EXTRACT FROM THE NEC VISION

EU NEC VISION REPORT

Prepared by the euronec consortium:

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

1 European Union (EU) institutions and Member States (MS) conduct military operations and civilian missions following the Common Security and Defence Policy (CSDP) by exploiting the full range of civil and military instruments. Information and intelligence is a key requirement and a valuable enabler for successful CSDP operations.

2 Ongoing efforts are underway in the EU, in Member States (MS), in North Atlantic Treaty Organisation (NATO) and in industry in order to develop Network Enabled Capabilities (NEC) for facilitating better access and exploitation of intelligence and information. The EU NEC concept has been developed by the EU for describing the potential of NEC for CSDP and for adoption of a Comprehensive Approach (CA) in EU-led Crisis Management Operations (CMO).

1.1 DOCUMENT SCOPE AND PURPOSE

3 The vision is a high level document to be used as reference book for the EU NEC implementation. The vision provides overarching, simple and easily understandable descriptions of the drivers, key capabilities and benefits related to EU NEC implementation in support of CSDP.

4 The NEC Vision document describes the desired level of achievements (WHAT is the expected result) while the Roadmap document describes the concrete steps necessary to implement the Vision in the specified time frame (HOW to get there).

5 The NEC Vision is ultimately an expansion of the NEC Concept into more details.

1.2 DOCUMENT OUTLINE

6 The EU NEC Vision document is divided in the following parts:

- EU NEC Background - describes the background of EU NEC in operational terms as well as giving the political background.
- EU NEC Scope - sets the scope of the vision in terms of time frames and operational context.
- EU NEC Principles gives the principles behind the vision
- EU NEC Overall Vision – describes the vision from an overall perspective taking multiple aspects into account.
- EU Network Enabled Capabilities – describes the vision in terms of operational capabilities.

7 The following EU NEC Vision document annexes have extended descriptions giving a deeper understanding of the EU NEC Vision and the Comprehensive EU CSDP Wide Architecture (CEWA).

- Annex A – Operational Perspective: describes some of the operational aspects of NEC in more detail
- Annex B – Services and Capability Perspective: describes the role of services and capabilities in EU NEC in more detail.
- Annex C – Core EU Net Enabled Services is a more detailed description of Core EU Net Enabled Services.
- Annex D – Information Assurance describes NEC aspects of Information Assurance in more detail.
- Annex E – Network Enabled Planning: describes Network Enabled Planning in more detail.

- Annex F – EU NEC Logistics: describes NEC aspects of Logistics in more detail.

1.3 REVISION HISTORY

Issue	Responsible	Date	Description
0.2	Lars Schylberg	2009-11-16	Draft Vision report delivered to EDA 2009-11-16.
0.5	Lars Schylberg	2010-05-17	Draft Vision report delivered to EDA 2010-05-17
0.51	Lars Schylberg	2010-05-18	Draft Vision report delivered to EDA 2010-05-18
1.0	Lars Schylberg	2010-07-28	Final version report delivered to EDA 2010-07-28

2. EU NEC BACKGROUND

8 This section gives the background for the EU NEC vision.

2.1 INTRODUCING NEC

9 In everyday life, computers and Information Technologies (IT) related to Communication and Information Systems (CIS) directly impact human activities. Every human benefits individually and collectively from the technological breakthroughs in IT. These changes add efficiency to:

a. administration in the civilian domain,

b. economy and business,

c. political, social, security or even defence domains.

10 Almost all individuals use IT tools and devices e.g. cell phones, laptops, notebooks and personal computers (PCs), for creating, modifying, and exchanging information contained and managed in CIS. This trend felt by everyone, is even more pervasive within the younger generation, "Born with a cell phone in one hand and a laptop in the other". This generation already lives in a Net Enabled world (Web 2.0).

11 CIS are global, available from everywhere and provide huge benefits for their user communities. Twitter™, Google™, Facebook™, stock exchange tools and the so called "web services" bring users closer together and allows collaboration within the virtual world, bringing more benefits to the users through collaboration and information sharing. These new technologies provide people with the capability to be better informed, more aware, to make well informed decisions, and to act more efficiently.

12 IT tools are becoming more and more mobile, smaller, smarter, and provides the users with the capability to hook into a network of information whenever they need and wherever they are.

13 Communications and Information Systems (CIS) domains are becoming more and more network enabled and provide by default Network Enabled Capabilities (NEC). The access to network enabled capabilities authorizes a level of interaction between users, user groups and other systems on the network. This level of interaction consists of the ability to:

a) Conduct cross domain interactive information manipulation;

b) Share applications and databases;

c) Conduct complex media exchange;

d) Conduct simple electronic exchange;

e) Conduct manual gateway.

14 NEC translates also a shift from a material world where human activities were targeted towards the creation and provision of material assets, to a virtual information world[1] where human activities create and provide information and knowledge in order to make informed and coordinated decisions. The human tends to use information as a multiplier interface for acting on real things and therefore achieve enhanced operational effects.

15 Implementing NEC means that CSDP operations and missions achieve:

a. Better Knowledge: through easy and complete information sharing,

b. Faster Decisions: through high speed networks, sense and respond mechanisms,

[1] This shift could also be referred as material age to information age.

c. Improved Awareness: through permanent connectivity, publication for users and web engines.

16 Within an NEC environment the average human achieves more output, receives more accurate information and is capable of making the right choice and taking the right action, in his private, public or professional life.

17 NEC is perceived predominantly through technology innovation and the application of technology. However although technology is an obvious element of NEC it is not the only driving factor. Information, cultural and human aspects deserve to be taken into consideration and are required to address NEC through People, Information and Technology dimensions (PIT) which are shown in figure 2-1. Assessing NEC capabilities against PIT dimensions helps characterising the change, in particular

a. Feeling and identifying the change as it happens
it is detected more by technology than information and people aspects,

b. Capturing the information which drives the change:
and is the main subject of NEC,

c. Defining the people aspects embracing human and cultural elements of the change:
The cultural aspects are the most important and effective factors for the success of NEC implementation.

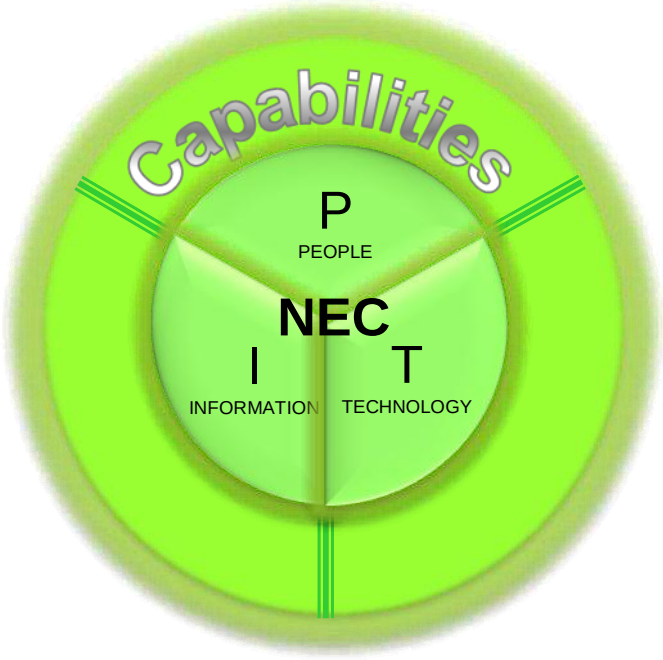

Figure 2-1: EU NEC capability dimensions (People, Information, Technology)

18 Change is unavoidable, especially because of IT progress. All EU activities will be impacted and the European actors must seize the opportunities that NEC will provide, in order to keep pace with change. Adopting NEC will require careful management of capabilities, acquisitions, systems and many other elements from the European Member States. This management demands a reference repository as a pre-requisite for effective implementation. Using strategic reference documents would facilitate adjusting NEC to deliver CSDP and conduct CMO specifics.

2.1.1 CURRENT SITUATION AND FUTURE ORIENTATION

19 Currently the structures for CMO and missions appear more to co-exist than to be integrated. The Information Exchange Requirements (IER) studies ref. [30] reports that "Military Standard Operating Procedures (SOPs) often make statements like 'the Operations/Force Commander is responsible for XYZ' or 'the activity is conducted 'in close coordination with XYZ' without clarifying who is actually conducting the activity and how[2].

20 The current situation can be summarised by the co existence of a military process and a civilian process for crisis management. CM supports the following phases:

a. **Prevention** includes those measures aimed at impeding the occurrence of a disaster/crisis or preventing such an event, having any harmful effect on a community. Prevention should reduce the risk to life and property in the pre and post-disaster environments. This is achieved through regulations, local ordinances, land use and building practices, as well as by means of mitigation projects that reduce or eliminate long-term risk from hazards and their effects.

b. **Preparation** consists of actions taken when disaster/crisis is anticipated or impending in order to ensure a rapid and more effective response. Unlike prevention and mitigation measures, preparative actions are generally short term but also include training, collaboration between organisations, and exchange of experts and personnel.

c. **Response** relates to the emergency operation activities conducted during the impact of a disaster/crisis and the short-term aftermath. The main emphasis put on the saving of human life but it also encompasses the protection of assets, the supply of vital goods and services, and the protection of the environment. Public warning can be classified as a response measure, whereas early warning instruments could either be considered as part of the preparation phase or the response phase.

d. **Mitigation** comprises all actions designed to reduce the impact of disasters/crisis. This is achieved through risk analysis, which results in information that provides a foundation for mitigation activities that reduce risks and protect citizens and economic interests.

e. **Recovery** is the process by which communities return to a normal level of functioning. In the initial stages of this process, the emphasis is on the restoration of basic services and facilities. However, in the longer term, the impact of reconstruction is crucial; agencies involved at this stage aim to ensure that vulnerabilities are reduced without simply reproducing the existing risk elsewhere. This phase also includes actions to restore the physiological, psychological and social health of victims.

2.2 EU NEC CONCEPT FOR CSDP

21 The “EU concept for NEC in support of ESDP” ref: [3] defines NEC for CSDP as follows :

“The ability to shape a cohesive environment for a comprehensive approach and for unified effort of civilian and military entities and actors at all levels in EU led Crisis Management Operations, through informed and timely decision making and coherent execution based on the seamless and efficient sharing and exploitation of information by competent personnel, properly tailored processes and developed networks”.

[2] IER Study Methodology – Final Report (EDA 08-CAP-001).

22 This document uses EU NEC to refer to network-enabled capabilities for crisis management operations following a comprehensive approach:

a. EU NEC refers to NEC for specific CSDP purposes and EU-led CMOs and missions. Its benefits and constraints will deal with mitigation, information sharing, decision making, awareness and effective and adequate actions for de-escalating crisis conditions,

b. EU NEC refers to the capabilities resulting from new technologies for CIS in general and its associated benefits in terms of information and human factors.

23 The Vision reflects the shift to an information centric paradigm in terms of :

a. Human and cultural adjustments maximising the use of information and technological advances and achieving more effective CSDP CMOs;

b. Information challenges to be addressed for better and faster decisions and for enhanced effects during CMO;

c. Technical opportunities impacting CSDP and CMO;

24 The ratification of the Treaty of the EU entailed the establishment of the High Representative for Foreign Affairs & Security Policy (HR/FA & SP) and of the European External Action Service (EEAS). These changes provide an opportunity for implementing EU NEC under a unique authority and in a coherent way. This new situation is expected to facilitate the implementation, the funding and the governance of EU NEC.

2.3 GENERAL BENEFITS OF NEC IMPLEMENTATION

25 The vision for the EU NEC may be captured in the following statement ref. [3]:

> *The high level operational concept for EU sponsored CMO is to conduct missions with highly responsive, well integrated and flexible elements, consisting of civilian and/or military elements, that have assured access to and freedom to operate effectively over the entire spectrum of EU missions. Civil/Military organisations must be able to thrive upon innovation in the field, confident that the actions they take will be intuitively consistent with the strategic and operational objectives. The aspiration is that NEC provides the ability to support effectively the execution of EU operations, taking into account EU specificities, and will become a dominant characteristic of future EU Operations and Missions.*

26 The degree of interoperability, compatibility and network linkage that this implies will need to be implemented in a gradual and evolutionary process - and will involve constructing over time a comprehensive federation of existing and future systems as part of a gradual process based on common information sharing approaches and agreed objectives. NEC must remain user oriented and satisfy user requirements.

27 **Activities**

28 The IER study ref. [30] describes the EU led CMO as a combination of the following activities:

a. Conduct Routine Activities

b. Plan EU led CMO

c. Conduct EU led CMO

   i. Conduct Activation of EU led CMO

d. Conduct Deployment

e. Conduct Redeployment

f. Evaluate EU led CMO

29 These activities are improved by EU NEC implementation. EU NEC provide a cross domain support and concern the following activities that can place before, during and after an operation and can exist to various degree:

a. Planning
b. Monitoring
c. Command and Control (C2)
d. Situation awareness
e. Consultation, briefing and decision support
f. Workflow supporting staff activities

30 By adopting a NEC approach to CMO a number of benefits can be realised.

31 **Advantages**

32 One of the main advantages of implementing NEC is to reduce the constraints on users. NEC has the ability to provide a significant step change in the conduct of CMO in connectivity and ability to exploit applications, services, and data across the operational and business space. A main theme is therefore:

The right information to the right user at the right time to enable the right decision and to achieve the right outcome

33 NEC frees the users from the constraints of operations: space, time and expertise are valuable fields of analysis.

34 **NEC reduces the dependency on space and location:**

35 CMO are joint and often expeditionary in nature. They are based on a dialogue between the deployed detachment and the home base exploiting the reach back concept. Reach back is a concept by which a forward element is kept as small as possible, thereby supported in its actions by a home base support desk of experts including contributing organisations and knowledge databases, available 24/7. Reach back supports resource saving, instant information sharing and synchronisation of the elements involved in crisis management operations. NEC implementation for CMO facilitates:

a. More agile deployment capability;
b. Co-location and the ability for individuals to act in the virtual space and to overcome time and space constraints.

