Net-Centric Environment

Joint Functional Concept

Version 1.0

7 April 2005

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
07 APR 2005		**00-00-2005 to 00-00-2005**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Net-Centric Environment Joint Functional Concept	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Department of Defense,Washington,DC**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**75**	

Table of Contents

List of Figures

List of Tables

Executive Summary

The purpose of the Net-Centric Environment Joint Functional Concept is to identify the principles, capabilities, and attributes required for the Joint Force to function in a fully connected framework. This concept also provides the net-centric functional context for other joint concepts, and it supports joint experimentation[1] and the measurement framework for evaluating joint initiatives.

The central idea this concept proposes is that if the Joint Force fully exploits both shared knowledge and technical connectivity, then the resulting capabilities will dramatically increase mission effectiveness and efficiency.

The Net-Centric Environment is a framework for full human and technical connectivity and interoperability that allows all DOD users and mission partners to share the information they need, when they need it, in a form they can understand and act on with confidence, and protects information from those who should not have it.

The Net-Centric Environment Joint Functional Concept is an information and decision superiority-based concept describing how joint forces might function in a fully networked environment 10 to 20 years in the future. Within this concept, the networking of all Joint Force elements creates capabilities for unparalleled information sharing and collaboration, adaptive organizations, and a greater unity of effort via synchronization and integration of force elements at the lowest levels.

The Military Problem

The Joint Force in 10 to 20 years will operate in an environment that is increasingly complicated, uncertain, and dynamic. Employment of asymmetric strategies by potential adversaries and the proliferation of advanced weapons and information technologies will create additional stresses on all elements of the force. Future operations will not only require increasing joint integration, but must also better integrate other federal agencies, state organizations, and coalition partners. The current state of human and technical connectivity and interoperability of the Joint Force, and the ability of the Joint Force to exploit that connectivity and interoperability, are inadequate to achieve the levels of operational effectiveness and efficiency necessary for success in the emerging operational environment.

Net-centric capabilities and attributes can be viewed through a model consisting of two areas: the Knowledge Area and the Technical Area. The Knowledge Area comprises the cognitive and social interaction capabilities and attributes required to effectively function in the Net-Centric Environment. The Technical Area is composed of the physical aspects (infrastructure, network connectivity, and environment) and the information environment where information is created, manipulated, and shared. None of these capabilities exist in

[1] Joint Operations Concepts, 2003.

isolation—there are dependencies among the areas, among capabilities, across areas, and among capabilities within an area. In defining these two areas, it is crucial to note that information is not regarded as integral to the physical technical infrastructure nor tightly coupled to applications. In a Net-Centric Environment, information is posted to shared spaces and can be accessed by both anticipated and unanticipated users, through loosely coupled, smart pull-based architectures.

The Net-Centric Environment Joint Functional Concept presents both materiel and non-materiel change implications. This concept also presents potential change implications for other functional areas, such as Command and Control. Specifically, capabilities identified in the C2 Joint Functional Concept that (1) are network-related and (2) appear to have application across multiple functional areas have been expanded upon in this concept in order to show an integrated, net-centric concept that, if implemented, will optimize information-dependent capabilities across all functional areas.

In addition to the basic requirements outlined in the Joint Concept Development and Revision Plan (JCDRP), this document contains a vignette to help explain the principles by which net-centric concepts can be applied in a future scenario. This concept provides the joint force with an illustration of an integrated Knowledge Area and the associated enabling Technical Area capabilities and attributes necessary to net-centric functionality in a future environment that is increasingly complicated, uncertain, and dynamic.

1.0 Concept Purpose

1.1 Statement of Purpose

The Net-Centric Environment Joint Functional Concept (NCE JFC) describes capabilities derived from the exploitation of the shared knowledge and technical connectivity of all Joint Force elements to achieve unprecedented levels of operational effectiveness and efficiency.

The purpose of the Net-Centric Environment Joint Functional Concept is to:

- Define the Net-Centric Environment and describe how the future Joint Force will function in that environment across the full Range Of Military Operations (ROMO);[2]
- Identify and describe the net-centric principles, capabilities and attributes, and the functional context for Joint Operating Concept (JOC) and Joint Integrating Concept (JIC) development and joint experimentation;[3]
- Provide the measurement framework for evaluating joint initiatives and conducting analyses in support of the Joint Capabilities Integration and Development System (JCIDS);[4] and
- Provide a basis for military experiments and exercises.[5]

1.2 Definition of the Net-Centric Environment

The Net-Centric Environment is a framework for full human and technical connectivity and interoperability that allows all DOD users and mission partners to share the information they need, when they need it, in a form they can understand and act on with confidence, and protects information from those who should not have it.

Military operations conducted within the Net-Centric Environment are considered network-centric operations. These operations can be further defined as the exploitation of the human and technical networking of all elements of an appropriately trained joint force by fully integrating collective capabilities, awareness, knowledge, experience, and superior decisionmaking to achieve a high level of agility and effectiveness in dispersed, decentralized, dynamic, and uncertain environments. For the purpose of this concept, the words “net” and “network” are used interchangeably. See Appendix B for additional definitions of related terms.

Net-Centric capabilities focus directly on human interaction through knowledge sharing enabled by the dramatic advances in information technology. The effectiveness and efficiency of operating in a mature Net-Centric Environment will be achieved through the

---

[2] Joint Operations Concepts, 2003.
[3] Joint Operations Concepts, 2003.
[4] CJCSI 3170.01D.
[5] Joint Operations Concepts, 2003.

evolutionary development and implementation of Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities (DOTMLPF) appropriately suited for the utilization of network-enabled information and interactions. The Joint Force can then derive and use knowledge in superior decisionmaking processes and apply capabilities effectively, robustly, and flexibly to achieve desired effects. This allows the Joint Force and its mission partners[6] to function more efficiently (faster and better) in the execution of traditional missions. More significantly, these new capabilities allow forces to be employed in fundamentally different ways by integrating the Joint Force across progressively lower echelons. The Joint Force will thereby increase its effectiveness and efficiency by having the capabilities to undertake new missions as well as capabilities to better execute its current missions.

The principles, capabilities, and attributes of the Net-Centric Environment are separated into two areas: the Knowledge Area and the Technical Area. The Knowledge Area comprises the cognitive and social interaction required to successfully function in the Net-Centric Environment. The Technical Area is composed of the information and physical aspects (infrastructure, systems, network connectivity, and environment).[7] Development in both areas is key to achieving a mature Net-Centric Environment.

The NCE JFC provides an enabling and integrating framework for the other joint functional areas. Because the NCE JFC is focused on information flow and organizational issues that have traditionally been aligned with the C2 area of research and development, some of the language used in the Net-Centric Environment has a strong C2 flavor. Part of this focus on what may be considered the traditional C2 area stems from the fact that most networks in the past have been designed to primarily support C2 functions, and in fact are commonly referred to as C2 networks, even though these networks are often the only network available for all required functions—particularly at the lower echelons of the force. Other users (admin, logistics, etc.) have been viewed as secondary customers. Since C2 nodes are already fairly well connected, the real power of the Net-Centric Environment will be in connecting the other functions and extremities of the force.[8] Accordingly, the NCE JFC addresses the application of the principles of the Net-Centric Environment to all of the functional areas described in the family of Joint Functional Concepts. Where possible, examples have been made of the application of the Net-Centric Environment to the other functional areas.

---

[6] Mission partners include allies, coalition partners, international organizations, civilian government agencies, non-governmental agencies, and other non-adversaries who are involved with the activities or operations of the Joint Force.

[7] This framework is an extension of the four domains (social, cognitive, information, and physical) as developed in the Network Centric Operations Conceptual Framework Version 2.0. Information is critical to both the Knowledge Area and the Technical Area. The Knowledge Area addresses how information is exploited and the Technical Area addresses how information is created and made available to users. Including Information and the physical aspects of infrastructure within the Technical Area supports the Joint Capabilities Integration and Development System (JCIDS) framework and processes for development of capabilities (such as information systems) which must support integrated characteristics from both domains.

[8] FORCEnet Functional Concept (draft version 1.1.1) 091404 pg 1.

2.0 Illustrative Vignette

2.1 Background

This vignette is illustrative only and is intended to provide the reader with an understanding of how the Joint Force might function in a future Net-Centric Environment (2015-2025). It is to be used only within the context of this functional concept.

In August 1999, strong earthquake tremors struck Turkey and caused significant damage. The North Anatolian Fault that caused these tremors stretches to Istanbul beneath the Sea of Marmara. With the help of the U.S., NATO, and the European Union, Turkish officials developed a robust, survivable network called Network Respond. Network Respond consists of numerous connected networks, strategically placed sensors, and databases to provide area data and information. The network uses a number of redundant communication and power systems and dispersed archives to protect against the effects of another catastrophic earthquake. Completed in 2020, this network connects the major cities that lie on this fault line through key nodes, which are interfaced with people and sensors in cities' high rise structures, hospitals, fire fighting stations, electrical, and telephone systems, transportation system, water and sewer systems, and oil refineries.

In 2022, U.S. Joint Forces are operating in a mature Net-Centric Environment. Knowledge and technological advancements have resulted in an unprecedented ability of joint forces to ***share awareness and create shared understanding.*** U.S. Joint Forces are able to operate seamlessly at the tactical level in dynamic ***Communities of Interest (COIs)*** that can access the numerous resources including Network Respond.[9] This agile force can rapidly combine capabilities from different services at the appropriate levels to efficiently accomplish an increased range of missions. This is the ability to ***achieve constructive interdependence,*** and it is the norm—not the exception.

2.2 The Networked Setting

During the period of 2010 to 2025, U.S. Joint Forces' relationships with U.S. civilian law enforcement agencies, the Department of Homeland Security and appropriate agencies within the intelligence community have grown significantly. U.S. Joint Forces have also maintained very strong military relations with NATO and other foreign militaries. Multinational Standard Operating Procedures (SOPs) and Tactics, Techniques and Procedures (TTPs) have been developed and are in use daily. Multinational training events have become commonplace, and foreign militaries have joined with the U.S. military in developing common interfaces, policies, and protocols. Individuals are able to filter, structure, and visualize shared data and information in meaningful ways. Initiatives to enable multinational information sharing are providing the capability for U.S. and Allied militaries to share data and information transparently and effortlessly.

[9] Collaborative groups of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes. (DOD Net-Centric Data Strategy)

In addition to improved multinational interoperability, many countries have paid particular attention to the need to develop seamless access to critical humanitarian information. The United Nations (UN) established a network to coordinate Humanitarian Assistance/Disaster Relief (HA/DR) among member nations and external groups such as participating International Organizations (IOs) and Non-Governmental Organizations (NGOs). This network, called the International Humanitarian Relief Network (IHRN), incorporates common interfaces, common standards, and common protocols (including security protocols) to allow all recognized participants the ability to ***access required information*** to support the range of required functions (e.g., medical, logistics, protection, engineering, etc.) through their organic networks. Numerous exercises have been held over the years using IHRN, and as a result, SOPs and TTPs have been developed for use by all participating countries and organizations. Participants have developed the required network interfaces, and have become accustomed to ***trusting*** one another through frequent ***posting and sharing information***.

2.3 Situation

At 4:15 a.m. on 25 March 2022, the Anatolia fault line ruptures causing a massive earthquake registering 8.2 on the Richter scale. The city of Istanbul is near the epicenter of the earthquake and suffers massive damage and destruction. The cities of Izmit, Golcut, and Bursa are also on the path of the fault and suffer significant damage and casualties. Aftershocks also contribute significant damage to the area. Combined, these cities have over 150,000 dead, 400,000 injured, and 600,000 people homeless.

Due to the magnitude and severity of the earthquake damage, the Turkish government officially requests support from the UN and NATO. The UN responds by directing its Office for the Coordination of Humanitarian Affairs in Geneva to facilitate UN-sponsored humanitarian support. NATO stands up a Combined Joint Task Force (CJTF), led by U.S. European Command (USEUCOM), and begins ***synchronizing its activities*** under the auspices of the Turkish civilian emergency management agencies and the Turkish General Staff. In response to the earthquake disaster, the CJTF launches Operation Combined Response to provide humanitarian relief and coordinate relief efforts supporting the areas in Turkey devastated by the earthquake.

