# Implementing NATO Network Enabled Capability: Implications for NATO Response Force's Envisioned Roles

**Colonel Reynold F. Palaganas**
United States Army

> ***…NATO will no longer have the large, massed units that were necessary for the Cold War, but will have agile and capable forces at Graduated Readiness levels… [to] prepare the Alliance to meet any threat.…***
>
> – General James L. Jones, Supreme Allied Commander Europe (SACEUR)[1]

The North Atlantic Treaty Organization (NATO) Response Force (NRF) represents a new dimension in deployability and interoperability of NATO and nationally provided rotational forces. Alliance heads of state endorsed the NRF concept during the 2002 Prague NATO summit. It is a work in progress with two envisioned roles: (1) operating as a high readiness, modular quick reaction force for strategic crisis response from the North Atlantic Council (NAC) that sets NATO priorities; and (2) serving as NATO's transformation catalyst as the entry point for capability improvements.[2] Future expeditionary operations will rely on NRFs in a Collaborative Information Environment (CIE) capable of conducting Effects Based Operations (EBO) and striving for "decision superiority" (DS).

NATO Network Enabled Capability (NNEC) – the vehicle for network-centric operations as a Transformational Objective Area (TOA) – is defined as "the Alliance's ability to federate various components of the operational environment, from the strategic level down to the tactical levels, through a networking and information infrastructure [NII]."[3] It has the objective potential to exploit economies of scale for collectors, decision makers, and effectors through coordinated capabilities distributed across nations.[4]

NNEC's vision and strategic challenge is to improve operational effectiveness through complex networking of Alliance and national capabilities.[5] To transform NRF operations from a "platform-centric" to a "network-centric environment," NATO Consultation, Command and Control (C3) elements, NATO's two strategic commands, member nations, and industry must move beyond CIE rhetoric and "business as usual" Cold War mindset as enterprise network stakeholders by implementing a Federation-of-Systems (FoS)[6] NNEC concept as the interoperability[7] driver that joins common interfaces and information services.

Research scope is based on an unclassified literature review and assistance from NATO subject-matter-experts. The paper introduces NRF principles and NATO commanders' relevant strategic vision concepts. It presents a working definition of Network Centric Warfare (NCW) and identifies tenets associated with the four domains of warfare. The U.S. Department of Defense's (DoD) Net-Centric Operations and Warfare (NCOW) and the United Kingdom's (U.K.) Network-Enabled Capability (NEC) models are highlighted as forerunners of NNEC. The paper describes roles of relevant NATO bodies and NNEC conceptual framework components. It then analyzes impediments to implementing NNEC and NRF role implications. These include dealing with a legacy oriented environment, technological insertion gaps, and national and NATO common funding contribution levels. Substantive details regarding potential participation from non-NATO nations, civilian, and Non-Governmental Organizations (NGO), an effects-based approach to joint operations construct, NRF operational attributes, or NNEC competency levels are beyond the scope of this research.

## NRF Principles and NATO Commanders' Strategic Vision Concepts

### NRF Principles

The deployability principle translates to a multinational expeditionary force of up to 25,000 troops with land, maritime, air, and special operations components and standard component command headquarters task organized for high and low intensity missions.[8] NAC approves its employment under the "first force in, first force

out" principle. The Combined Joint Statement of Requirement (CJSOR) is a force catalog indicating types of capabilities for NATO defense planning scenarios. NRF readiness requires 5-30 days notice-to-move within or beyond the Euro-Atlantic area for an operation usually 30 days long, depending on the element deployed and embedded logistics capabilities.[9]

The scalability principle means the NRF commander configures the modular force to a scenario. Minimal required capabilities range from a stand-alone force for NATO Article 5 (collective defense) or non-Article 5 (crisis response, out-of-area) operations such as evacuation operations, disaster consequence management, humanitarian crisis, or counter-terrorism with specialized forces commanded by a single headquarters; to an initial entry force facilitating follow-on units' arrival; to being assigned to a larger force for high intensity missions.[10]

The rotation principle allows equitable burden sharing and broadening of joint operations experience. At NATO force generation conferences, member nations contribute rotating forces for a minimum capabilities package. The NRF goes through a process of training and SACEUR certification, followed by a six month operational stand-by period. Joint Force Command (JFC) of the NRF rotates among one of NATO's three permanent headquarters based in Brunssum, (the Netherlands), Naples (Italy), or Lisbon (Portugal).[11]

The NRF's initial operating capability was declared in October 2004. Full operational capability will occur following a June 2006 exercise.[12] NRF force packages were activated in contingencies, however, including humanitarian assistance to U.S. Gulf Coast victims of Hurricane Katrina and Pakistan's earthquake relief efforts in 2005.[13]

## NATO Commanders' Bi-Strategic Vision: EBO, CIE, DS Enabling Concepts

"Strategic Vision: The Military Challenge by NATO's Strategic Commanders" reflects guidance from SACEUR (General Jones) and Supreme Allied Commander Transformation (SACT – then Admiral Edmund P. Giambastiani, Jr.) regarding Alliance transformation of

forces, concepts, and capabilities (Figure 1). It sets the scene for the *Concept for Alliance Future Joint Operations* (CAJFO).[14]

This section summarizes mutually exclusive definitions for EBO, CIE and DS. They collectively describe an expeditionary force able to create desired battlespace effects, employ "net-centricity" (a robustly interconnected information environment enabling horizontal and vertical collaboration), and conduct multinational operations interdependently.