36 **NEC increases the ability to work in parallel:**

37 Operation planning, Command and Control (C2) and all tasks related to crisis management such as decision making, information collection, dissemination and reception of communications, orders and reports are based on a specific activity rhythm, the so called "battle rhythm" in a military operation. EU NEC provides the end-users at every level with the ability to conduct activities during crisis management at their own pace and to synchronise information with peers, subordinates or superiors in a transparent way. This capability is provided with the "publish-subscribe" and "self-synchronisation" processes. Both processes are among the key enablers of EU NEC.

38 Facilitating real-time connectivity while ensuring the freedom of action of end users are some of the main benefits expected from the NEC. NEC implementation for CMO facilitates:

a. Improved control of tempo;

b. Speed: for the dissemination and capture of information supporting planning, knowledge management and real-time situation awareness.

39 **NEC improves knowledge and expertise dissemination:**

40 NEC technologies enable a wide and free circulation of information governed by policies. Hence, expertise, best practices and advice can be disseminated and retrieved at any point of the NEC information sharing environment. NEC provides valuable information where and when it is needed. Implementation of NEC entails a shift from the current hierarchical model to a more transversal organisation where nodes are collaborating.

41 Experts, usually based in strategic locations, can not be reached by operators or users engaged in operations. Some CMO deploy experts in the field. NEC provides the capability to send advice from a large palette of experts in the field[3]. NEC will not turn every user into an expert, but will provide all actors with access to the most relevant advice, whatever the expertise field could be for meeting the requirements of a specific situation.

42 Collaborative tools[4] like wikis, web forums, social networks and other NEC features enable the bottom-up improvement to the information flow and knowledge elicitation. Simultaneously, experts can be located where they are most needed, while still being capable of sharing their skills with the widest community of users. NEC implementation for CMO facilitates:

a. Better decision making;

b. Better synchronisation[5] of end-users,

c. Better control and delivery of effects through synchronisation;

d. Improved optimisation of resources;

e. Increased interoperability between civilian/military MS, non EU MS[6], and third parties;

f. Accuracy of information quality for supporting knowledge management, collaboration and reach-back;

g. Trust in information and identities for supporting decision making, situation awareness and quality of information through the management of sources

2.3.1 RISKS WITH NEC IMPLEMENTATION

43 The adoption of NEC will also bring some new vulnerabilities and difficulties.

44 **Vulnerabilities**

a) An over dependency on information;

b) Potential exposure to cyber attacks (potential access to networks);

c) Increased complexity;

d) Limited interoperability with non aligned agencies and/or states.

---

[3] The need to have more expertise in the filed has been stated in Military lessons learned Chad #704#698 and civilian lessons learned called for a better use of seconded staff, experts and interpreters;

[4] Required from Military lessons learned ATALANTA #579, ALTHEA #122 and civilian lessons learned page 4

[5] Synchronisation enables any user, after operating in a non networked mode, to benefit from all information available on the network..

[6] Non EU MS can be current Troop Contributing Nations (TCN) or potential TCN

45 **Difficulties**

a) High bow wave cost;

b) Cultural resistance;

c) Coordination of equipment acquisition;

d) Integrating legacy bespoke systems;

e) Judicial and administrative difficulties

f) Reaching agreements on common standards and interfaces

2.3.2 OPERATIONAL IMPLICATIONS

46 EU NEC architecture will facilitate the identification of common parts between the processes and deliver the capabilities for ensuring interoperability between all actors of CMO. The identification of common tasks executed systematically in any CM operation or mission is necessary. This capture will feed the constitution of a body of knowledge available for military and civilian operations. It helps in providing a common reference for building synergies and aligning military and civilian activities for CM[7].

47 Analysing the following activities provide a coherent start for building on the common elements of CM which could be supported by EU NEC implementation :

a. Conduct Routine Activities;
Detecting crisis situations, capturing information to be used as reference for operations (geographical and geospatial , data on experts to engage in operations),

b. Plan EU led CMO:
Building and reaching agreement on the measures to engage for mitigation the crisis situation and the forces, equipment and capabilities to be used as part of the tool set,

c. Conduct Activation of EU led CMO:
Organising the appropriate mix of means and capabilities in a coherent way ensuring support and lines of communications are in place and support to force generation

d. Conduct Deployment and Conduct EU led CMO:
Conducting the deployment of personnel, and equipment and conducting the operation/mission in line with the "comprehensive approach" principles, support to coherent transportation, management of assets, training in the field and provision of CIS.

e. Conduct Redeployment:
Redeploying personnel and equipment and terminating the operation when normalised conditions occur,

f. Evaluate EU led CMO:
Drawing lessons learned from the crisis and its management[8].

48 EU NEC implementation guarantees that action is based upon all the information available, operations are conducted in a true collaborative manner among all actors involved in crisis

[7] Having one community aligning its procedures on the other is not the preferred option. A case by case assessment is the basis.
[8] Requirements for lessons learned tools expressed in Military lessons learned (page 22)

management (EU and MS, civil and military, International Organisations (IO) and Non-Governmental Organisations (NGOs)) when needed and as needed, as well as being able to synchronise effects. The interplay between operational effectiveness and improved information quality as a result of NEC is shown in the figure below. The EU Battle Group (EUBG) should also be considered as one of the most important actors that uses EU NEC.

49 Figure 2-2 describes the cascading effects to expect from EU NEC implementation. The Net Enabled Information Sharing Environment supports the trusted information which supports better decisions cascading to improved operational effects. At each level of the diagram, a "based on – supports" relationship exists. Hence, the improved operational effectiveness supports the networked enabled sharing of information and vice-versa.

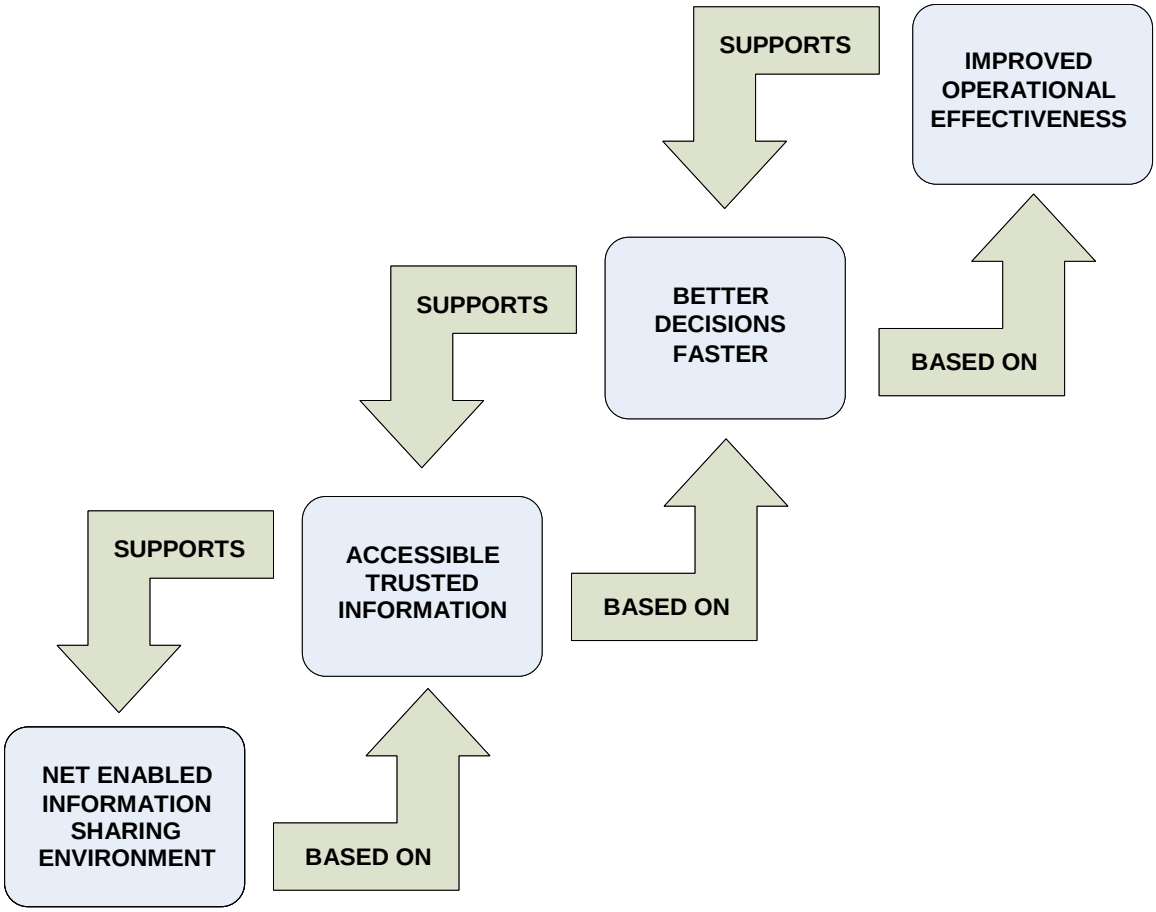

Figure 2-2: Relations between improved operational effectiveness and the NEC Information Sharing Environment including intermediate stages.

3. EU NEC SCOPE

50 The scope of the EU NEC Vision is set in many different dimensions. This report proposes a Mission[9] dimension describing the activities of EU NEC, a Content dimension for meeting the objectives of CSDP[10] and a capability dimension for meeting the people, information and technology aspects of EU NEC.

51 The purpose of the EU NEC Vision is to describe the goal for the development by the EU and MS of EU Network-Enabled Capability in support of the CSDP and EU-led CMOs[11]. The Vision also identifies the drivers for its implementation thus supporting prioritisation of efforts and initiatives.

52 The Vision thereby provides guidance to decision makers regarding:

a. What should be done?

b. Who could act for supporting the success?

c. What will be the benefits, vulnerabilities and constraints?

53 The Vision is achieved through a federated approach to ensure the transition to the target EU NEC through three time-phased increments :

a. Short term - 2012

b. Mid term - 2018

c. Long term - 2025

54 There are a number of constraints to the vision based on the operational context of CSDP CMOs which are described below.

3.1 CSDP AND THE EXTENDED PETERSBERG TASKS

55 The EU NEC Vision is directly based on the EU Concept for NEC in support of CSDP, a concept with enough flexibility to adapt to the application of the Lisbon Treaty ref [35] including modifications of institutional provisions for CSDP and extension of the scope and range of the Petersberg tasks which form the basis of the CSDP missions and operations.

56 The Petersberg tasks included:

a. humanitarian and rescue tasks,

b. peace-keeping tasks

c. tasks of combat forces in CM[12], including peace-making.

57 They are part of the Common Foreign and Security Policy (CFSP) of the Treaty of the EU (TEU).

58 The extended Petersberg tasks under the Lisbon Treaty include:

---

[9] "The high level operational concept for EU sponsored CMO is to conduct missions"

[10] "with highly responsive, well integrated and flexible elements, consisting of civilian and/or military elements, that have assured access to and freedom to operate effectively over the entire spectrum of EU missions. Civil/Military organisations must be able to thrive upon innovation in the field, confident that the actions they take will be intuitively consistent with the strategic and operational objectives".

[11] EU NEC in support of CSDP and EU-led CMOs will hence forward is referred to simply as EU NEC, unless specified otherwise.

[12] Crisis management refers to the organisation, regulation, procedural frameworks and arrangements to contain a crisis and shape its future course while resolution is sought.

a. joint disarmament operations,

b. establishment of "military advice and assistance tasks",

c. establishment of "conflict prevention" and "post-conflict stabilisation" tasks.

59 The Lisbon Treaty includes modification of institutional provisions such as the creation of the HR/FA&SP, the establishment of a European External Action Service (EEAS), new cooperation procedures, a solidarity clause in the event of a terrorist attack or natural or man-made disaster and a mutual assistance clause if a MS is the victim of armed aggression.

3.2 CRISIS MANAGEMENT AND THE EU'S COMPREHENSIVE APPROACH (CA) AND CMCO

60 The changing character of crises caused an evolution within CM. Expanding timelines, extension of tasks and a closer embedding of civil and military actors for better effectiveness constitute the new trends for this evolution. There is a need to manage more efficiently various actors from different cultures and the interfaces between overlapping phases. Civilian operations historically demand more resources[13].

61 Comprehensive Approach is considered as a driver factor for NEC ref [33]. Although the civil-military interoperability may face some limitations in practice, the requirement for a comprehensive approach had been clearly recognised. By definition,for the purposes of the EU, NEC supports the EU's comprehensive approach and CMCO. This supporting link should be retained in order to ensure that NEC also remains user oriented and satisfies their requirements, both in the military and civilian sphere. From this perspective, NEC is the main enabler of any EU developed comprehensive approach.