Numerous IOs and NGOs respond to the Turkish appeal for help. Among these organizations are the International Federation of Red Cross and Red Crescent Societies (IFRC), CARE, and World Relief. The Organization for International Relief and Support (OIRS), a Syrian-based group chartered in 2015, also participates in the earthquake relief effort.

The U.S. Federal Government is inundated with offers from States and U.S. agencies to support Operation Combined Response. Many States have stand-by quick reaction Emergency Response Teams (ERTs), Urban Search and Rescue (USR) teams, and equipment that immediately deploy to Turkey.

2.4 Execution

The headquarters of the CJTF is formed from a standing EUCOM element supported by a pre-established ***collaborative*** network consisting of both standing and dynamic communities of interest**.** Permanently assigned CJTF personnel are cross-functionally organized and have established strong, standing relationships with other functional experts within the military and humanitarian relief communities. Because of this, the CJTF is able to stand up very quickly and, while deploying to a location near Eskisehir, Turkey conducts seamless en route planning, coordinating, and directing of tasks and activities for Operation Combined Response. The CJTF consists of the U.S., Bulgaria, Greece, Italy, U.K., Canada, and France. Non-NATO members such as Israel, Japan, Russia, Austria, and Switzerland also begin coordination with the CJTF and deploy ERTs and USRs to provide assistance as necessary.

The CJTF commander immediately establishes an interactive and distributed collaboration session with all of his commanders, their primary staffs, the State Department, U.S. Embassy, the Defense attaché, and key IOs and NGO participants who enter the IHRN network to begin mission analysis and COA development. All CJTF participants are ***granted access*** to the Operation Combined Response COI to allow the sharing of information they will need to conduct this HA/DR support operation.

The CJTF is able to immediately access Network Respond and display realistic visualizations of structural damage to key buildings and the operational status of the area hospitals, firefighting stations, and police stations from protected archives of existing databases constructed, populated, and initially updated by the Turkish civil authorities. Seventy percent of the Network Respond sensors placed in strategic locations survived the earthquake and are able to send data regarding the location of casualties. Network Respond ***information quality and availability is assured*** through the use of automated network management tools designed to maximize the accuracy and reliability, utility, and integrity of data and information.

Turkey provides a collaborative team to the CJTF that functions as an information "broker" and uses various software tools to tag Turkish source data and information for specific content and releasability to respective nations and organizations participating in Operation Combined Response. This is done based on pre-determined COI data standards, supporting a framework with multiple levels of security.

Through a standing IHRN COI, all participating IOs and NGOs that had previously supported UN-led operations through the IHRN are able to access the network and get the same data and information (situational awareness) that is available to the CJTF. Those IOs and NGOs that did not participate in developing IHRN are able to rapidly connect to the IHRN and gain access as full participants in the COI. Intelligent user-defined agents assign each of these organizations a level of participation in the COI commensurate with their roles, authorities, requirements, and risk profile.

By operating in a Net-Centric Environment, ERTs and USR teams are able to collaborate with CJTF units, other response teams, and all pertinent relief organizations, ***synchronize***

their actions, quickly deploy to areas where people are potentially trapped inside buildings, and execute immediate search and rescue actions. All organizations responsible for casualty activities ***automatically post casualty updates***, allowing network participants to access near-real-time information on current casualty locations, status, severity of injuries, availability and location of nearest ERT and USR teams and equipment, supplies, current on-site conditions, and status of casualty logistical/medical support infrastructure.

On March 27, two days after the earthquake, a massive car bomb explodes outside the Hotel Bandora in Ankara, approximately 250 miles from the Istanbul area relief effort. The bomb kills 10 key members of the Greek Cypriot-controlled government and 20 high ranking members of the Turkish contingent who are attending a Cyprus Unification Seminar. The explosion kills 45 bystanders and injures 150 individuals. Shortly after the bomb explodes, the terror group Al Shalib Hurstat claims credit for the incident citing their disapproval of the Cyprus Unification Seminar and threatening more terror activity if the unification efforts continue.

The CJTF is given the ***additional mission*** of providing force protection and support to help the Turks locate and neutralize the terrorist cell responsible for the bombing. This new mission is designated Operation Stomp Out. Taking advantage of the shared situational awareness and understanding achieved during Operation Combined Response, the CJTF immediately establishes an interactive collaboration session with all commanders and primary staff members to update the situation and begin mission analysis.

The CJTF establishes the Stomp Out COI to assemble all relevant information related to active and inactive terrorist cells operating in and around Turkey. The CJTF Commander tasks this COI to develop a recommendation on the likely terrorist cell responsible for the bombing, its disposition, and its likely location. To accomplish this task, the COI immediately realizes that it needs the means to assemble and analyze all data and information related to terrorist cells, terrorist supporters suspected of planning and/or conducting terror in the Area of Responsibility (AOR), local leaders, previous terrorist incidents, and responsible parties. Therefore, the COI quickly expands to include not only the organic CJTF ISR assets but also the Turkish Liaison Officer and his resources, the EUCOM J2, CENTCOM JTF-CT, the Defense attaches at the American Embassy, and a North Atlantic Council Counter Terrorism Force that was established in 2008. The network allows the CJTF to quickly and easily reach back to other assets without increasing the footprint of the forces required to support operations in Turkey. This reduces the time and resources needed to bring additional information sources and counter-terrorism capabilities to bear on the problem at hand. Because of the nature and location of the event, the Turkish liaison officer is identified as the COI leader.[10]

[10] The COI leader acts as the main contact point and spokesperson for the group. The COI leader does not necessarily have any additional network administrator or user privileges. For the purposes of the scenario, the COI leader is the Turkish liaison officer because the group is working terrorism issues inside the officer's home country.

There is a great deal of data and information pertaining to Ankara and its surrounding areas on Network Respond, and the Turkish government allows the CJTF access. CJTF mission partners' ***access is based primarily on operational roles,*** as delineated by the CJTF and as stipulated by the COI leader.

A logistics COI is established that plans for acquiring and managing the resources needed to provide logistical and medical support to Operation Stomp Out. This dynamic COI provides peer-to-peer connectivity for logisticians in each unit supporting the operation, EUCOM logistics planners, and U.S. military component logistical planners. The logistics COI conducts collaboration necessary to support the new operation allowing this COI to assess the logistical status of Operation Combined Response, identify the support requirements necessary to respond to the event in Ankara, and analyze the in-transit status of supplies. This provides the means to develop a comprehensive recommendation to the CJTF to redirect certain critical support from Operation Combined Response to Operation Stomp Out.

The NATO Rapid Reaction Force (RRF) is placed under the operational control (OPCON) of the CJTF. In 2022, the RRF consists of a Brigade Combat Team (BCT) with battalion-sized combat units, military intelligence, engineer units, military police units, and signal/communication units as well as RRF level support units. The RRF planning element is able to tie into the COIs for both Operation Combined Response and Operation Stomp Out.

The RRF tasking in Operation Stomp Out allows its units appropriate role-based access to network operational data and information. The plans cell ***automatically subscribes to any data or information posted*** on the network related to terror activities, terrorist supporters, and weapons, then further ***processes this information*** on its tactical network. Smart agents alert RRF units with mission specific information as determined by individual users. Individuals further selectively filter this information based on their specific information needs.

On March 28, a Turkish doctor working in an OIRS medical facility in Izmit reports overhearing a conversation of one of her coworkers that leads her to believe that the coworker and possibly other OIRS members have ties with Al Shalib Hurstat. This information is reported to the Turkish government, which directs that the information be ***immediately sanitized, tagged with appropriate security labels, and posted.*** The report is fused with other data and information related to Al Shalib Hurstat and OIRS and, as a result, the OIRS's ***access to information on the network is quickly restricted*** due to a perceived security risk. However, OIRS retains access to local non-sensitive humanitarian relief data and information.

Concurrently, numerous other data and information related to terrorists are posted by various mission partners in Operation Combined Response and Operation Stomp Out, intelligence agencies, and sensors. Local inhabitants who are on the ground providing assistance and relief also provide key information to members of CJTF. These Human Intelligence (HUMINT) reports are automatically tagged and posted as they are reported.

The Stomp Out COI has subscribed to information related to suspected terrorists in the AOR. As a result, the COI automatically receives the OIRS report and begins the collaboration necessary within the intelligence community. The COI collaboration is focused on assessing the fused data/information that is coming in to provide an update to CJTF and the RRF's situational awareness. Based on the comprehensive collaboration amongst the COI participants and the new information related to Al Shalib Hurstat, the COI ascertains that the terrorist group Al Shalib Hurstat is indeed responsible for the bombing and that these same terrorists are assembling in the city of Kayseri about 250 miles from Syria.

The RRF immediately deploys the BCT to Kayseri; however, the BCT has little information on the city's design, layout, and transportation network. Though available, satellite imagery will not provide the details needed to fully plan a combat mission in Kayseri. The RRF commander considers a request to EUCOM to provide additional forces capable of providing detailed imagery of Kayseri.

One of the military units supporting Operation Combined Response is a U.S. Army Unmanned Aerial Vehicle (UAV) unit that is providing aerial support to locate and rescue casualties. The UAV unit has a platoon that can provide long range urban/MOUT aerial reconnaissance support and this platoon is not currently supporting Operation Combined Response. The UAV commander is connected to the network and has visibility of the situation unfolding. The UAV commander contacts the BCT commander and, after collaborating on the situation, offers his platoon as a quick solution to providing aerial reconnaissance over Kayseri. The mission change requires extra security for the UAV downlink sites, which the BCT is able to easily accommodate. Logistics clerks from both units use the CJTF logistics COI to arrange for delivery of supplies needed to support the new arrangement. Members of other functional areas also make appropriate adjustments to ensure that this important task is adequately supported.

The RRF commander has configured his information visualization system to track this type of development and informs the CJTF, EUCOM, and the Turkish General Staff of the situation. Within hours, the BCT receives metadata tagged imagery with embedded geospatial data from the UAV platoon. The BCT in collaboration with units and COIs throughout the CJTF (including the Turkish General Staff and its civilian leadership) quickly exploits the information and develops a plan to strike the terrorists. The ***constructive interdependence*** achieved by the rapid tactical level integration of UAV, BCT, and supporting COI capabilities allows the CJTF to successfully execute a mission that results in the capture of the terrorists.

3.0 Central and Supporting Ideas

3.1 Statement of the Military Problem

The Joint Force in 10 to 20 years will operate in an environment that is increasingly complicated, uncertain, and dynamic. Employment of asymmetric strategies by potential adversaries and the proliferation of advanced weapons and information technologies will create additional stresses on all elements of the force. Future operations will not only require increasing joint integration, but must also better integrate other federal agencies, state organizations, and coalition partners. The current state of human and technical connectivity and interoperability of the Joint Force, and the ability of the Joint Force to exploit that connectivity and interoperability, are inadequate to achieve the levels of operational effectiveness and efficiency necessary for success in the emerging operational environment.

3.2 Emerging Operational Environment

The changing character and conduct of warfare and conflict resolution require a fundamental shift in the way the U.S. military integrates and employs the elements of the Joint Force. Joint Force elements are increasingly being put into unfamiliar situations within complex, uncertain, and rapidly changing operating environments. To succeed in these environments, they need the ability to rapidly integrate varied, dynamic, and often unanticipated sets of capabilities, potentially drawn from across and beyond the Joint Force and its mission partners, in order to achieve the effects they require to meet their mission objectives. They need to reduce the impediments to the flow of information and reduce the inherent friction[11] of adjusting Joint Force and mission partner capabilities to new tasks and missions. The Joint Force and its mission partners need to greatly increase the level of integration among their various capabilities and function at increasingly lower echelons.

