistan and the war in Iraq. However, NEC is still in a nascent phase. According to Terrence Morgan, Director of Net-Centric Operations, Cisco Systems, in today's operational environment, sensor and shooter have too much separation: bandwidth is limited with choke points and interoperability issues, infrastructure is too diverse and complex to support 'plug-and-play', and time to field “new” applications is unacceptably long.[3]

7. In addition to technical issues, NEC requires revolutionary changes in command and control (C2). The traditional hierarchical C2 structure is not flexible enough to deal with a situation when even low-level commanders have access to all relevant information and are in a position to make a decision without waiting for instructions from their superiors.

8. A number of authors also raise negative aspects of net-centricity. For example, Alfred Kaufman from the Institute for Defense Analyses, emphasises the destructive consequences of network centrism, such as:

- a relentless drive for innovation may hurt security
- wishful thinking becomes strategy
- bureaucracy takes over the dynamics of war
- command and control loses its human dimension

---

2. Network Centric Warfare: Developing and Leveraging Information Superiority, by David S. Alberts, John J. Garstka and Frederick P. Stein. – DoD C4ISR Cooperative Research program. 2nd edition, 2000. p. 2.
3. Transformation, Netcentric Defense, Space and Security, by Terrence Morgan, Director of Net-Centric Operations, Cisco Systems. Special Presentation for the members of NATO PA STC. San Jose, California. June 15, 2006.

- machines replace humans
- overwhelming power disdains war diplomacy.

9. Some NATO officials also expressed concern that the increased visibility into lower-echelon activities that network-enabled capabilities provides will encourage senior officers to meddle and micromanage, potentially destroying junior officers' initiative.[4] During the visit of the STC delegation to NATO Joint Warfare Centre (JWC) in Stavanger, Norway, Air Marshall Peter Walker, Director of JWC, admitted that new emerging technologies, such as network-enabled capabilities or unmanned systems, are altering traditional C2 chains, as they allow strategic level commanders to interfere into tactical level operations. The Director of JWC replied that the fundamental task of the Centre is to discourage such practice and to bring top-level commanders out of detail so that they could concentrate on a broader picture and on future-oriented decisions.

B. NEC PROGRAMMES IN THE ALLIANCE

1. The United States

10. The United States is an undisputed global leader and pioneer in developing NEC. The Network-Centric Warfare (NCW) programme is at the heart of the US transformation strategy, as defined in the Joint Vision 2020. According to Former Deputy Secretary of Defense Paul Wolfowitz, "our (US) ability to leverage the power of information and networks will be key to our success".[5] By 2012, NCW should reach full capability, which will include a single network of sensors, deciders and shooters; IP addressable warriors, weapons and sensors; and commanders' shared awareness and knowledge.[6]

11. Major American network-enabled capabilities are:

- *US Secret Protocol Router Network - SIPRNET*. In effect, SIPRNET is the US army's own internet, and the Department of Defense's largest network for the exchange of classified information. It has matured to be the core of US command and control capability. SIPRNET is extremely similar to Internet in that it also uses TCP/IP protocols and standard web browsers to provide access to websites written in standard HTML language. Just like the Internet, it enables communication via e-mails, fora or chat rooms and peer-to-peer connections. However, since the SIPRNET is an obvious target for hostile penetration, a number of strict security procedures are applied. All users must be approved, registered, and passwords must be changed at least every 150 days. A similar but much looser system, the Non-classified but Sensitive Internet Protocol Router Network (NIPRNET), provides seamless interoperability for unclassified combat support applications, as well as controlled access to the Internet. SIPRNET is a comfortable and useful tool, which is highly valued by US military commanders. However, foreign access to SIPRNET is, quite understandably, very limited. Only America's closest allies, the British and Australians, were granted access, albeit temporary and limited, in certain joint missions. Intelligence information on SIPRNET is routinely marked as Secret-Not Releasable to Foreign Nationals (NOFORN). In some cases in Iraq, the British could not even see or copy intelligence data gathered by British operatives themselves, when it fused with the Americans' own data stored on the SIPRNET and marked NOFORN.[7]

---

4. Network-Enabled Capabilities – Issues and Implications, by Dr. Linton Wells II, US Assistant Secretary of Defense for Networks and Information Integration. - Presentation at the 21st International Workshop on Global Security. Berlin, 7-10 May 2004.
5. See Global Information Grid. National Security Agency website.
6. C2 Constellation, by Skip Liepman. - Military Information Technology. Volume 8, Issue 6. 17 August 2004.
7 US Kept Spying Data from Blair, by Sarah Baxter. - The Sunday Times. 1 October 2006

- Global Information Grid (GIG). The GIG system will be the largest information network in the world and the key element of US network-centric capabilities. Based on commercial technologies, it will provide processing, storage, management, and transport of information to support all DoD, national security, and related Intelligence Community missions and functions. GIG capabilities will be available from all operating locations: bases, posts, camps, stations, facilities, mobile platforms, and deployed sites. The GIG will interface with allied, coalition, and non-GIG systems. Next-generation satellites will provide massive amounts of real-time information to platforms and weapon systems deployed on the tactical edge. Every square metre of the globe will have its own IP address, thus enabling effective tracking of all actors on the battlefield. The $34 billion programme should be completed by 2011.[8] Thanks to GIG, deployed American soldiers will no longer be at the mercy of someone remote from the fight determining what information they need.[9]

- FBCB2-Blue Force Tracking. This satellite-based system is credited with creating battlefield picture during the Operation Iraqi Freedom, and enabling US and British armed forces to track each other's and the enemy's positions.

- LandWarNet. Includes all networks of US ground forces - from sustaining military bases to forward-deployed forces. It provides for processing, storing, and transporting information over a seamless network. Its main enabler, the $10 billion Warfighter Information Network-Tactical (WIN-T), will be the backbone communications network for the US Army and is expected to provide enhanced digital C4ISR capabilities that are mobile, secure, survivable and seamless. The first Army unit is scheduled to field WIN-T by 2008.

- FORCEnet is the Navy's equivalent of LandWarNet. FORCEnet, as integrated information technology architectural framework, will link warfighters ashore, at sea and in the air.