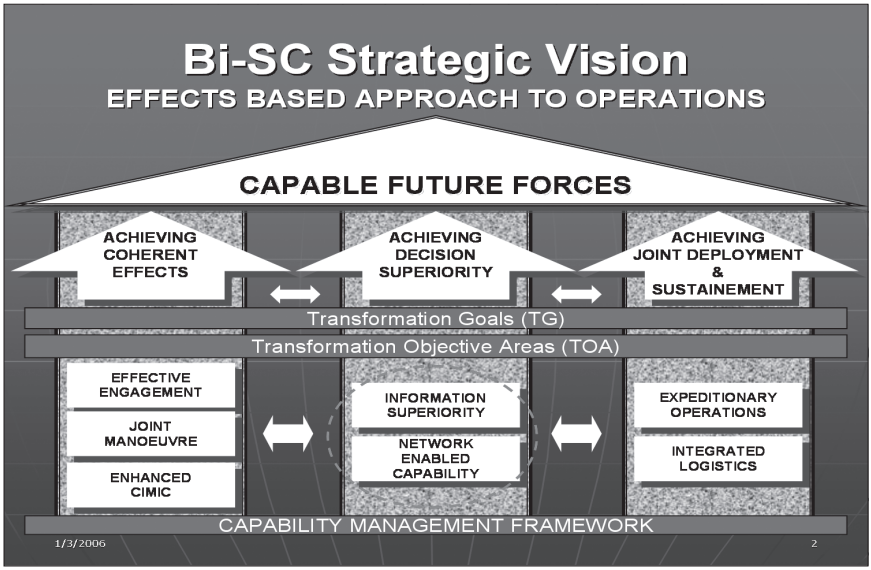


Figure 1: Framework for Transformation[15]

EBO. All elements of Alliance power – diplomatic, information, military, economic – (DIME) are applied and integrated to create campaign effects to achieve desired outcomes.[16] John Admire, an expert on transforming coalition warfare, interpreted EBO's significance to the NRF: "[The] objective is a responsive and networked force to influence and adapt to an adversary's actions by enabling us to shape and reshape our options and actions amid the uncertainty of battle and crisis situations."[17] The NCW effects-based system links sensors, shooters, and decision makers as knowledgeable entities to achieve desired functionalities such as surveillance or precision strike, rather than distinguishing between platforms and military services.

CIE. Admire cites U.S. Joint Forces Command's definition:

> The aggregation of individuals, organizations, systems, infrastructure, and processes structured for…creating and sharing data, information, and knowledge necessary to plan, execute, and assess joint force operations and enable the commander to make better and faster decisions than the adversary.[18]

For NRF defense planning, it would transition from a vertical or hierarchical serial process to parallel collaborative planning with a flattened structure.[19]

DS. NATO's strategic vision defines "decision superiority" as follows:

> The state in which better-informed decisions are made and implemented faster than an adversary can react, [sic] allowing the future joint force commander to shape the environment to best fit his needs and objectives. [It] is critically dependent on achieving and maintaining a position of information dominance [read: information superiority] and shared situational awareness during all phases of an operation.[20]

In Figure 1's transformation framework, "information superiority" (IS) and "network-enabled capability" (NEC) underpin the DS pillar and serve as key enablers for all TOAs.

## Network Centric Warfare and NATO Network Enabled Capability - Background

NCW Tenets

NATO C3 Agency (NC3A) Chief Architect Dr. Tom Buckman stresses in the *NNEC Feasibility Study* (NNEC FS) that further NNEC development as a Federation-of-Systems has to incorporate NCW tenets into NATO concepts of operation.[21] Numerous literature exists advocating NCW as a new way of thinking on how a force operates. NCW experts David Alberts, John Garstka, and Frederick Stein offer a widely acknowledged NCW hypothesis in *Network Centric Warfare, Developing and Leveraging Information Superiority*:

> *An information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization.*[22]

NCW's four tenets in Figure 2 comprise the theory behind NNEC: that is, a flexible network creating an information advantage among geographically dispersed forces which results in a decisive warfighting advantage.[23] There are two takeaway points from this diagram. First, joining static, deployable, and mobile segments accentuate the potential power of "networked" robust military nodes. Second, the theoretical NCW "value chain" refers to "networking" interactions present in a warfighting force's four domains: information, cognitive, social, and physical.