62 An important aspect is that the EU actors involved in a comprehensive approach are the same ones in need of exchanging, sharing and protecting information, benefitting from the NEC implementation. This means that exactly the same set of actors are involved in both the comprehensive approach and NEC.

63 The EU is capable of using a large gamut of civilian and military instruments for CM. It is faced with the core challenges of assuring coherence between the instruments of the Commission and the CSDP and between civilian and military instruments of the CSDP. In order to address those challenges, the EU has developed the concept of CMCO (Civil Military Co-Ordination).

64 Core CMCO concept and instruments at the strategic-political level for the EU include Crisis Management Procedures (CMP) and Crisis Management Concept (CMC) for individual missions in the case of the EU.

3.3 ROLE OF MS

65 MS will support EU NEC development as a governance function. The processes to govern are concept development, capability development and research and technology projects. MS should seek consistency between EU and NATO NEC approaches where countries participate in both organisations. A lot of cooperative work is needed among the member states (and industry) in order to have common roadmaps for interoperability and capability development on relevant areas.

[13] Total staff deployed in civilian operations increased between 2005 and 2009 (from 1386 to 4019) in 2009. The CSFP follows the same trend in the same period (from 62.5 M€ to 243M€). The forecast for 2013 is at 406M€ (Ref: Third revised draft 2009 Annual Report on the identification and implementation of lessons and best practices in civilian ESDP operations).

3.4 RELATION TO NATO

66 EU NEC cannot be implemented in isolation of NATO Network Enabled Capability. EU and NATO have specificities but synergies must be found for supporting cost effectiveness and industry coherence. Moreover, agreements exist which can provide some of the common permanent and common technical features needed for effective CMO with NEC.

67 NATO has engaged some initiatives in the people and information fields for implementing the information strategies, architecture development and human factors. These efforts could be investigated with a view for re-use and the identification and building of synergies. As an example, the EU could benefit from the acquisition procedures in usage within NATO concerning common funding for procuring an EU autonomous infrastructure[14] to be a common backbone feature like NGCS[15].

68 Synergies must be found, but EU cannot align systematically to NATO orientations and must preserve its future freedom of action. In this perspective, it is recommended to formally delineate the EU NEC elements[16] (architectures, maturity level, interoperability standards, profiles of standards) and to align as much as possible and acceptable with those with initiatives currently underway in NATO. Synergies and complementarities are easier to be found in the domain of Technology, as the Information and especially the People domains contain most of the specificities of EU.

3.5 CURRENT SITUATION INFORMATION EXCHANGE REQUIREMENTS

69 The current situation of Information Exchange Requirements (IER) has been and is under investigation by the Council and EDA within a number of different initiatives.

70 The EDA IER Study ref [30] investigated the current situation for information exchange in CSDP operations across all C2 levels (Political-Strategic, Military-Strategic, Operational and Tactical Level).

71 The results of these efforts are used as input to the NEC vision in such a way that, even though the NEC vision has a much broader operational scope, it must be able to handle the current information exchange requirements, by using exchange mechanisms.

72 Future information requirement will most likely change by the introduction of EU NEC.

3.6 NEC SYNERGY CAMPAIGN

73 European Defence Agency (EDA) is internally executing an integrated approach to NEC (called “The NEC Synergy Campaign” ref [32]), by establishing coordination actions among the Project Teams (PT) and Research & Technology (R&T) Captechs in order to develop Network Enabled relevant capabilities, activities, armament cooperation initiatives, research, studies and projects, in various domains such as CIS, Intelligence Surveillance and Reconnaissance (ISR), Intelligence Information Management (IIM), Maritime Surveillance (MarSur), Software Defined Radio (SDR), Counter Man-Portable Air Defense Systems (CManPads), Radio Spectrum, Unmanned Air Vehicles (UAVs), Intelligence (Intel), Satellite Communications (SatCom), Strategic Situational Awareness (SSA), Logistics, Third Party Logistic Support (TPLS), Strategic Transport; European Air Transport Fleet (EATF),

[14] NATO Security Investment Programs
[15] NATO General purpose Communication Systems provides the backbone of communication from the static headquarters and the theatres.
[16] A proposal could be the EU AF which could be inspired from the NAF but capable of evolving in a different way if needed by EU.

Chemical, Biological, Radiological and Nuclear (CBRN), Counter Improvised Explosive Device (CIED), Personnel Recovery Equipment (PRE).

74 This integrated approach is the consolidation of the answers to a questionnaire, provided by the communities of experts in the projects above. The EDA NEC Synergy Campaign results further sets the scope and gives focus to the proposed EU NEC Vision.

75 The NEC Synergy campaign is going to continue and expand through a dual relation-ship: on one hand it will provide various Supporting Effects and fulfill some of the Decisive Conditions and on the other hand will be impacted by the NEC principles, architecture, maturity model and design/assesment criteria and guidelines.

3.7 EUMC INTEROPERABILITY STUDY

76 European Union Military Committee (EUMC) Interoperability Study ref [34] assesses interoperability in the framework of Headline Goals 2010, from a military perspective, with a view to contributing to capability development. The study points out seven Potential Areas of Improvement (PAI) that were considered to be critical. The most urgent areas of improvement are focused on;

- Air Operations (conceptual development on establishing and providing airspace control measures);
- Maritime Security Operations (conceptual development in the framework of mobility and counter mobility movement, surveillance and security operations, and protect and secure Sea Lines Of Communication);
- Force Protection (conceptual development related to the task providing protection for own forces and non-combatants, as well as conceptual development and harmonisation of technical requirements for providing identification of friendly forces);
- Comprehensive Approach (conceptual development within the capabilities of coordinating coalition support and of providing support to other bodies, including NGOs and IOs);
- Communication and Information Systems (CIS) (technical development on Information Exchange Gateway as well as conceptual development and harmonisation of technical requirements for establishing and contributing to a Common Operational Picture).

77 Additionally, the requirement to examine the effectiveness of current structures for comprehensive planning and conduct of operations has been noted.

78 The findings in the proposed EU NEC Vision can in many ways support the resolution of the areas of improvements found in the EUMC study.

3.8 SUPPORTING EFFECTS

79 Supporting effects (SE) to the EU NEC Vision are ongoing or planned related activities, initiatives, projects or programmes, either national or multinational, which may influence the development and implmentation of NEC. The concept of SE is further described in the Roadmap document of this study.

80 The supporting effects include:

- NEC related projects of the European Defence Agency;
- NEC developments and efforts within the Member States;
- NEC developments within EU institutions;
- NEC efforts within other organisations and within industry.

81 Many of the projects described in chapter 3.6 about NEC Synergy Campaign and chapter 3.7 about EUMC Interoperability study provides good references to SEs. The SE identified in the Roadmap Annex III are examples as well.

EU NEC Principles

82 Within the given scope a number of principles have been identified to which the vision must adhere to. These are based on existing policies, doctrine, plans, lessons learned and best practices of EU, NATO, national programs civilian, military and industry. The principles are described below.

3.9 NETWORK ENABLED CAPABILITY AND CAPABILITIES

83 One can differentiate the EU Network Enabled Capability, which is general and independent from the Communities of Interest (COI), to the “network enabled capabilities”, which are capabilities of the respective COI underpinned by the EU Network Enabled Capability.

84 The Network Enabled Capability reflects the architectural environment, the framework to be constructed. It is referred to by the definition in the NEC Concept and the NEC Vision.

85 The “network enabled capabilities” are the ones to be integrated in the above mentioned environment, as individual capabilities, with the attribute of being “network-enabled”.

86 From this perspective, implementing NEC as a capability means constructing the environment which allows capabilities to become “network enabled”.

3.10 COMMUNITIES OF INTEREST

87 For the EU to realise the real benefits of NEC there is a need to start thinking in terms of Operational Communities and other COI and not just individual platforms, agencies, directorates, and systems. One of the key elements of NEC is the need to support different COI which will be required to collaborate within cyberspace. The COI can be regarded as a group of users who require exchanging information in pursuit of shared goals, interests, or business processes.

88 A more detailed discussion about COI can be found in Annex A.

3.11 UBIQUITOUS NEC

89 From a users point of view the capabilities of the EU NEC shall, to the largest extent possible, appear to be ubiquitous.

90 The ubiquitous aspect EU NEC from the users’ perspective is summarised in the following sentence:

One person, One Information profile, wherever connected.

91 This expresses the link between the human factor, information exchange and supporting technology:

a) **One person**... in real life and in the networks,

b) ...**one information profile**...(each user has a role, belongs to a COI, accesses services tailored according to the profile and gets (only) relevant appropriate information)

c) ...**wherever connected**. (Networks provide an access point, fixed or mobile (deployable), route the person to the appropriate COI within the environment and manage information in compliance with security and business rules).

3.12 CA AS THE DRIVER FOR NEC

92 The EU's Comprehensive Approach influences importantly the operational context and constitutes the overall operational driver for the EU NEC Vision.

93 CMCO needs to be possible at any level of command, including and ranging from strategic comprehensive planning down to the military tactical/civil first line responder level. This calls for doctrinal and technical solutions, which are addressed in the proposed NEC Vision statements below.

3.13 RE-USE OF INVESTMENTS

94 Investments already committed within the crisis management context by EU institutions or by the Member States shall be reused in EU NEC. This includes:

a. civilian infrastructure and structures,

b. development and production of military forces and technology.

3.14 EU NEC FEDERATION

95 The EU NEC is envisioned as forming a federation: which comprises control, or management of the EU NEC PIT distributed throughout the CSDP and its MS. It provides a common vision and focuses EU NEC developments by the CSDP and MS decision makers toward a common objective – the target EU NEC.

96 Many of the organisations and CM actors within the EU context will for a number of reasons never subordinate themselves to an integrated command chain, even if this unique structure may see, more effective at first sight when a crisis emerges. On the other hand building these arrangement takes a long time, and they are crisis specific, hence they can't be valid for a future crisis. Non EU partners may be highly valuable in a specific crisis and not so powerful in another situation.

97 Adhering to the principle of "Federation" seems a mitigation option for ensuring a set of core requirements are met in any type of crisis. When possible the federation can be adjusted and organisations or systems tailored to support the specific mission in the best way. The governance body to stand up should define these core elements for the "federation". Actors in the CM domain must be willing to share some basic values and behaviours, a "Need to Share" culture. During all phases of Crisis Management Operations, participants in the federation will regulate their internal activities through agreements/contracts.

98 The driving factor for participation in the federation must be the understanding that each contribution to the federation will bring more value collectively and to each of the parties. Collaboration in multilateral operations has previously been based on bi-lateral agreements between all participants, but in order to achieve the speed and flexibility needed today, there is a need to establish a baseline federation agreement which can be used as a starting point when creating new missions.

99 Actors which participate in the federation, connect networks and systems within their responsibility area (i.e. domain) for exchanging information. Information exchanges are protected by using one or more Information Exchange Gateways (IEG). The IEG represent the boundaries of the federation which contain one or more service interfaces, physically instantiated

100 Within an actor's domain there can be one or more networks where information is stored. The decision regarding which internal networks shall be connected is taken by each actor (Federation member) independently of the other actors. In Figure 4-2 two example networks are depicted, one federation network which holds information only relevant to the federation and one that is the actors' internal network. In this case, the IEG handles information

exchange between these two networks as well as information exchange with other actors IEGs.

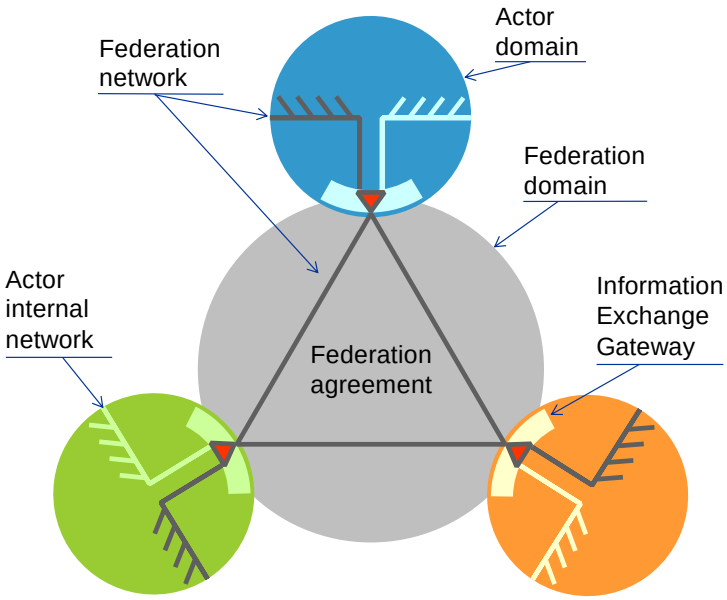

Figure 4-1: Federation overview

4. THE OVERALL EU NEC VISION

101 The future EU NEC CMO is envisioned as a federation of multiple national and trans-national EU public and private enterprises where PIT seamlessly operate together in achieving a global CMO mission for EU. That enterprise of enterprises will provide a continuum within which, governmental, military and civilian EU CMO enterprises will operate as a team, consisting of subordinates, peers and/or partners according to the nature of the crisis and developments, each bringing their own skills and capabilities for the mutual benefits to be realised. The EU NEC will also enable cooperation to be more easily achieved with non EU enterprises.