3.2.1 Current Platform Centric Environment

The current approach to Joint Force integration is largely platform-centric at the echelons below the JTF headquarters level. In a platform-centric environment, individual and largely autonomous systems are brought together in a rigidly structured fashion to accomplish a mission. The central principles of a platform-centric environment tend to create barriers to the flow of information across the Joint Force and its mission partners. They frequently use organic or system-specific components that generate data using system-specific data management strategies supported by dedicated command or organizational support elements. These platforms have optimized their processes to support only their particular systems. The systems in a platform-centric environment especially lack horizontal integration with other systems, creating stovepipes of data and information. Platform-centric integration is done in a centralized command center

[11] Referring to friction in the context of Clausewitz in *On War*, friction here refers to the amount of organizational effort required to bring a certain set of capabilities to bear in a specified amount of time.

supporting higher echelons (See Figure 3-1). The result is that the platform-centric environment tends to have a high level of friction, impeding the smooth or fluid transition between different types of missions and reducing the potential effectiveness and efficiency of the Joint Force. The platform-centric environment tends to employ coordination mechanisms between the Joint Force and its mission partners that are brittle and have little utility except across a narrow range of potential missions. In the platform-centric environment, the content, speed, format, and quality of information are dictated in large part by formal requirements generation and fulfillment processes that employ centralized and functionally specialized information management, collection, processing, and consumption practices. This approach is inadequate because it produces a series of inherent social and technical barriers to the flow of information that prevents tactical level integration of capabilities and ultimately restricts the effectiveness and efficiency of the force.

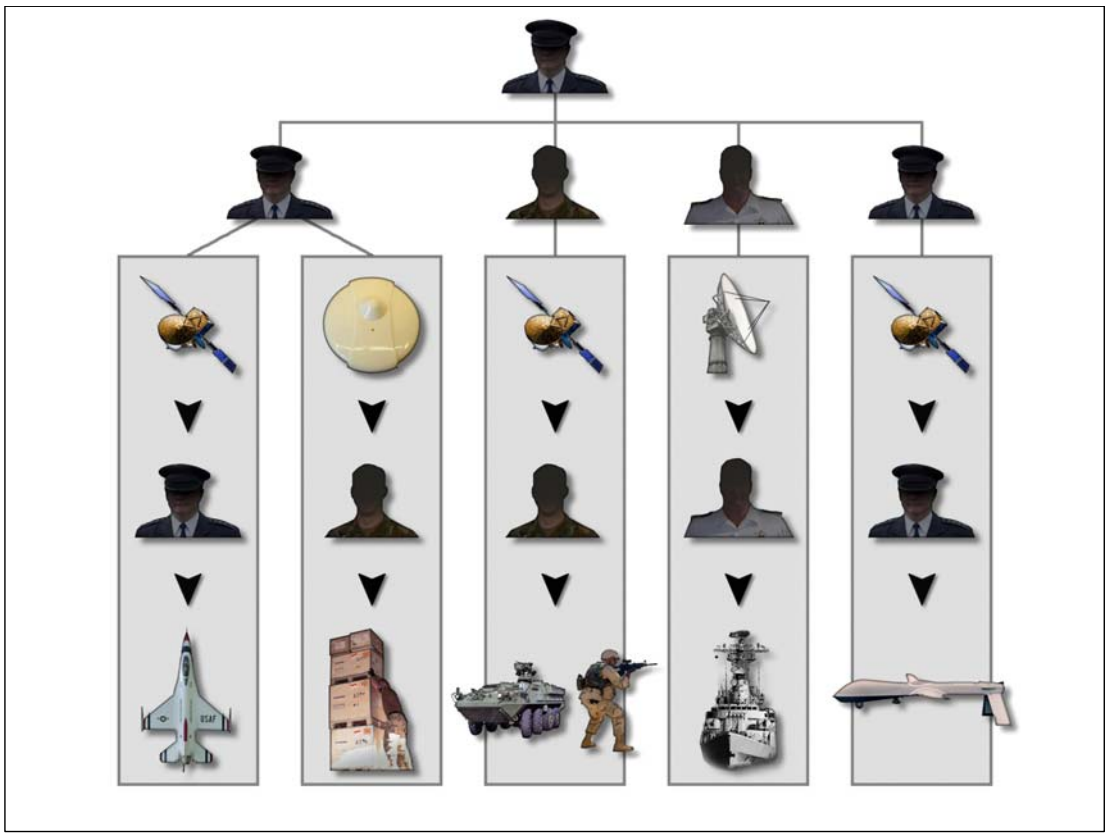

Figure 3-1. Platform Centric Environment

3.3 Central Idea

If the Joint Force fully exploits both shared knowledge and technical connectivity, then the resulting capabilities will dramatically increase mission effectiveness and efficiency.

Advances in information technologies are revolutionizing the ability of all members of the Joint Force and mission partners to share information and collaborate,[12] creating new central principles and paving the way for significant increases in the effectiveness and efficiency of the Joint Force and its mission partners. Collaboration is defined as joint problem solving for the purpose of achieving shared understanding, making a decision, or creating a product[13] across the Joint Force and mission partners. It allows experts to integrate their perspectives to better interpret situations and problems, identify candidate actions, formulate evaluation criteria, decide what to do, and execute those decisions. In the context of this concept, collaboration is used to share and improve information, awareness, and understanding among the elements of the Joint Force and its mission partners—support decisionmaking and synchronize activities.

Current Technical Area investments focus primarily on the realization of a robust end-to-end network infrastructure as typified in Global Information Grid (GIG)-related initiatives. The success of GIG-related initiatives currently underway is vital to building the technical architecture and foundation of the Net-Centric Environment.[14] Users throughout the force must be connected with adequate resources to allow reliable, near-continuous access to enterprise information and services—even on the move. The Net-Centric Environment does not imply infinite resources, but does allow all echelons to manage available resources to meet changing mission needs. While traditional technical network investments have centered on specific C2 requirements and nodes, the Net-Centric Technical Area will provide common capabilities for individuals across all functional areas.

However, investments that only address the technical and informational aspects of this environment will only garner limited gains in the overall agility and utility/effectiveness of the Joint Force. Transitioning from a platform-centric environment requires surmounting internal and external organizational and policy barriers to the sharing of awareness, understanding, decisionmaking, and the synergistic application of force capabilities. This cultural change must be supported by training and education, as well as by ensuring that Joint Force elements have incentives to use the technical networks of the Joint Force and its mission partners to draw on appropriate capabilities, regardless of their geographic or organizational location. While this can be done to a limited extent

---

[12] This information sharing and collaboration is done formally and informally, directly and indirectly, and across the force and between the force and appropriate extra-force elements and resources.
[13] Joint Command and Control Functional Concept.
[14] The GIG is defined by the DODD 8101.1, Global Information Grid Overarching Policy, 19 September 2002 as a globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. However, current investments focus on procurement of critical enablers in the information and physical infrastructure domains.

through the formal coordination mechanisms within and among institutions, the agile operation of a force requires the enabling of both formal and informal collaboration across the Joint Force, and the ability to establish and utilize relationships with mission partners.

Realization of a Net-Centric Environment requires exploitation of the capabilities from *both* the Knowledge and Technical Areas. At its heart, the Net-Centric Environment is a social construct supported by an advanced information infrastructure. The total capability within the Net-Centric Environment is greater than the sum of the Knowledge and Technical Areas. The two areas need to be integrated in order to exploit their full potential. To understand the relationships between the two areas, it is crucial to note that information is not regarded as integral to the physical technical infrastructure nor tightly coupled to applications. In a Net-Centric Environment, information is posted to shared spaces and can be accessed by both anticipated and unanticipated users, through loosely coupled, smart pull-based architectures. The maturation of the Net-Centric Environment is dependent upon the coevolution of both areas, best seen as investments along the entire DOTMLPF spectrum. Figure 3-2 represents the progressively increased total capability of the Net-Centric Environment when both Technical Area and Knowledge Area are integrated and exploited.

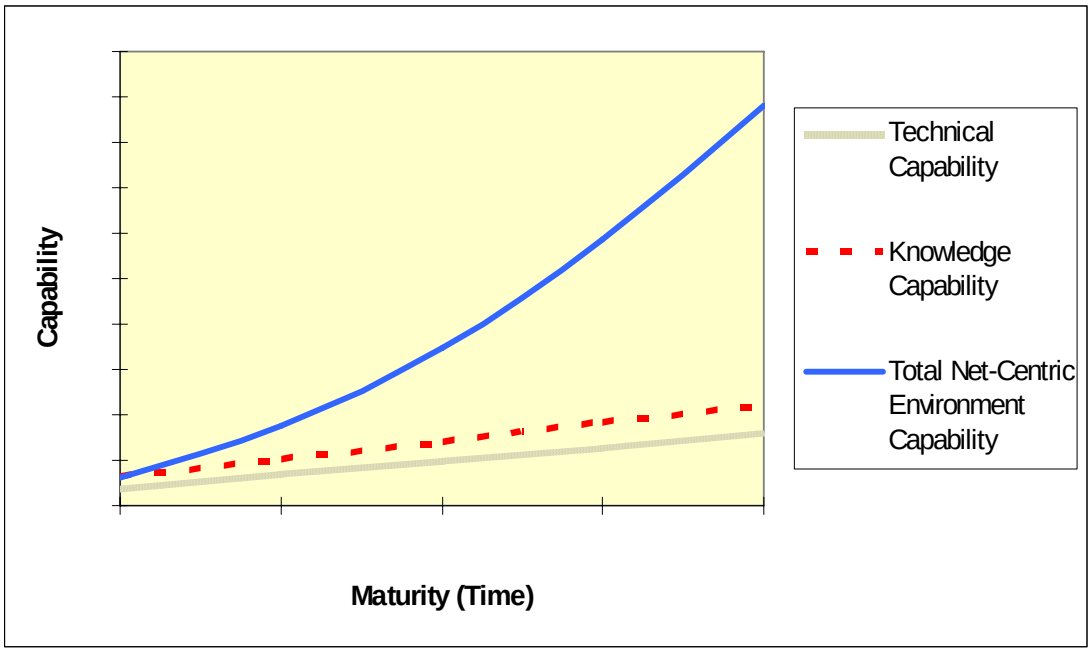

Figure 3-2. Net-Centric Environment Capability: Greater than the Sum of its Parts

3.4 Principles Essential to Applying the Concept to a Wide Range of Scenarios

The central principles of the Net-Centric Environment establish a set of guidelines for using net-centric functions to integrate tasks across functional areas and enable a wide range of Joint Force capabilities, such as those described in the Joint Operating Concepts.

Ultimately, these principles work together to form new capabilities not available to a less than fully connected force.

3.4.1 Technical Area Principles

3.4.1.1 Intelligent Infrastructure

Infrastructure includes the physical portions of the network. It facilitates the sharing of information and collaboration among individuals and groups. The infrastructure needs to support the organizational structures, processes, and information flows required for users to interact in the Net-Centric Environment. Broadly, the development, deployment, and employment of infrastructure need to follow this guidance:

- Adapt to the changing priorities, policies, and requirements generated by the information moving across it. Support persistent and dynamic shared space.
- Connect groups as well as individuals in a global network, removing the barriers imposed by geography (natural and man-made), and physical movement. The infrastructure should be able to provide persistent global connectivity, but at the same time should allow users to maintain tactically and operationally necessary capabilities when disconnected. Connecting to the network cannot be a prerequisite for access to basic or limited functionality as units may be forced or choose to operate without network access for short periods of time. Connectivity needs to be provided to forces moving to, from, and inside the battlespace. This includes support for "comms on the move." At the minimum, systems should:
  - Maintain local connectivity (peer-to-peer) even when external connectivity is down;
  - Provide the ability to cache/display the last information received;
  - Provide the ability to input local and/or manual updates that are automatically synchronized when connectivity is restored.
- Regulate network connectivity and the visibility of data based on an individual's clearance level and their role in the Joint Force or as a mission partner.
- Dynamically adjust network security as the roles of actors change and as the missions of the Joint Force and its mission partners dictate.
- At lower echelons, there will be progressively less distinction between unit-specific platforms and the systems used to connect to broader service in the Net-Centric Environment. The ability to access the network and utilize network services will require unit-specific platforms that can also provide network connectivity.
- Provide automated information management, fusion, and visualization tools.

