NATO Consultation, Command and Control Agency

Agence de Consultation, de Commandement et de Conduite des Opérations de l'OTAN

# NATO NETWORK ENABLED CAPABILITY FEASIBILITY STUDY EXECUTIVE SUMMARY :

VERSION 2.0

## CONDITIONS OF RELEASE

With reference to NATO Documents C-M(2002)49 and AC/322-D/1, this document is released to a NATO Government at the direction of the NATO Consultation, Command and Control (C3) Agency subject to the following conditions:

1. The recipient NATO Government agrees to use its best endeavours to ensure that the information herein disclosed, whether or not it bears a security classification, is not dealt with in any manner contrary to the intent of the provisions of the Charter of the NATO C3 Organization.

2. If the technical information was originally released to the Agency by a NATO Government subject to restrictions clearly marked on this document the recipient NATO Government agrees to abide by the terms of the restrictions so imposed by the releasing Government.

# NATO NETWORK ENABLED CAPABILITY

## FEASIBILITY STUDY

## EXECUTIVE SUMMARY:

## VERSION 2.0

T. Buckman

Communications and Information Systems Division

*Keywords: NNEC, NEC, NCW, NCO, Network Centric, Network Enabled, NBO*

***Abstract***

*The NNEC Feasibility Study is an 18 month study funded by 12 nations who have contributed organized within the context of NC3B. The aim of the study is to develop the scope and vision for NNEC and to establish the necessary context for developing the C3 aspects of NNEC. This document focuses on presenting an executive summary of the contents of Volumes I and II of the NNEC Feasibility Study Final Report.*

The work described in this report was carried out under Project Multinational NNEC Feasibility Study of the NC3A Programme of Work for 2004/2005.

NATO Consultation, Command and Control Agency
October 2005

This document consists
of **vi** + 34 pages
(excluding covers)

*This page is left blank intentionally*

*This page is left blank intentionally*

# TABLE OF CONTENTS

## TABLE OF FIGURES

**Page**

*This page is left blank intentionally*

## 1. BACKGROUND

At their meeting in November 2002, the NATO C3 Board (NC3B) agreed that there was a need to develop a NATO concept to adapt national initiatives such as the U.S. Network-Centric Warfare (NCW) and the U.K. Network Enabled Capability (NEC) to the NATO context. This NATO concept is referred to as “NATO Network Enabled Capability” (NNEC).

Under the heading of new capabilities agreed to at the Prague Summit, the Heads of State approved a comprehensive package of measures, based on NATO’s Strategic Concept to strengthen the ability of the Alliance to better carry out the full range of its missions and respond collectively to new security challenges by creating a NATO Response Force (NRF), streamlining NATO’s military command arrangements and by approving the Prague Capability Commitments.

The utilization of these new capabilities by an NRF in conducting new NATO missions raises a range of new requirements, to include fundamentally new requirements for supporting C4ISR systems.

## 2. MOTIVATION

In response to the measures agreed at Prague, the NATO Strategic Commanders (SCs) have developed a set of “Transformational Goals” and “Transformational Objective Areas” (TOAs) ( Figure 1 ) to support the development of capable future forces that are able to undertake the future missions of the Alliance.

One of the key TOAs identified by the SCs is Network Enabled Capability (NEC). This capability, as described by the SCs, involves the linking together of sensors, decision makers, and weapon systems, as well as multinational military, governmental, and non-governmental agencies in a seamless, collaborative, planning, assessment and execution environment. The NEC must provide for the timely exchange of secure information, utilising communication networks which are seamlessly interconnected, interoperable and robust, and which will support the timely collection, fusion, analysis and sharing of information.

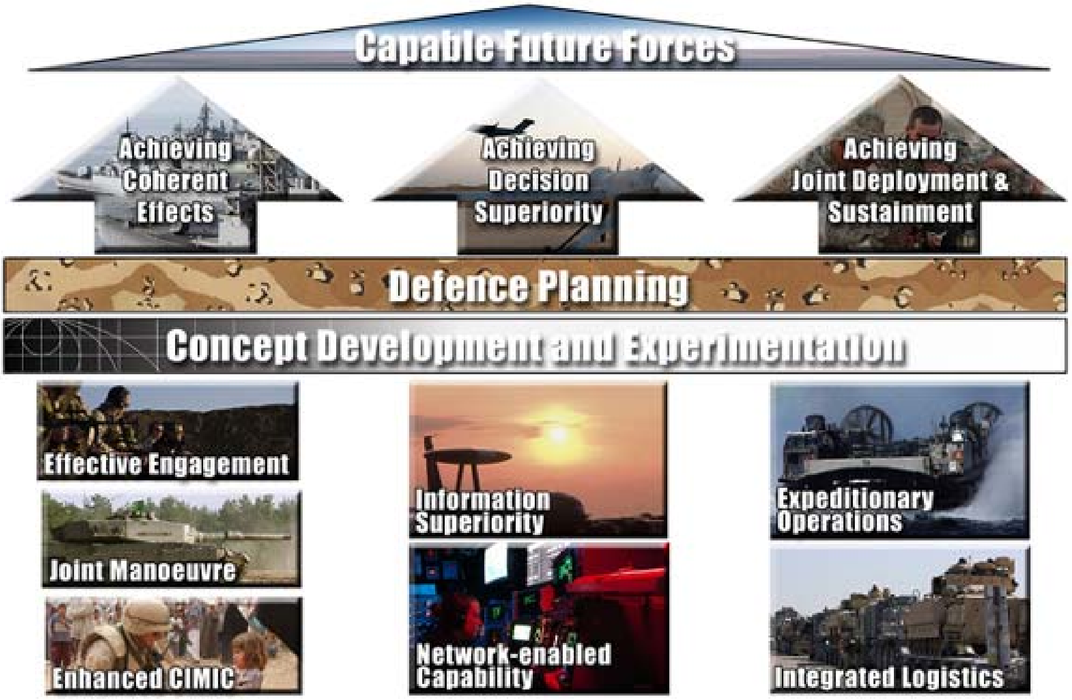

Capable Future Forces
Achieving Coherent Effects
Achieving Decision Superiority
Achieving Joint Deployment & Sustainment
Defence Planning
Concept Development and Experimentation
Effective Engagement
Joint Manoeuvre
Enhanced CIMIC
Information Superiority
Network-enabled Capability
Expeditionary Operations
Integrated Logistics

Figure 1 Bi-SC Framework for Transformation

### 2.1.1 To Effectively Utilize National Capabilities

The development of a NATO NEC is viewed by many nations as the most effective way for their nation to be able to use their own investments to the full in information age technologies and 'NCW type' capabilities in supporting future coalition operations. NNEC provides the right environment for developing a common approach to the conduct of these future operations, developing the architectures, standards, process and procedures necessary to enable the flexibility and agility needed to conduct future network-centric operations in a collation context. The decision taken by twelve NATO nations to fund the NNEC Feasibility Study is a strong endorsement on their part for the need for such a common approach. In effect nations are saying that they wish to do within an Alliance, what they plan to do as a nation: i.e. develop network enabled capabilities.