102 EU NEC vision has been inspired by the impact of World Wide Web (W3) and Service Oriented Architecture (SOA) which has affected the way individuals and organisations conduct business, private, and social activities. W3 technologies have tremendously improved the facilitation of connectivity and information sharing, while SOA facilitates adaptation to users' needs and collaboration between the users. Together, W3 and SOA technologies has enabled and changed the current way of doing business and changed the behaviours of users. The use of these technologies and techniques has allowed people take greater profit from information, to attain greater information superiority, and enhanced cooperation.

103 In the civilian domain, applying those changes is sometimes named Effective Business[17] (responsive, variable, resilient and focused). In the military domain, applying those changes is covered by Revolution in Military affairs or Battle Space Transformation.

104 The EU NEC vision recognises the need to transform the way that CMCO and Civil Military Cooperation (CIMIC) are conducted for the execution of EU CM. This is now even more important in the light of the CSDP articulated within the Lisbon Treaty.

105 Security and CM has in many cases ceased to be just a national concern and require multi national collaboration, which in turn requires willingness to coordinate policies, institutional structures, and capabilities. The European Union within the framework of the CSDP and Lisbon Treaty have a unique opportunity to develop common operational capabilities for CM. This will include civil/military actors cooperating in missions encapsulated within the Petersburg tasks. More importantly transformation and implementation of NEC will help substantiate the European Union's capacity to act as an international and global actor.

106 It is postulated that NEC, which encompasses People, Information and Technology, will greatly improve the EU's ability to execute CMCO by:

a) Enabling general enhancement of EU, MS and other actors e.g. cooperation and Host Nations (HN);
b) Better coordination during routine phases, such as early warning assessment and control;
c) Consolidation and coordination of planning activities of a civil/military cell;
d) Enhanced coordination and collaboration in the field;
e) Ability to capture lessons learned and improve organisations and processes;
f) Provide better resource and capability management;
g) Enable CMCO specific training;
h) Being able to incorporate CMCO in an agreed exercise policy.

107 W3 and SOA have the ability to transform current ways of doing business, but introducing W3 and SOA technologies alone is not sufficient to realise the full benefits of EU NEC such as: :

a. Ubiquity

[17] The Four Pillars of Effective Business – M.Jurgens/H.Nieuwenhuis

b. Trust

c. Teaming

d. Cost-effectiveness

108 Ubiquity is that ability for any CMO Responder to get the same information services whether located within EU, being in transit towards a destination or operating within a Crisis Theatre where all infrastructures may have collapsed.

109 Trust is about security and Information Assurance, but also about the semantics and quality of information. Trust is about getting time-stamped context-aware verifiable information and forwarding it to interested parties including public opinion to cut down rumours and false assertions.

110 Teaming is about collaborating in many ways with various people having a different culture and references, speaking another language, applying unknown procedures and using unfamiliar resources. Teaming also requires trust, about information sharing and moving from "Need-to-Know" attitude to "Will-to-Share". Teaming is also about regulation (doctrine, legal, etc), about organisational structures, about learning and training.

111 Cost-effectiveness is about decreasing significantly the development and maintenance costs involved by multiple 1-to-1 interfaces[18] and replace them by more generic 1-to-N interfaces. Cost –effectiveness is also about quickly reusing existing services to build required new ones in order to decrease testing costs[19].

112 Achieving the above benefits also imply the addressing of overarching architectural qualities like:

a. Security to sustain trust and team efficiency

b. Interoperability in order to cooperate effectively

c. Maturity taking into account different, evolving EU MS skills and capabilities

d. Agility to adapt to unique crisis features

e. High-responsiveness recognising that crisis response is led by urgency

f. Openness so as to easily host any EU responders and also interoperable with non EU responders[20]

113 W3 and SOA models and EU CSDP enterprise are based on different and sometimes conflicting principles. As an example, the W3 model is based on the "good enough" principles while the EU CSDP effectiveness relies on the detailed definition of structure, organisation and rules (with Standard Operating Procedure, table of equipments, order of battle). On the Internet, security is based upon an individual's responsibility, whilst the EU CSDP enterprise relies on a tied accountability, where individuals would be responsible for enforcing security in their part of the enterprise and be held accountable for the behaviours of their subordinates. Hence a balance must be found in order to maintain the EU CSDP as a cohesive, coherent, and effective whilst implementing the flexibility and pragmatism of W3 and SOA.

114 The W3 and SOA model have established an "ecosystem" for "collaborative working". This model is "self-guided", auto-adaptive to spontaneous changes, agile and meets changing

---

[18] Connecting N systems together may lead to define and maintain (N-1)! Interfaces (e.g.: 24 for 4 systems) and sometimes more when interfaces are specialised for a purpose (e.g.: interface for e-mail exchanges, interface for database ....)

[19] For mission-critical systems, testing costs commonly reach 60% of total development costs.

[20] The value added of Berlin Plus arrangements, even if they need time has been highlighted in the military lessons learned case ALTHEA 0057 provided by EDA

needs. It is based on a "business model" relying on the interest of individuals, at all levels, working in collaboration.

115 The vision of EU NEC promotes a "balanced model" between the individually driven W3 model and the heavily structured EU CSDP, by combining small local changes of capabilities, in conjunction to an overarching plan capturing the main changes within the CSDP institutions.

> The EU NEC vision is a progressive transition for achieving incremental change. It includes an overarching plan for developing new capabilities in liaison with local plans for changing existing capabilities.

116 The progressive transition for achieving the incremental change is illustrated in the figure 5-1 below.

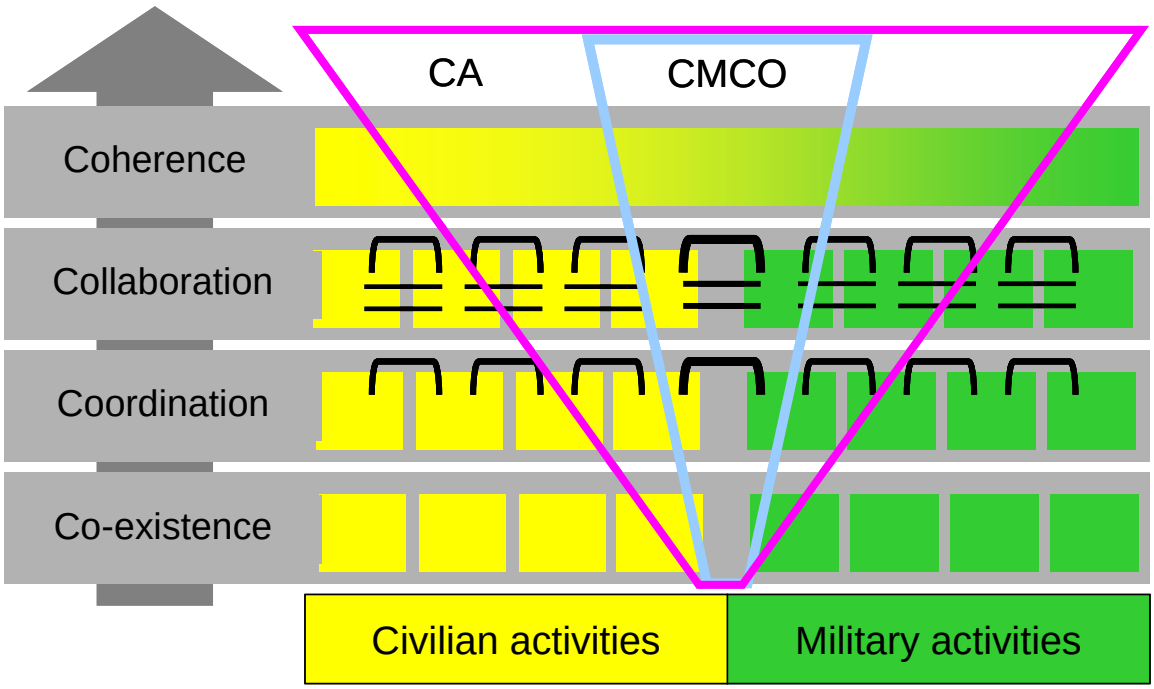

Figure 4-1: The EU NEC vision establishes a link between technical services, value of information and empowerment of people effects for both civilian and military activities. The figure shows the gradual growth of CMCO within the CA and how activities are be performed better through the development stages of Co-existence, Coordination, Collaboration and finally the activities can be performed in a coherent way.

117 NEC recommendations foresee the management (identification and planning) of a set of policies, processes, assets (infrastructures, capabilities and services) and tools to guarantee a coherent and efficient development and an adequate training of the users. It is also very useful and crucial to support military and civilian traditional exercises and to create new opportunities to play the exercises.

118 NEC environment allows to support integrated functions, such as the identification of operational and performance requirements, analysis of all environmental factors (scenarios and threats), modelling and simulation of all environmental factors, validation, verification of candidate systems, technical architectures identification, simulation and validation of Human Factors, feedbacks and lesson learned analysis which are some important goals of exercise activities.

4.1 PIT DIMENSIONS OF THE OVERALL VISION

119 This part of the document describes the status that may be achieved in the long term by a successful EU NEC implementation. The short and mid term objectives are described in more detail described in chapter 6.4, together with the EU NEC capabilities.

4.1.1 PEOPLE ASPECTS:

120 EU Civil and Military entities involved in CMO have acquired a culture of collaboration by fully exploiting the collaborative possibilities of the EU NEC.

121 CM is defined in detail with no ambiguity with regard to knowledge on available capability and coordination of actions between the EU and the MS. EU NEC is conducted using a bottom-up and top-down approach. The policies, guidance, structures, organisations, new ways of conducting operations have been developed, agreed and tested by EU and MS.

122 Security policies based on risk management have substituted legacy policies based on risk avoidance.

123 Regular exercises involving EU, MS, NATO and other third party states occur on a yearly basis.

124 EU and MS share their capabilities development list, mission areas and domains. Information sharing is effective between the capabilities provided by the MS and EU. The EU and MS develop complementary or even common CM capabilities in full coordination.

125 A prioritisation process directs the development of CM systems. The Research & Development (R&D) and R&T programs of work are coordinated between the EU and MS. A list of gaps and overlaps is developed by EU.

126 A capability development organisation exists in the EU for bringing expertise and workforce together to develop autonomous EU Core capabilities, not provided or developed by the MS. This organisation covers also a wide range of industries.

127 Collaboration exists between the COIs. The users involved are using a coherent set of tools supporting coherent and synchronised processes.

128 The Network enabled information sharing environment relies on a mesh of COI. The roles, responsibilities, structures, relationships and processes within or among COIs are clear, well defined and well enforced. Ontology's facilitate information management according to the 'need to know" or to the "will to share" depending on the maturity of EU NEC.

129 The battle-groups, constituting of the main element involved in CM, operate seamlessly in conjunction with civilian agencies and organisations and experts.

130 Individuals have direct access to the different workspaces, provided either by the EU or by each member state in operations or in the static structure they belong to, as required by their functional roles. Identities and profiles can be exchanged seamlessly.

4.1.2 INFORMATION ASPECTS:

131 Information is captured, managed, disseminated and stored in order to be visible, accessible, understandable and trusted using an organisation, rules and services that meet users' requirements. COI, mission areas and governance bodies exist for sorting and managing information and ensuring an easy and effective search and retrieve mechanism between EU and the MS as well as non EU actors involved in an operation.

132 Information is tagged and stored in vast data repositories. Authoritative data sources are listed to ensure that critical information remains valid, regularly updated and maintained. IA processes exist between the EU and MS and are in place.

133 EU and MS policies with regard to information release, assignment of roles and object descriptions are distributed within an agreed ontology. The ontology enables the access control service to understand the information content, the release policy of the information and the role of the receiver.

134 Services span all domains, across EU Member States, regardless of security levels,. The access control service is based on an object description, current policy and on the active role of the subject. Thus policy changes are enforced immediately and the dynamic assignment of roles in CMO does not prejudice sharing. In a dynamic CMO environment, where post incumbents and role type's change as new parties join in; this approach ensures that information sharing is seamless and that updates to the operational environment are immediately reflected by the access control service.

135 Object labels also have ontology's enabling the understanding of the content of information that is being manipulated. Hence, it is possible to take access control decisions that include evaluation of the need-to-know of the receiver and the releasability of the information itself. IA devices and their environment provide the proper trust to allow object-level sharing.

136 Mechanisms[21] for building the Common Operational Picture (COP) are in place and enable constitution of COP and the related cognitive ability for shared situation awareness. Services enable data sharing between the MS and the EU.

4.1.3 TECHNOLOGICAL ASPECTS:

137 CMO effectiveness relies on the quality of EU NEC capabilities. Networks and systems providing a coherent set of capabilities supporting EU NEC and CM. The systems are either the same or highly interoperable.

138 Technology efforts focus on loose coupling, re-use of existing capabilities and inclusion of NEC elements from a bottom-up perspective in conjunction with Concept Development and Experimentation (CD & E). A new trend of short spiral development occurs in program procurement for urgent matters e.g. Urgent Operational Requirements (UOR).

139 Two networks are in place for supporting EU CM at EU RESTREINT and EU CONFIDENTIEL levels. Due to easy interconnection with MS, they provide seamless connectivity between the MS and EU systems and can be accessed by any type of device. Connectivity is enabled by national and EU systems which provide each individual with access, according to his connectivity needs. The technical solutions are in place. The legal regulations are however missing today and needs to be solved by EDA and MS.