- ConstellationNet, the US Air Force counterpart of LandWarNet and FORCEnet, will store and communicate voice, data, imagery and video information and will serve as the interface to GIG.

- Joint Tactical Radio System (JTRS) is a critical communication tool for ground and air forces and a pivotal US transformation programme. JTRS is a class of software-defined radios, intended to replace a massive assortment of conventional military radios that are built to different standards and operate on different fixed frequencies. By introducing a common set of standards, JTRS will considerably facilitate interoperability of joint forces and dramatically increase the amount of data that can be transmitted. JTRS will provide not only voice communication but also instantaneous video and data download and network connectivity. JTRS-equipped troops and platforms would be able to log onto the network much like a wireless computer can pick up a signal and connect to the Internet. However, despite the significant promise of JTRS, the US Government Accountability Office found that a number of related management and technical issues must be overcome. For example, integrating the radio's hardware onto diverse platforms and meeting respective size, weight, and power limitations has been a longstanding challenge that must be overcome.[10]

8. Live GIG. By Tony Skinner. – Jane's Defence Weekly. 25 October 2006.
9. See Network Centric Warfare: Coalition Operations in the Age of US Military Supremacy, by Paul T. Mitchel. – The International Institute for Strategic Studies. Adelphi Paper 385. December 2006.
10. Restructured JTRS Program Reduces Risk but Significant Problems Remain. - US Government Accountability Office Report to Congressional Committees. September 2006.

2. NATO Allies

12. Besides the United States, of all the NATO countries, only the United Kingdom, Germany, France and Italy consider network-centricity a priority in their military transformation efforts. The United Kingdom has the most conceptual approach with its Network-Enabled Capabilities Initiative. Having recently achieved the initial state of interconnection, the United Kingdom expects to reach the stage of "full integration" by 2015 and "full synchronization" by 2025. The UK is also the only Ally that has participated in network centric operations: the British Expeditionary Forces were granted access to exploit American networks during the Iraqi campaign. Examples of British network-centric capabilities include Bowman, Cormorant, DII (Future Deployed) and Falcon digital communications systems; the SKYNET 5 next-generation military satellite communications system; the Watchkeeper UAV (Unmanned Aerial Vehicle) for ISTAR missions; ASTOR ground surveillance system and OPLOC system designed to track personnel on operations.

13. To France, net-centricity is more of an operational than a technological term. France's central network-centric programme is *Bulle Opérationnelle Aéroterrestre (BOA),* the cooperative fighting system concept. The €129 million contract tasked the Thales-led consortium to design and development the TACTIC3 network-enabled architecture and technology demonstrator for close combat in the air-land theatre (infantry, armoured vehicles, unmanned vehicles, unattended or remotely deployed sensors, all networked by a communication and information system). The TACTIC demonstrator will be used for evaluation of the capability gains provided by the BOA concept.[11] France is also developing a cooperative engagement capability project called *Capacité d'engagement multi plates-formes* (CEMP) as well as TSMP multi-platform situational awareness programme. Thales is working on the next-generation command information system SIC 21 and RIFAN (naval aviation intranet network) for the French Navy.[12] Another defence company, *Sagem Défense Sécurité*, is engaged in developing FELIN V1 and SITEL infantryman's communication system.[13]

14. Several years ago, Germany revised its military strategy to include emphasis on out-of-area missions. Germany's network-centric *Netzwerkgestützte Operationsführung (NetOpFü)* programme is a very important building block of its military transformation efforts. NetOpFü aims to provide reliable, relevant and on-time information-sharing for German troops that are in a crisis zone. The Federal Office of Technology and Procurement (BWB) is responsible for procurement of network-capable sensors, effectors and systems. In addition, BWB is tasked to integrate different systems into a "system of systems", thus exploiting synergy effects.[14] Germany is actively working on solving technical challenges with regard to establishing a "Role-Based Common Relevant Operational Picture" (ROBOCROP) which shall provide the leader on the battlefield and the commander at the HQ with the relevant information to enable him to make the right decision in time, avoiding an overload of information. Germany is also fielding the most advanced C2 and battle management systems (FüInfoSys, FAUST, GIATS/DCRC), which comply with NATO Interoperability Standards, in order to enable the German Army to participate in NATO network-enabled operations.

15. The Italian Army has launched the Forza NEC initiative, which aims to have three Army brigades digitised by 2014. The key element of Italy's net-centric forces, the SICCONA system, will combine communications and situational awareness capability with navigation and vehicle data. This system, developed by the Finmeccanica-led consortium, is currently being tested. SICCONA

11. France awards BOA demonstrator contract to Thales, Giat Industries and Sagem Défense Sécurité. – Thales Group Press Release. 8 December 2005.
12. Serving the World's Navies: Thales's Response to the Challenges Ahead. – Presentation by Thales Group at Euronaval 2006. Paris, October 2006.
13. Network Centric Warfare/BOA. - Sagem Défense Sécurité website www.sagem-ds.com/
14. The BWB Role in Transformation. – Military Simulation and Training magazine. February 2006.

will allow battlefield data to be sent from command post to vehicle and then via wi-fi signal to the handheld equipment of individual soldiers.[15]

3. NATO

16. NEC is becoming a buzzword within the Alliance and one of the key elements of its military transformation. The Riga Summit Declaration made a reference to NEC and NEC-related programmes emphasising the need to:

- work to develop a NATO Network-Enabled Capability to share information, data and intelligence reliably, securely and without delay in Alliance operations, while improving protection of our key information systems against cyber attacks;

- [activate] an Intelligence Fusion Centre to improve information and intelligence sharing for Alliance operations;

- [continue] progress in the Alliance Ground Surveillance (AGS) programme, with a view to achieving real capabilities to support Alliance forces.

17. NATO Network-Enabled Capability (NNEC) is being developed by NATO agencies both in Norfolk (ACT Information Superiority & NATO Network-Enabled Capabilities Integrated Capability Team - IS&NNEC) and Brussels (NATO Command Control and Communications Agency - NC3A). The ACT team is preparing a strategic framework and a road map that will modernize joint Alliance capabilities and enable NATO to create a truly networked force, while NC3A is striving to create technical standards and templates for new architectures. Admiral Sir Mark Stanhope, former Deputy Supreme Allied Commander, Transformation, testified that NEC “underpins all of what we're doing [at ACT]”.[16] NATO agencies have prepared the NNEC Feasibility Study which provides the basis upon which the requirements that the Alliance as a whole has to address to achieve a network-enabled capability are pulled together. The remaining challenge lies in enforcement and governance.