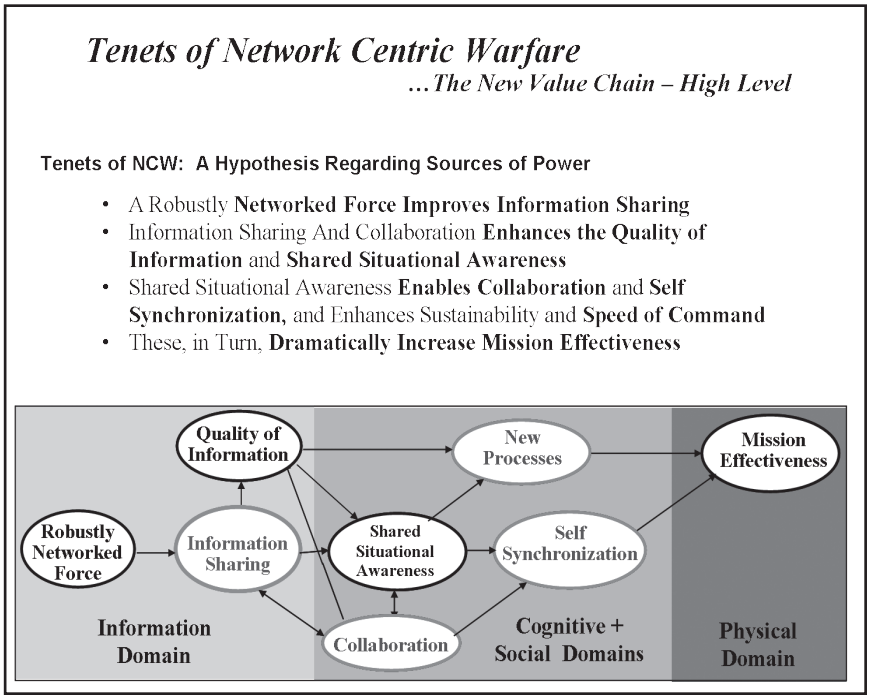


Figure 2: Tenents of Network Centric Warfare[24]

"Information Domain": This is cyberspace where information is created, managed, shared, and protected. Command and Control (C2) of military forces is communicated and commander's intent is conveyed.[25]

"Cognitive Domain": This is the mind of the warfighting participants and supporting populace – the realm of EBO in which the force is capable of sharing awareness via collaboration, making decisions, and taking actions based on commanders' intent. It is characterized by intangibles such as leadership, unit cohesion, morale, situational awareness, and public opinion.[26]

"Social Domain": This domain operates in the societal background of cultural awareness and assessing change.[27]

"Physical Domain": This is the traditional warfare domain where strike, protect, and maneuver take place across the environments. Operations are synchronized with the right information at the right place at the right time in the right format because this is where physical platforms and networks connecting them reside.[28]

## NATO Network-Centric Frames of Reference

NATO's network-centric frames of reference can be traced to two leading NATO nations: the U.S.' NCOW and U.K.'s NEC models. The NCOW model supports DoD's *Joint Vision* and *Joint Operations Concepts* strategic documents to describe conduct of future joint military operations. A Joint Force's emphasis on full spectrum dominance necessitates a capabilities-based approach.[29] NCOW describes how DoD applies net-centricity to daily business and warfighting activities. NCW results from fully applying NCOW. To transform forces away from a platform-centric to a networked force,[30] DoD strategy requires: (1) centralized, policy-based planning; (2) decentralized execution; (3) shared awareness; and (4) agility (flexibility and adaptability).

U.K.'s NEC model supports the operational goal to "conduct effects based operations with highly responsive, well integrated and flexible joint force elements that have assured access to an unprecedented freedom of manoeuvre within the entire battlespace."[31] Its core elements are sensors, a network, and strike assets. NEC aim is to support the U.K.'s "Defence Capability," the armed forces' ability to support government policy in the future strategic environment.[32]

U.K. defense policy mindset requires that it "…act[s] as an effective and capable member of a U.S.-led coalition as [its] most likely principal partner in any major military operation."[33] NEC development strategy will not be wholesale transformation as this is cost-prohibitive, but rather evolve as prioritized capabilities when equipment and systems become obsolete. NEC's envisioned role is to enable formation of agile forces (i.e., traditional warfighting communities, including core and ad hoc mission groupings), by assembling prescribed building blocks so NEC supports a set of different communications systems optimized for different environments.[34]

## Relevant NATO Bodies

Table 1 (facing page) summarizes NATO relevant bodies involved in NNEC development and implementation.