140 The security device is embedded within the equipment. Confidentiality protection can be provided at the object level given the security device and the provision of a secure signature environment. All services can handle all security classifications.

141 Users and devices have one cryptographically secured digital ID issued and managed by their MS. Authentication requests are all transparently relayed back to national IA services to allow for authentication, non-repudiation and key management in general.

142 Network is provided with high quality of service to the front edge users.

143 Experimentation, testing and validation can be carried out by simulating real life situations, and the feedback from the user is taken into account for future development. The coordinating structure for capability development has produced roadmaps for technological monitoring and a large and coherent architecture program for monitoring the improvement of the EU NEC implementation at the Enterprise level.

---

[21] Data Integration and Data Fusion are the mechanisms supporting the elaboration of the COP¨.

144 The critical resources limiting technological development are identified and the relevant regulations are passed to enable assurance not to fail in case of crisis.

145 EU, MS and other organisations are capable of full synchronisation of the nodes wherever they operate together.

5. THE EU NETWORK ENABLED CAPABILITY AND THE EU CAPABILITY AREAS

146 EU NEC provides a basic EU Network Enabled Capability, an environment that supports most existing capability areas; further network enabled capabilities are envisioned to be developed within the respective capability areas. Those and the basic NEC capability are described in the different vision statements of the EU NEC vision, described in chapters 6.3 – 6.9. The decisive conditions that must be fulfilled in order to have a certain network enabled capability at a certain time are identified in the roadmap. The decisive conditions of the roadmap refer to the capability vision statements in the EU NEC Vision document.

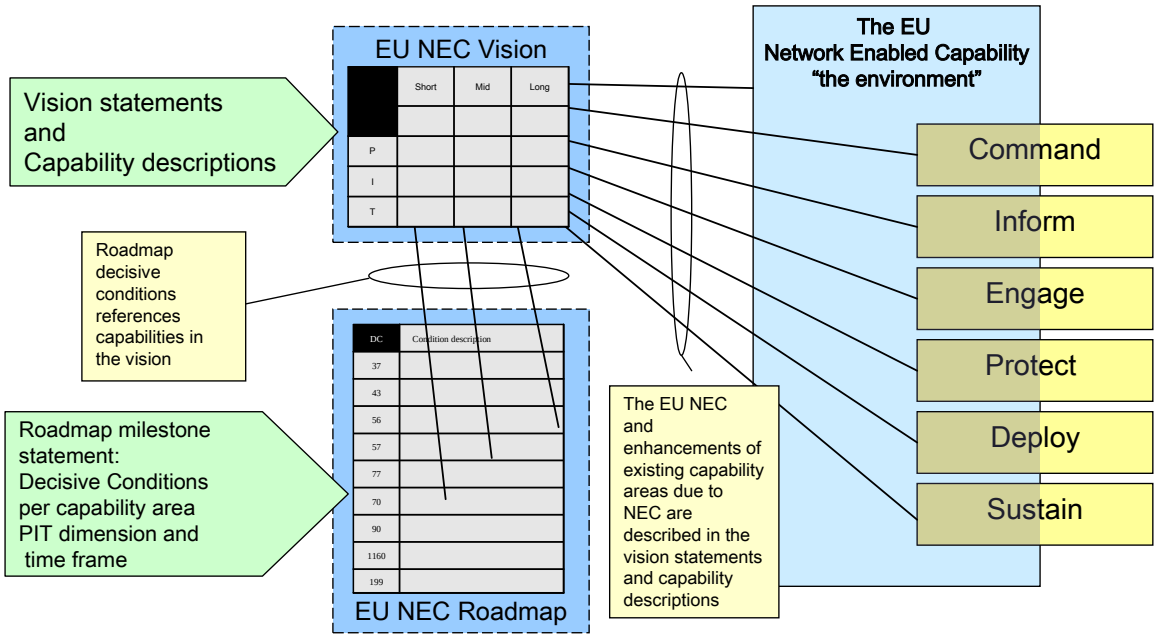

Figure 5-1: Relation between Capability Areas, and NEC Vision and Roadmap

147 The Vision foresees that the users and systems providing and using information (including sensors and effectors) are interconnected within a network. However, it does not require that connection to the network to exist at all times or that all networks are interconnected[22]. The network itself is a federation of any networks available at any moment in time that are compliant with the EU NEC architecture and are suited for the specific type of CMO.

148 Users interact with other users and systems over the network through services. The devices used by the users to access services are envisioned to be the most practical at hand, including workstations, laptops, note-books, cell phones, military workstations in offices, vehicles or carried equipment. User interfaces for the services must adapt accordingly to the device used and to the operational needs of the user. Systems interoperate with each other by using services that are published on the network.

149 The services are provided by the different interconnected systems. All services are standardised so that different providers of a given service are supported, thereby supporting cloud computing abilities. Services are published in directories and can be discovered by

[22] The ability to operate in isolation requires the ability to self-synchronise in order to ensure the correct dissemination of information to users.

users or systems using the SOA paradigm. An effective SOA implementation depends on rigorous management of information and effective tagging of related data.

150 A specific user's ability to access a service or piece of information provided by a service is only limited by the operational policies, security policies, laws and regulations. These limitations are however, enforced to a suitable level by the technical systems providing the services. The information flow to a given user for a given role in an operation is thereby being tailored so that the user only receives relevant information and will not be overloaded with data.

151 It is envisioned that interoperability amongst users and systems external to the CSDP enterprise are made possible by the use of information gateways providing information exchange according to any existing treaties and laws[23]. This includes the basic exchange of data, as well as providing services to the external party, and using services provided by the said external party.

152 It is also envisioned that tools for configuring and supervising the services and information flows are highly transparent and allow re-configuring in near real time.

153 Finally the vision foresees that existing investments in technical equipment can be re-used to a high degree with only minor costs for adapting to the EU NEC architecture. The key to this is the use of a SOA approach for integration.

154 The most important elements providing the capabilities of the vision are:

a) **Users** – civilian and military individuals appropriate trained to their roles in a NEC supported CSDP CMO using the services of the NEC implementation.

b) **Services** – standardised sets of functionality that technically supports the CMO.

c) **Systems** – providers of services or any types of technical systems providing or using information. These are provided by EU institutions, NATO, MS or third parties. Requirements on systems and the services they provide are described as capabilities when they are modelled. EU must be capable of providing its own autonomous and independent capabilities for conducting EU operation outside of "Berlin Plus" arrangements[24].

d) **The network** – conceptually a single network made up of a federation of fixed deployable and mobile networks, provided by EU institutions, MS, NATO or other third parties.

e) **Organisation and policies of the mission** - providing the structure, business and acquisition processes and rules of the operation. These structure and rules are converted to technical configurations which are enforced with the suitable strength.

f) **The EU NEC architecture** – The specifications for polices, business processes, and technology to be used in the supported CSDP CMO

g) **Multinationality –** The fact that most missions involved several nations.

5.1 EU NEC SUPPORTING CONCEPT AND MECHANISMS

155 This section describes a set of concepts and mechanism that are vital for and supports the envisioned EU NEC.

---

[23] Adapting the laws and regulations to the sharing requirements of EU NEC is one of the major challenge governance of EU NEC will face.

[24] Especially because " implementation of Berlin Plus arrangements takes time" Lessons Learned military ALTHEA 0057

5.1.1 BUSINESS PROCESSES IN EU NEC

156 By 'business process' in this context is understood any human activity used for CSDP CMOs which can range from very well defined military procedures to the civilian business processes and work flows of EU institutions national government, NGOs and private businesses and any ad hoc work flow. Business processes exist between organisations as within. NEC will eventually give rise to new or modified business process where human relations, organisation and existing business processes for CSDP CMO (both civil and military) are essential factors.

5.1.2 SERVICES AND SOA

157 Within this context, by a 'service' is understood any kind of functionality possible to access remotely using a network[25]. The service provided can range from the access of a piece of information to any physical effect. The service providers can be humans or technical system or a combination of both. The driving factor is that they can be discovered, reached and executed remotely over a network.

158 SOA delivers effective, flexible, user-friendly and agile[26] solutions to the end user. Achieving these advantages depends on well organised, well structured information repository build with interoperable services. This is even more demanding when information needs to be shared by the EU and the Member States.

159 Service oriented architecture puts further constraints on services. Among these is that all services should be published in a directory (which also can be a service) for discovery and access purposes. Furthermore, implementing SOA implies that the services shall use standard interfaces so that different providers of the same service use the same or type of interface.

160 SOA is a key element for the EU NEC implementation. MS could gradually build services according to common capability needs under the governance of EDA. A good example is the commission program INSPIRE[27] where EU countries are establishing services for environmental monitoring and mapping. Cloud computing technology can be an enabler to implement SOA in a cost efficient way.

5.1.3 INFORMATION PROFILES

161 Every individual acting within CSDP CMO will need to access and distribute information depending on several conditions

a. Role in a CMO business process
b. Security clearance
c. Other legal and mission aspects.

---

[25] Ref NAF V3

[26] Agility is the ability to successfully cope with change. Agility has both a passive and an active component. Passive Agility involves possessing a set of characteristics that allow an entity to continue to operate effectively, despite changes in circumstances or conditions. Active Agility is the ability to effectively respond or adapt when required. This may involve taking an action, stopping an action, changing a process, changing one's approach to management, governance, or command and control. It may also involve changing one's perceptions or even the way success is defined. Change for change's sake is not Agility. Agility implies effectiveness. This means that an entity's capabilities and behaviours are not considered to be agile unless they enable the entity to maintain or improve its measures of value. Agility is the basis for NEC, because NEC is not just connecting people, services and networks. It's the way of improving performance in a cost-effective way! It's a mind change and new way of 'thinking'

[27] http://inspire.jrc.ec.europa.eu/

162 Such information profiles exist in effect (but not in name) today, and are roughly defined by doctrines, regulations, treaties etc. It is envisioned that such profiles can be further defined and implemented in order to support information management. This implementation will authorise, access to the appropriate services and appropriate information, but also limit the information flows that are not relevant for the user in a given situation to avoid information overload.

163 Information profiles are envisioned to be role-based and to provide information flows and access to services according to the role and task of the user. A dynamic adjustment to the evolution of the situation is a key feature of profile implementation.

5.1.4 INFORMATION GATEWAYS

164 Information gateways are mechanisms for providing a very controlled exchange of information between to domains needing to communicate, i.e. cross-domain information exchange. The number of reasons calling for delineating are:

a. Different nations and/international organisations
b. Different laws directing the working rules, SOPs and guidance etc
c. Different information security classification
d. Different technical environments

165 The mechanism can be implemented technically following a scenario based on a business process. The business process is defined by the following use cases:

a. A treaty, regulation, law etc that determines what data is allowed to be exchanged
b. An enforcement mechanism which ensures that only the allowed data is exchanged
c. A log mechanism which keeps track of what data has been exchanged
d. An optional translation mechanism that translates the data to fit the receiving entity, the responsibilities of the owner, the data custodian and the consumers of data.

166 Technical implementations of Information Gateways exist currently to various degrees called data diodes, information stairs, cross-domain guards, data bridges etc, both as commercial products and in systems developed by NATO and the different MS. A simple technical example is a network firewall.

167 In the EU NEC Vision it is foreseen that existing and improved technical implementations of these kinds of mechanisms will be an integral part of the federating assets from the MS, EU institutions, NATO, third party providers etc to support future NEC based CSDP CMOs.

5.1.5 PUBLISH/SUBSCRIBE CONCEPT

168 Publish/subscribe is an information distribution mechanism where an information provider (human or technical) publishes information and can subscribe to that information. The publish/subscribe mechanism is based on the information profile. The benefit of the publish/subscribe mechanism is that the information flow can be tailored to the needs of the user and thereby providing the right information at the right time without causing information overload.

169 In the EU NEC Vision, it is foreseen that publish/subscribe will be one of the major mechanisms to be used for supplying humans and technical systems with timely and relevant information. Publish/subscribe mechanisms are currently in use in many forms, both in the military and the civilian world and many commonly used standards exists, examples being Really Simple Syndication (RSS) and Extensible Messaging and Presence Protocol (XMPP) used on the web.

5.2 THE EU NETWORK ENABLED CAPABILITY AND NETWORK ENABLED CAPABILITY AREAS

170 This section describes the most important of the envisioned EU network enabled capabilities. The capabilities are grouped in six groups reflecting the agreed capability areas (Command, Inform, Engage, Protect, Deploy and Sustain) ref. [5] with the addition of the basic NEC environment supporting the other capabilities i.e. the “EU Network Enabled Capability”. In the contexts of this document the areas include CA, civilian and military, capabilities.

171 The capabilities are described below and for each capability include:

a. A brief description focused on envisioned operational benefits also highlights the NEC aspects and indications of any interoperability aspects.

b. People aspects

c. Information aspects

d. Technology aspects

e. Time frame indications – in what time frame the capability may be available.

172 Some of the EU network enabled capabilities are of a more cross-cutting nature, these are in essence security or more specifically IA, interoperability and system management, while other capabilities are more directed toward certain communities of interests.

173 Other cross cutting capabilities are possible to define such as training and simulation, capabilities for producing and managing of geographic data etc, but are not yet included.