18. NEC is particularly critical in the context of the NATO Response Force (NRF), which was declared fully operational at the Riga Summit in November 2006. The absence of joint network architecture might seriously impede the viability of this rotational multinational force and, particularly, its ability to operate with the United States after every rotation. Therefore, the ACT IS&NNEC team is assigned to analyse the differences in each six-month NRF rotation and develop the common core network-centric capability for the Force.[17]

19. Major NATO NEC-related programmes include:

- Alliance Ground Surveillance (AGS). NATO's ambitious $4.24 billion project will include manned and unmanned ISR (Intelligence, Surveillance and Reconnaissance) platforms and will enable Alliance commanders to get a complete, theatre-wide picture of the situation on the ground in real time, and even at night and in poor visibility. Thus, just like NATO AWACS programme provides situational awareness in the air, AGS will provide a common ground picture. Once deployed, AGS should become an essential capability for coalition missions and especially for the NRF. AGS is scheduled to achieve full capability by 2013. AGS will be owned and operated by NATO itself.

15. Italy, Finland, France Focus on C2 Technologies,by Pierre Tran. Defence News. 4 June 2007.
16. Interview with Admiral Sir Mark Stanhope, DSACT. – NATO Review. Spring 2005.
17. IS and NNEC ICT works to develop better interoperability standards, by U.S. Navy Chief Petty Officer Joel I. Huval. – ACT News. 12 January 2007.

- The NATO Air Command And Control System (ACCS) is a €1.5 billion project intended to provide a unified air C2 system, enabling NATO's European nations to seamlessly manage all types of air operations over their territory, and beyond. ACCS will incorporate the most modern technologies, and will enable NATO members to adapt to the requirements of network-centric operations. ACCS will provide an initial operational capability within the next few years.

- Other NATO efforts include the development of the NATO Messaging System (secure and reliable integrated electronic messaging system), standards for software-defined radio, and the Multi-Sensor Aerospace-Ground Joint ISR Interoperability Coalition (MAJIIC – a project of 10 NATO countries designed to develop operational, architectural and technical requirements for collaborative employment and use of coalition ISR assets in support of military mission).

20. Responsible NATO agencies closely cooperate with the private sector through the Network Centric Operations Industry Consortium (NCOIC). Initiated by NATO's HQ in Norfolk, the NCOIC is a unique collaboration of 80 companies that are premier leaders in the aerospace, defence and information technology sectors. The NCOIC aims at keeping NATO abreast of developments in the industry. The primary goals of the NCOIC are to adopt common open standards, share best practices and processes and encourage collaboration, enabling the industry to develop compatible products.

21. Various interoperability committees and fora under the aegis of NATO are usually very productive and constructive. As Keith Hooey, the representative of Canada in some of these meeting, testified to the Committee, national experts usually manage to reach consensus on recommendations for operational procedures, information architectures, and information exchange technologies. The very constructive attitude was most notable among the US participants. However, when the assembled experts agree on how to proceed, it generally means one or more states must change the direction of one or more of its major system acquisitions, at considerable economic penalty. They may agree in principle to change direction, but commitments to a schedule are difficult to extract. This requires political will at the highest levels.

C. TECHNOLOGICAL AND POLITICAL CHALLENGES TO NEC

1. Technological challenges

22. From the technological standpoint, in order to effectively participate in network-centric operations, coalition partners need, firstly, to have the necessary technology and, secondly, to be able to connect to their partners' networks. Even if military commanders were granted significant authority to release pertinent information in a timely manner, they may lack technical means for doing so, releasing what is necessary without opening sensitive non-relevant files. As one study asserted, in coalition operations in Afghanistan and Iraq in 2003, US Central Command (CENTCOM) had to deal with more than 84 different coalition networks, of which only 26 had an acceptable level of security. Under these circumstances, interoperability and information exchange among coalition partners was often sluggish and virtually non-existent.[18] These data-exchange problems, for example, constrained the operational tempo of the British forces by the inability to access US targeting systems such as JSTARS and Global Hawk.[19]

18. Network Centric Warfare: Coalition Operations in the Age of US Military Supremacy, by Paul T. Mitchel. – The International Institute for Strategic Studies. Adelphi Paper 385. December 2006.

19 The NATO Response Force. Facilitating Coalition Warfare through Technology Transfer and Information Sharing. Jeffrey P. Bialos and Stuart L.Koehl. Center for Technology and National Security Policy, National Defence University. September 2005.

23. Responding to these challenges, the United States Defense Information Security Agency (DISA) has recently fielded the Combined Enterprise Regional Exchange System (CENTRIXS), designed to allow the United States to securely and seamlessly exchange operational-tactical information with its coalition and mission partners in Afghanistan and Iraq. CENTRIXS is a combination of multilateral and bilateral networks and it includes 77 participating states. More than 26,000 people use the system at 150 sites worldwide.[20] However, CENTRIXS lacks a comprehensive security system and is not connected to other classified networks. Therefore, in order to transfer information between the national and CENTRIXS environments, additional infrastructure such as terminals and communications links is required.