| RELEVANT NATO BODIES | NNEC ROLE |
|---|---|
| NATO Military Committee (MC) | - Responsible for overarching NNEC concept<br>- Advises the North Atlantic Council (NAC) on NNEC |
| NATO Consultation, Command, and Control Board (NC3B) | - Acts as the Board of Directors of the NATO C3 Organization (NC3O); oversees the work of two NC3O constituent agencies: the NATO C3 Agency (NC3A) and NATO Communications and Information Systems Services Agency (NCSA)<br>- Serves as NNEC link to the Nations and coordinates with other NATO staffs, such as the Infrastructure Committee and Military Agency for Standardization<br>- Keeps MC informed on NNEC activities; overarching authority in C3 architectures to enable effective integration of C3 capabilities |
| -- NC3A | - Chartered to develop, procure, and implement state of the art capabilities for NATO and provide high level scientific advice and testbed support to NATO bodies<br>- Formed NNEC Integrated Capability Team<br>-- Developed NNEC Feasibility Study (NNEC FS)<br>- Provides Integrated Project Team (IPT) for NRF and coalition interoperability |
| -- NCSA | - Chartered as a military command to provide end-to-end secure NATO-wide information exchange and information processing services using fielded Communications and Information Systems (CIS) |
| NATO Headquarters Consultation, Command, and Control Staff (NHQC3S) | - Provides support to the NAC, MC, and other NATO committees as a single integrated civilian and military staff; supports NC3B<br>- Coordinates all C3 aspects of NNEC, including policy and standards guidance |
| NATO Bi-Strategic Commands | |
| -- Allied Command Transformation (ACT) (Commanded by Supreme Allied Commander for Transformation (SACT): Norfolk, VA) | - Formed an ACT IPT<br>- Under authority of the MC:<br>-- Developed NNEC Foundation Document<br>-- Developed overarching NNEC Vision and Concept<br>-- Develops NNEC Strategic Framework documents<br>-- Develops NNEC capabilities; lead for Concept Development & Experimentation (CD&E) to focus on how emerging solutions are to be used operationally<br>-- Adapts military doctrine and training for the NRF |
| -- Allied Command Operations (ACO) (Commanded by Supreme Allied Commander Europe [SACEUR] Casteau, Belgium) | - Has military operational command over the NRF<br>- Focuses on current operations; has operational planning/mission execution that includes NRF standards, certification, and exercises/contingencies |

Table 1: Relevant NATO Bodies and NNEC Roles[35]

## NNEC Conceptual Framework

ACT's *NNEC Foundation Document* presented initial NNEC perspectives as a precursor to NC3A's *NNEC FS* and ACT's *NNEC Vision and Concept*. These are starting points for the *NNEC Strategic Framework*, a series of five sequential documents under development detailing key activities, milestones, and identifying investment requirements for NNEC delivery.[36] NNEC's complexity has steered ACT to incrementally seek nations' endorsements of these documents staffed for MC approval.

Whereas the centerpiece for NCW tenets in Figure 2 is oriented to a theoretical behavior chain interaction supporting the four warfare domains, the conceptual framework centerpiece in Figure 3 encompasses NNEC's components: integrating "human processes" with "information" in a "network" to link collectors, decision makers, and effectors in an open standards environment commensurate with changing technology and doctrine.

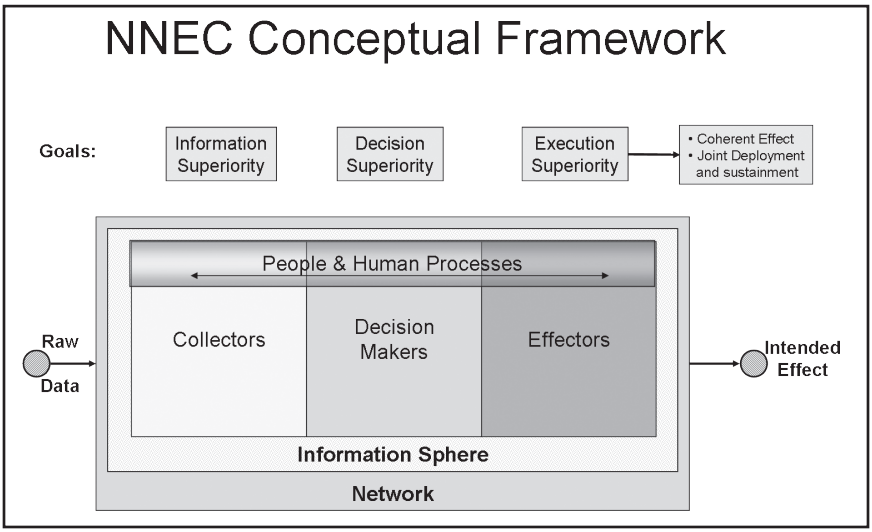


Figure 3: NNEC Conceptual Framework[37]

The "network" component comprises NII's physical infrastructure: communications, network, computer, and core services layers. Service Level Agreements (SLAs) specifying adequate performance levels for the user such as extended reach and increased bandwidth,

rapid reconfiguration on short notice, and network security are keys to effectively managing scarce system resources. This component constitutes the framework's "technical" aspect.

The "information" component encompasses information management aspects oriented toward a need-to-share. In the information sphere resides a collection of logical busses or virtual databases. This component constitutes the framework's "organizational" aspect.

The "people" component constitutes the framework's "social" aspect that includes organizational users, national stakeholders, industry, and cultures. NATO and the nations can be interconnected between human aspects of information technologies and shared networks.

These broad components express NATO's blueprint transformation from a stovepiped to an NII enterprise. What has yet to be nested into the NRF environment are redefining tactics, techniques, and procedures as part of an evolving CIS management strategy. For instance, to allow operational commanders more flexibility to develop their tactics and deploy NRF packages, NNEC must federate evolutionary capability changes that redefine interoperability boundaries or apply enterprise controls to preclude disjointedness.