### 2.1.2 The Need for a Networking and Information Infrastructure (NII)

The motivations for developing NNEC outlined above have a number of far-reaching implications. Firstly, there is the need to extend communication networking capabilities to 'wherever they are needed, whenever they are needed', implying the need for a 'flexible global networking capability'. Secondly, there is a need to support smaller, modular, multinational force structures such as the NRF, generating new information-sharing and security requirements that will increase critically of interoperability requirements and could redraw NATO/national interoperability boundaries. Thirdly, there is the need to support the rotation of national force elements within the NRF and to support seamless interoperability with force elements from non-NATO nations that may not even be identified until a mission is already underway. These points imply the need for an unprecedented degree of flexibility, agility, adaptability and interoperability in the force structures involved and in the networking and information systems that support them.

It is clear that the Alliance will only be able to achieve its operational ambitions if future force structures are well supported by flexible, adaptable, highly interconnected, communication networks and information systems. The collection of information and communication networking infrastructure capabilities needed to support these future missions is referred to in the remainder of the Report as the "Networking and Information Infrastructure" (NII).

# 3. AIM OF THE STUDY AND STUDY APPROACH

## 3.1 AIMS

The NNEC FS has been conducted with two aims in mind: to support further development of the concept of NNEC, and to establish a strategy and a roadmap for developing the Communication and Information Systems (CIS) aspects of NNEC.

## 3.1 FURTHER DEVELOPMENT OF THE CONCEPT OF NNEC

The further development of the concept of NNEC begins with the tenets of Network-Centric Warfare (NCW) and their incorporation into NATO concepts of operation. The aim of using the tenets is to establish clear linkages between new NATO operations, the military vision of NATO's strategic commanders for conducting these missions and the types of CIS capabilities required to support them. The tenets of NCW, listed in Table 1, can be related to three fundamental dimensions which need to be considered in establishing these linkages: Networks, Information and People.

**Table 1 Basic Tenets of Network-Centric Warfare**

| Basic Tenets of Network-Centric Warfare |
|---|
| 1. A robustly networked force improves information sharing. |
| 2. Information sharing enhances the quality of information and shared situational awareness. |
| 3. Shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command. |
| 4. These, in turn, dramatically increase mission effectiveness. |

### 3.1.1 Networks

The focus on networks is highlighted in the first tenet, pointing to the need for a 'robustly networked force' to enable improved information sharing. The size, scope and reach of the network(s) required are determined by the missions, force structures and concepts of operations involved. A major focus of the NNEC FS is to establish a clear linkage between the shape of future NATO operations and the types of networking capabilities required to 'robustly network' future NATO forces.

### 3.1.2 Information

The focus on information and its use is highlighted in the second and in parts of the third tenet. These tenets point to the need to exploit robust networking capabilities to improve information sharing; to enhance the quality of information shared, collaboration, and shared situational awareness.

The type of information which needs to be shared, the people with whom it needs to be shared, and the speed with which the information needs to be gathered and made available, is determined by force structures, concepts of operations, and the way the information is utilized to support a mission. A major focus of the NNEC FS is to establish a clear linkage between the shape of future NATO operations and the types of information, information processing and information sharing capabilities required to support these missions.

### 3.1.3 People

The focus on people and the benefits of working together in a networked environment is highlighted in portions of the third and fourth tenets. These highlight the role of improved information sharing and shared situational awareness in allowing people to work together in new more effective ways and thereby to improve speed of command, leading to dramatic increases in mission effectiveness. The tenets make it clear that implementing NCW involves adapting the way people think and work together

The NNEC FS addresses the dimension of ‘people’ from the perspective of achieving “Decision Superiority”. Decision Superiority is defined as *“the state in which better-informed decisions are made and implemented faster than an adversary can react”*. Decision superiority is critically dependent on achieving and maintaining a position of information dominance and shared situational awareness during all phases of an operation, to enable a better understanding of the operational situation than the adversary. It means that the pace, coherence and effectiveness of operations can be dramatically improved, resulting in dramatic reductions in the length of decision cycles.

A major focus of the NNEC FS is to establish a clear linkage between the shape of future NATO operations and the types of information collection, processing, and dissemination capabilities needed to enable decision superiority.

There are other aspects to the ‘people’ dimension of NCW which are not addressed within the NNEC FS. These are the cognitive and social aspects of NCW, which relate to the longer term impact of networking and information sharing on the way people think and work together. Just as the Internet has fundamentally changed the way in which most people communicate and work together, in business and in their private lives, so will the introduction of new networking and information sharing capabilities within NATO ultimately change the way that people think and work together in conducting future NATO operations.

## 3.2 DEVELOPING A STRATEGY AND A ROADMAP

Development of NNEC calls for the development of new strategies and new planning techniques to help structure and coordinate development activities of NATO and NATO nations. The NNEC FS outlines new strategies for developing future Consultation and Command

and Control (C3) capabilities as well as developing supporting networking and information sharing capabilities.

### 3.2.1 Strategy For Future C3 Capabilities

The strategy for developing future C3 capabilities is based on the Capability-Based Planning (CBP) approach. A capabilities-based paradigm focuses more on how an adversary might fight than on whom the adversary might be and where a war might occur. It requires us to identify capabilities that military forces will need to deter and defeat a particular type of adversary. This approach involves a functional analysis of operational requirements, leading to the identification of capabilities required to accomplish a mission. Once the required capability inventory is defined, the most cost effective and efficient options to satisfy these requirements are sought. This process involves the mapping of operational capability requirements to a supporting set of system functional requirements, which identifies the system capabilities required to support a mission.

While the concept of CBP is key to the identification of required system functionality, the concept of Service Oriented Architectures (SOAs) and a unified communications networking infrastructure is key to meeting those requirements and are an essential part of the overall strategy. SOAs provide a flexible modular approach for implementing system functional requirements in the form of services and a unified networking makes sure that those services can be accessed and utilized. This strategy for developing future C3 capabilities responds to the need for a flexible, modular approach for meeting future Consultation and C2 requirements.

### 3.2.2 Strategy for the Networking and Information Infrastructure (NII)

The strategy for developing the networking and information sharing aspects of NNEC focuses on the ‘joining together’ of networking systems and core information systems from NATO and NATO nations, to form a Federation-of-Systems (FoS) capability that implements the NII. The FoS concept is used here to refer to a set of different systems, which are not centrally managed, but are so connected or related so as to produce results beyond those achievable by the individual systems alone. In effect, the NII is to be made up of a combination of national Networking and Information Infrastructures segments and a NATO Networking and Information Infrastructure (NNII), which together will provide capabilities that no one system can provide by itself.

# 4. OPERATIONAL NEEDS

## 4.1 MISSION CONTEXT AND TRANSFORMATIONAL OBJECTIVE AREAS

A realistic and pragmatic approach has been taken in identifying representative operational needs for NNEC. The process is based on agreed Defence Requirements Review (DRR) planning situations and involves the use of operational concepts, which in some cases, goes beyond those currently approved by the NATO Military Committee (MC).