24. On the strategic-operational level, the US has established the classified "Griffin" network designed to facilitate communication among defence planners using secure e-mail and chat services. Only a handful of states - the closest US partners and those that develop network-centric capabilities - are authorised to access the Griffin. According to Dr. Linton Wells II, the US Principal Deputy Assistant Secretary of Defense (Networks and Information Integration),

> "We need to move beyond present coalition networks like CENTRIXS and Griffin to truly multinational information systems, but this will take hard work both in designing the systems and in constructing the information sharing policies to support them."[21]

25. Connectivity itself is not difficult to achieve. NEC technologies are based on the same standards used in civilian sector. In fact, these technologies are mostly developed not by covert military laboratories, but by commercial companies such as Cisco Systems, Ericsson or Boeing. The US military, and increasingly NATO, use Internet protocols (TCP/IP) for command, control and communications. One major implication, however, is the existence of one dominant player that sets these standards. Just like computer software and hardware companies realise that their products would be worthless if not compatible with Microsoft Windows operating system, so producers of NEC technologies have to adjust to the SIPRNET, which is the national network of the world's leading military power.[22]

26. The NATO C3 Agency, responsible for implementation of NNEC, suggests a service-oriented rather than system-design-oriented approach, i.e., moving from a closed black-box system architecture to a 'system-of-systems' where differently developed systems could plug in and interoperate. This will require a different set of technical non-proprietary standards that remain to be developed. Such an approach will help to diminish the cost for NATO countries seeking to participate in network-enabled operations, as it will not require procurement of completely new equipment. However, some Allies, particularly new NATO members, have a different position: they have a relatively 'clean slate' as their C4ISR technologies are either utterly obsolete or non-existent. These states have to build their communication and information systems infrastructure almost from scratch, thus making it easier to avoid problems of compatibility.[23]

27. Another important NEC-related technological challenge is the growing demand for radio frequencies for military use. The electromagnetic spectrum is the key enabler of NEC and wireless communications are becoming indispensable in modern-day military operations. However, the spectrum of frequencies is a limited natural resource, which needs to be carefully managed and

---

20. DISA Leads Efforts for Multinational Information Sharing, by Miriam Moss. - The Grid, DISA journal. February 2007.
21. Network-Enabled Capabilities – Issues and Implications, by Dr. Linton Wells II, US Assistant Secretary of Defence for Networks and Information Integration. - Presentation at the 21st International Workshop on Global Security. Berlin, 7-10 May 2004.
22. Network Centric Warfare: Coalition Operations in the Age of US Military Supremacy, by Paul T. Mitchel. – The International Institute for Strategic Studies. Adelphi Paper 385. December 2006.
23. In NATO, Technology Challenges Yield to Political Interoperability Hurdles, by Robert K. Ackerman. – Signal, magazine of the Armed Forces Communications and Electronics Association. February 2006.

co-ordinated in order to avoid bottlenecks. The problem is aggravated by the fact that the demand for bandwidth is skyrocketing in the commercial sector as well. The US Department of Defense (DoD) has taken a number of initiatives to tackle this issue by encouraging new spectrum management technologies,[24] and updating its governance rules on the military use of the spectrum. Nevertheless, additional high-level guidance, including the involvement of NATO, is necessary to accommodate the frequency needs of networked coalition forces. According to Paige Atkins, director of the US Defense Spectrum Organization (DSO), the challenge is to find new ways for Allies to share the spectrum: “as the environment gets much more crowded, we have to find new ways of understanding when systems are not using pieces of the spectrum, to be able to more efficiently use them”.[25]

28. Protection of networks is another technical challenge of paramount importance. As information is the key facet of NEC, its security is of critical importance. Digital information can be easily changed, added, deleted or disseminated. The problem of malicious interference, identity fraud or “malicious insiders” poses a serious security threat. Therefore, it is understandable why the increasingly networked US military sector has been alarmed by reports that China is developing a cyberwar capability. According to Pentagon officials, China’s competence in information technology has evolved from defending its own networks to attacking the networks of adversaries.[26] China’s ability to threaten satellite systems, which are critically important to the American military, was prominently displayed in January 2007, when an anti-satellite weapon was used against an aging weather satellite. Thus, the biggest challenge is to find an optimal solution that would permit a seamless flow of information among authorised entities and personnel, at the same time preserving the integrity of the network.

29. There are many technological solutions that are offered in this situation. For example, software can be customised and data labelled to restrict access only to authorised individuals. Furthermore, based on one’s clearance, individuals might have different access rights for reading, posting, editing or forwarding information. The concept of guarded gateways or dynamic firewalls must be vigorously pursued if true operational interoperability is to be achieved. In addition, information can be prioritised in order to avoid the risk of information overload. The development of GIG as an all-embracing ‘system of systems”, made it an attractive target. In order to increase the security of this emerging network architecture, the US National Security Agency initiated efforts to develop an information assurance component of the GIG. Information must be labelled and catalogued using metadata, allowing users to search and retrieve the information required to fulfil their mission under a "smart-pull" and information management model. This requires the GIG to know where the information is posted and to recognize who the user is, regardless of location. System access will be available regardless of location; however, access to information will be restricted based on the threat inherent to that location.[27]

30. While it is important to keep track on the developments of network-protection technologies in the commercial sector, Dr. Linton Wells II points out that it would be a mistake to rely solely on commercial off-the-shelf technologies (COTS) to protect military networks as “market forces are not likely to make software strong enough to withstand dedicated attacks by well-funded, persistent, state-sponsored adversaries. Accordingly, there will almost certainly be a need for

24. One technological solution could be cognitive radios that transmit and receive data “jumping” from one frequency to another, depending on which frequencies are ‘quiet’ and available.
25. Crowded Spectrum, by Peter A. Buxbaum. - Military Information Technology. Volume 11, Issue 1. 1 February 2007.
26. Pentagon: China Developing Cyberwar Capability, by William Matthews. Defence News. 18 June 2007.
27. See Global Information Grid: IA Defence-In-Depth Implementation. – National Security Agency website.

government-only solutions (GOTS) to support those special functions that won't be generated by the marketplace".[28]

2. Political challenges

31. Technical experts can rapidly agree on standards for enabling NEC, but this does not solve a persistent information release problem. According to Mr. Keith Hooey, one could even sense that there is a willingness for commanders of multi-national forces to be more forthcoming of critical elements of information, but they are blocked by policies in many cases. A means for negotiating and distributing release policies in near-real time is required to take full advantage of NEC.