## Impediments to Implementing NNEC and NRF Role Implications

The Alliance justification to equip the NRF with NNEC is to enable "operational effectiveness" – what a 2001 RAND report calls "a transformation of NATO from a regional defensive alliance to a worldwide responsive and offensive force"[38] in highlighting deployability, scalability, and rotational burden-sharing principles. Yet the litmus test – achieving nations' commitments of providing robust and capable linkages to reinforce network-centric tenets – reveals slow progress and a "business as usual" mindset. At the outset, NATO has to clearly define NRF minimal capabilities in the CJSOR for each scenario against what rotating nations will earmark for C3 capability. Challenges with implementing NRF NNEC are rooted in overcoming interoperability impediments. This section analyzes three implementation concerns with implications on the NRF's envisioned roles: dealing with a legacy environment,

technological insertion gaps, and national and NATO common funding contribution levels.

## Dealing with a Legacy Platform-Centric Environment

One impediment to implementing NNEC is dealing with the legacy environment. Standardization Agreements (STANAGs) and CIS policies in the mid-1980s reflected single service force doctrine characterized by inflexible, point-to-point connectivity ("one-to-one" static network relationships).[39] Maritime, air, and land forces were previously task organized as separate services, relying on rigid interoperability via direct information exchange requirements (IERs – also called information flows). IER elements included who needed to talk to whom, over what means/system, in what format, and with what products and volume. This vertical linear thinking meant national military services separated their geographical battlespace areas to optimize their platform-centric systems at the expense of network synchronization.

A network-centric operations environment represents a paradigm shift. The right side of figure 4 depicts NNEC's reliance upon standardized layers of network common interfaces and protocols to allow horizontal interoperability across functional areas without regard for national origin, vice vertical connectivities within service component functions as shown on the left.

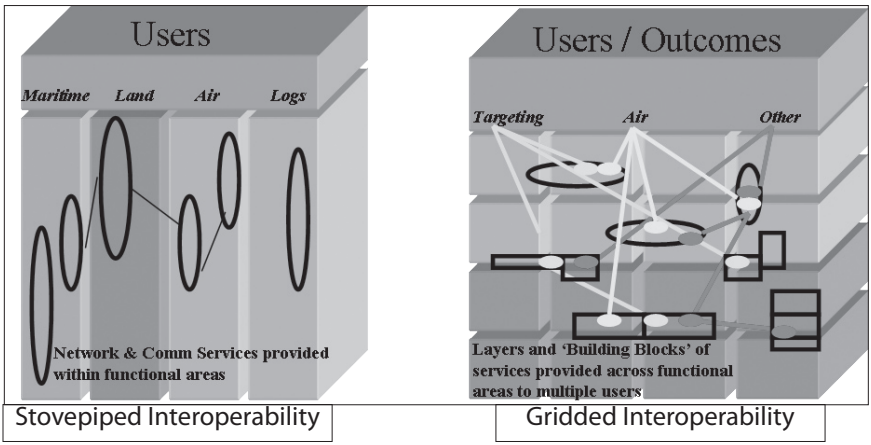


Figure 4: Joint Interoperability: A Stovepiped Versus Gridded, Multi-layered Approach[40]

An NII grid consists of point-to-multipoint connections ("one-to-many" or "one-to-network" dynamic relationships) between sensors, decision makers, and weapons systems for improved IERs. Dr. Buckman views the NII as a "flexible global networking capability"[41] serving as the "entry fee" or initial technical foundation for static or deployed elements. This advantageous situation will allow the NRF to jointly task organize air/space, land, and sea packages ad hoc, enabling the massing of effects without necessarily massing forces in planning scenarios.

Although technology exists to support the NRF's transition between platform-centric and network-centric environments, the potential mismatch between operational needs and actual C3 capabilities requires that NATO C3 bodies institute and enforce doctrinal changes to overcome transformational resistance. First, the lack of coherent network-centric environment guiding principles or keystone authoritative reference for NRF CIS support has created a cultural void to adapt alliance relationships to NNEC's emergence. Beyond the *NNEC Vision and Concept* document, an Allied Joint Publication (AJP) for CIS doctrine[42] does not exist that: (1) incorporates NCW tenets, defines critical network-centric capabilities/characteristics, establishes a common NEC language, and delineates operational imperatives; and (2) dovetails the bi-strategic Commands' *Strategic Vision or Concepts for Alliance Future Joint Operations*. Developing and agreeing to an AJP for MC approval can be a lengthy, frustrating process, especially when NC3 proponents consider revising promulgated Allied publications in tandem for NNEC consistency.

Second, lacking an authoritative reference has impeded NNEC common understanding as nations restructure their forces or play catch-up in basic expeditionary military capabilities. During ACT's first NNEC workshop conducted 29-30 March 2004, conferees of one working group observed that human and system interoperability inefficiencies are exacerbated for NRF decision makers:

> *Each nation's drive toward jointness in the past decade or so has exposed a total lack of interoperability between the services, and even different echelons. Every organization created their own unique standards, systems, and communications networks. In*

> *NATO, we can multiply the problem by 26 [each with their own particular Service methods and culture]. Trying to prevent these interoperability problems is the reason we have STANAGs, but they don't address everything.*[43]

Outdated STANAGs do not help situations in which a coalition of the willing with NATO, non-NATO countries, civilian agencies, and international organizations are not on the same networks, as evidenced by interoperability issues experienced in the Balkans.[44] In the transformation catalyst role, dynamic STANAGs are required to adapt NRFs to commercial-off-the-shelf (COTS) technology and industry open standards such as web technologies.[45]

Updated CIS doctrine and policy supports the NRF with improved techniques of collaborating and planning in its crisis response role. Capabilities include fusing a NATO Common Operational Picture or friendly force tracking for shared situational awareness among networked units, sensors and weaponry. Overcoming NATO's platform-centric doctrine is as much a disciplined approach in the organizational learning, cultural, and intellectual efforts of high-tech or lower-tech militaries as it is a technological effort.