The use of draft ACT and ACO coordinated operational concepts strikes a reasonable balance between unbridled speculations as to how NATO may choose to operate in the future and limiting the assessment of operational needs to the automation of existing processes based on current operational concepts. It should be noted that one of the primary reasons for developing a network-enabled capability is the possibility it holds for enabling new ways of doing business, which in military terms translates into new operational concepts. The development of NNEC and the assessment of the feasibility of developing a NATO NEC necessarily considers emerging thinking on how NATO might operate in the future which go beyond currently approved MC concepts.

The backdrop for assessing operational needs stems from work within the biannual NATO Defence Requirements Review (DRR) process. The 2005 DRR Planning Situations, approved by the Military Committee, have been utilized to produce a set of design reference scenarios covering counter terrorism operations, urban operations and maritime entry. These scenarios have been used with the NATO "Concept for Joint Precision Engagement" developed within the 2005 DRR, to develop "Concepts of Employment for NRF Forces" that have been used with the Design Reference Scenarios developed within the study.

The assessment of operational needs is structured in accordance with the Bi-SC Framework for Transformation shown in Figure 1. The assessment covers operational needs associated with the Transformational Objective Areas (TOAs) of: Effective Engagement, Integrated Logistics, Expeditionary Operations and Enhanced CIvil MIitary Cooperation (CIMIC).

### 4.2 OPERATIONAL NEEDS WITHIN EFFECTIVE ENGAGEMENT

Within the study, the assessment of operational needs within the TOA of Effective Engagement focused on the 'sensor, shooter and decision maker' relationship, specifically focusing on the area of Time Sensitive Targeting (TST). TST is concerned with the conduct of rapid, flexible, precision engagements, where the emphasis is on reducing response times associated with the detection and engagement of targets from days and hours to minutes. TST raises some of the most demanding requirements for networking support and timely information sharing.

A careful assessment of operational needs in the area of TST has been conducted during the course of the study based on the emerging concept for Joint Precision Engagement, under development by the Strategic Commands. It is clear that are urgent operational requirements which need to be addressed in this area. The details of this assessment are contained in Volume I, Chapter 3 and Annex C to Volume I.

### 4.3 OPERATIONAL NEEDS WITHIN INTEGRATED LOGISTICS SUPPORT

The design reference scenarios generate demanding requirements for logistics support to NATO forces located in the tactical area of operations. Distribution of logistic supplies from airports or seaports of disembarkation to manoeuvring NRF forces can be particularly demanding, involving the movement of supplies across distances of a 1,000 kilometres or more to supply NRF forces made up of troops from a number of contributing nations.

Recent and on-going NATO operations have been challenged by inefficiencies in the provision of logistics support to deployed forces due to redundancies and duplication of effort inherent in separate national supply chains. If NATO is ever to achieve the levels of operational agility in expeditionary operations implied by the design reference scenarios, such inefficiencies must be eliminated

### 4.4 OPERATIONAL NEEDS WITHIN ENHANCED CIMIC

Enhanced CIMIC is the NATO Joint Force Commander’s primary means of building relationships between NATO forces, the indigenous political authorities and civilian organisations within his JOA. Development of strong relationships greatly helps to shape and establish a stable environment within which the mission may be completed more easily. In order to be successful in this, military activities must be harmonised with those of the relevant civilian organisations and agencies where possible and appropriate.

Operational workshops conducted with the Strategic Commands during the course of the study highlighted the importance of enhanced CIMIC, based on operational lessons learned of workshop participants. Reaching political consensus on NATO’s future CIMIC role will be an important first step in clarifying operational requirements in this important area.

### 4.5 OPERATIONAL NEEDS WITHIN EXPEDITIONARY OPERATIONS

The section on the TOA of Expeditionary Operations is limited to considering issues associated with the distribution of headquarter staffs into theatre. Current exercises have identified this as a key area impacting improved deployability of mission-ready forces and allowing a reduction in the footprint of deployed forces. This is an area where the availability of a robust communication and information infrastructure is a critical enabling element in overcoming many of the problems associated with the distribution of staff.

## 5. A TRANSFORMATIONAL STRATEGY FOR NNEC

A Transformational Strategy for NNEC has been developed based on concepts for operational transformation, originally developed by the Supreme Commander, Allied Command Transformation (SACT). These concepts are used in conjunction with the Overarching NNEC Architecture Framework, developed under the NATO Overarching Architecture (OAA) project, along with material presented in Volume I to develop this transformational strategy.

### 5.1 THE OPERATIONAL PHASES OF TRANSFORMATION

SACT’s vision for the attributes of a transforming force, includes four phases, referred to in this document as the Operational Phases of Transformation. These phases capture the idea that operational change will be an ‘evolutionary’ process involving a ‘step-by-step’ approach to the way force elements and supporting organization work together to realize the longer term ambitions of NNEC. These ideas are illustrated in Figure 2, which is based on a similar diagram used by SACT.

Each phase of transformation emphasizes different operational needs that in most cases will require the development of new system capabilities. This progression in operational needs can be related to a progression in types of system capabilities required to help meet those needs.

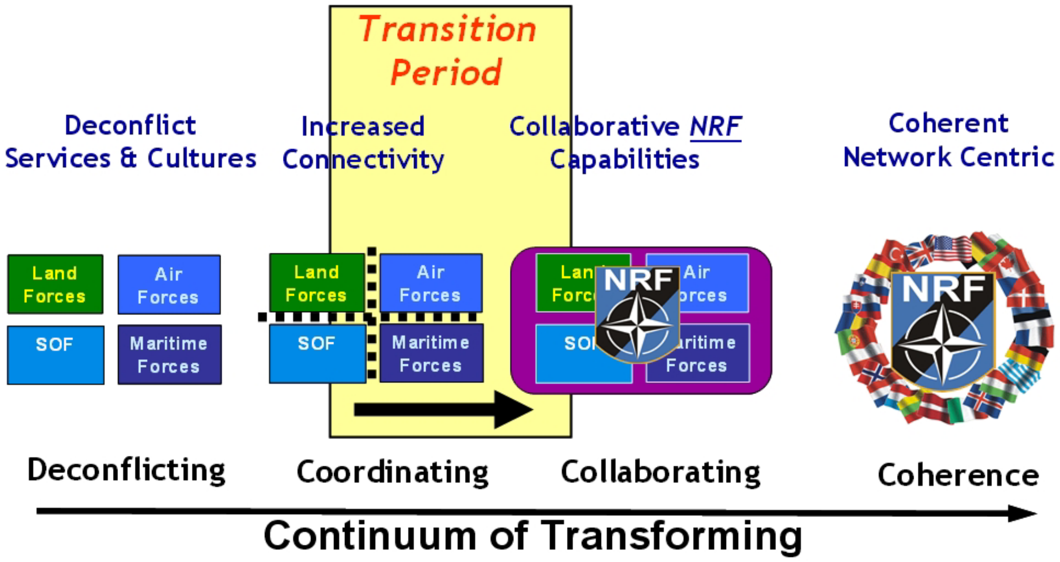


Figure 2 Attributes of a Transforming NATO Force

Relating progressions in operational needs to types of system capabilities, requires an architectural framework to help organize and categorise system capability requirements.