32. High-ranking NATO officials also emphasise the importance of political and cultural aspects of networked interoperability. For example, Mr. Dag Wilhelmsen, NC3A General Manager, stated that the political and cultural arenas pose a greater challenge to NEC than technical architectures and standards. As a solution, he suggested that the NATO C3 Agency could act as "an unbiased coherent agent", assisting states in finding good, workable solutions between national systems and international infrastructures.[29]

33. The political challenge of net-centricity basically comes down to the question of trust between the United States and its allies. As the US armed forces are becoming increasingly network-enabled, the security of its networks might become more important than co-operation with partners. Unless the US has complete trust in its allies it would be reluctant to grant access to its military networks. While Europe is benefiting from American technology in programmes like Joint Tactical Radio System, Global Hawk, MEADS or night-vision devices, the list of critical US NCW-related projects with limited, no-release policy, is also quite extensive and includes programmes such as Future Combat System (FCS), Future Battle Command - Brigade and Below (FBCB2), Blue Force Tracking (BFT), Army Field Artillery Tactical Data System (AFATDS) and Warfighter's Information Network - Tactical (WIN-T).[30]

34. There are indications, however, that the US government is moving towards greater information and technology sharing with its allies. For example, in June 2007, US signed landmark agreements with the UK and France to ease up military technology transfer policy. US officials seem to agree that this policy has been cumbersome and has to be modified. According to L. Gen. Jefferey Kohler, the Director of the Pentagon's Defence Security Cooperation Agency, "there is a recognition that there need to be improvements to the [technology transfer] process". The US aerospace industry association (AIA) is also strongly pushing the government to reform the policy. In a joint statement with its European counterpart ASD, AIA stated that "modernising the US system to make it more predictable, transparent and efficient would boost trans-Atlantic trade, cooperation and interoperability among friends and allies".[31] The experts disagree, however, whether the reform would receive sufficient support in the US Congress.

35. In the unipolar world of *Pax Americana*, the US leaders will be increasingly facing an acute dilemma: while the US will continue to need allies in its military operations for political reasons, the effectiveness of these operations can be compromised by inclusion of other states' forces. In other

28. Network-Enabled Capabilities – Issues and Implications, by Dr. Linton Wells II, US Assistant Secretary of Defence for Networks and Information Integration. - Presentation at the 21st International Workshop on Global Security. Berlin, 7-10 May 2004.
29. In NATO, Technology Challenges Yield to Political Interoperability Hurdles, by Robert K. Ackerman. – Signal, magazine of the Armed Forces Communications and Electronics Association. February 2006.
30. The NATO Response Force. Facilitating Coalition Warfare through Technology Transfer and Information Sharing. Jeffrey P. Bialos and Stuart L. Koehl. Center for Technology and National Security Policy, National Defence University. September 2005.
31. Focus on Cooperation, by Pierre Tran. Defence News, June 25, 2007.

words, the main question for the American policy-makers is whether the US national interests would be better guarded and foreign policy goals better achieved by:

- keeping its global military supremacy unchallenged, although at the expense of losing its partners; or
- building multinational coalitions, but risking its military pre-eminence.

36. Thus, albeit unintentionally, the development of NEC will have serious repercussions for the integrity of the Alliance. The strive for security of relevant information is likely to force the American leaders to opt for *ad hoc* "coalitions of the willing" rather than NATO as a whole. The experience with the War in Iraq has demonstrated that NATO members can have very different philosophies with regard to foreign policy and defence strategy. Therefore, releasing sensitive information to all Allies might seem awkward and perilous from the US standpoint. Officially, the US strategic documents, such as the Quadriennal Defense Review (QDR) or the US National Security Strategy, emphasise the need for the allies. In reality, however, the latest developments induced the then US Secretary of Defense Donald Rumsfeld to state that the US must "avoid trying so hard to persuade others to join a coalition that we compromise on our goals or jeopardise the command structure".[32] As Paul T.Mitchel has put it, NEC "may be painting the US into a very secure digital corner".[33]

37. It has to be noted that other NATO nations also have information-sharing restrictions. For example, Germany has recently provided Tornado reconnaissance aircraft for the ISAF. This is an extremely valuable contribution to support NATO troops fighting Taliban insurgency in southern Afghanistan. However, Germany has put limits on the use and distribution of gathered information. There are technological limitations as well: since the Tornados have no air-to-ground downlink, imagery will have to be downloaded and analysed only after the planes land.[34]

III. UNMANNED SYSTEMS

A. THE PROMISES AND CHALLENGES OF UNMANNED SYSTEMS

38. While NEC and unmanned systems are two different technological developments, there is a great degree of cohesion between them. In a way, emerging drone technology is a physical extension of NEC. Network-centric C4ISTAR systems will increasingly depend on Unmanned Aerial Vehicles (UAVs) as a tool to collect intelligence and reconnaissance data and even to attack targets. Unmanned vehicles, on the other hand, cannot operate without being plugged into the network. Given that unmanned systems tend to become increasingly autonomous, it will be essential for them to be connected to other sensors in the theatre so that they could independently make corrections to their flight path in order to complete their mission. Both NEC and unmanned systems are expected to dramatically reduce the need for deployed troops and increase their survivability.

39. The emergence of unmanned, autonomous and robotic technologies is often perceived as the next wave of technological revolution. The most prominent technology gurus, such as Bill Gates, predict that the world is at the dawn of the age of robots. He compared the current state of robotics industry to that of computers in mid-1970s, when he and Paul Allen launched Microsoft. Mr. Gates envisioned that robotics will open "a new era, when the PC will get up off the desktop and allow us to see, hear, touch and manipulate objects in places where we are not physically present". He also stated that autonomous systems "will be a central feature of security systems."

32. Network Centric Warfare: Coalition Operations in the Age of US Military Supremacy, by Paul T. Mitchel. – The International Institute for Strategic Studies. Adelphi Paper 385. December 2006.
33. Ibid.
34. NATO Seeks More ISR for Afghan Combat, by David Pugliese. Defence News. 4 June 2007.