5.3 THE BASIC EU NETWORK ENABLED CAPABILITY

174 The EU Network Enabled Capability provides the core network enabling that is fundamental and general for all capability areas. The EU Network Enabled Capability supports network enabling the existing capability areas: Command, Inform, Engage, Protect, Deploy and Sustain. This is described below in chapters 6.4 – 6.9.

5.3.1 BASIC INFORMATION EXCHANGE AND COLLABORATION

175 Fundamental to the EU Network Enabled Capability is the capability to do basic exchange of information and collaboration. It includes the basics of Network Enabled Information Sharing Environment operating other Network enabled capabilities.

176 The EU Network Enabled Capability is e.g. to be able to efficiently use:

a. Messaging/Mail –E-mail and instant messaging,

b. Chat –text/image group communication,

c. Distributed information management – Publishing, retrieving, versioning and configuration management, tagging, notifications of updates and changes of data such as documents, images, recorded and streaming data such as audio, video and other sensor data,

d. Distributed conferencing support – Setup and perform conferences using audio, video, shared desktops, etc,

e. Information searching –enterprise (CSDP) wide searches of information and data restricted by only information assurance policies,

f. Directory posting and lookups –look up of users, organisation units, systems, published data etc for initiating communication and or data retrieval,

g. Distributed work spaces –set up and use distributed work spaces for permanent semi-permanent and ad hoc work teams,

h. Distributed document authoring – the ability to distributed concurrently author documents e.g. plans,

i. Access to and use of information from the public Internet.

177 The EU NEC is to be supported by the core Network Enabled Capability services.

178 **People dimension aspects**: NEC policies, doctrines and business processes for the utilisation of the EU NEC must be developed and decided. The personnel preparing and executing NEC support for CSDP CMOs must be trained. An EU institution should provide governance coordination and guidance, regarding service provider technology and standards to be used for service provision and use, and also for the federation of networks. An EU autonomous process for certification of service and network providers should be considered.

179 Within the CSDP, NEC policies and doctrines ensure interoperability (see above). For interoperability with an international organisation, governmental organisation and/or NGOs information gateways are used to exchange information and share services.

180 **Information dimension aspects**: The EU NEC can be used in all contexts. Information and information assurance must be handled accordingly. It will include the authentication of authorisation of information and service access of users and systems, protection of information by encryption, protection of systems by intrusion detection and prevention mechanisms. See the NEC Security section for details

181 **Technology dimension aspects**: The EU NEC is to be supplied by the Core NEC Services. These can be provided by Commercial-of-the-Shelf (COTS) or custom made products, hosted either by EU institutions, MS, NATO and/or third party providers. The NATO Core Enterprise Service Framework is a framework most likely suited to for the definition of Core NEC. The definitions in this framework can be re-used by EU, wherever applicable and only to be extended when and if EU specifics need to be addressed.

182 A prerequisite to any Network Enabled Capability is the existence of an available EU network for interconnecting users and service providers. It is foreseen that this is a network federated from different types of networks i.e. fixed networks, deployable networks and mobile networks[28].. This federated network is envisioned to be one single black core IP network, an IP convergence layer, interconnecting every connected system. It will be possible to partition this network into different logical networks e.g. for information assurance reasons.

183 The networks could be provided by different EU institutions, MS and NATO. Other third parties can also be providers of network capacity e.g. in the mission area and/or for satellite communication to it. Tunnelling across the public internet and mobile telephone networks are also an option to be considered at EU RESTREINT level.

184 For deployed and mobile networks it is foreseen that the technical development in the area of software defined radio will have a considerable impact not only on connectivity, but also on security and force tracking. In the mobile domain, the management of radio spectrum becomes an issue that needs be managed and/or coordinated between EU and MS but also between governmental and industry actors.

185 One possibility is that a core backbone federated network in combination with a number of EU NEC Core service providers could provide a permanent NEC communication and information

[28] Interconnection of network with MS and autonomous secure communications EU CSDP wide are strong requirements of synergy campaign, Military and civilian lessons learned documents impacting also provision of CIS.

system supporting CSDP CMOs. Providing this backbone of communications will require that governance adjusts acquisition and funding principles for more autonomy in delivering and building capabilities.

186 Service Level Agreements (SLAs) are needed to regulate the federated network services.

187 **Time frame:** Since most of the technology needed for the fundamental NEC exist today and to some extent are already in use, it is foreseen that a substantial part of the EU Network Enabled Capability is in place within the short time frame (2012), at least for the fixed and deployable network domains. For mobile networks, a mid to long time frame is expected.

5.3.2 INTEROPERABILITY

188 . Interoperability is paramount for a CSDP CMO since success of the operation is based on the ability of the actors from different nations, using different methods and systems to work together. It is by no means specific to network enabled capabilities, but highlighted since the services and networks (potentially) provides means for interoperability. Interoperability can be viewed in the following aspects:

a. Vertical interoperability – This is the interoperability between higher and lower levels of command within the CSDP CMO. This of course exists today in a certain form but can be improved significantly (see ref [30]). NEC can automate several of the tasks performed by hand or imperfect technical systems of today. Bridging the gap between systems on the operational and the tactical level can be performed through gateways, possibly used in combination with Multilateral Interoperability Programme (MIP) replication mechanisms.

b. Horizontal interoperability – This is the interoperability on roughly the same command level but between entities that use different types of technical systems. In the military context it would e.g. be between different military branches or between units using different national equipment. Information gateways are expected to bring the solution of interoperability on the technical level. Horisontal interoperability is the most obvious factor for the change of organizations in the EU NEC implementation.

c. CMCO – This is expected to take place on most levels. Ranging from strategic level down to the tactical level. The civil side can be either an EU civil institution or government organisations (police force, local government etc), and/or NGOs.

d. Culture of Collaboration - In the long run, the CSDP will become really effective when utilising a culture of collaboration within EU NEC, where cooperative actions can be performed while maintaining the integrity of each respective organisation. It is foreseen that this culture of collaboration can be developed by means of training and experience on actual CSDP CMOs,

189 **People dimension aspects:** Concept, doctrines and business processes must be developed and implemented to build the operational basis for interoperability. In many cases, it relates to harmonising existing doctrines and business processes.

190 **Information dimension aspects:** None other than those identified in the Basic EU Network Enabled Capability identified section.

191 **Technology dimension aspects:** None other than those identified in the Basic EU Network Enabled Capability identified section.

192 **Time frame:** Mid to long.

5.3.3 MANAGEMENT OF THE BASIC EU NETWORK ENABLED CAPABILITY

193 The EU NEC system management is the ability to manage the whole life cycle of the EU NEC technical system used in a CSDP CMO. It involves:

a. System assembly;
b. Configuration of systems and networks including basic situation data such as maps;
c. Verification of the systems and networks;
d. Deployment of the systems and networks;
e. Supervision and control of the systems and network during the mission;
f. Perform maintenance and repairs;
g. Disengagement of the systems and networks at the end of the mission, including archiving and disposal of data.

194 EU NEC Vision is that all system management should be possible with a minimum of human effort using capable tools for creating and changing configurations and to have repositories with best practice configurations available to provide a quick start for the configuration of a technical system of a new CMO.

195 **People dimension aspects:** A CSDP wide architecture must govern the rules for technical interoperability and manageability. There must also be a body of trained personnel at hand for EU NEC system management. This body can be provided by EU institutions, the MS or by a third party, or a combination thereof.

196 **Information dimension aspects:** Information dimension aspects: Configuration data must follow EU approved standards. NATO standards will play an important role in this context. The data must be managed by a EU specific certification process.

197 **Technology dimension aspects**: It is foreseen that commercial technologies based on commonly used open standards will be used.

198 **Time frame**: Short to Mid.

5.4 CAPABILITY AREA: COMMAND

5.4.1 NETWORK ENABLED PLANNING

199 Planning occurs on many different levels and in many contexts ranging from strategic comprehensive planning to tactical planning or planning for purely civilian action and CMCO. The EU NEC Vision supports planning mainly via the basic EU Network Enabled Capability described above in chapter 6.3, which provides means for developing a plan by providing access to information, using templates, a distributed collaboration environment and by supporting administration and distribution of plans.

200 The operational benefits are that plans can be developed faster and with better precision, due to the access of the relevant information on which the plan is based upon. Furthermore, any change to the plan can be initiated, decided, included, and communicated faster.

201 **People dimension aspects:** Existing doctrines and business processes need to be modified to encompass Network-Enabled (NE) planning, liaison between all actors and the personnel trained accordingly.

202 **Information dimension aspects:** The access to relevant information is one of the factors of success in planning. Relevant information could be background information, situation information and/or intelligence. Core services are to provide access to such information.

203 Plans need to be developed by actors in different organisations and contexts. The services for collaboration and exchange of plan content must be interoperable. Information gateways are expected to achieve this requirement.

204 **Technology dimension aspects**: Most activities associated with planning are supported by the Core NEC Services, in particular the access to Geographical Information Services (GIS) and Geospatial Data. The specific aspects of planning need complementary services to be designed as new requirements for decision making appear.

205 **Time frame:** Most parts of network enabled planning are foreseen to be introduced in the short and middle time frames.

5.4.2 NETWORK ENABLED COMMAND AND CONTROL

206 Network Enabled Command and Control deals with the military command and control (C2) mechanisms of planning, tasking, execution and follow-up activities. These are often supported by technical mechanisms for distribution of plans, orders and reports, and the maintaining and distributing one or more situation pictures, typical applications would be “Recognised Situation Pictures” for Air, Land Maritime, Space, Logistics. Combining Recognised Situation Pictures with Data integration and Data fusion will provide the Common Operation Picture shareable with the actors involved in the operation.

207 In the EU NEC vision it is foreseen that a plethora of different C2 systems is developed within the NATO context. The different NATO, national and military branches will be interoperable using services and information gateways Utilising existing investments in C2 systems make sense and support the cost effectiveness objective of EU NEC. Furthermore it is envisaged that interoperability for CMCO purposes on different levels will be possible e.g. the exchanging situation information and plans will be possible using similar mechanisms.

208 The operational benefits from having C2 systems interoperable and being interoperable with civilian structures is envisioned to be significant. Speed, effectiveness and precision are enhanced. Furthermore CMCO is supported and thereby enabling a CA on all levels. Also the possibility to the effective tracking of forces will minimise risks for mistakes such as 'blue on blue engagement etc.

209 **People dimension aspects:** Interoperability of C2 is primarily a matter of harmonising doctrines, business processes and vocabularies. Military branches, nations and international organisations have engaged this harmonisation which needs to be extended to doctrine and business processes of CMCO and civilian activities.

210 **Information dimension aspects:** The primary information aspect is how to handle the differences in information models used by different military branches and nations and civilian actors. A second aspect is the IA e.g. how to handle information exchange between systems in different security domains. It is envisaged that this can be solved by the use of information gateways and proper tagging of information.

211 **Technology dimension aspects:** There are currently several developments addressing interoperability and service orientation of C2 systems such as the MIP Joint Consultation, Command and Control Information Exchange Data Model (JC3EIDM) effort and NNEC and more such as the Joint Common Operational Picture (JCOP). Also real time tactical level standards are existing and emerging, such as NATO Friendly Force Identifier (NFFI) for tracking of own and allied forces. The vision states that these systems are re-used for CSDP. The re-use underpins coherence of investments done in each MS, in NATO and in EU.

212 **Time frame:** Although many technical developments are at hand or ongoing, reaching consensus on military, civil-military doctrine and regulations on C2 may take longer time and is expected to be achieved in mid to long terms.

5.4.3 ENVIRONMENTAL (GEOSPATIAL AND METOC) SUPPORT

213 Environmental (Geospatial and METOC) support is required to support all existing capabilities. The capability "Environmental support" is much more comprehensive than collecting METOC

data or using GIS as a core service. In the civilian world geospatial services are already standardised and are on the way in NATO as well. The main principle is to deliver geospatial information through services. A good example how this is achieved is the European Commission INSPIRE[29] program. The NATO Core GIS program from NC3A is also following the same lines of development by using Open Geospatial Consortium (OGC) standards[30] to create interoperability. The military profiles of OGC standards are developed by Defence Geospatial Information Working Group[31] (DGIWG)

214 **People dimension aspects:** Geospatial data is often much more dynamic than expected. Information that is considered to be geo spatial intelligence information in the military world is often to vital geospatial information for the common operational picture in a CMO. Concept, policy and doctrines need to be developed for EU NEC concerning sharing of Geospatial data.

215 **Information dimension aspects:** Standards for the exchange of Geospatial information is required. The preferred way to exchange such information is through services.

216 **Technology dimension aspects:** Tools for Environmental support exist largely in the civilian world and open standards are available to be used in the technical tools..

217 **Interoperability aspects:** Core EU NEC is to relay INSPIRE program from the commission and NATO Core GIS

218 **Time frame:** Short to long. In the short time the geospatial and METOC services are already available in the civilian world. The military domain should adapt in the mid term to basic map services and to more advanced analysis services in the long term.

5.4.4 NETWORK ENABLED MONITORING, MENTORING AND ADVISORY

219 EU NEC will support monitoring, mentoring and advisory activities. In civilian operations, situations requires that several observer and/or mentors are working geographically distributed within an area and need to collaborate share/coordinate their information. Providing remote export support to the monitors or experts is a possible. This Network enabled monitoring; mentoring and advisory capability meets the requirements expressed in lessons learned documents for better liaisons, more actors involved and a better access to reference[32] and local information sources. The capability should operate cross domain for civilian and military members. The NEC Core capabilities will provide support of collaboration processes and ensure the quality of the services and the value of information and data sources.