3.4.1.2 Individual Information Management

Advances in information technology will enable the infrastructure to move greater volumes of higher quality information more quickly from producers through processors

to consumers.[15] The key advantage is that the generation and fulfillment of information requirements are significantly more efficient because they can be dynamically defined and generated by the consumer of the information. *Information management shifts from a command function to an individual function.* Interoperability is enhanced through use of common enterprise services supported by a unified data strategy rather than service, command, and function-specific information management practices.[16] Because resources will never be infinite and sometimes severely restricted,[17] command and organizational responsibilities will focus increasingly on management of available resources. This focus shift implies a significant cultural change supported by education, and increased joint training at lower echelons, including the use of a live virtual constructive joint training environment.[18]

Evolving the information requirements generation and fulfillment process increases the speed and quality of decisions, enabling decision superiority across the Joint Force and its mission partners. It also implies that the individual will need to be able to filter, structure, and visualize the information in ways that are meaningful to them without degrading the value of the information to others. The consumers of the information can discover and access the information they need in a timely fashion, in a context that is appropriate to them, and with enough confidence in the quality of the information that they can act on it with confidence. In many cases, the producers of information may not know who needs their product. (See Section 5.4 for more details on potential implications for individual information management.)

To support individual information management, information will need to be clearly and properly tagged[19] to help individuals and groups more quickly discover and access it. Tagging also allows for the creation of useful ontologies for the information that they produce. A variety of tagging methods, including auto-extraction and auto-generation tied together by an interoperability of the metadata that they produce, will help to make information easily accessible and to help intelligent agents to provide that information to those individuals and groups who have subscribed to it. Information will need to be presented in a proper operational context, so tagging will need to relate contextual information as well.

---

[15] At various times during a mission, a given force element may be any one or a combination of these types of information actors.

[16] See the DOD Net-Centric Data Strategy of 9 May 2003 for detailed vision of the Department's data and information management vision.

[17] FORCEnet, page 14.

[18] A live virtual constructive joint training environment is one that seamlessly integrates live and virtual elements into a training program.

[19] While tagging is a specific method for including metadata, it is used in this context to mean the systematic collection and inclusion of metadata during the collection, processing, and consumption of information over its life cycle.

3.4.2 Knowledge Area Principles

3.4.2.1 Information and Decision Rights and Responsibilities[20]

Each individual actor in the Net-Centric Environment has rights and responsibilities as they apply to information and decisions. This significant cultural shift must be supported by training and education. Individuals will have the proper incentives to fulfill their roles as producers, processors, and consumers[21] of information. Individuals will also need the knowledge, experience and confidence to interact effectively. Individuals need to be prepared to not only exploit the information made available to them, but also to engage in behaviors that encourage transparency, including ensuring that exploited information is shared with those who are supposed to have it. The behavior of individuals can be assessed by feedback they receive from those who interact with them on the network. Good behavior[22] is rewarded with positive feedback—much like a credit score or online auction rating system. Feedback will be important in building and establishing trust when operating with new partners because it will be used to determine their ability to discover and access information. Individuals who do not engage in acceptable behavior will receive negative feedback, which may be used as a mechanism to specify additional training or limit the types of tasks deemed appropriate. The quality and quantity of the shared information across the Joint Force and its mission partners is dependent upon each individual exercising their rights and fulfilling their responsibilities.

Individuals in the Net-Centric Environment also have decision rights and responsibilities and will be empowered and enabled to act freely in making decisions. They have the responsibility to make those decisions within the context of command intent and to share situation understanding across the Joint Force and its mission partners. These rights and responsibilities apply to both the formal command and control process and to less formal collaborative decision structures. Decisions in the Net-Centric Environment are heavily influenced by dynamic, self-defining patterns of collaboration.

The rights and responsibilities found at the individual level can also be ascribed to the group level.[23] The important distinction between individual and group rights and responsibilities as related to information and decisions is the set of additional factors that describe the structure and quality of relationships among the individuals within the group. Groups that do not engage in acceptable behavior will receive negative feedback, which may be used as a mechanism for additional training or limits on the types of tasks deemed appropriate for the group. Groups are adaptable, which means that they are prepared to quickly respond to any contingency with the appropriate capabilities mix. This requires

---

[20] In addition to the general rights and responsibilities listed here, an individual can have specific rights and responsibilities assigned to them by their commander. These individuals may have access more akin to a "super user," but are still constrained by the requirements for proper clearance for access to classified materials.

[21] Army's Core Architecture Data Model defines nodes as having these three roles relative to the network in which they reside. It is not strictly limited to individual people, but can also apply to larger organizations.

[22] "Good behavior" occurs where the individual or group has not abused its information or decision rights and has fulfilled its information and decision responsibilities to the satisfaction of the group.

[23] Groups are defined as any formal or informal association of two or more individuals. A COI is a group.

versatile and agile forces that are tailorable and scalable for employment and able to employ new capabilities in a multi-use manner. Adaptability ensures that groups can rapidly shift from mission to mission.[24]

3.4.2.2 End-to-End Transparency

End-to-end transparency is a central principal of the Net-Centric Environment that requires both a culture of openness and visibility of information across the Joint Force at the tactical level. The information that is generated, processed, and consumed in a Net-Centric Environment will need to be visible, accessible, understandable, verifiable, current, and trusted.

Access to information and its visibility to other users will be based on the level of clearance and the role of the individual and group in the Joint Force and its mission partners. Role-based access to information and the visibility of information to certain users are akin to a dynamic "need to know" requirement. This protects sensitive information from individuals or groups who have access under the current construct, but no longer have a need to know, or those who do not have a need to know that certain pieces of information even exist. Technologies like Public Key Infrastructure and Biometrics will need to evolve significantly to support dynamic role-based security. For example, if a Common Access Card is lost, it may take weeks to replace. Identity management concepts need to mature to support the dynamic requirements of the Net-Centric Environment.

Removing the impediments to the flow of information, save the need to protect the information from those who should not have it, requires formal and informal organizations to make their structures and processes transparent to each other so as to increase the visibility of their information and capabilities. Transparency requires a move from a "share information by exception" model to a "withhold by exception" model. Improving the transparency among information consumers, processors, and producers enables geographically separated individuals and groups to build the trust required to share critical information and integrate collective capabilities at a much lower and effective level.

3.4.2.3 Using Communities of Interest

The use of Communities of Interest (COIs) throughout all echelons of the Joint Force and its mission partners is a critical principle that supports many capabilities of the Net-Centric Environment, such as flexible organizations, shared situational awareness, and collaboration. COIs are generally temporary organizations formed to address specific problems, but there can also be standing or permanent COIs to deal with persistent issues. They interconnect resources from more stable and permanent organizations, giving those organizations a flexibility that is central to addressing issues in the complex, uncertain, and dynamic operating environment of 15 to 20 years in the future.

---

[24] JOpsC, p. 16.

COIs can form as the result of top-down efforts, as in the case when commanders use COIs to rapidly and easily bring together expertise from across the Joint Force and the mission partners to address specific issues of concern. COIs can also be self-organizing from the bottom-up, allowing, for example, logisticians to collaborate on the location of available supplies across a number of Joint Force and mission partner elements. As shown in Figure 3-3, COIs can support all types of organizations within the Net-Centric Environment.

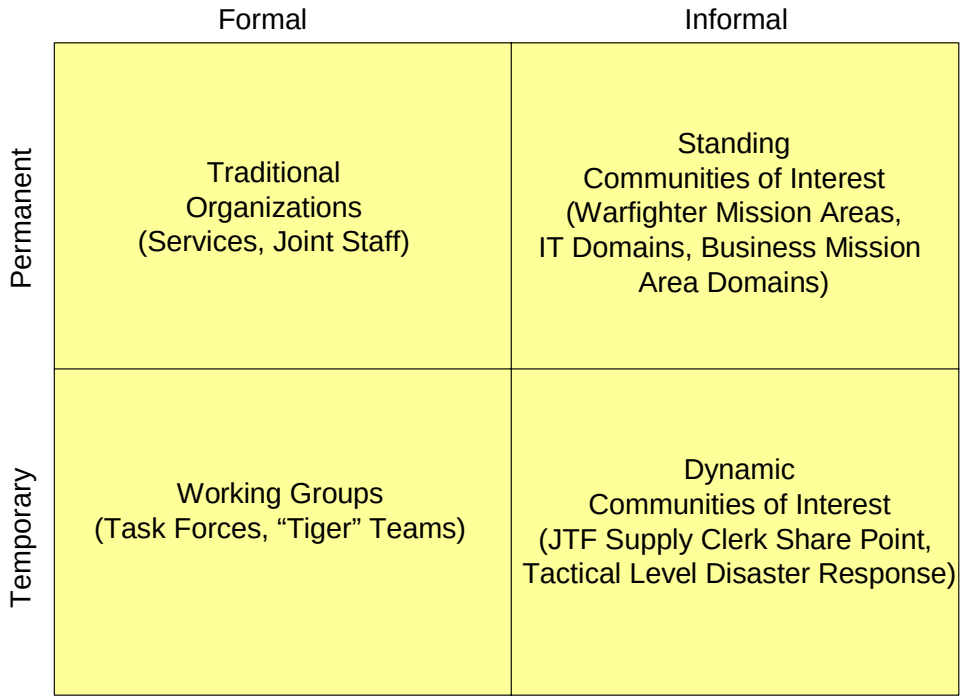

Figure 3-3. COIs within the Net-Centric Environment

COIs can be employed to meet a wide range of needs across the JTF. For example, through the use of COIs, shared situational awareness will be improved by increasing the volume and quality of information being shared across the Joint Force and its mission partners. Improving shared situational awareness will in turn make collaboration more effective because the effort spent on synchronizing facts and establishing shared situational awareness are reduced and more is spent on higher cognitive activities (e.g., developing a shared understanding or potential courses of action.)

3.4.2.4 Interdependence

Interdependence is a mode of operations based upon a high degree of mutual trust, where diverse members make unique contributions toward common objectives and may rely on each other for certain essential capabilities rather than duplicating them organically.

Currently, integration of the Joint Force normally occurs at the component or JTF headquarters level, and is often characterized by autonomy and deconfliction, the lowest levels of integration. Here the capabilities of each organization or unit stay entirely

separate, even when the parent organizations have some overlap. Because units rarely employ every capability at their disposal in support of Service or component tasking, significant capability within the JTF remains latent or unused.

By removing the barriers to the flow of information and connecting geographically dispersed elements, the Net-Centric Environment provides the Joint Force and its mission partners with the ability to exploit the efficiencies of the specialization of labor. Units across the echelons will no longer need the same degree of organic capabilities to achieve mission success because they can confidently rely upon their ability to access the capabilities that they require, but which are provided by other units, organizations, or individuals. Capabilities with a relatively low utility or usage in a particular mission can either remain in garrison or can be more easily employed by other units that have a greater need. Figure 3-4 illustrates the relative increases in integration, efficiency, and effectiveness of constructive interdependence achieved by moving from a platform-centric to a Net-Centric Environment.