## Technological Insertion Implications

A second impediment to implementing NNEC involves NRF technological insertion concerns. These focus on two themes: (1) getting nations' consensus to open standards architecture to drive NATO interoperability and synchronization of NRF data, applications, and systems; and (2) bridging the technology gap with technological innovation and support of technology transfer or related information sharing.

The first theme impeding technological insertion is convincing nations to adopt an open standards backbone architecture. The federation of networks in which participants can join or withdraw at will, emphasizes an evolving capability in the NNEC vision keenly dependent on NATO's interoperability coordination role: "…NNEC cannot be a single, well-defined and centrally controlled solution with final, long-term answers for how…[these] capabilities will be used. Rather…NATO must progress…efforts along intermediate sets of objectives and capabilities."[46] For nations to independently

develop and insert NII compatible systems, NC3A and ACT have the lead to redefine existing architectures to address NATO-to-nation and nation-to-nation connectivity.[47]

For NATO-to-nation connectivity, NCSA provides enterprise service delivery of NII common services accessible to the NRF. This includes provisioning NATO communications infrastructure such as wide area networks, wireless, and deployable satellite communications as points of presence for reach back of geographically dispersed forces.[48] NCSA supports communications hub interfaces and information exchange gateways to numerous NATO C3 systems such as Alliance Ground Surveillance capability or Battlefield Information Collection and Exploitation System for intelligence collection.[49] In theory, nations access NII baselined communications and core information services such as office automation or messaging. It implies nations adopt commercial tools and open standards (such as Internet Protocol [IP] based solutions[50]) to enhance C2 systems interoperability and shorten decision cycles faster than national/military specific standards would otherwise.

In practice, the challenge with implementing overarching NNEC architectures – whether short term (2008) or mid term (2012) target architectures, or a long term (2020) reference architecture[51] linked to the *NNEC FS* – lies in the nations' capability or political commitment to technologically keep pace with agreed upon common standards and services to meet essential NRF requirements or ad hoc C2 arrangements. These contributions are fundamental to successfully operationalize the NNEC concept, since nations fund and own a substantial portion of CIS capabilities like sensors and tactical network equipment.

The burden rests with NC3 bodies to provide proof of concept that transforming to NNEC given these immature, "work-in-progress" architectures will improve NRF net-readiness, cost less money than current operations, and improve service levels. NCW skeptics like Australian Strategic Policy Institute Director Aldo Borgu argue the unintended consequences of implementing architectures that are too technology-centered and information-driven when he stated: "…[execution of] NCW should result in larger numbers of smaller, less complex and less costly platforms/systems operating as

nodes in a wider network. In reality, it [is] more likely to result in a smaller number of more complex and more expensive platforms and systems."[52]

Case in point: as JFC Naples' Land Component Command (LCC) Headquarters, the 1 (German/Netherlands) Corps faced difficulty integrating its higher to lower responsibilities with subordinate multinational elements to operate over extended lines of communication during the 2005 NRF-4 rotational preparations. LCC communications planners could not assure total system interoperability within multinational deployable force packages. Their workaround was to collocate organic CIS assets with subordinate elements. They found this procedure more reliable than installing and managing gateways and interfaces. They did not disregard the latter where possible; however, they considered employing equipment interfaces as "a bonus, and not a guarantee."[53] For joint integrating architectures to operate seamlessly in an NRF implies more cooperative effort and training rehearsal than any one nation can provide.

The lack of unified multinational systems engineering also impedes NRF NNEC implementation. Dr. Buckman's study suggests establishing an NII Systems Engineering Group from NATO and member nations to allow independently developed national networks to interconnect and interoperate, similar to the way the Internet has been built and operates.[54] In its field testing catalyst role, the NRF can interact with ACT to validate the Group's common technical standards or "minimum building codes" set for national systems engineering solutions. Opportunities include COMBINED ENDEAVOR, Coalition Warrior Interoperability Demonstration, or training package trials at Stavanger, Norway's Joint Warfare Center.[55]

The second theme impeding NNEC technological insertion is bridging the technology gap. NC3A's objective role in consulting the nations is to determine how best to deliver NII capabilities between national systems and international infrastructures so nations can implement a minimum set of capabilities.[56] NNEC offers the opportunity for nations, large or small, for NRF "contributions" either with a broad set of capabilities or specialized areas.