Microsoft even launched Microsoft Robotics in order to earn a prominent place in the new field, which is expected to grow ten-fold by 2025.[35]

40. From a technological standpoint, there is an important difference between “remotely-piloted” and “autonomous” systems. While every move of the remotely-piloted (or “uninhabited”) vehicle is remotely controlled and guided by a trained officer, autonomous systems (or “drones”) are able to perform various tasks, including obstacle avoidance and situation assessment, with minimal or no intervention from a remote human operator. As the experts of BAE Systems, the largest European defence company, testified to the members of the STC during the Sub-Committee visit to London, autonomous systems have clear advantages over remotely-piloted ones, as they better react to changing environment and never get tired or bored. The challenge is, however, how to programme an autonomous vehicle in a way that it would change its course when confronted with unforeseen obstacles, but would still continue to execute its mission. One of the solutions is defining an aerial ‘corridor’ within which a drone could have liberty to alter its trajectory. The BAE Systems experts noted that the United States is clearly in the lead when it comes to developing and especially fielding the remotely-piloted vehicles, while in R&D (Research & Development) of autonomous systems, Europe is rapidly catching up. BAE Systems' Corax UAV, for example, is fully autonomous and has demonstrated its reliability. It also has to be noted that not only aerial systems are going autonomous. Israel recently introduced a system called “See-Shoot” along its 60-km border with Gaza. This system – consisting of sensors and gun turrets – will initially be controlled by humans, but eventually will operate autonomously.[36]

41. Unmanned systems are further classified according to the medium (air, ground, water or underwater) they operate in. Unmanned aerial systems (UAS) are by far the most developed category, which is already widely used in military operations. UAS are remotely-piloted or self-piloted aircraft that can carry cameras, sensors, communications equipment or other lethal/non-lethal payloads. For decades all kinds of remotely piloted aerial vehicles have been called UAVs (Unmanned Aerial Vehicle). However this term hides the fact that these aircrafts actually need ground control stations, satellites links, and communications facilities. The term Unmanned Aerial Systems reflects better the complexity of the system as a whole.

42. At first glance, UAS have many advantages:

- First and foremost, unmanned systems save lives by removing pilots from the cockpit. UAS are expected to take over the so-called 3D (dull-dirty-dangerous) missions. The use of ground or underwater drones is already widespread in demining operations.
- Leaving some troops at home yields clear logistical benefits. Equipment and manpower does not have to move forward. This reduces the amount of lift, lodging, catering and security forces needed to support troops in the theatre.
- The price constitutes a strong incentive too. A F16 fighter aircraft costs US$ 30 million, while a MQ-9 Reaper, the latest US combat drone (UCAV) with a payload capacity approaching that of the F16, costs approximately US$ 7 million. Moreover, UCAV could be a cheaper alternative to skyrocketing costs of some fighter programmes in which NATO member states are involved (For instance one F35 Joint Strike Fighter costs US$ 100 million and a F22 Raptor US$ 200 million while the estimated costs of X-45 UCAV is US$ 40 million.)
- Their long endurance is also an asset. Close air support aircrafts generally orbit 30 minutes over the battlefield before having to leave for refuelling. In comparison, a MQ-1 Predator could fly as much as 24 hours over the target area. Nonetheless, these aircrafts do not have air-refuelling capabilities, and are still extremely slow, needing more time to reach their mission area.

35. A Robot in Every Home, by Bill Gates. - Scientific American. January 2007.
36. Israel’s Robo-Shooters, by Barbara Opall-Rome. Defence News. 4 June 2007

- UAS can be updated more frequently and in reasonable cost, thus making them much more flexible and attractive than manned aircraft when it comes to meeting new emerging threats. UAS have already proved to be effective against asymmetric threats. For example, the US has developed tactical UAVs called BUSTER, weighting 1.5 kg. Soldiers in missions can carry these systems in their bags and launch them to get extraordinary situational awareness in the area.[37]
- Finally, removing humans from the cockpit opens the gates for technological innovations that were previously unimaginable. Indeed, the presence of humans puts very strict limitations on the size, shape, speed, altitude and many other technical characteristics of an aircraft.[38] Without these limitations, engineers can create machines that would change our understanding of what an aircraft can do and it could look like. Unmanned systems that exist today range from miniature Wasp, which weights less than 225 grams an is only 20 cm long, to Global Hawk, weighting more than 14 tons and being 15 meters long.[39]

43. Nevertheless, serious pitfalls command attention. First of all, the massive number of UAVs in congested skies dramatically complicates air traffic control. Because altitudes below 3000ft are usually crowded with helicopters, low-flying aircrafts and "blind" UAVs, crashes can occur and reportedly occurred at least three times in Afghanistan since the war operations began. According to a Congressional Research Service Report, "the current UAV accident rate is 100 times that of manned aircraft".[40] High UAV accident rates even forced the US military to put inscriptions in Arabic written on their fuselage of UAVs fielded in Afghanistan, saying that a bounty will be offered if lost vehicles are handed back to their owners. Equipping UAVs with collision avoidance system or transponders is impractical for any but the largest. As a consequence they do not meet civilian regulations and therefore would not be allowed to fly in civilian airspace. Hence, detecting and avoiding airborne objects is the most pressing and technically challenging task for engineers.

44. There is a serious danger of UAVs being used as a terrorist weapon. Being in many ways similar to cruise missiles and capable of flying at low altitudes, they make ground control systems unable to detect intrusion of a hostile UAS, particularly the small ones. Hypothetically, hostile groups could either convert an anti-ship cruise missile into one capable of flying over land or convert a small aircraft into an armed UAV. According to the Director General of Intelligence for Canada's armed forces, terrorist groups have already purchased ultra-light aircraft and hang-gliders.[41]http://www.nti.org/e_research/_-_fn5 Furthermore, the existing multinational non-proliferation and export-control regimes seem to be ill-equipped to handle UAV transfers. According to prominent defence analyst Dennis Gormley, unarmed UAVs can be transformed into armed ones simply by changing their payload, meaning that an unmanned UAV purchased for one stated purpose could easily be converted into a weapon.[42]

B. THE DEVELOPMENT OF UNMANNED CAPABILITIES IN THE ALLIANCE

45. Military UAS have been used in reconnaissance and intelligence-gathering role since the 1950s, and more challenging roles are envisioned, including combat missions, detection of WMD

37. Unmanned Aircraft Systems: Refocusing the Integration of Air & Space Power, by Gen. Tom Hobbins, Director of the JAPCC. NATO's Nations and Partners for Peace. Volume 52. II/2007.
38. The Evolving Capability of UAV Systems, by Prof. Ian Poll. NATO's Nations and Partners for Peace. Volume 52. II/2007.
39. Unmanned Aircraft Systems: Refocusing the Integration of Air & Space Power, by Gen. Tom Hobbins, Director of the JAPCC. NATO's Nations and Partners for Peace. Volume 52. II/2007.
40. Unmanned Aerial Vehicles: Background Issues for Congress, by Elizabeth Bone and Christopher Bolkcom. – CRS Report. April 2003.
41. Unmanned Air Vehicles as Terror Weapons: Real or Imagined? by Dennis M. Gormley. – Issue Brief, Nuclear Threat Initiative. July 2005.
42. Deadly Arsenals. Nuclear, Biological, and Chemical Threat, by Joseph Cirincione, Jon B. Wolfsthal and Miriam Rajkumar. – Carnegie Endowment for International Peace, Washington D.C., 2005.