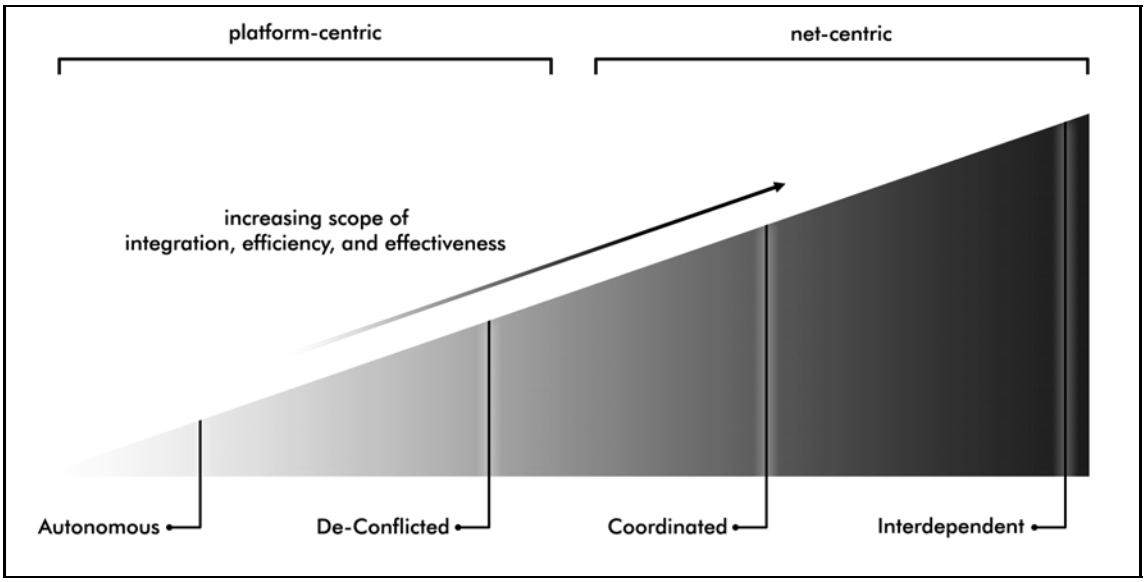

Figure 3-4. Increasing Integration toward Constructive Interdependence

The Net-Centric Environment allows for the creation of capabilities that were heretofore unavailable or possibly unknown, but which are adapted to the characteristics of the specific environment in which they are intended to function. This creation of new capabilities from the connection of the latent capabilities within the Joint Force is referred to as *constructive interdependence*. Figure 3-5 illustrates the creation of additional combinations of capabilities (potentially unusable in a platform-centric environment) that may be derived from the Net-Centric Environment. Note that although Figure 3-5 focuses on a sensor-decisionmaker-shooter scenario, this idea can easily be extended to other scenarios such as producer-processor-consumer.

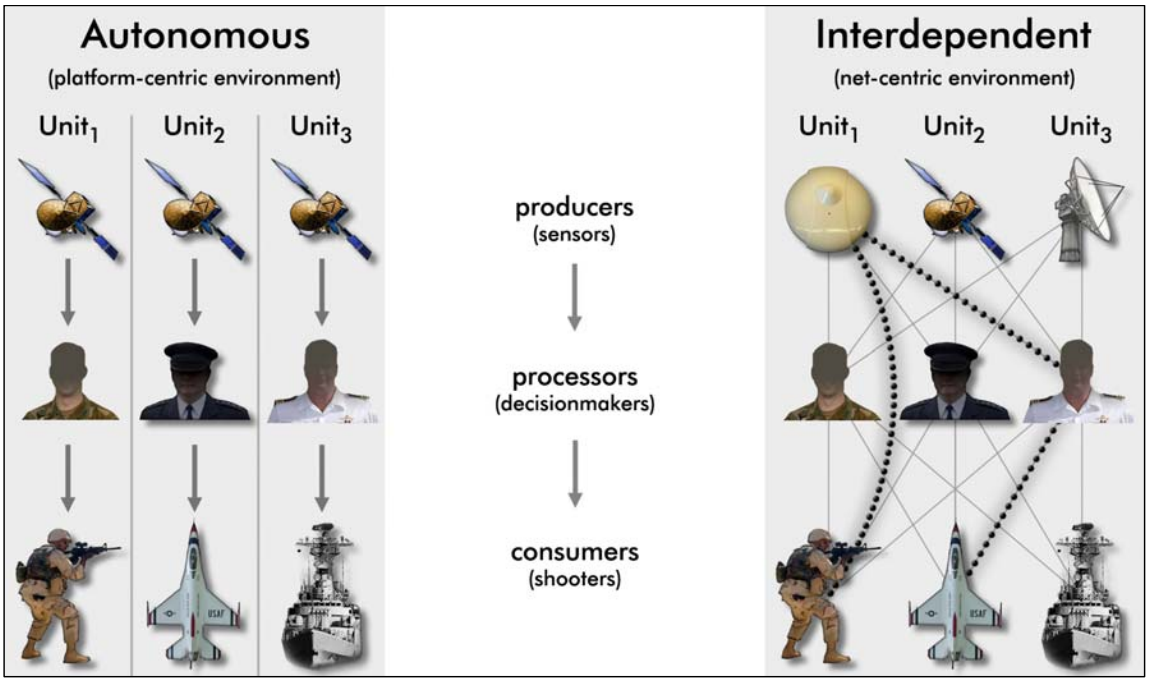

Figure 3-5. Increased Combinations of Capabilities in the Net-Centric Environment versus the Platform-Centric Environment

3.5 Application of Concept within a Campaign Framework

Operations in a Net-Centric Environment will be significantly different than operations conducted under the current platform-centric environment. Net-Centric capabilities will support all phases of the current campaign framework, as well as support potential future new frameworks with less well defined boundaries between phases. Information sharing and collaborative processes will be the engines of change that will lead to the development and adoption of new organizational principles that will, in turn, facilitate the transformation of existing capabilities and the development of new ones. By removing the knowledge and technical barriers to the flow of information, the Joint Force and its mission partners will be able to operate with a significantly higher degree of agility and effectiveness as a result of their increased integration and constructive interdependence.

The advantages of operating in a Net-Centric Environment impact all of the functions of the Joint Force and its mission partners. For example, U.S. forces could assist local governments, international relief agencies, and NGOs coordinate humanitarian assistance efforts much more easily in a Net-Centric Environment because the barriers to information flow would have been removed. COIs, supported by the transparency of the constituent organizations, will be able to coordinate the distribution of food or medical assistance more rapidly and effectively than with traditional coordination mechanisms (Focused Logistics Area). Information exchange[25] will depend less on information exchange agreements, liaison officers, and formal coordination meetings. There will be

[25] Information sharing within a COI could also be supported by an Information Exchange Broker who ensures information arrives at the right time, at the right location, and in the proper format required.

formal barriers in place (clearance and role) and informal barriers (behavior as good citizens in the Net-Centric Environment) to establish the visibility of data and address security needs. Joint Force and mission partner planners will be able to share situational awareness, the availability of resources, and readiness of capabilities to be deployed with greater ease, efficiency, and effectiveness.

The Net-Centric Environment will reduce the friction[26] of both large and small mission transitions. The lessoning of friction in the course of transitioning from one task or mission to another creates opportunities for the Joint Force to use combinations of capabilities. Over the course of the operation, joint forces are less reliant on unwieldy or brittle synchronization mechanisms in a Net-Centric Environment because the information and decision rights and responsibilities are guiding the flow of information and the decision points across a singular effort. As the mission in a complicated, uncertain, and dynamic operational environment unfolds, access to the network and the visibility of data will adjust in response to the changing roles and missions of elements of the Joint Force.

The fluidity with which the Joint Force can transition from one phase or mission set to the next will be a significant advantage of operating in the Net-Centric Environment. If the mission to support the humanitarian assistance action changes and requires U.S. and coalition forces to provide protection to convoys, the transition to the additional mission requirements will be done more effectively in a Net-Centric Environment than in a platform-centric one. This is because the reduced barriers to information flow would increase transparency, which in turn would also reduce the friction inherent in such a transition. Information on current environmental conditions and the location of hostile forces will be distributed more quickly to the units protecting the convoys and those same units will pass back information on the conditions they find while in route in near-real-time, updating the shared awareness of all of the units involved in the operation (Battlespace Awareness). New routes will be selected on the basis of better information regarding the local conditions both in terms of the environment and the activity of hostile forces (Command and Control). If hostile forces are encountered, the convoy can quickly relay their location to strike aircraft offshore or helicopter gunships using a convoy protection COI specific to the operation to pass sensor data to act on targeting information (Force Application). Vehicles in the next convoy may be provided with additional protection against small arms fire and the order of vehicles may be changed based on the information coming through the Protection COI (Force Protection) from a previous convoy.

---

[26] Aaron ,MAJ (NS) Chia Eng Seng, Ph.D. “Countering the Fog and Friction of War in the Information Age.” Pointer: *Journal of the Singapore Armed Forces*, April-June 2003, vol. 29, no. 2.

4.0 Capabilities and Attributes

This Chapter describes the capabilities as well as attributes and related measures required in the Net-Centric Environment. A *capability* is the ability to achieve an effect to a standard under specified conditions through multiple combinations of means and ways to perform a set of tasks,[27] and an *attribute* is a measurable characteristic of a capability. Appendix D lists the capabilities and supporting tasks as well as attributes and supporting measures in tabular form.

4.1 Areas

The capabilities and attributes of the Net-Centric Environment can be thought of as existing in two areas: the Knowledge Area and the Technical Area. The Knowledge Area comprises the cognitive and social interaction capabilities and attributes required to effectively function in the Net-Centric Environment. The Technical Area is composed of the physical aspects (infrastructure, network connectivity, and environment) and the information environment where information is created, manipulated, and shared. A matrix depicting the relationship between net-centric capabilities and attributes for each area is included in Appendix F.

4.1.1 Knowledge Area

The Knowledge Area is where human interactions occur between elements of the Joint Force and its mission partners, for example, the exchange of information, shared awareness, shared understanding, and collaborative decisionmaking. Because of the increasing diversity and scope of organizations and forces involved in Joint Force operations, the interactions between them become more complicated, requiring new and more capable collaborative efforts. It is within this area that individuals develop situational awareness and share this awareness with other entities to produce a shared awareness. This leads to improved understanding at the individual level and to improved shared understanding. This process enables the creation of faster, higher quality decisions both individually and collaboratively as the situation requires. The Joint Force and its mission partner components will set up ad hoc (and sometimes dispersed) mission-based organizations that will change as the missions and tasks change, which in turn will alter the information exchange requirements among the entities. Participants in these networked organizations will be selected based on their knowledge of the problem or task at hand and the capabilities they provide, and will function with a minimum set of formalized rules and procedures.[28]

4.1.2 Technical Area

The Technical Area includes the infrastructure and information properties of the network. The focus of this Section is on the connectivity and information flow and quality aspects

---

[27] JCDRP (7/2004).

[28] Air tasking orders and joint targeting processes are examples of formalized rules and procedures.

of this area. In this context, networking can be viewed as an interconnection of a system of computers, communications, data, applications, security, people, training, and other support structures that provide local and global information processing and service needs.[29] For smaller units, infrastructure will be more tightly integrated into their specific systems because they will not have the luxury of supporting additional systems in austere conditions. The information domain facilitates the communication of information across the network. It is the area where the command intent is communicated and where information sharing occurs. The requirements of this area enable and constrain the formation of communities of interest to solve problems, exploit opportunities, and mitigate risks in an ever-changing operational context.

4.2 Capabilities

Functioning in the Net-Centric Environment depends in large measure on the achievement of capabilities in the Knowledge Area, supported by capabilities in the Technical Area. None of the capabilities exists in isolation—there are dependencies between the areas, between capabilities across areas, and between capabilities within an area. The Knowledge Area comprises the individual and group capabilities (e.g., understanding and decisionmaking) achieved through the employment of various collaborative techniques, organizational options, and force arrangements.

The individual cognitive capabilities are enhanced through the group sharing capabilities. Situational understanding becomes shared situational understanding and decisionmaking becomes collaborative decisionmaking, providing a more powerful set of capabilities. The Technical Area capabilities provide the means for achievement of the Knowledge Area capabilities. For example, shared understanding is dependent on knowledge, the flow of information, and the ability of the network to provide that flow.

4.2.1 Knowledge Capabilities

Ability to establish appropriate organizational relationships. This is the ability to set up and change formal organizational and command relationships in accordance with mission and task needs, as well as to use flexible organizational constructs that extend across multiple commands and organizations for task accomplishment. The Net-Centric Environment supports existing frameworks and provides a new COI framework to support both formal and informal organizational needs. To operate successfully in this environment, people and organizations must be capable of dealing with flexible authority relationships (senior/subordinate, supported/supporting). This requires appropriate training, an understanding of the various organizational relationships, and the ability to work within an implied command intent environment. The Net-Centric Environment provides the transparency and trust mechanism necessary to use these new organizational constructions for military missions across the ROMO.

---

[29] Network Centric Operations Conceptual Framework, Version 2.0.

Ability to collaborate. Collaboration is extremely important to operating in the Net-Centric Environment. Collaboration must be continuous, include geographically separated participants, and involve all relevant parties. To develop trust in collaborative decisionmaking processes and organizational structures, doctrinal, cultural, and organizational limits will need to be removed to achieve full collaboration. Leaders will need to be trained, and procedures will need to be implemented.