ACT information technology chief Major General Rudd S. van Dam notes one concern is countries conducting unilateral NEC technological pursuits with differing levels of ambition or resources.[57] Nations furthering projects that are non-NNEC compatible – for example, recapitalizing legacy systems – mean the NRF continues to operate with stovepiped linkages. There is also not a clear "top-down" disciplined methodology or single integrated roadmap to synchronize nations' system fielding capabilities. The lack of harmonization means nations place different emphasis on funding priorities and timelines for program updates or technological advances.[58] Even if basic commercial technology is shared, a rotating nation assuming risk in one of its capability programs or a delayed national system fielding may impact on the NRF's degree of interoperability.

The cumulative effect is this: for ACT, this limits the NRF's field testing catalyst role in striving for quick wins to incorporate CIE technologies, such as dealing with information collection, management, and dissemination functions. In the NRF's quick reaction force role, ACO's training focus means each rotation identified in the CJSOR would have to be certified to a different interoperability baseline to validate network and system integrity, as equipments with limited proven interoperability are introduced in live operating environments.

A second more sensitive concern involves technology transfer or information sharing. John Hopkins University researchers Jeffrey Bialos and Stuart Koehl are critical of current U.S. technology transfer and information sharing restrictive policies. For instance, access to developmentally advanced U.S. NCW enablers, such as the Blue Force Tracking System (BFTS) or Digital Rosetta Stone, is either limited or not technologically releasable.[59] Little cooperation has existed on exchanging detailed technical information on critical C2 systems between the United States and Europe so proper interfaces and bridges are developed. Europeans view their exclusion from meaningful participation in U.S. transformational programs as contributing to a European capabilities gap. This will lead to the NRF implementing an unsatisfactory least-common-denominator or applying solutions intentionally chosen for their incompatibility, resulting in a "dumbed down [degraded] NRF."[60]

Even when nations' ambitions are similar, tremendous differences exist in transatlantic spending patterns. Bialos and Koehl conclude that without significant U.S. cooperation or "top-down" policy changes to transatlantic technology transfers, rotating nations will "likely operate at different levels of [affordable] capability in the next decade and beyond."[61]

The technology transfer impediment is also prevalent within the European continent. First, a framework of rules is lacking to formally share information of defense technology enablers among themselves, so the NRF benefits from the "plug and play" of each other's equipment. This includes a lack of cross-border research sharing of European Union (EU) members and NATO programs. National administrative barriers and intellectual property rights considerations such as proprietary software code and system architectures can undercut less capable NNEC nations in fusing time-sensitive intelligence for tactical data links from diverse sensors, for instance. The result is increased risk to support certain mission scenarios if CIS investments offer lower acceptable performance levels.

Second, Bialos and Koehl cite hindrance factors such as the fragmented and inefficient nature of European defense procurement, or national defense decisions to allocate more spending for operations and maintenance instead of future investments. These have made nations reluctant to share technologies or not rely on those which are innovative. This barrier detracts from ACO's intent to certify and rotate national forces through the NRF system as modernized and interoperable forces for expeditionary missions.[62]

European NATO members could mutually benefit by collaborative ventures among themselves. For example, the Network-Centric Operation Industry Consortium (NCOIC) is a not-for-profit program. Formally established in September 2004, it helps promote dialogue among industry, academia, and government subject-matter-experts to share architectures, open standards and common protocols, best practices, and systems engineering techniques. It can also bind European allies with a sense of commitment to defense procurement transformation. It does not, however, take the place of formal technology transfer agreements between nations.

## National Funding and NATO Common Funding Support Implications

A third impediment to implementing NNEC involves friction between NATO C3 bodies and member nations' capabilities in national funding and NATO common funding levels for NRF support. Despite nations' political commitment, what matters are actual significant pledges NATO's nations provide to ensure NRF requirements are funded by the right source.

A *Defense News* article noted that Spain, which provided the NATO Rapid Deployable Spanish Corps headquarters for NRF-5's LCC, was aggrieved the Pakistan earthquake relief operation cost about 16 million euros ($19 million) because it was one of the countries whose turn it was to provide NRF military resources.[63] In another *Defense News* report, General James Jones, SACEUR, told U.S. congressional committees in March 2006 that only eight of 26 NATO countries are fulfilling a 2002 Prague Summit pledge to dedicate at least two percent of their gross domestic product to defense. He warned of a "train wreck" if other countries did not increase their financial contribution.[64]

These juxtaposed views of varying contribution levels to Alliance interoperability reflect a broader debate of lingering political uncertainties to the NRF's progress in its expeditionary military capabilities.[65] Nations are concerned about what "upfront" investments are required to interface within a broader network. The NRF implication is this debate has created tensions in defining its quick reaction force role on when it should be deployed and how it is funded. This has caused some member nations "to call for more of the NRF's costs to be financed out of shared NATO funds. But Britain, Germany, and France are wary of the NATO principle of common funding, arguing it could deter nations from investing in their own national forces."[66]

National funding is the individual nations' responsibility for provision and investment in national military assets.[67] Each nation's operational level of ambition for network-enabled capability is shaped by its national interests to help determine its policies and priorities for multinational contributions. To put in perspective:

during the ACT sponsored 2004 NNEC conference, 19 of 26 NATO nations' representatives participated in an NNEC questionnaire to discern their understanding of NNEC's transformational impact. The conference report summary inferred most desired a national and an Alliance capability as a high priority.[68] However, an NRF technology gap remains as some nations are just beginning their NEC venture while others have made considerable advances with their national systems.