## 5.2 RELATING OPERATIONAL PHASES TO SYSTEM CAPABILITIES

Relating the Operational Phases of Transformation to system capability requirements involves the use of the Overarching NNEC Architecture framework shown in Figure 3 This framework is taken from earlier work done on the NATO Overarching Architecture in 2003 .

Layers 5 and 4 of the diagram relate to the Consultation and C2 system needs, while the areas shown inside the dotted line make up the NII.

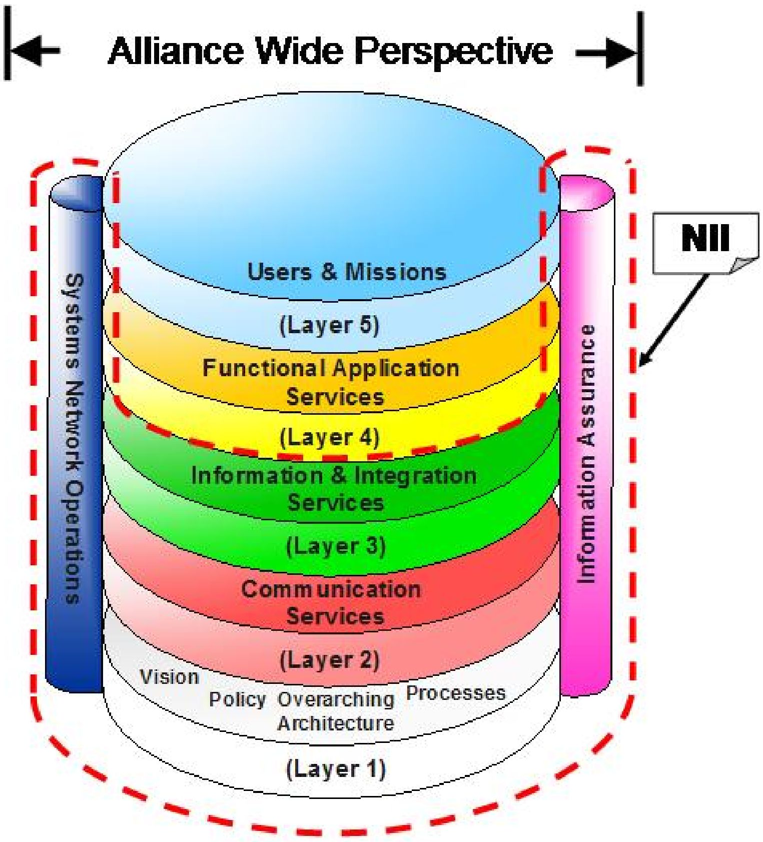
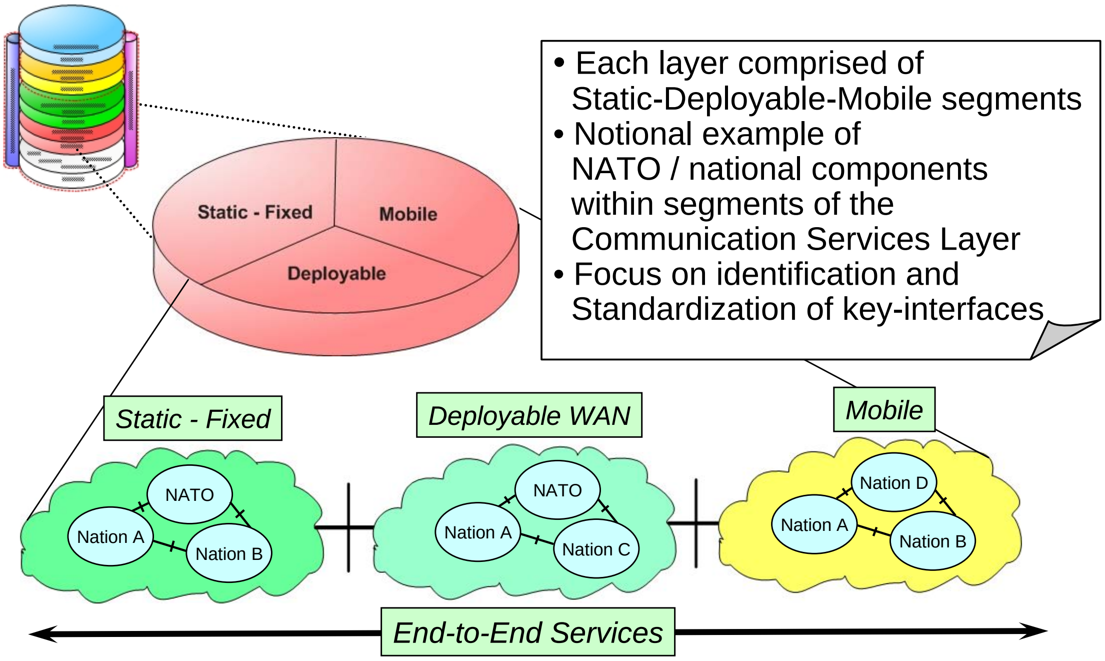

Alliance Wide Perspective
NII
Systems Network Operations
Information Assurance
Users & Missions
(Layer 5)
Functional Application Services
(Layer 4)
Information & Integration Services
(Layer 3)
Communication Services
(Layer 2)
Vision
Policy Overarching Architecture
Processes
(Layer 1)

Figure 3 Framework for development of an Overarching NNEC Architecture

Each layer of the system engineering framework diagram can be expand to show additional structural details An example for the Communication Services layer is shown in the 'cloud' diagram at the bottom of Figure 4. This diagram provides a notational view of the NII Communications Layer, illustrating contributions from NATO and national segments and key interfaces between these segments.



- Each layer comprised of Static-Deployable-Mobile segments
- Notional example of NATO / national components within segments of the Communication Services Layer
- Focus on identification and Standardization of key-interfaces

Figure 4 Details of the Overarching NNEC Architecture Framework

Figure 5 represents an amalgamation of Figure 2 and Figure 3. It illustrates the idea of evolving operational needs, leading to assessments of architectural concepts and required technology needed to support these needs. All of the components shown in Figure 3 are impacted by this evolution in operational needs:

- Functional Application Services
- Information Integration Services
- Communications Services
- Information Assurance Services
- System Management and Control
  (i.e. System and Network Management)
- Policy, Processes and Architectures

Figure 5 highlights the impact of this process on the Functional Application, Information and Integration, and Communications Services layers. Information Assurance and System Management and Control Services operate as a kind of a “back plane” behind these the layers shown in the diagram, in the sense that their services are to be provided to all of the layers shown in Figure 5.