Ability to synchronize actions. The fast pace of operations in the Net-Centric Environment requires that entities be able to rapidly synchronize among themselves, independent of direction from superiors: self-synchronization. This will enable them to flexibly adapt actions to take advantage of opportunities and minimize impacts of changing or emerging threats. It will enable a more thorough incorporation of effects-based operations and planning.

Ability to share situational awareness. Individuals will need not only to develop their own situational awareness, but they will need to share this awareness with a wide range of participants. They will need to see how others perceive the situation, and be capable of processing information from many sources while remaining focused on current tasking(s).

Ability to share situational understanding. Where situational awareness is the "who's where and what are they doing" aspect of battlespace knowledge, situational understanding is the "what does it mean and what can I do about it" aspect. Individuals will use reasoning methods and tools to achieve the required level of understanding.[30] Sharing their understandings with a wide array of participants will provide a synergy that leads to a higher quality collective understanding and contributes to high quality decisionmaking.

Ability to conduct collaborative decisionmaking/planning. The ever-changing nature of the battlespace environment will require that commanders involve many elements, including other commanders and non-traditional communities of interest, in the decisionmaking process. Decisionmakers will need collaboration tools and sophisticated decision support tools in order to succeed in this environment. They will also need to deal with analyzing potential courses of action quickly and with sufficient resolution to address potential second and third order effects. The collaborative decisionmaking process will enable commanders to be aware of other entities' changing tasks and missions and their ability to perform those tasks and missions.

Ability to achieve constructive interdependence. Joint Operations establish formal rule sets for combining capabilities from multiple Services together to form new capabilities. The idea of constructive interdependence extends this further by employing the network (both human and technical) to allow a virtually limitless combination of latent Service and component capabilities in ways that create capabilities not previously achievable. For example, an Army unit has pushed quicker than its organic logistics can support

[30] Reasoning methods and tools include determination of cause-and-effect through trial and error, analyzing "what-if" scenarios or using influence diagrams and probabilistic reasoning tools to look at potential alternative outcomes.

ammunition requirements and is in need of quick re-supply. Fortunately, the unit does have an attached truck unit with plenty of fuel. The most direct route to the supply depot requires using a bridge that has been weakened by the fighting, and which is now unsafe. A nearby Marine unit has captured its objectives and has an amphibious capability that has already been used and can ferry supplies past the bridge. By looking across the network, the Army unit ascertains the status of the amphibious equipment and its capabilities, and establishes direct contact with the Marine unit to coordinate their activity. The Army unit also discovers via the network that the Marine unit needs fuel immediately. The two units are able to combine their respective unused capabilities efficiently and effectively at the tactical level to accomplish their assigned missions. The Net-Centric Environment will also allow for the identification of opportunities for constructive interdependence that can be employed in wargaming and other training exercises.

4.2.2 Technical Capabilities

Ability to create/produce information. This is the capability to collect (in the case of sensors) data and transform that data into information. It includes the on-board processing of sensor data and/or the transmission of that data to an analysis or processing entity.

Ability to store, share, and exchange information and data. This includes all actions necessary to store, publish, and exchange information and data. Data must be appropriately identified and labeled (tagged), placed in a database or other data/information repository, and its presence announced to those who need it (post/publish/advertise). There must be mechanisms in place such as intelligent agents for others to retrieve the data/information (share) and/or mechanisms must exist to provide the data/information on a timely basis to those who need it (smart push/message). There must be a method to store the data/information in such a manner as to facilitate the easy retrieval by those who need it the most (stage content/smart store). There must be a way for users to identify the data/information that they need so that they are alerted to its availability (subscribe). Multiple users must be able to simultaneously work with data and information, producing unified, integrated updates (collaboration). Finally, there must be a means to maintain the historical record (archive).

Ability to establish an information environment. This involves the establishment of criteria, processes and procedures for the storing and sharing of data/information, including the sharing across different environments and the support for multiple changing communities of interest. The ever-changing situation and high operational tempo will require the capability to achieve fluid allocation of resources in accordance with shifting priorities and the command intent (dynamic, priority-based resource allocation).

Ability to process data and information. The user must be able to filter, correlate, and fuse data and information into useful forms. The system must be able to mediate and translate between different systems with varying characteristics.

Ability to employ geo-spatial information. All coordinates should be properly formatted, tagged, and correlated to other geo-spatial information in an underlying database (e.g., population, utilities, transportation, services, climate). This feature is many times more powerful than a standard map display in that it allows layering of information and drill-down capability from the display.

Ability to employ information. The existence of information on the network is useless without a means of providing this information in an understandable form to the user. Formatting must be translatable (or interfaces must exist) to the extent that machine-to-machine information sharing is enabled.

Ability to find and consume information. Users must be able to locate the required information and extract it. This includes discover and search capabilities, the use of intelligent agents, smart pull/smart push, etc.

Ability to provide user access. The net-centric model will result in users shifting roles as mission requirements dictate. The different roles will have different information and security access requirements; therefore, role-based and COI access controls need to be developed and employed. This will apply to both individuals and groups, including COIs. This will likely entail strong authentication procedures.

Ability to access information. This capability refers to the need for multiple levels of security to allow information sharing between users across different security domains.

Ability to validate/assure. This capability addresses the need for confidence and trust in networks, systems, and information. Capabilities include the ability to restore and recover networks, systems, and data, and ensure data availability, integrity, confidentiality, and auditing during its lifecycle.

Ability to install/deploy. The net-centric model depends on the capability to have connectivity where and when required. The network must be capable of forward deployment and must be tailored to mission requirements. It must be capable of dynamic reconfiguration as missions/tasks change, and be functional in harsh and/or unimproved infrastructure environments.

Ability to operate/maneuver. Once in place, the network must be capable of dynamic allocation of resources, operate regardless of geography (distance, obstructions, etc.), and support all operations and transitional states along the ROMO. It must manage access and denial to the network and associated data, while providing ad hoc coalition and inter-agency connectivity. The network will provide continuous, rapid, and error-free delivery of information.

Ability to maintain/survive. Once deployed, the network must be able to maintain service while under both physical attack and information attack. It should degrade gracefully, that is, continue operations at a gradually reduced capacity in accordance with prioritization plans as systems/equipment are destroyed and/or damaged. The network must be capable of dynamically rerouting services as nodes are incapacitated and/or as

information flow requirements change. The network must be capable of obtaining additional resources as required to maintain or increase capacity.

Ability to provide network services. The network must be capable of providing all services generally associated with network operations such as connecting all assets, sharing information among interagency/coalition/IO commercial/NGO participants, archiving large volumes of data, maintaining network status, keeping all nodes informed, supporting separate constellations of COIs, and supporting geographically transitioning nodes.

4.3 Attributes

The attributes are the measurable aspects of the capabilities such as those listed in Section 4.2.1. The relationships are not one-to-one, but one-to-many, and many-to-many (see Appendix D). In order to assess the effectiveness of capabilities in the Net-Centric Environment, it is necessary to develop a set of performance-related metrics. Measures provide the linkage between overarching attributes and metrics by identifying the important qualities of each attribute. The most appropriate metrics and associated units of measurement differ based upon the operational context. Specific metrics are below the scope of this version of the functional concept. However, metrics with scale and unit of measure are required to evaluate specific capabilities. Future versions of this document should include more detailed metrics derived from both the current JIC processes (see Section 6.6) and specific net-centric metric development efforts.

4.3.1 Knowledge Attributes

Agile

Agile is defined as moving quickly and easily. It is assessed using the following measures:

- Flexible: The extent to which individuals or organizations dynamically meet evolving mission requirements.
- Innovative: The extent to which tasks are performed in novel ways.
- Resilient: The extent to which the command/organization is able to recover from or adjust easily to misfortune or change.
- Responsive: The extent to which decisions and actions are based on timely analysis and synthesis of the current situation.
- Scalable: The extent to which organizations can seamlessly adjust size and scope to meet a given mission requirement.

Quality

Quality is defined as lacking nothing essential or normal. Quality is assessed using the following measures:

- Appropriate: The extent to which understandings and decisions are suitable and useful for the mission/situation at hand.
- Relevant: The extent to which an understanding/decision matches command intent and mission objectives.
- Correct: The extent to which understandings agree with fact.
- Consistent: Extent to which understandings and decisions are in line with prior understandings/decisions.
- Accurate: The granularity and precision with respect to fact.
- Complete: The extent to which all required elements are present.
- Timely: The extent to which the currency of understandings or decisions are appropriate to the mission.

Trustworthy

Trustworthy is defined as the extent to which confidence or assurance is held in information or decisions. Trustworthiness is assessed using the following measures:

- Robust: The extent to which individuals or organizations exhibit strength or vigorous health.
- Confident: The extent to which assurance is held in information or decisions.
- Willing: The extent to which a force entity possesses the desire to function in a shared information environment.
- Competent: The extent to which one is able to perform a task and/or function.

4.3.2 Technical Attributes

Assured

Assured is defined as having grounds for confidence that an information-technology (IT) product or system meets its certainty or security objectives. Assurance is assessed using the following measures:

- Authentic: The extent of a security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information
- Confidential: The extent to which confidence or assurance is held in information or decisions.
- Non-repudiated: The extent to which the senders/receivers of data are prevented from denying having processed the data. Non-repudiation is measured by the extent to which senders are provided with proof of delivery and the recipients are provided with proof of the sender's identity.
- Available: The extent to which authorized users are provided with timely, reliable access to data and information services.
- Integrity: The extent to which information is protected from unauthorized modification or destruction.

Robust

Robust is defined as having or exhibiting strength or vigorous health. It is assessed using the following measures:

- Survivable: The extent of assurance provided a system, subsystem, equipment, process, or procedure that the named entity will continue to function during and after a natural or man-made disturbance, for example, a nuclear burst. (*Note:* For a given application, survivability must be qualified by specifying the range of conditions over which the entity will survive the minimum acceptable level or post-disturbance functionality, and the maximum acceptable outage duration.)
- Redundant: The extent to which surplus capability is provided to improve the reliability and quality of service.
- Distributed: The extent to which the network resources, such as switching equipment and processors, are dispersed throughout the geographical area being served. (*Note:* Network control may be centralized or distributed.)
- Resilient: The extent to which recovery from or adjustment to malfunction (misfortune) or change is easily achieved.

Agile

Agile is defined as moving quickly and easily. It is assessed using the following measures:

- Flexible: The extent to which success is achieved in different ways and the extent to which the network dynamically meets evolving mission requirements.
- Responsive: Responsiveness is the extent to which service is provided within required time.
- Diverse: The extent to which the network is not dependent on a single element, media, or method.
- Dynamic: The extent to which the network can adapt when there is a change in status.
- Autonomous: The extent to which tasks are undertaken or carried on without outside control. It is the ability to exist independently; responding, reacting, or developing independently of the whole.

Manageable

Manageable is defined as capable of being controlled, handled, or used with ease. It is assessed using the following measures:

- Scalable: The extent to which the network/system/organization can grow to accommodate additional users; hardware or software either co-located or globally distributed from the original system configuration.
- Reconfigurable: The extent to which the network/system/organization can accommodate changes in hardware, software, features, or options.
- Controllable: The extent to which a network manager has the ability to exercise restraint, direction over, or perform diagnosis to ensure optimal function and security; power or authority to guide, monitor, or manage.

- Maintainable: The probability that an item will be retained in or restored to a specified condition within a given period of time, when the maintenance is performed in accordance with prescribed procedures and resources.
- Upgradeable: The extent to which the network or system can accept new versions of software to meet changing requirements.
- Repairable: The probability that the system/network can be to be restored to satisfactory operation by any action, including parts replacements or changes to adjustable settings.