Common funding reflects nations' expenditures governed by NATO finance regulations. Of note are collective requirements for infrastructure projects or acquisitions through agreed cost shares.[69] NATO Security Investment Program (NSIP)[70] requirements, such as an Alliance-wide general purpose communications segment, are categorized as a Capability Package (CP) of projects submitted to the NATO Infrastructure Committee.

The *NNEC Foundation Document* contends an upfront investment is needed in a number of specific projects leading to tangible products that reduce risk to NNEC incremental delivery.[71] At ACT's Industry Day 2004 conference, information technology chief Major General van Dam noted defense organizations have traditionally purchased systems as platform-based projects to optimize vertical information exchanges, placing less emphasis on horizontal information integration with each other and other nations' systems.[72] Subsequently, continuing common funding for platform-centric projects has reinforced the interoperability barrier illustrated in Figure 4's stovepiped portion.

NSIP acquisitions require various NATO resource management committees broaden CP representation of common funded requirements.[73] Ideally, NC3 audits conducted using eligibility criteria would reappraise projects within existing CIS acquisition topics[74] and rescope those to correct a CIS capabilities imbalance, accept those planned to support NC3A's NNEC architectural guidance, and discontinue legacy programs not aligned with NNEC FS recommendations.[75] Case in point: ACT's *NNEC Data Strategy* document refers to current platform-centric model support for data storage where information is typically collocated with the information-processing platform itself.[76] A planned software

capability shift to enterprise network storage access within a NATO funded CP is consistent with the NNEC provision of service-oriented architecture to help reduce network and server bottlenecks for wider authorized user information sharing.

Implementing NNEC for the NRF implies NATO manages nations' expectations of common funding for evolutionary program development. Budget-constrained nations are not about to expand NATO owned assets using their agreed cost shares without knowing how assets are used or what quick wins will result from CP audits.[77] As architectures mature, a broadening of NATO CP crosscutting topics impacted by NNEC and leveraging economies of scale wherever political consensus is acceptable, help mitigate fiscal constraints so NRF's testing focus involves prototype solutions pragmatically aligned with the NNEC concept.

## Conclusions

NATO and member nations will rely upon the NRF in its two envisioned roles as the focal point to operationalize CIE network enabled common services. As a complex federation of independent NATO and national networks, implementing NNEC in the NRF presents interoperability challenges for NATO stakeholders.

In analyzing three broad impediments to implementing NNEC, there are two main implications to the NRF's roles. One is the NRF cannot robustly leverage its quick reaction force capabilities without NATO C3 bodies breaking away from their "business as usual" stovepiped policies, architectures, and management approaches that have helped perpetuate or create interoperability seams and gaps NNEC is intended to overcome with NII's plug and play infrastructure. Slow consensus in developing and implementing key network enterprise standards, interfaces, and unified flexible doctrine for NNEC will lead to interoperability differences for each NRF rotation, impacting on robustness and quality of services delivered for collaborative planning, information sharing, persistent and shared situational awareness to enable DS.

The second implication is the NRF cannot accelerate NNEC evolutionary programs or improve NATO/national systems in

its transformation catalyst role without firm mutual stakeholder commitments to reduce the technology and capabilities gaps. Otherwise, the lack of clear joint network ownership or accountability from nations, conflicting national interests to support NII capabilities due to disparate levels of NEC ambition, insufficient national or common funding levels, and delayed timelines for NRF technological insertions will jeopardize the *NNEC Strategic Framework* being developed supporting the NNEC concept.

## Recommendations

To better accommodate the NRF's high combat readiness role, the first recommendation is for NC3 bodies to reassert their overarching CIS interoperability roles and responsibilities. Focusing on NRF quick wins, such as NATO conducting periodic audits of existing and planned CP programs or establishing an NII Systems Engineering Group to emphasize standards and interface capacity, will present innovative NRF opportunities to be operationally effective with reduced risk and cost. Nations should leverage ACT's Joint Analysis and Lessons Learned Center to share NRF experiences and engage in ACT's training centers of excellence, such as Stavanger's JWC.

To address the NRF's capability transformation role, the second recommendation is for NC3 to exploit distributed Alliance crosscutting capabilities, integrating NNEC economies of scale wherever political consensus is acceptable. This includes convincing nations to share information on developmental work of new technologies. In parallel, nations must have the political will to invest upfront in network-centric initiatives and refresh their technologies through a rolling program, while reducing investments to recapitalize national legacy systems.

The third recommendation is for both NC3 bodies and the nations to stay connected with industry fora such as NCOIC. NRF NNEC interoperability needs to be an intellectual teaming effort so plug and play capability differences are narrowed to meet defense planning requirements.

Although NNEC capabilities are still immature, the NRF cannot fall back on a platform-centric environment. NNEC adaptation is more

than NATO/nations being "networked"; it is also about overcoming the "networking" (people and information) challenges. Through clearly understood NNEC roles, objectives, shared responsibilities, and nations' compliance, the NRF will remain relevant in executing NAC approved missions as Alliance military capability shifts from a regional to global focus.