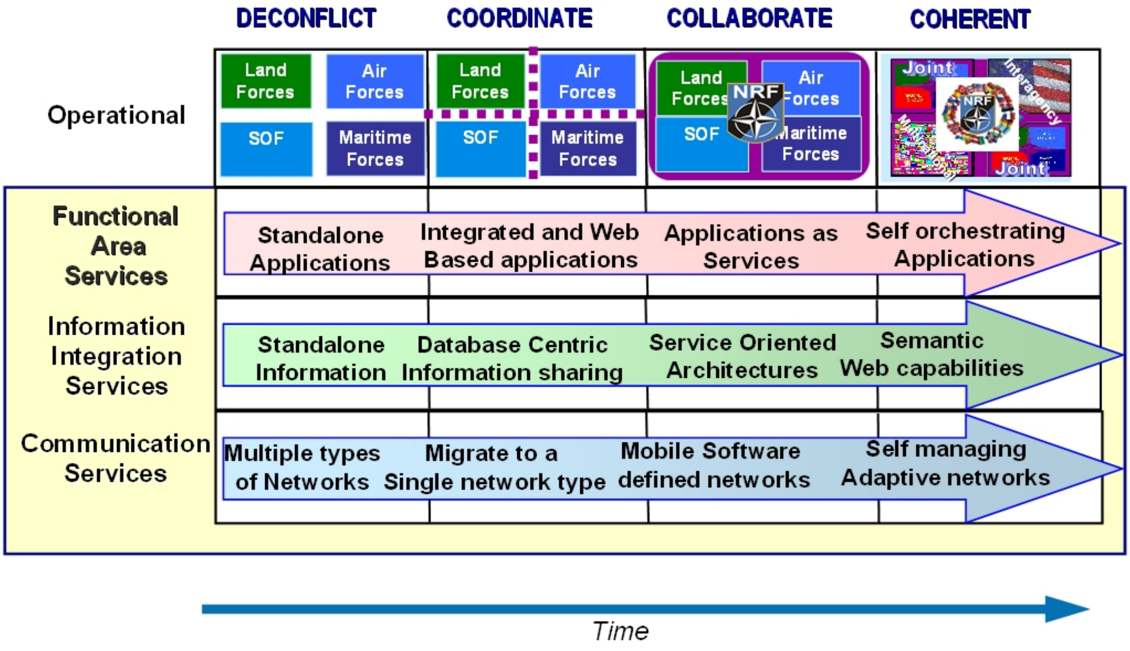

DECONFLICT
COORDINATE
COLLABORATE
COHERENT
Operational
Land Forces
Air Forces
SOF
Maritime Forces
NRF
Joint
Interagency
Multinational
Functional Area Services
Standalone Applications
Integrated and Web Based applications
Applications as Services
Self orchestrating Applications
Information Integration Services
Standalone Information
Database Centric Information sharing
Service Oriented Architectures
Semantic Web capabilities
Communication Services
Multiple types of Networks
Migrate to a Single network type
Mobile Software defined networks
Self managing Adaptive networks
Time

**Figure 5 Evolving C3 Requirements and Technology Trends for NNEC**

## 5.3 TRANSFORMATIONAL MATURITY LEVELS

An initial assessment of operational needs revealed common patterns across the TOAs that could be readily associated with the operational phases of transformation. These ideas are illustrated in Figure 6, and described below in terms of operational phases and associated C3 development ‘themes’. This model provides a key input to Volume II and is used in Volume I in the chapter on “Developing The System Aspects of NNEC”.

### 5.3.1 Deconfliction Phase – Functional ‘Stovepipes’

The general theme for CIS support associated with this phase is ‘Functional Stovepipes’ and is used to describe the condition, prior to the start of transformation. It is characterized by the use of standalone applications, databases and multiple types of communication networks. There is little joint situational awareness and little collaboration due to incompatibility of applications, networks and data. In this phase the operational effectiveness is hampered by inadequately structured CIS support.

This phase assumes the use of current doctrine, organizations, process and equipment. Organizations are largely hierarchical and specialized according to functional criteria. Interoperability is, for the most part, limited, involving human intervention or limited physical connectivity that provides for some interaction between systems.

### 5.3.2 Coordination Phase – to Communicate and Inform

The general theme associated with this phase is ‘Communicate and Inform’, viewed as the initial phase of transformation. This phase aims at breaking the information barrier. Better sharing of information will lead to better shared situational awareness, and is regarded as the first step in transformation. It will be characterized by the introduction of an improvement in basic communications and information sharing capabilities, thereby immediately improving operational effectiveness. Improvements in communications will involve migration towards a single type of network for voice, data and video traffic and will include improved interoperability between static, deployable and mobile networks utilizing data link technology. Improvements in information sharing will involve the introduction of major improvements in position reporting capabilities among expeditionary forces and improved utilization of various forms of messaging technology to support machine-to-machine, user-to-user and machine-to-user data interchange. Simple collaborative tools are in place, and joint situational awareness will improve through the introduction of a joint Common Operational Picture (COP) capability.

This phase assumes the use of current doctrine, but involves some organizational and process changes. There is a move towards collaborative organizations, with improved collaboration occurring across functions and echelons of command within predefined Communities of Interest (COIs). Interoperability is generally improving, involving the ability of independent applications to exchange and use independent data components.

### 5.3.3 Collaboration Phase – to Collaborate and Plan

The general theme associated with this phase is ‘Collaborate and Plan’ and is viewed as the transitional phase. This phase aims at breaking the collaboration barrier. By exploiting the shared situational awareness in a better way, decisions can be made towards better actions in the field. This phase will be characterized by the introduction of advanced collaboration and planning capabilities. Advanced collaborative tools will be used to support large scale vertical and horizontal collaboration and to support advance adaptive-planning processes within and across COIs. Situational awareness will improve through collaboration and planning activities and through the continued integration of data sources into the COP. Users will be able to generate and understand the battlespace in a manner that is appropriate to their task and consistent with the understanding of others.

This phase assumes major organizational and process changes. Organizations will be fully collaborative at this stage, working within pre-planned and ad-hoc COIs. Vertical synchronization of activities through collaboration and planning will ensure a full understanding of commander’s intent, while lateral synchronization will be achieved through shared awareness of the operational situation. Interoperability will continue to improve and include domain data and meta-data models and the development of new procedures for COIs. Improved data and meta-data sharing among independent applications will allow theses applications to work together in an integrated fashion.

### 5.3.4 Coherent Effects Phase – to Sense and Respond

The general theme associated with this phase is ‘Sense and Respond’ and is viewed as a mature phase of NNEC. This phase aims at breaking the interaction barrier. It is thought that the seamless and transparent collaboration of all parties involved will lead to unprecedented mission effectiveness. This phase is characterized by the proliferation of sensor capabilities and information sharing capabilities at all levels, and by continued improvements in functional capabilities to enable extremely rapid and agile responses to changing circumstances and fleeting opportunities.

This phase assumes that new doctrines and organizational structures are in place and that COIs may be formed dynamically and in an ad hoc fashion. Interoperability will generally improve to a point where a top-level perspective including enterprise data and meta-data models and procedures will exist, and where data will be seamlessly shared among applications able to work together across domains in an integrated fashion.