Expeditionary

Expeditionary is defined as supporting a military operation conducted by an armed force to accomplish a specific objective in a foreign country. Expeditionary is assessed using the following measures:

- Deployable: The extent of effort required to relocate personnel/systems to a Joint Operations Area (JOA).
- Maneuverable: The extent to which network elements support warfighters on the move.
- Modular: The extent to which the network/system comprises “plug-in” systems/ units/forces that can be added together in different combinations.
- Transportable: The extent of mobility within the JOA.
- Rugged: The extent to which the system/network can support operations in extreme environments and/or under conditions of high physical stress.
- Reach: The extent to which the network/system can operate over extended distances to meet mission requirements.
- Employable: The time and effort required to commence system operation upon arrival in the JOA.
- Sustainable: The extent to which the network/system is able to maintain the necessary level and duration of operational activity to achieve military objectives. Sustainability is a function of providing for and maintaining those levels of ready forces, materiel, and consumables necessary to support military effort.

Quality

Quality is defined as lacking nothing essential or normal. Quality is assessed using the following measures:

- Accurate: The extent to which a transmission/data stream is error-free.
- Traceable: The extent to which information is capable of being tracked or traced; the ability to follow, discover, or ascertain the course of development of something.
- Complete: The extent to which all necessary parts, elements, or steps are present.
- Consistent: The extent to which information is free from variation or contradiction.
- Timely: The extent to which information is received in time to be useful.

Integrated

Integrated is defined as all functions and capabilities focused toward a unified purpose. Integrated is assessed using the following measures:

- Interoperable: The extent to which systems, units, or forces can provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together.
- Accessible: The extent to which all authorized users have the opportunity to make use of information capabilities.
- Visible: The extent to which users and applications can discover the existence of data assets through catalogs, registries, and other search services. All data assets are advertised or "made visible" by providing metadata that describes the asset.
- Usable: The extent of difficulty regarding the initial effort required to learn and the extent of recurring effort to use the functionality of the system and/or the extent to which the context of the information used and/or created by an information capability can be derived.

5.0 Implications

Net-Centric future force implications impact all of the DOTMLPF areas.

5.1 Doctrine

- The Information Age may refine the application of the principles of war and the role of information in warfare will be made more explicit in doctrine.
- Doctrine will continue to be a point of departure, guiding principles, and best practices.
- Tactics, Techniques, and Procedures (TTPs) will evolve to reflect the increasing significance of information in all aspects of military operations.
- Development of doctrine will be more dynamic and collaborative and will be driven increasingly by wargaming and experimentation.
- Joint operations will become the norm at successively lower organizational hierarchical levels.

5.2 Organization

- The effective application of the elements of national power in the Information Age will require new organizational relationships between DOD and its mission partners.
- Within the Joint Force, organizational structures will transform as information and understanding are shared. New organizations will emerge, existing organizational structures will change (e.g., flatten), and some organizational structures will disappear.
- The Net-Centric Environment will facilitate, to a greater extent than is currently possible, the formation of new organizations with diverse structures, resources, degrees of persistence, charters, and missions. For instance, the diverse natures of Communities of Interest (COI) are best exploited in a Net-Centric Environment.
- The extremities of organizations will become increasingly important as these nodes are fully connected in the environment. Horizontal relationships between organizations (both formal and informal) will become more important.

5.3 Training

- Training curricula will need to change to develop the knowledge, experience, and desired behaviors for operating in a Net-Centric Environment. The curriculum change process must also become more responsive to rapidly transforming operational practices.
- Exercises will need to focus more on gaining experience and familiarity with a broad spectrum of players drawn from the Joint Force and its mission partners and utilizing the Net-Centric Environment as the medium for interaction.
- The concept of “train as you fight, fight as you train” will require training and exercises to take place on portions of operational networks in order to properly

simulate the complex interactions that occur in the Net-Centric Environment. Live Virtual Constructive training environments will emerge.
- Training will need to support the ability of individuals and small groups to plug into ad hoc teams or COIs without the benefit of the unit cohesion that comes from training and operating with a standing unit over a longer period of time.

5.4 Materiel

- Solutions will be developed to connect traditionally disadvantaged users (those at the extremities of force or that operates in challenging mediums such as under the sea). These solutions must support near-continuous access to enterprise services regardless of location or rate of movement. When disconnected from the network, these systems must continue to operate and allow graceful re-entry to the network to include automatic synchronization of information between the disconnected systems and enterprise resources.
- Emphasis must shift to developing solutions that support all functional areas as primary customers, as opposed to building better C2 networks.
- Materiel solutions must support multiple levels of security in a dynamic COI architecture.
- Identification verification technologies will need to evolve significantly to support dynamic role-based security. Identity management concepts need to mature to support the dynamic requirements of the Net-Centric Environment.
- Information systems must be designed to work with metadata from a wide range of communities of interest.
- Capabilities must be increasingly interoperable at the information and physical layers. Increased emphasis on the Net-Ready Key Performance Parameters and additional interoperability and net-centric processes, in particular systems engineering of end-to-end performance to implement real-time requirements, is necessary to ensure Technical Area Interoperability.
- Digitally Assisted Aids/Tools help the commander to assemble the information in ways that improve visualization and help create a rich understanding and assessment of potential alternatives that enable superior decisionmaking. They provide advanced planning and cognitive capabilities to aid in courses of action development, modeling, and simulation capabilities to evaluate COAs and predict results, and supporting analytical information to aid in dealing with uncertainty.
- Intelligent user-modified agents will filter and frame user information requirements within the network, allowing commanders and staffs to access the information that they need quickly and efficiently. The user-tailored information flow provides feedback to those teams publishing information so that they can continually adjust their collection and fusion processes in such a way as to provide the most meaningful products, for example, information pull as well as push.
- Fielding of materiel solutions must be better tied to joint training. Fielding of critical materiel solutions must include resources and planning for recurring training.

5.5 Leadership and Education

- Leadership will need to deal with the dispersion of authority across the set of temporary and informal organizational structures that will evolve under collaboration.
- Leadership must embrace the cultural change required to function effectively in the Net-Centric Environment.
- Education at all levels must address the new framework provided by the Net-Centric Environment and reinforce the cultural and cognitive changes required for success in this environment.
- Leadership development will need to address the challenges of decisionmaking in a Net-Centric Environment.
- Educational institutions must continually adapt to provide the best research and analysis on future warfighting concepts.
- Leadership development will need to address the possibilities offered by self-synchronization and other concepts and their impact on the idea of unity of command or the command process.

5.6 Personnel

- Administrative functions that require simple, repeated decisions will be phased out; administration will be more efficient, given the enhanced physical, psychological, and mental demands, and more personnel will be made available for duty in currently understaffed units.
- Operating in a Net-Centric Environment will create new mental and physiological demands on personnel. These will need to be addressed through a combination of human engineering (such as ergonomics), process engineering, and personnel development.
- Expertise not organic to units may be provided by a virtual presence or personnel, negating the need for a physical presence and/or assignment (e.g., analysts, advisors, maintainers). Through the use of reachback capability, distributed operations are enabled allowing for smaller deployed footprints and enhanced mobility, both strategic and tactical, for joint forces.

5.7 Facilities

- Bases and facilities in CONUS and OCONUS will require continued investment and partnership with commercial information services to support a net-centric infrastructure and supported data management strategy for forces in garrison.
- Training and exercise facilities will require a higher level and more thorough instrumentation to evaluate unit performance beyond the most basic metrics for success and to assess the use of information.

6.0 Scope

6.1 Timeframe and Applicable Military Functions and Activities

The NCE JFC is written for the Joint Force Commander at the operational level 10 to 20 years in the future with applicability across all levels of command from strategic to tactical and across the ROMO.

The NCE JFC provides functional support to the JOCs, other JFCs, and describes the net-centric capabilities, attributes, and measures in support of the JICs and the Capabilities Based Assessment (CBA) analysis process. It also provides a conceptual basis and analytical framework for the operation of the Net-Centric Functional Capabilities Board.

6.2 Impact of Strategic Guidance and Deviations in the Concept

The challenges of the evolving operational environment require that U.S. military force, all relevant agencies, and coalition partners work together with the Joint Staff and other DOD agencies to enhance, integrate, and develop new Joint warfighting capabilities. The mandates set forth in the National Security Strategy, 2004 National Defense Strategy, and National Military Strategy serve as a basis for the development of strategic and operational Joint Force capabilities required for operating in the Net-Centric Environment. The NCE JFC conforms to the strategic guidance by providing the net-centric capabilities and attributes that enable the U.S. military to conduct the required net-centric tasks and activities necessary to meet the strategic guidance.

- National Security Strategy (NSS): The NSS directs an active strategy to counter transnational terrorist networks, rogue nations, and aggressive states that possess, or are working to gain, Weapons of Mass Destruction or Effect (WMD/E). It emphasizes activities to foster relationships among U.S. allies, partners, and friends. The NSS highlights the need to retain and improve capabilities to prevent attacks against the United States, work cooperatively with other nations and multinational organizations, and transform America's national security institutions.
- National Defense Strategy (NDS): The NDS supports the NSS by establishing a set of overarching defense objectives that guide the DOD's security activities and provide direction for the National Military Strategy. The NDS objectives serve as links between military activities and those of other government agencies in pursuit of national goals.
- National Military Strategy (NMS): The NMS derives objectives, missions, and capability requirements from an analysis of the NSS, NDS, and security environment. The NMS provides focus for military activities by defining a set of interrelated military objectives and Joint operating concepts from which the Service chiefs and combatant commanders identify desired capabilities and against which the Chairman of the Joint Chiefs of Staff assesses risk.

6.3 Impact of Future Context Documents and Deviations in the Concept

This concept was developed in the context of numerous DOD efforts to transform the force. The Network Centric Operations Conceptual Framework 2.0, Net-Centric Operations and Warfare Reference Model 1.1, and DOD Net-Centric Data Strategy played particularly important roles in the identification of required capabilities and attributes. This document provides a unifying framework of principles, capabilities, and attributes to integrate the many net-centric efforts underway. Future updates to these and other net-centric related documents, such as the Net Ops Conops and the future NCOE CONOPS should reflect the capabilities identified in this concept.

Deviations from this concept (particularly in foundational elements such as definitions) in future context documents will likely hinder progress toward achieving a net-centric force by furthering the lexicon issues that have already been identified as problematic.[31] However, this concept acknowledges that the understanding of the net-centric functional area is immature and rapidly expanding. As the community's understanding of Network Centric Operations evolves, new principles, capabilities, and attributes are likely to be identified and should be incorporated into future revisions of this concept.

6.4 Risks and Mitigation

Military commanders and leaders at all levels will need to manage risks as they operate in a Net-Centric Environment. Risks remain inherent in the planning and execution of military operations. Additionally, there are risks associated with identifying, developing, attaining, and maintaining future net-centric capabilities 10 to 20 years in the future. Military leaders must employ prudent risk management strategies, including both the acceptance of calculated risks and the development of comprehensive risk mitigation techniques. The risk mitigation discussed below is only a point of departure and the implications Section of this concept provides more details on necessary changes, most of which address one or more risks. The following list is intended to identify significant risks associated with implementing a Net-Centric Environment. This list is not intended to be exhaustive.

- The increasing dependence on information processes, systems, and technologies adds potential vulnerabilities that, if not adequately defended, could be exploited by adversaries, or result in serious mission consequences. Mitigation: Increased network security training and emphasis at all levels. Development of new Information Assurance strategies and technologies.
- Elimination of intermediate echelons and the ability to monitor force activity at an arbitrary level of detail may lead to information-enabled micromanagement, inhibiting the decentralization of decisionmaking to lower echelons. Mitigation: Wargaming and experimentation to inculcate value of decentralization. Education.

[31] DOD Inspector General Report, "Management of Network Centric Warfare Within the Department of Defense" (D-2004-091) June 2004.

- Overwhelming levels of information may lead to increased decision times or the inability of leaders to locate and identify decision-relevant information. Mitigation: Investment in smart agent technology. Training. Wargaming in a Live Virtual Training Environment.
- Capability and interoperability gaps in training, equipment, physical interfaces, and doctrine may pose challenges for operations with less digitally-capable forces. Mitigation: Retain key legacy interfaces. Increase training with allies in scenarios such as described in the vignette.
- Over-reliance on information and communications technologies may result in forces incapable of operating effectively in the absence of those technologies due to failure or attack. Mitigation: Increased reliability of new equipment and appropriate levels of integrated redundancy in system architectures. Training and exercises that realistically simulate conditions of failure and attack.
- Failure to coevolve technological, organizational, and doctrinal innovation may lead to inefficiencies in the deployment and utilization of net-centric systems and concepts. Such failure may arise from, for example, unresponsive acquisition processes, organizational and cultural inertia, insufficient scientific advancement, or overly optimistic assumptions about technical or organizational capabilities. Mitigation: Increased joint wargaming and exercises, particularly at the small unit level. Increased investment in commercial technology. Integrated Joint Concept Development and experimentation.
- Insufficient scientific understanding of the psychological and sociological foundations of cognitive and social behavior results in fielding systems, designing organizational structures, and developing doctrine that is not effective in real-world Knowledge systems. Mitigation: Increased research in this area.