220 **People dimension aspects**: Working methods need to be established modified and personnel subsequently be trained.

221 **Information dimension aspects:** None other than those identified in the Basic EU Network Enabled Capability identified

222 **Technology dimension aspects**: None other than those identified in the Basic EU Network Enabled Capability identified

223 **Time frame:** This capability can be deployed together with the Core NEC in the short and mid

[29] http://inspire.jrc.ec.europa.eu/
[30] http://www.opengeospatial.org/
[31] http://www.dgiwg.org/dgiwg/
[32] This capability could disseminate the documents produced from the lessons identified processes (ref Third revised draft 2009 Annual Report on the identification and implementation of lessons and best practices in civilian ESDP missions) p15

5.4.5 COMPUTER NETWORK OPERATIONS

224 Computer network operations (CNO) is expected a key capability of the future. CNO is defined as the capability and action taken to protect, control and optimise computer networks, associated hardware and software and to contribute towards information superiority and thereby deny an adversary this capability. CNO comprises three interrelated elements:

a. Computer Network Attack (CNA). CNA includes actions taken via computer networks to disrupt, deny, degrade, or destroy the information within computers and computer networks and/or the computers/networks themselves. CNA can also achieve effects outside the adversary's IT-Infrastructure.

b. Computer Network Defence (CND). CND includes actions taken via computer networks to protect, monitor, analyse, detect, recover and respond to network attacks, intrusions, disruptions or other unauthorised actions that would compromise or cripple information systems and networks.

c. Computer Network Exploitation (CNE). CNE includes enabling actions and intelligence collection via computer networks that exploit data gathered from target or enemy information systems or networks.

225 CND is treated in section 5.7 and is not further discussed here. Regarding CNA and CNE the areas are still immature and the future EU level of ambition in these areas is difficult forecast The vision foresees that, if corresponding capabilities are developed and used in different parts of the world the world, CNA and CNE will become an important part of EU NEC in the long term.

226 **People dimension aspects:** Concept, policies and doctrines need to be developed for CNA and CNE. These may take a long time to develop and agreed upon within EU.

227 **Information dimension aspects:** Information regarding actual CNA and CNE operations objectives and means will require a high level of protection. Open source (as well as closed source) information for CNE will likely be utilized.

228 **Technology dimension aspects:** Civilian open source technology will likely provide a significant fraction of the technology needed..

229 **Time frame:** Long.

5.5 CAPABILITY AREA: INFORM

5.5.1 NETWORK ENABLED INTELLIGENCE SURVEILLANCE AND RECONNAISSANCE

230 Network Enabled Intelligence, Surveillance and Reconnaissance (ISR) provides all sensor capability, sensor data processing systems and intelligence processing capabilities. Trackers, data fusion systems and automatic classification are the main features of Network Enabled ISR capability

231 Furthermore, as the use of sensors on unmanned vehicles increases, the use of such sensors will extend from the purely military to the civilian domain e.g. for the assessment of disaster areas or monitoring of critical installations. Rapid mapping technologies are envisioned to be used for providing geographical data for supporting both military and civilian components of a mission.

232 Using part of Intelligence information is foreseen to be possible for collecting, processing and disseminating information with services while maintaining a very high degree of information assurance for protecting sources.

233 An unprecedented quality of situation awareness is the major operational benefit to be expected from delivering this capability.

234 **People dimension aspects:** The existing concept, policies and doctrines need to be modified to connect to other NEC approaches. NNEC is one of the elements which likely to play an important role in this matter. Insertion of Unmanned Aerial Vehicle (UAV) in the Common Air Traffic Systems is one of the key issues to be solved as well.

235 **Information dimension aspects:** Information sources will be extended and include the wider range of types from sensors to open information sources coming from EU, MS and local sources. The wide range of sources and types of information puts additional stress on information assessment and information fusion. Meta data and ontologies need to be developed together with methods and technologies to support information assessment.

236 Meta data and ontology for sensor data must be developed for the discovery of sensor data streams on the network.

237 **Technology dimension aspects:** Technologies are largely at hand but the appropriate services must be developed. Managing the high performance and real time requirements of ISR within a service oriented architecture must be handled by proper the definition of the ISR specific services. This is done by defining the services so that they use protocols and formats appropriate for ISR, both existing standards and emerging e.g.OMG Data Data Distribution Service. The NATO efforts in this area will be substantial and will be re-used to maximum possible extent, with the EU specifics taking into account.

238 **Time frame**: Mid to long.

5.5.1.1 Permanent surveillance

239 A second aspect of Network Enabled ISR is the permanent surveillance of sea, airspace, ports and airports are not a support to CSDP operations as such but rather a means for prevention of crisis. It is envisioned that the current efforts such as MARSUR and SUCBAS are developed into large 24/7 fully operating surveillance systems and being complemented by similar interoperable network systems for surveillance of airspace, airports and harbours.

240 Permanent surveillance envisions a full coordinated gathering, processing and dissemination of civil and military information in and between the respective domains of permanent surveillance such as maritime, air as well as interoperability with other relevant EU institutions.

241 It is furthermore envisioned that the systems include mechanisms for anomaly detection and alert. These alerts could provide input to early warning systems and command and control.

242 **People dimension aspects:** The existing concept, policies and doctrines need to be modified to include NEC.

243 **Information dimension aspects:** None other than those of Network Enabled Intelligence Surveillance and Reconnaissance and the Basic EU Network Enabled Capability identified.

244 **Technology dimension aspects:** None other than those of Network Enabled Intelligence Surveillance and Reconnaissance and the Basic EU Network Enabled Capability identified.

245 **Time frame:** Short to mid.

5.6 CAPABILITY AREA: ENGAGE

5.6.1 NETWORK ENABLED WEAPON ENGAGEMENT

246 EU NEC supports weapon engagement by providing services for planning, targeting, synchronisation of engagement also services for battle damage assessment are provided. These services will most likely re-use business processes and the technology provided by NATO. In the near term tactical data links such as Link 16 or Link 22 will be used. These will later evolve as service providers do further development within the NATO NEC.

247 The operational benefits will include

a. Precise engagement
b. Time sensitive targeting / engagement
c. Avoidance of collateral damage

248 This is enabled by accurate and timely situation information on targets, friendly forces, platforms, effectors and the physical environment (see also section 5.5).

249 **People dimension aspects:** The existing concept, policies and doctrines will need to be modified to include NEC.

250 **Information dimension aspects:** Those of existing and future tactical data links and NATO NECC.

251 **Technology dimension aspects:** Those of existing and future tactical data links and NATO NECC.

252 **Time frame:** Short to mid term

5.6.2 NETWORK ENABLED SEARCH AND RESCUE

253 EU NEC supports civilian and military search and rescue by providing services for planning, tasking, targeting and execution as well as situation awareness including services e.g. for synchronisation of search areas and rescue progress.

254 **People dimension aspects:** The existing concept, policies and doctrines need to be modified to include NEC.

255 **Information dimension aspects:** Information standards for communicating search and rescue information must be identified/developed and enforced.

256 **Technology dimension aspects:** Existing and future technical system will be modified accordingly to handle the information.

257 **Time frame:** Short to mid term.

5.7 CAPABILITY AREA: PROTECT

5.7.1 NEC SECURITY

258 NEC security is the capability to maintain information security while utilising other network enabled capabilities. It deals with the authentication of users and systems, authorisation of users and systems to access information and using and providing services, the protection of systems and networks, protection of information, handling of security classification and re-classification of information.

259 It is envisioned that users and systems can be authenticated by the use of tokens such as smart cards with certificates and biometrics etc based on open standards. A public key infrastructure will be used for authentication of humans and systems. Services for verification and revocation of security tokens will be present on the net.

260 Authorisations will be based on the information profile of each user or system. A trusted link between the real identity and information profile is one of the major enabler for building trust and security. Accessing to the authorisation rules for enforcing information assurance is expected to be done through a web service. This approach enables dynamic security policy which possibly can be adjusted in real time.

261 A common CSDP standard for encryption and exchange of encryption keys is ultimately needed.

262 Separation and interconnection of systems in different security domains is achieved by information gateways.

263 The security requirements will have to be harmonised at organisational, procedural, and technological level to balance information and decision superiority at the strategic, operational, and tactical levels and security aspects. That can be provided through a complete identification, characterisation and implementation of the Information Assurance capabilities, System and Network Management capabilities and Computer Network Operations.

264 The capabilities, provided by Information Assurance and Computer Network Operations, will manage and monitor the infrastructures and the end-to-end information flows and to respond to threats and to other operational impacts.

265 **People dimension aspects:** The existing concept, policies and doctrines need to be modified to include NEC. EU autonomous certification process is required. Changes in connectivity and Information assurance policies and guidance are required.

266 Some areas that need specific attention are:

- The automatic exchange of classified data where the classification is based on different legal systems which might conflict.
- Managing of encryption keys and mechanisms for interoperability where the different legal systems of the MS might conflict.

267 **Information dimension aspects:** Metadata regarding the security classification of information objects and the clearance for individuals and systems must be managed. The overall quality of security depends on the capability of EU to sort, tag and manage all of the information used.

268 **Technology dimension aspects:** There are many open standards that exist and are widely used for supporting, authentication, authorization, encryption and intrusion detection. These open standards are the major opportunities for implementation of security through COTS assets.

269 **Time frame:** Mid to long term.

5.7.2 COMPUTER NETWORK DEFENCE[33]

270 Within the defence part of Computer Network Operations, the EU NEC vision deals with the protection of network infrastructure as an objective for CSDP CMO. Protecting the network infrastructure against cyber attacks, hacking, denial of service, the spreading of computer virus and malware are key missions of this capability.

271 **People dimension aspects:** Concept, policy and doctrines need to be developed for EU NEC Computer Network Operations.

272 **Information dimension aspects:** Standards for the exchange of attack pattern and profiling information must be developed.

273 **Technology dimension aspects:** Tools for Computer Network Operations exist largely in the civilian world.

274 **Interoperability aspects:** The Basic EU Network Enabled Capability is to relay the Computer Network Operations services across EU NEC capabilities.

275 **Time frame:** Mid to long term.

---

[33] Computer Network Operations is covered in the generic list of military capabilities in capability (1.1.7 :" Provide Effects in Cyberspace")

5.7.3 NETWORK ENABLED FORCE PROTECTION

276 NEC provides force protection by friendly force tracking (see section 5.5) and the detection of threats by enabling processing (automatically and/or manually supported) of all available sensor and intelligence information in order to create alerts and warnings displayed in the COP and distributed to the concerned personnel.

277 Threat detection based on sensor information using single or multiple sensors is a well known but constantly developing technology for conventional threats like missiles, aircrafts, torpedoes etc. NEC can improve handling of conventional threats and also in the future manage newer threats like Improvised Explosive Devices (IED) considering NECs potential of combining information from multiple sources from different domains, perform analysis of the information and distribute the result to the relevant actors within fractions of a second.

278

279 **People dimension aspects**: Concept, policies and business processes for NEC Force Protection must be modified and/or developed.

280 **Information dimension aspects:** None other than those in The Basic EU Network Enabled Capability and the Inform capability area have been identified.

281 **Technology dimension aspects:** Appropriate analysis systems must be developed.

282 **Time frame:** Mid to long term.

5.8 CAPABILITY AREA: DEPLOY

5.8.1 NETWORK ENABLED DEPLOYMENT

283 EU NEC supports deployment by providing services for planning for deployment, executing deployment and tracking the progress the deployment. Services for planning deployment are the similar as the services supporting planning for Network Enabled Command and Control. The services tracking the progress of deployment are partly the same as those for Network enabled logistics e.g. the services for asset tracking.

284 The field of air transport is a prominent case driving NE Deployment the services planning and executing deployment will need to take air transport specifics into account.

285 The operational benefits are e.g. that the deployment can be done faster and with more precision due to near real-time tracking of the progress.

286 **People dimension aspects:** Concept, policies and business processes need to be modified or developed in order to encompass network enabled deployment. And subsequently personnel need to be trained.

287 **Information dimension aspects:** Integration and fusion processes are applied to deployment information for creating an unambiguous picture of the deployment status and progress.

288 **Technology dimension aspects:** The technology solutions for network enabled command and control, and network enabled logistics should also be able to support network enabled deployment.

289 **Time frame:** Mid term.

5.9 CAPABILITY AREA: SUSTAIN

5.9.1 NETWORK ENABLED LOGISTICS

290 EU NEC supports logistics by providing requesting and tracking services for assets or supplies, logistic planning and forecasts. Interoperability with third party logistics providers is

supported by logistic services. Liaison with third party logistics providers within the EU NEC context is possible.

291 The operational benefits are more accurate and in time logistics support to a CMO.

292 **People dimension aspects:** Concept, policies and business processes need to be modified or developed in order to encompass network enabled logistics. Subsequently personnel need to be trained.

293 **Information dimension aspects:** Integration and fusion processes are applied to logistic information for building recognised logistic situation pictures.

294 **Technology dimension aspects:** Civilian solutions for networked enabled logistics exist today like LOGFAS, which is available for the EU. Another one is LOGFS, a system implementation of logistics services done in NATO for supporting the Logistic COI.

295 **Time frame:** Mid term.