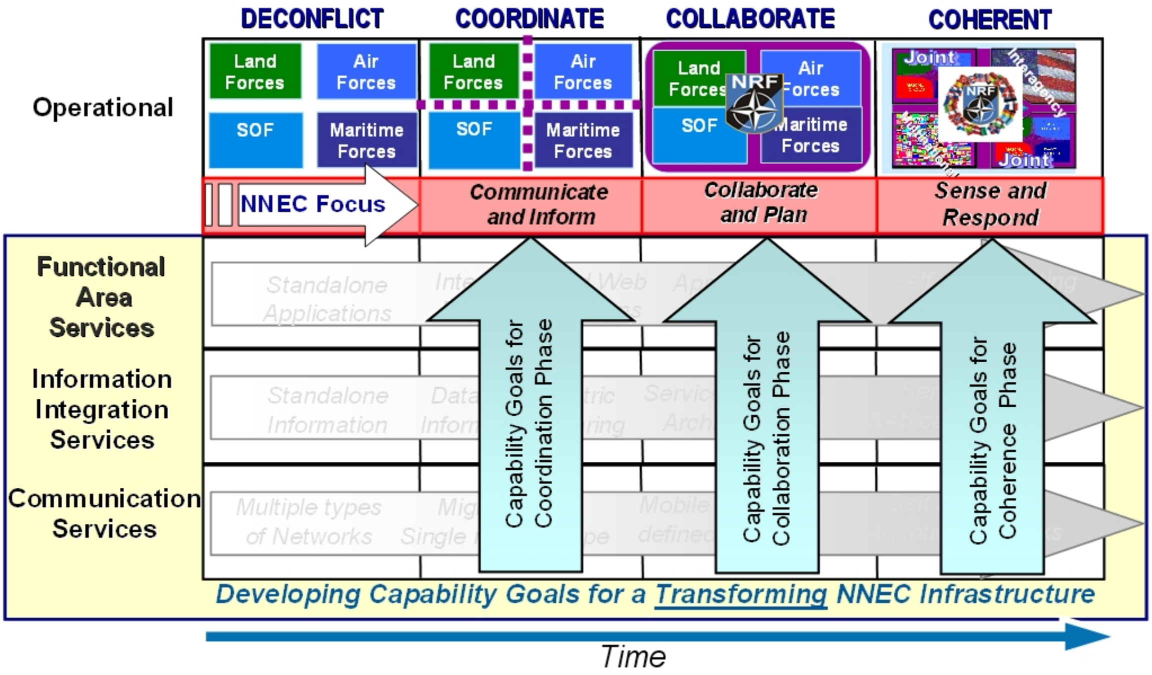


Figure 6 Transformational Maturity Levels

# 6. PLANNING FOR IMPLEMENTATION

## 6.1 INTRODUCTION

The Transformational Strategy, presented in Chapter 5, provides the context for planning a series of transformational phases that respond to the operational needs of the Alliance. These phases provide a step-by-step approach for implementing C3 capabilities that provide operational benefits at each step along the way.

The development of a common Networking and Information Infrastructure (NII) is a key element of the Transformational Strategy. In essence, the NII is the networking capability that enables future C3 and NNEC. Volume II of the study has focused on developing a Strategy and a Roadmap for the NII that responds to the operational needs that arise from the Transformational Strategy.

This chapter outlines steps that need to be taken to implement the NII and translate the ‘Transformational Strategy for NNEC’ into reality.

## 6.2 AGREE A STRATEGY FOR THE NII

The implementation of the NII involves the independent efforts of NATO and NATO nations to build systems which can be joined together to implement the NII. The success of such an approach beings with participants sharing a common view of what it is they are building and agreeing to comply with a minimum set of ‘building codes’ to ensure that the pieces will ‘fit’ together to achieve the common purpose.

The strategy proposed for building the NII is similar to the way in which the Internet has been built and operates today. The Internet has no central control authority. At its core it depends on the Internet Engineering Task Force (IETF) to coordinate the development of common standards that allow independently developed networks to interconnect and interoperate to create the common set, of world-wide, accessible services, that we know as the Internet today. The success of the approach is evident, with the Internet being made up of more than 60,000 networks.

A description of what it is that we are trying to build is provided in the remainder of this section in terms of key elements, which give the NII its defining characteristics. A detailed description of the main components making up the NII is provided in Volume II, Chapters 3 through 6.

### 6.2.1 Key Communication Elements

The communications component of the NII is characterized by the intended use of the Internet Protocol (IP) to provide a common, secure transport mechanism for all types of information moving across all types of transmission media. The process of adoption IP as the common transport mechanism will take time. It requires that IPv6 be adopted for any new systems and that IPv4 continues to be support for some time to come. This will happen first across static network infrastructures and needs to move quickly to be supported across deployable networks. Key to this process will be the standardization of interfaces between deployable SATCOM terminals, and static networks and the optimization of these deployable networks to support IP traffic. This standardization process will help support the development of a SATCOM pooling concepts for the Alliance, which will be particularly important in supporting Expeditionary Operations.

Development in flexible IP encryption devices and supporting key management systems is a key pacing technology for all NII services. The rapid fielding of interoperable IP encryption devices is key to the development of a so called “black” core network, a single, virtual, network-of-networks, operating at the NATO UNCLASSIFIED level, that can handle voice, video and data traffic for multiple security domains and classification levels.

Along with development in IP encryption devices, rapid progress is needed in the area of passing of information between IP and non-IP networks. “Edge Proxy” is the name given within the study to standardized devices that sit on the edge of IP networks, acting as an interface to non-IP networks and providing information proxy services as well as communications layer services. The use of edge proxies to support the interfacing of Tactical Data Links to IP networks is particularly important in the near and mid term.

The adoption of a common IP transport mechanism requires that significant progress continues to be made in a number of technical areas to support the longer term needs of mobile users. These areas include waveform standardization, the development of common software architectures for tactical radios, improved spectrum usage, and improved mobile networking protocols. The long-term goal of supporting mobile IP depends on the maturing of Mobile Ad Hoc Networking (MANET) protocols to include full Quality of Service (QoS) support.

Development activities to support all levels of maturity need to start now. This involves activities focused on the development and fielding of capabilities to support near-term objectives, activities focused on concept development and experimentation to support mid-term objectives, and activities focused on research and development of key technologies to support long-term objectives.

### 6.2.2 Key Information And Integration Elements

The Information and Integration component of the NII is characterized by the use of Service Oriented Architectures to expose software functions as consumable services that can be discovered and invoked across the network. The use of SOAs ease application and data sharing and provide a flexible mechanism for reusing existing services to enable the development of new, value-added information services.

A primary goal of the SOA approach is to make information resources available to all consumers on the network and support the efficient discovery and delivery of that information to the consumer.