(Weapons of Mass Destruction), emergency supplies delivery, etc. UAS manufacturers even began working on civilian applications, such as protection against natural disaster, maritime surveillance and forest fire detection.

46. Nonetheless, explosive interest for unmanned aircrafts has been slow to come. In the early 1990s the United States DoD sought UAS to satisfy surveillance requirements in close range, short range or endurance categories.[43] Close range missions were defined to be within 50 km and performed by man-portable micro UAS at the platoon/section level. “Short Range” was defined as within 200km, the range of Tactical UAS (TUAS), the most commonly used. Finally strategic UAS took on the endurance missions in either HALE mode (High Altitude Long Endurance) or MALE mode (Medium Altitude Long Endurance). With their stealth, speed, payload, price, sometimes auto-repair abilities, autonomous strategic UAS are offering the most tempting prospects for air warfare. Strategic UAS may have yet to grow past their infancy, but their long-term potential should not be underestimated.

47. By the late 1990s, technological thresholds were crossed and UAS were no longer considered to be toys that could easily find their place in a remotely-controlled model airplanes enthusiasts’ show. They became ‘must have weapons’ for all those wanting-to-be modern armies. The unmanned systems are rapidly becoming an increasingly important part of the armed forces, particularly that of the United States. According to the US Defense Department's "Unmanned Systems Roadmap 2005-2030" study, “unmanned aircraft have matured to the point where one no longer needs to ‘look for niche missions’… Instead of asking, ‘Can we find a mission for this [unmanned aircraft], one will ask “why are we still doing this with a human?”. Gen. William T. Hobbins, the commander of US Air Force in Europe, asserted that from the year 2000 to 2010, unmanned aircraft are expected to grow from 4% of total US funding for all aircraft to 31%.[44] The US Army alone plans to have 10,000 UAS by 2011, compared with around 1,200 today.[45]

48. Consequently, a technology spillover is bound to come: nowadays 32 countries are developing more than 250 different models of UAV; customers across Europe, the Middle East, North Africa and Asia are expected to capture nearly 40 percent of the global market. Currently, 17 NATO countries have more than 25 operational models of aircraft, with more than 3,600 operational unmanned aircraft in NATO, of which approximately 3,000 (15 models) are owned by the United States.[46] As an attempt to catch up with the US, several European countries, led by France, launched the multinational EuroMALE UAV initiative in 2002. However, after initial enthusiasm, European countries failed to elaborate a joint approach with regard to technological requirements for these UAVs, and chose to concentrate on their national UAV programmes.

49. The issue of unmanned systems appeared on NATO’s agenda in 2002, when a NATO Standardisation Agreement (STANAG) for Unmanned Aerial Vehicles was published. In addition, NATO countries have committed to acquiring HALE or MALE systems in accordance with the Prague Capabilities Commitment. Acquisition of Global Hawk UAV is also envisaged in NATO’s network-centric Alliance Ground Surveillance (AGS) programme. These initiatives are very significant, because in recent years the Alliance encountered serious difficulties recruiting unmanned aircraft for reconnaissance purposes from member states. According to the NATO

43. L’évolution des programmes de drones de combat aux Etats-Unis à l’aune de l’UAS Roadmap: quelles conséquences doctrinales et industrielles à l’échelle transatlantique, by Alain De Neve - Cahiers du RMES, Vol. 2, No. 2, Winter 2005.
44. COMUSAFE: unmanned aircraft key to future decision superiority, by Capt. Elizabeth Culbertson, US Air Forces in Europe Public Affairs. – Air Force Print News. 19 October 2006.
45. See Unmanned Aircraft Systems Roadmap 2005-2030. – Office of the Secretary of Defence. Washington, 2005.
46. Unmanned Aircraft Key to Future Operations, General Says. - by Capt. Elizabeth Culbertson, US Air Forces in Europe Public Affairs. – Air Force Print News. 20 October 2006.

study, generated by the Joint Air Power Competence Centre (JAPCC), NATO's premier aerospace think tank, NATO needs approximately 50 HALE and 20 MALE aircraft. While there seem to be enough aircraft in NATO to fill these needs, in reality things are somewhat complicated. Firstly, the United States is the only country that has HALE UAVs. Other Allies, despite the Prague Capabilities Commitment, are not actually acquiring these capabilities. As for MALE, technically these aircraft exist, but, as NATO is not the only "customer", these assets are not usually available when needed. According to one NATO official, UAV access for the Alliance in Afghanistan is merely "intermittent".[47] In addition, NATO lacks appropriate ground control and C2 systems and it does not train personnel on how to interpret data from UAVs.[48]

50. In order to tackle these problems effectively, JAPCC experts suggests that NATO:[49]

- establish a body that is responsible for all NATO UAV-related activities;
- procure its own unmanned systems to ensure that these systems would be available when needed in NATO operations;
- encourage procurement of HALE UAVs by US NATO allies;
- incorporate unmanned systems into its C4ISTAR and network-enabled capabilities;
- develop a clear policy with regard to combat UAVs, including defence against enemy UCAVs.