6. SUMMARY

6.1 THE VISION IN MATRIX VIEW

296 The following table summarises the vision in a structured way. It is a summary of the findings within the capability areas described in this report and the deeper analysis found in the annexes.

Table 1 Vision in matrix form

Time Frame / Dimension	▪ *Stovepipes* ▪ *Confliction* ▪ *Lack of interoperability*	**Goal & Objective** ▪ ***Deconfliction (doctrine, organizations, information,…)*** ▪ ***Communities of Interests*** ▪ ***Basic Information Sharing***	**Goal & Objective** ▪ ***Improved information sharing (cross-functional exchange)*** ▪ ***Improved security*** ▪ ***Collaborative working***	**Goal & Objective** ▪ ***Full Collaboration*** ▪ ***Self-synchronization***
	CURRENT	**SHORT TERM**	**MID TERM**	**LONG TERM**
PEOPLE	DOCTRINE, ORGANIZATION			
	"Different cultures, skills, doctrines, and methodologies; desires to coordinate but not to be coordinated; desires to get information but not to share it; unconsciousness of available information or tools" Reference [3], §A3, p.5	▪ De-confliction of doctrines, Organisation and Procedures ▪ Moving from "need-to-know" to "will-to-share". Responsibility of sharing info.	▪ A culture of "will to share" is established	▪ The culture of "will to share i fully established and widely used
	COLLABORATION: *"will to share"*			
	▪ Resistance to share information	▪ De-confliction	▪ Co-ordination	▪ Full collaboration and coherence
	TRAINING			
	▪ Sparse	▪ Focused effort on training & education regards CMCO (civilians involvement)	▪ Directed training ▪ Common training between civilian and military	▪ Self training
	GOVERNANCE			
	▪ No SOA governance strategy for the overall enterprise ('service chaos')	▪ Initiation of a SOA Governance framework (focused on the long-term)	▪ SOA and IT infrastructure governance alignment	▪ Governance through policy ▪ SOA delivers its promises though governance

Time Frame / Dimension	▪ *Stovepipes* ▪ *Confliction* ▪ *Lack of interoperability*	**Goal & Objective** ▪ *Deconfliction (doctrine, organizations, information,…)* ▪ *Communities of Interests* ▪ *Basic Information Sharing*	**Goal & Objective** ▪ *Improved information sharing (cross-functional exchange)* ▪ *Improved security* ▪ *Collaborative working*	**Goal & Objective** ▪ *Full Collaboration* ▪ *Self-synchronization*
	CURRENT	**SHORT TERM**	**MID TERM**	**LONG TERM**
INFORMATION	INFORMATION SHARING			
	▪ "different information management and document handling; multiplicity of data bases; different security requirements and standards" Reference [3], §A3, p.5	▪ Basic information and data shared between COI, civil and military ▪ Enforced rules on Information Management	▪ Information sharing is well defined and enforced across a growing mesh of civil and military COI	▪ Information sharing between COI supports full coherent and synchronized collaboration processes
	▪ Lack of joint shared situational understanding	▪ Information Exchange Gateways contribute to shared situational awareness improvements	▪ Information/Data integration and fusion support Common Operational Picture	▪ High level of awareness is delivered ▪ Real-time joint situation awareness
	▪	▪	▪ Structured information	▪ Self describing information
	INFORMATION MEANING			
	▪ Lack of common vocabularies	▪ Development of ontologies	▪ Ontologies facilitates the integration of information and its cross-functional exchange. ▪ Information begins to be understandable (semantics) by machines	▪ Semantic data vocabularies ▪ Ontological Vocabularies ▪ Semantic web
	▪	▪ Raw data and information sharing	▪ Data transformation ▪ Information sharing to construct knowledge.	▪ Information shared evolves into knowledge sharing ▪ Information superiority transforms into decision superiority
	INFORMATION STRUCTURE			
	▪ Lack of integration of information	▪ Sharing of raw information/data ▪ Integration of information ▪ Content management	▪ Structured information/data facilitates content management ▪	▪ Structured information/data ▪ Knowledge and content management

Time Frame / Dimension	▪ *Stovepipes* ▪ *Confliction* ▪ *Lack of interoperability*	**Goal & Objective** ▪ ***Deconfliction (doctrine, organizations, information,…)*** ▪ ***Communities of Interests*** ▪ ***Basic Information Sharing***	**Goal & Objective** ▪ ***Improved information sharing (cross-functional exchange)*** ▪ ***Improved security*** ▪ ***Collaborative working***	**Goal & Objective** ▪ ***Full Collaboration*** ▪ ***Self-synchronization***
	CURRENT	**SHORT TERM**	**MID TERM**	**LONG TERM**
	▪	▪ Metadata tagging is applied to information and data to facilitate its organization and retrieval.	▪	▪
	SECURITY POLICIES			
	▪ Fixed-domain specific security ▪ Confliction in security policies	▪ Deconfliction of security policies ▪ Risk avoidance evolves into Risk Management	▪ Accuracy and trust in information and identities	▪ Uniform Identification of citizens (“one person-one information profile”)
TECHNOLOGY	SERVICES & SOA			
	▪ Point-to-point integration ▪ Emerging SOA	▪ SOA adoption ▪ Initial SOA applications (legacy systems encapsulated as services)	▪ SOA leveraging (discovery, repositories, ESB, management, monitoring, etc) ▪ SOA governance implementation	▪ Full SOA
	▪ Componentized developments	▪ Initial Core Enterprise Services (security, discovery, collaboration, interaction, infrastructure and control, …)	▪ Completing the Core Enterprise Services packs ▪ Use of service repositories ▪ Services are architected through SOA implementation	▪ Full use of services repositories ▪ Measured and optimized business services ▪ Composite services and information flow for “meta-application”.
	▪	▪ Initial collaborative services for CoI’s	▪ Collaborative services across COIs	▪ Harmonized services support all COIs
	COMMUNICATIONS AND INFRASTRUCTURE			
	▪ “deficiencies in compatibility, connectivity or interoperability of systems and equipment” Reference [3], §A3, p.5	▪ Interoperability (voice, video, data, …): between MS, EU agencies, civil/military, … ▪	▪ Increased interoperability between MS, EU agencies, civil-military,… ▪ Evolution in Service Level Agreements (SLA)	▪ Communication networks: flexible, secured, reliable, available ▪ Ubiquity of information ▪ Full interoperability all actors
	▪ Cloud Computing is an	▪ Advances in legal,	▪ IT transition	▪ Cloud Computing revolution

Time Frame / Dimension	▪ *Stovepipes* ▪ *Confliction* ▪ *Lack of interoperability*	**Goal & Objective** ▪ ***Deconfliction (doctrine, organizations, information,…)*** ▪ ***Communities of Interests*** ▪ ***Basic Information Sharing***	**Goal & Objective** ▪ ***Improved information sharing (cross-functional exchange)*** ▪ ***Improved security*** ▪ ***Collaborative working***	**Goal & Objective** ▪ ***Full Collaboration*** ▪ ***Self-synchronization***
	CURRENT	**SHORT TERM**	**MID TERM**	**LONG TERM**
	emerging standard for enabling computing resources and services	standards, security, management and compliance aspects regarding Cloud Computing	progressively from 'as a product' to 'as a service' ▪ Growth of Cloud Computing (private and public) ▪ Advances in Cloud Computing (standards, management, compliance,..)	(becomes IT standard) in certain fields of application ▪ Cloud is auto-managed ▪ Profound changes in current models (dynamic provisioning of resources, software in the cloud,…)
	INTEROPERABILITY			
	▪ Lack open and shared standards between civil and military	▪ Identification of open standards ▪ Application of Service Level Agreements	▪ Full use of open standards	▪ Full use of open standards
	FEDERATION OF SYSTEMS			
	▪ Standalone and heterogeneous systems with proprietary interfaces ▪ Expensive systems duplication	▪ Reuse of existing systems ▪ Implement MS gateways to interface networks ▪ Wrap legacy systems in services interfaces	▪ Federation of systems within a specific mission	▪ Wide use of federated systems between MS ▪ Full interoperation within the network

6.2 EU NEC KEY MESSAGES

297 A centralised "top down" approach is necessary for delivering common elements of EU NEC. This approach demands governance and autonomous budgets for supporting EU NEC Capability. A centralised EU plan would describe the realisation of the EU NEC environment.

298 The plan would address the three dimensions of NEC (PIT) and focus on:

- Better collaboration:
  - Synchronisation of exoisting and planned efforts/initiatives, more services, definitions of COI, new business processes and better definition of existing ones, more portals and information exchange mechanisms, unified education and training, more horizontal exchanges.
- Better information:

        - Better quality of information, more sharing, improved protection, more structured information, same language, information discovery, Information Services registry, management of information profiles, adapted legislation.
    - Better connectivity:
        - Federation of networks, interconnection of networks, better access of individuals;

299 The plan cannot be conducted in isolation. It must include the efforts done by NATO for the military area; hence coordination of capability development and C3 activities is a must.

300 Technology development will provide new capabilities for EU CMO. These new technical capabilities along existing ones (legacy) support the "bottom-up" approach which improves existing EU NEC Capabilities. This development can be conducted in a decentralised approach.

301 EU NEC has a cost. The efficiency is provided by synergetic effort of MS and EU, facilitating that MS do not pay twice. However, the overall costs of continuing to develop non-coordinated initiatives will be higher.

7. REFERENCES

[1]. Treaty on European Union

[2]. Treaty of Lisbon, signed 13 December 2007

[3]. EU concept for NEC in support of ESDP (doc. 12737/08+COR 1);

[4]. "Developing network-enabled capabilities in support of ESDP" (document 9453/1/09 REV 1 + COR 1)

[5]. European Security Strategy, adopted 13 December 2003

[6]. An Initial Long-Term Vision for European Defence Capability and Capacity Needs, EDA, October 2006

[7]. Civil Military Co-ordination (CMCO), Doc 14457/03, 07 November 2003

[8]. Network Enabled Capability, JSP 777 Edn 1.Ministry of Defence UK.

[9]. Headline Goal 2010. Endorsed by the European Council. 18 June 2004

[10]. Civilian Headline Goal 2010. Doc. 14823/07. 19 November 2007.

[11]. EU Concept for CIS for EU-led Military Operations. Doc 11702/08. 10 July 2008.

[12]. Chaillot Paper nº 90. Civilian crisis management: the EU way. (Institute for Security Studies, Jun 2006)

[13]. EDA Tendering Specifications (EDA 08-CAP-19 NEC Implementation Study, 2008)

[14]. Global Overview and roadmap for identification of Information Exchange Requirements (2007)

[15]. McGraw-Hill Concise Encyclopaedia of Engineering. © 2002 by the McGraw-Hill Companies, Inc.

[16]. The American Heritage® Dictionary of the English Language, Fourth Edition copyright ©2000 by Houghton Mifflin Company. Updated in 2009. Published by Houghton Mifflin Company.

[17]. Dictionary of Military and Associated Terms (DoD, Joint Publication 1-02, 31 August 2005)

[18]. NATO C3 Technical Architecture. V5 - NC3 Common Operating Environment (NCOE). Appendix C. TERMINOLOGY

[19]. UK MoD (The Information Warfare Site, 2003).

[20]. NATO Architecture Framework (NAF) version 3.

[21]. NATO Interoperability Standards & Profiles (NISP) version 2 (http://nhqc3s.nato.int/architecture/_docs/NISPv2/index.html)

[22]. Final NIAG Interoperability Study Report SG-137: Achieving NATO Interoperability Industrial contribution (NATO Industrial Advisory Group, 2009)

[23]. Operations Research Applications for ISR (Defence Science Board, 2009)

[24]. European Approaches to Civilian Crisis Management (Report of Cris Lindborg, Basic Special Report, March 2002, p.4)

[25]. Summary of a Workshop on Information Technology Research for Crisis Management (National Academy of Sciences, 1999)

[26]. Understanding Command & Control (David S. Alberts and Richard E. Hayes, CCRP 2006)

[27]. National Information Assurance Glossary (CNSS Instruction No. 4009, Revised June 2006)

[28]. Global Information Grid Information Assurance Policy Recommendations (National Security Agency Information Assurance Directorate, June 2004)

[29]. NIF™ v2 Solution Description Reference Manual (NSD-RM), NCOIC, 16 November 2008.

[30]. Net-Centric Services Framework, Version 2.1, NCOIC, 2009-10-01

[31]. Final Report: IERs for ESDP Operation, 08-CAP-001, EDA, 28.05.2009.

[32]. CDP - List of generic military tasks, Internal EDA document.

[33]. EDA - NEC Synergy Campaign, version 1.0, As of 22 December 2009 for euronec use.

[34]. EUMC View on the Network Enabled Capabilities (NEC) Implementation Study (IS) Draft Final Report, 11488/10, Brussels, 24 June 2010.

[35]. EUMC Interoperability Study – Final Report, 16741/09, Brussels, 26 November 2009

[36]. DIRECTORATE GENERAL FOR EXTERNAL POLICIES OF THE UNION DIRECTORATE B, The Lisbon Treaty and its implications for CFSP/ESDP, DG EXPO/B/PolDep/Note/2009_169 01 September 2009

8. GLOSSARY AND ABBREVIATIONS

302 Glossary of terms and abbreviations are found in the separate document “euronec 09_029 NEC IS CEWA AV-2”.