The use of the SOA approach requires that we adopt a common Net-Centric Data strategy to ensure that we make information visible, accessible, understandable and interoperable with other sources of information. Trusting the information we get and trusting that the information we supply will be handled correctly will be a key success factor. The ability to provide flexible, secure, role-based, information access that can be quickly configured to support changing policy is foundational to the long-term success of the NII.

Realizing the benefits of the SOA approach will require that we agree on a standardized set of foundational services covering such areas as service discovery security, metadata management, identify management, service management and mediation.

Utilization of an SOA approach requires that end-users on non-IP networks also be taken into account. Edge Proxies will need to help manage information flows between high-bandwidth and low-bandwidth users.

Making rapid progress in securely sharing ‘text based’ information, coupled with rapid progress in the use of “XML-enabled technologies will be key to the development of Information and Integration services in the near to mid term.

Robust, secure messaging - e-mail, formal messaging, instant messaging – is foundational to the development of IIS, and the ability to support secure, text-based, information exchange means that XML-encoded information can also be exchanged securely. This will support the interaction between databases, applications and users to enable the development of a wide variety of secure, interoperable information services.

One of the keys to the widespread use of XML-enabled technologies is meta-data standardization and this is an area where it will be vital that the Alliance establishes strong leadership position. Much of the standardization work to be done involves the development of domain specific (i.e. COI specific) vocabularies, which requires the participation of domain experts. Military specific vocabularies require the participation of military experts, not only to define the core vocabularies for various COIs but to also define the semantic relationships that exist between the words themselves (i.e. ontologies). This standardization activity is key to information interoperability at all levels of maturity, key to future concepts of information security and key to the use of machine based reasoning / agent based technology that will provide the foundation for meeting the longer term objectives for IIS and the NII in general.

### 6.2.3 Key System Management And Control Elements

Supporting secure, end-to–end, service management and control, and the use of Service Level Agreements across multiple, independently managed sub-networks with Quality of Service support is the challenge which best characterizes the System Management and Control component.

Service Level Agreements (SLAs) play a vital role in the overall architecture in ensuring adequate levels of performance. The concept of SLAs is well known in the world of communications services, but the concept will need to apply to the provision of information and security services as well to system management and control services themselves. The demand of providing adequate levels of performance is often crucial in the tactical domain, where bandwidth is typically limited. Meeting this challenge will depend on technical progress being made in a number of technical arenas, such as provisioning of increased bandwidth to mobile users, supporting security services and the dynamic mapping of SLA across NATO and national segments.

There are many technical details to be worked in this area which will require technical experts from contributing nations to work together to agree and implement common approaches to support end-to-end services.

### 6.2.4 Key Information Assurance Elements

Information Assurance mechanism are embedded into every aspect of the overall architecture and work together to achieve the overall aim of protecting information whether at rest or in motion. These mechanisms help ensure that the right information, can be delivered to the right people at the right time, and that the information that they receive can be trusted. The emerging approach of “Duty to Share Balanced with the Need to Know” captures this intent. Duty to Share helps ensure that policies, procedures, and systems are developed and implemented with an inherent capability to share information, but have the necessary security measures in place to ensure only authorized users can access the information.

In the near-term IP encryption and key management infrastructures are key to meeting the needs for secure communications. Work also needs to begin now with PKIs and XML technologies to enable the fielding of dynamic, role-based, policy-based, information access schemes in the mid-term. One of the major challenges that the Alliance faces will be the deployment of an Alliance-wide, interoperable, PKI infrastructure and identity management scheme to support information access schemes.

Continued, rapid technology development in the areas discussed above will be the key to scaling these technical approaches to meet long-term ambitions for information security, which is aligned with the concept of object level encryption, where information is protected at the information object level and access is controlled based on a users identity and a users role within any particular operation. The sheer scale of encryption, key management and rapid policy based access decisions that will need to be made will require some major technology breakthroughs.

## 6.3 DEVELOP A TRANSFORMATIONAL PLAN

The implementation of the Transformational Strategy requires that participants share a common plan and that nations implement agreed capabilities.

### 6.3.1 Utilize A Capability Based Planning Approach

The mechanism for formally identifying and agreeing national contributions to a common plan, within NATO, is Defence Planning. NATO Defence Planning is currently being supported by a Capability Based Planning approach conducted through the biennial NATO Defence Requirements Review process. The shift to a CBP approach within the DRR began in 2003 and is being extended in 2005 to provide a more comprehensive approach to Defence Planning. The comprehensive DRR goes beyond traditional force planning to consider armaments, resource, and C3 capabilities in more detail.

Annex A of Volume I describes an extension to the DRR, CBP approach which effective replaces NATO's traditional C3 Planning process. This approach ensures that C3 capability and investment requirements can be directly linked to mission requirements. Defence planning in the age of Network Enabled Capabilities requires that the beneficial effects of network enabling forces be reflected in the development of force proposals and force goals. The outcome of this process needs to be reflected in C3 capability planning.

It has not been possible to fully utilize the NNEC CBP methodology during the course of this study. However the logic of the CBP methodology underpins the approach taken in conducting the study and it has been possible to provide an example of how the methodology might be implemented. The example involves the analysis of NATO Time Sensitive Targeting requirements, and the results of this analysis are included in Annex C, to Volume I.

The conclusion drawn from the work done during the course of this study is that the proposed NNEC CBP should be further developed to support NATO C3 planning and used to support the development of capability proposals for national C3 systems.

### 6.3.2 Develop An Overarching NNEC Architecture

CBP identifies capability requirements, but it does not provide a 'blueprint' telling us how systems need to function and work together to satisfy these requirements. For this we need an architecture to help NATO and NATO nations program system development activities. The current NC3 Board sponsored, C3 Overarching Architecture provides the starting point for accomplishing this task.

The NATO C3 Overarching Architecture (OAA) is structured to support CBP, taking capability requirements and translating them into a Federation-of-systems architecture that specifies what systems need to do and how they need to work together to satisfy these requirements. Detailed plans have been developed for extending the OAA to incorporate results from the NNEC FS. However, execution of the plan is dependent on NATO nations adopting the outcomes of the NNEC FS.

It is recommended that the current NATO C3 OAA be extended to produce an Overarching NNEC Architecture that specifies what NATO systems need to do to support NNEC and how they need to interoperate with national systems to support the operational ambitions of the Alliance.

### 6.3.3 Develop An NII Interoperability Framework

System planners and developers in NATO and NATO nations will need to share a common set of specification that describe how their systems need to interoperate. The proposed Overarching NNEC architecture will generate these types of interface specifications and can be used to develop a 'NII Interoperability Framework' (NIIF).

The NII Interoperability Framework (NIIF) will play a crucial part in supporting the process of implementing the NII. It is to be made up of two principal components: the NII Capability Maturity Model (NII-CMM), and the NII, $I^2$ Index. Broadly speaking, the role of the NII-CMM will be to support programme planning and auditing activities, across NATO and the nations while the $I^2$ Index will serve as a much more detailed, technical reference document, intended for use by project managers, architects, system engineer and developers.