51. Procuring NATO's own UAV fleet, in a similar way to the manned AWACS aircraft, might seem like an attractive option, but it would be extremely difficult to implement, as NATO countries prefer to pursue their own defence programmes. According to Lt. Gen. Hans-Joachim Schubert, Executive Director of JAPCC, "the reality is that nations are sovereign and have their own programmes. If you are looking at acquisition then the tendency in Europe is quite clear". Therefore, NATO's approach focuses on the integration of communications standards and control methods rather than on platforms.[50]

52. The question whether NATO should procure unmanned combat vehicles (UCAVs) is a controversial one. Currently, only the United States has operational UCAVs. US Predators armed with Hellfire missiles have been used in Afghanistan and Iraq to destroy Al-Qaeda or insurgency-related targets. CIA-controlled Predators also hit headlines in November 2002, when this unmanned aircraft killed six suspected Al-Qaeda terrorists in Yemen.[51] The Europeans also have started to look into UCAV development or procurement options, for instance, the French-led multinational Neuron UCAV project. However, the European efforts are seem to be rather sluggish, possibly due to the controversy of using semi-autonomous machines as instruments of killing. Nonetheless, moral considerations rarely succeed in stopping technological progress, and it is likely, as predicted by Gen. Wolfgang Schneiderhan, Chief of Staff of the German Bundeswehr, that UCAVs will "form an essential part of airpower in the 21st century".[52]

53. The issue of bandwidth limitations is also extremely acute for unmanned systems, since they are more dependent upon wireless communications than manned systems. For example, as the NATO study notes, frequency conflicts caused British forces to lose connection with their Phoenix UAV, thus putting British ground troops in jeopardy.[53] Furthermore, remotely-controlled aircrafts need totally secure connections. These connections do not always exist: many links with UAV were lost because of the so-called 'electronic fratricide' (interference from friendly sources). NATO

47. Plotting a Course, by Robert Wall. - Aviation Week & Space Technology. 4 December 2006
48. See The Joint Air Power Competence Centre Flight Plan for Unmanned Aircraft Systems in NATO.
49. Ibid.
50. Interview with Lt. Gen. Hans-Joachim Schubert. – Jane's Defence Weekly. 26 October 2006
51. UCAV Update. Edited by Luca Bonsignore. NATO Nations and Partners for Peace. Volume 52. I/2007.
52. UV's – an indispensable asset in operations, by Gen. Wolfgang Schneiderhan. NATO Nations and Partners for Peace. Volume 52. I/2007.
53. Plotting a Course, by Robert Wall. - Aviation Week & Space Technology. 4 December 2006

experts suggest dedicating a certain part of the bandwidth spectrum specifically for UAV use.[54] Frequency issues are also extremely important when it comes to discussing the feasibility of unmanned ground vehicles, which are expected to carry out a number of tasks, including reconnaissance and surveillance, demining and transportation. However, the guidance of these vehicles becomes problematic when operating in dense urban landscape where concrete and steel buildings impede radio communications.[55] The solution usually presented to reach full interactive effectiveness is proper integration into "network-centric warfare". If the United States is on the brink of this, European armies are clearly lagging behind. One should stress that this will extend the technology gap between the two shores of the Atlantic and threaten the capacity to mount complex joint operations.

54. NATO has created a working group to address the issue of developing standards for unmanned ground vehicles. Respective STANAGs, due to be adopted by 2008, will seek to facilitate interoperability among the robotic combat devices of different NATO and partner countries. As Frank Schneider, chairman of the NATO working group, put it, these STANAGs "should enable a French high-resolution camera to be plugged into a Swedish robot and to communicate the data to another robotised military vehicle, for instance." The EU's European Defence Agency (EDA) goes even further than suggesting mere standardisation. EDA pushes European national defence agencies to jointly pursue critical robotic technologies and pool assets.[56]

IV. CONCLUSIONS

55. The development of network-centric and unmanned systems raises questions that are far greater than purely technological ones. The ability to remotely detect, analyse, target and attack elements of the battlefield and instantly share information requires a substantial review of existing military doctrines and philosophy. The actual consequences of these trends can only be guessed. For example, network-enabled capability will allow strategic leaders, up to commander-in-chief, to make decisions even on a tactical level. On the other hand, commanders on the ground will have full situational awareness and will be able to act without instructions from their superiors. How these two contradictory trends will interact remains to be seen, but it is obvious that the traditional hierarchical decision-making method will change profoundly.

56. Net-centricity and unmanned systems are already substantially contributing to the increasing military superiority of NATO Allies, thus saving lives of our soldiers. The Rapporteur urges NATO parliamentarians to consider the promise of these technologies when it comes to discussing defence budgets, force structure, acquisition and technology transfer policies in their national parliaments.

57. However, these systems should not be seen as a panacea of all problems. While some enthusiasts, such as Robert Finkelstein, a professor at the University of Maryland's School of Management and Technology, predict that "well before the end of the century, there will be no people on the battlefield",[57] there is an equally strong tendency to emphasise the importance of human and cultural factors that are necessary to win the hearts and minds of population. Using unmanned (and especially autonomous) systems as combat vehicles also raises acute moral issues.

54. See The Joint Air Power Competence Centre Flight Plan for Unmanned Aircraft Systems in NATO.
55. Multinational Robots, by Brooks Tigner. Defence News. May 29, 2006.
56. Ibid.
57. War of the Machines, by Yuki Noguchi. – Gulfnews.com. 27 February 2004.

58. Although the political side of these problems, discussed in this report, is the most relevant one, additional efforts are also necessary to encourage development of common technical standards and protection mechanisms both for networks and unmanned systems. The issue of bandwidth limitations needs to be effectively addressed on the NATO level.

59. Developing an effective information-sharing arrangement among coalition partners is of particular importance in the Information Age. Some authors believe it is impossible to overcome the problem net-centricity poses to effective functioning of military alliances. According to Paul T. Mitchel, “seamless interoperability will be impossible. Information is simply too central to the competitive advantages offered by NCW to be jeopardised by automatic disclosure”.[58] However, if the political will was there, NATO countries could agree on a workable solution. As Gen. Harald Kujat, chairman of NATO's Military Committee, has put it, “if you can't operate together, you not only get less efficient, but you risk mission failure and put soldiers' lives at risk. We shouldn't be a coalition of the willing, but a coalition of the interoperable”.[59]

---

58. Network Centric Warfare: Coalition Operations in the Age of US Military Supremacy, by Paul T. Mitchel. – The International Institute for Strategic Studies. Adelphi Paper 385. December 2006.
59. The Collection of Statements - The Joint Air Power Competence Centre website.