The development and maintenance of the NIIF depends on an architectural development process that supports the development of each the constituent parts of the NIIF. This process will involve the use of the NNEC Overarching Architecture.

The development of the NIIF will necessarily involve domain experts from NATO and NATO nations working together and ideally should involve domain experts from industry as well. If we are to produce a NIIF that is relevant and up to date, it should involve the people who actually build the systems that we specify.

The NIIF will need to be developed. It is a key enabler, underpinning the development of the NII, providing the interface specifications that nations need to be able to independently develop systems that can be joined together to form the NII.

### 6.3.4 Develop Net-Readiness Criteria

Developers of NIIF compliant systems will need to be able to test their system to ensure that they satisfy NIIF interface specifications and that they perform adequately. Systems that are able to do this are ready to be connected to the NII, and are referred to as being NII 'Net-Ready'. The specification of adequate testing and certification criteria needs to be based on the contents of the NII Interoperability Framework and in particular on the contents of the NII $I^2$ Index.

### 6.3.5 Conduct A Capability Audit

The Overarching NNEC Architecture describes a desired end state at future point in time and provides an essential element for conducting a capability audit of existing and planned systems. The Overarching NNEC Architecture along with the NIIF and NII Net-readiness criteria provide a sound basis for conducting a detailed capability audit of projects in existing NATO Capability Packages. A detailed capability audit will lead to recommendations to eliminate some projects, modify other projects and suggest new projects that need to be incorporated into NATO's capability plans.

It is recognized that the development of Overarching NNEC Architecture, the NIIF and NII Net-Readiness criteria will take some time, and that it will be necessary to continue to make progress in developing and fielding capabilities. Hence it is recommended that an initial capability audit be conducted using the results of the NNEC FS to identify projects that clearly do not contribute to the development of NNEC and to suggest project that will clearly be required. The initial audit can be done, while preparatory work for the detailed audit is underway. The output from the initial audit will provide a valuable input to the detailed audit.

It is recommended that both an initial and a detailed audit be conducted. This will provide NATO with an evolutionary approach to reviewing and modifying its capability plans to bring them in line with NNEC requirements.

### 6.3.6 Develop A NNII Capability Roadmap

The final phase in the planning process involves the development of a time-phased plan for implementing required capabilities.

The technology and capability availability roadmaps developed in Volume II provide examples of the types of planning products that will be needed to develop a NNII capability roadmap. These diagrams provide summary descriptions of required NII capabilities tied to estimates of when it may be possible to field such capabilities. These estimates were produced using the Technology Availability Roadmaps coupled with optimistic estimates of the time required to develop and field capabilities within NATO.

Information from the capability and technology availability roadmaps need to be compared with project descriptions from the modified capability plans to produce the NNII capability roadmap.

The NNI Capability Roadmap can be used to sequence project development work, schedule resources and keep nations informed of NATO’s plans to develop its segment of the NII.

## 6.4 SUPPORTING THE IMPLEMENTATION OF THE PLAN

Implementing the NII will require nations to work together on common architectural and system engineering issues and to work together to ensure a consistent approach to testing and certifying systems as being Net-Ready.

### 6.4.1 Develop An NII System-Engineering Group

There are certain capabilities that the NII will need to possess that require the adoption of common architectural and system engineering solutions. End-to-End Quality of Service support for the transport of information across the NII is one example. Other examples exist in areas such as Network Management, Traffic Engineering, and Information Assurance. In addition, there will be problems encountered as we begin to field system and interconnect them. Some of these problems will require the identification and adoption of a common solution.

The development of the NII will require that architects and system engineers from NATO and NATO nations meet together to develop these common solutions and that they continue to support the continued development and evolution of the NII. Just as the Internet required and continues to require an Internet Engineering Task Force, so will the NII require a dedicated System-Engineering Group.

A key recommendation from the NNEC Feasibility Study is that an 'NII System-Engineering Group' be established to work with subject matter experts from NATO and NATO nations to address common requirements and facilitate the development of common solutions.

### 6.4.2 Develop Test And Certification Capabilities

Testing is a necessary part of building any large complex system. When developing a Federation -of-Systems solution like the NII, it is particularly important that developers have access to testing facilities that allow them to interconnect their system to other systems, to simulate the Federation-of-Systems environment and verify the ability of their system to function properly.

MC/477 lists a general requirement for NRF certification testing to verify the readiness levels of NRF units. It is anticipated that this certification requirement will need to include Net-Readiness certification.

It is recommended that NATO and NATO nations accelerate their efforts to interconnect their testing facilities and make them available to support system development testing and Net-Readiness certification testing.

## 7. SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

### 7.1 SUMMARY

The NNEC FS has been conducted with two aims in mind: to support further development of the concept of NNEC and to establish a strategy and a roadmap for developing the Communication and Information Systems (CIS) aspects of NNEC.

The further development of the concept of NNEC began with the tenets of NCW, which call for the 'robust networking' of forces and improved information sharing. An initial review of NATO operational needs made it apparent that the provision of the networking and information sharing to NATO operational forces would necessarily involve the 'joining together' of communication systems and core information systems from NATO and the nations. The term Networking and Information Infrastructure (NII) was adopted to refer to this collection of systems.

The focus shifted to determining what kinds of capabilities the NII will need to provide, and when they will need to provide it by. Current and future operational needs were assessed for a representative expeditionary force structure, the NRF, conducting a counter terrorism type mission. The identification of operational needs involved the use of Design Reference Scenarios and the new NATO concept for Joint Precision Engagement. Operational lesson learned and results from experimentation work were also used in identifying operation needs. The operational needs were used to develop requirements for the NII, which are representative of the types of capabilities that the NII will need to provide in the future.

The NII requirements were organized to allow for a time phased evolutionary development of system capabilities, and used as the starting point for developing the NII strategy and roadmap. Architectural concepts were formulated and technology availability accessed to develop capability availability roadmaps. The capability roadmaps provide an assessment of when capabilities might be fielded and generally available to support NATO operations.

## 7.2 CONCLUSIONS

Operational needs have been accessed, a Transformational Strategy proposed, capability and technology availability roadmaps developed, and possible implementation schedules accessed. The overall conclusion is that NNEC is needed to meet the future operational needs of the Alliance and that the networking capability needed to enable NNEC is the NII. We have concluded that it is challenging, but technically feasible to implement the NII. However it seems evident, based on the work done during this study, that without major changes in NATO CIS implementation and operational structures, policies, and processes that, NATO will find it difficult to achieve NNEC

The Transformational Strategy presented in Chapter 5 outlines a series of transformational phases that provide a step-by-step approach for planning and implementing capabilities that respond to the operational needs of the Alliance. The proposed architectural approach, involving, the use of the NII responds to the needs we can identify today and is flexible enough to respond to the needs of tomorrow, which we may not be able to foresee today. Change is one constant in our future, and modularity, flexibility and agility will have to be the hallmarks of future forces and of the systems that support them. The NII development strategy developed during the course of this study and presented in this report is capably of meeting those demanding requirements.

.