6.5 Assumptions

There are several assumptions common to all Joint Functional Concepts that provide the overarching environment in which U.S. military operations will take place:

- Future U.S. joint military operations will take place in a Net-Centric Environment;
- Affordable technology will allow coalition partners and other agencies to acquire net-centric materiel;
- The U.S. will be operating in a complicated, uncertain, and dynamic global security environment 10 to 20 years in the future; and
- There will be greater emphasis on asymmetric threats and the possession and potential use of weapons of ever-increasing power.

There are also critical assumptions that are relevant to the NCE JFC:

- Substantial continued investment in research and development will overcome unanticipated barriers to technical advancement that would preclude sustained change in military operations; and

- DOD and Service cultures will evolve at an increasing rate to accept and employ knowledge area capabilities.

6.6 Relationship to Other Joint Concepts

An assumption common to all joint concepts is that future U.S. military operations will occur in a Net-Centric Environment. The relationship among the various families of concepts is depicted in Figure 6-1. The Net-Centric Environment Joint Functional Concept must provide net-centric support to each of the joint concepts, thereby assisting the Joint Force Commander in shaping the battlespace. The Net-Centric Environment Joint Functional Concept:

- Identifies essential Net-Centric Environment capabilities that enable the conduct of net-centric technical tasks and activities across the ROMO in support of joint operations using a network that is ubiquitous, autonomous, interoperable, and reliably supports tactical, operational, and strategic needs;
- Identifies essential Net-Centric Environment capabilities that enable humans to leverage the technology and conduct comprehensive collaboration in support of decisionmaking, staff planning, and battlefield management in a distributed and decentralized manner;
- Supports the Net-Centric Environment capabilities identified in the joint operating concepts, joint functional concepts, and joint integrating concepts;
- Provides a single point of reference to inform and influence the joint concepts regarding the net-centric military function (net-centric capabilities and attributes); and
- Provides a single point of reference to synchronize net-centric terms and activities.

Capabilities identified in Version 1.0 of the C2 Joint Functional Concept that (1) are network-related and (2) appear to have application across multiple functional areas, have been expanded upon in this concept in order to show an integrated, net-centric concept that, if implemented, will optimize information-dependent capabilities across all functional areas. These capabilities do not replace the need for specific C2 capabilities, but rather complement the C2 capabilities by providing a framework to integrate the Joint Force at a lower, more informal, and more efficient level. Figure 6-2 depicts the relationship of the Net-Centric Environment to the other functional areas.

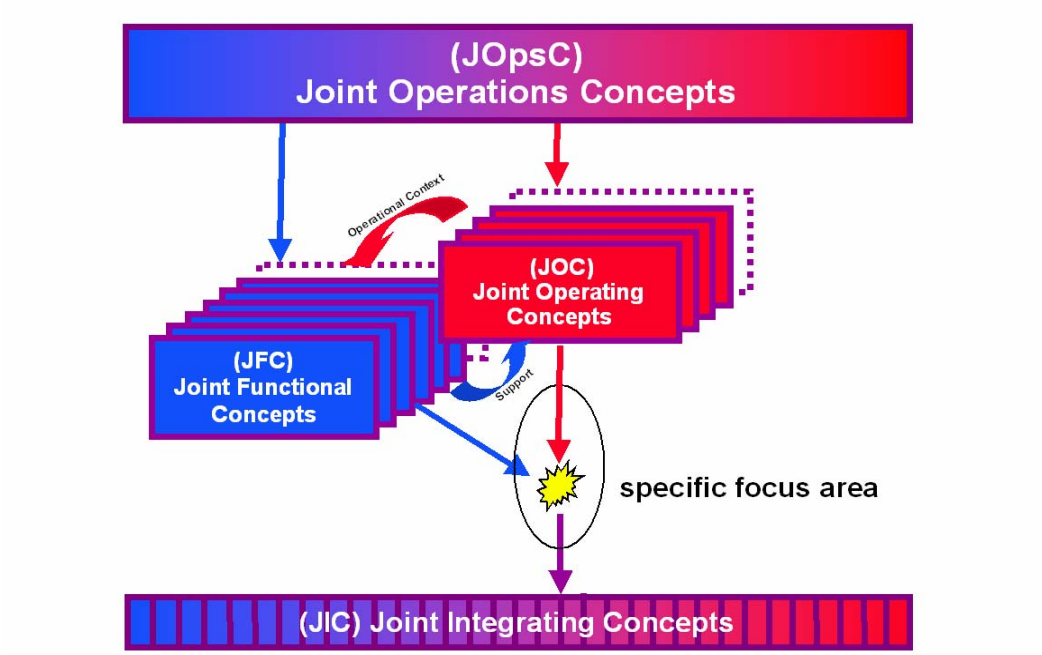

Figure 6-1. Relationships of Joint Concepts

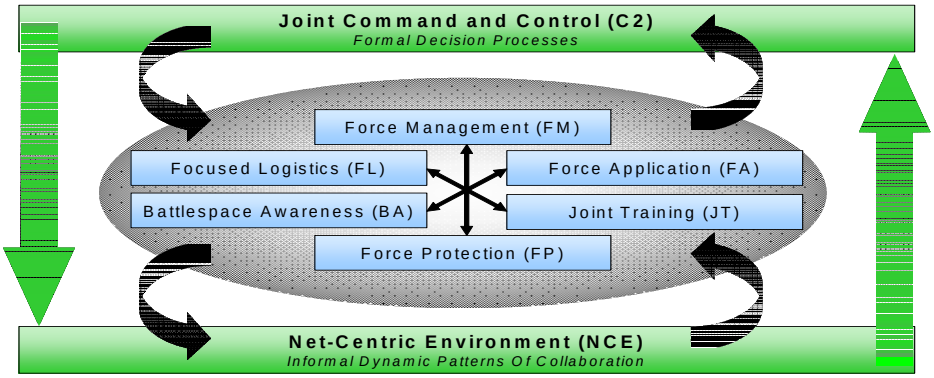

Figure 6-2. Formal and Informal Interaction between Functional Areas

Appendix A. Reference Documents

1. "Net Ready Key Performance Parameter, (v1.0)" briefing, n.d.

2. 2004 National Defense Strategy, 2004.

3. ADM GIG BE, 3 January 2003.

4. Alberts, David S., John J. Garstka, Richard E. Hayes, and David T. Signori. *Understanding Information Age Warfare*. Washington, DC: CCRP Publication Series. 2001.

5. Alberts, David S., Richard E. Hayes, Daniel T. Maxwell, John E. Kirzl, and Dennis K. Leedom. *Code of Best Practice for Experimentation*. Washington, DC: CCRP Publication Series. 2002.

6. Alberts, David S. and Richard E. Hayes. *Power to the Edge*. Washington, DC: CCRP Publication Series. 2003.

7. ASD NII Memo Subj: Joint Net-Centric Capabilities, 15 July 2003.

8. ASD NII Net-Centric Checklist v. 2.1, 13 February 2004.

9. Battlespace Awareness Functional Concept, 4 February 2004.

10. C4ISR Architecture Framework, 18 December 1997.

11. CJCSM Instruction 3170.01, "Joint Capabilities Integration Development System," 12 March 2004.

12. Concept of Operations for Global Information Grid Net Ops (Net Ops CONOPS) Final Version, n.d.

13. Data Visibility Component Guidance, 24 October 2003.

14. DOD Architecture Framework (DODAF), v. 1.0, Desktop, 11 February 2004.

15. DOD Architecture Framework (DODAF), v. 1.0, Volume 1, 9 February 2004.

16. DOD Architecture Framework (DODAF), v. 1.0, Volume 2, 10 February 2004.

17. DODD 8101.1, Global Information Grid (GIG) Overarching Policy, 19 September 2002.

18. DOD Discovery Metadata Standard Review, 2 June 2003.

19. DOD Net-Centric Data Strategy, 9 May 2003.

20. Focused Logistics Functional Concept, 4 February 2004.

21. Force Application Functional Concept, 4 February 2004.

22. Force Protection Functional Concept, 4 February 2004.

23. Global Information Grid Enterprise Services (GIG ES): Core Enterprise Services (CES) Implementation, 10 November 2003.

24. Homeland Security Joint Operating Concept, 2 February 2004.

25. Joint Capabilities Integration and Development System (CJCSI 3170.01D), 12 March 2004.

26. Joint Command and Control Functional Concept, 4 February 2004.

27. Joint Concept Development and Revision Plan, July 2004.

28. Joint Operations Concepts (JOpsC), 3 November 2003.

29. Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," 12 April 2001. (as amended through 23 March 2004)

30. Joint Transformation Roadmap, July 2004.

31. Joint Vision 2020, n.d.

32. Major Combat Operations Joint Operating Concept, 5 March 2004.

33. Merriam-Webster Online. Merriam-Webster Incorporated. 2005. http://www.m-w.com/ (Jan 2005)

34. Military Acronyms, Initials and Abbreviations: http://www.fas.org/news/reference/lexicon/acronym.htm

35. National Military Strategy, n.d.

36. Naval Operating Concept for Joint Operations, n.d.

37. Naval Transformation Roadmap 2003: Assured Access and Power Projection …From the Sea, n.d.

38. Net-Centric Operations and Warfare Reference Model Version 1.0, 9 December 2003.

39. Net-Centric Operations and Warfare Reference Model Version 1.0, 9 December 2003.

40. Net-Centric Operations and Warfare Reference Model Version 1.0, 9 December 2003.

41. Network Centric Operations DOD Report to Congress, 27 July 2001.

42. Network Centric Warfare: Developing and Leveraging Information Superiority, August 1999.

43. Quadrennial Defense Review Report, 30 September 2001.

44. Stability Operations Joint Operating Concept, March 2004 (Draft).

45. Strategic Deterrence Joint Operating Concept, 11 February 2004.

46. The National Security Strategy of the United States of America, September 2002.

47. The U.S. Air Force Transformation Flight Plan, November 2003.

48. Transformation Planning Guidance, 30 April 2003.

49. United States Army Transformation Roadmap 2003, 1 November 2003.

50. *Webster's Third New International Dictionary, Unabridged*. Merriam-Webster. 2002.

Appendix B. Glossary

Term	Definition
Action	A structured behavior of limited duration. (JCDRP 7/2004)
Activity	A structured behavior of continuous duration. (JCDRP 7/2004)
Agility	The ability to move quickly and easily. (*Power to the Edge*)
Assured	Having grounds for confidence that an information-technology (IT) product or system meets its certainty or security objectives. (NCE JFC)
Assumption	A supposition on the current situation or a presupposition on the future course of events, either or both assumed to be true in the absence of positive proof, necessary to enable the commander in the process of planning to complete an estimate of the situation and make a decision on the course of action. (JP 1-02)
Attribute	A testable or measurable characteristic that describes an aspect of a system or capability. (CJCSI 3170.01D)
Capability	The ability to achieve an effect to a standard under specified conditions through multiple combinations of means and ways to perform a set of tasks. (JCDRP 7/2004)
Collaboration	Joint problem solving for the purpose of achieving shared understanding, making a decision, or creating a product across the Joint Force and mission partners. (NCE JFC)
Communities of Interest	Collaborative groups of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes and who therefore must have a shared vocabulary for the information they exchange. (DOD Net-Centric Data Strategy)
Condition	A variable of the environment that affects performance of a task. (JCDRP 7/2004)
CONOPS (Concept of Operations or Commander's Concept)	The overall picture and broad flow of tasks within a plan by which a commander maps capabilities to effects, and effects to end state for a specific scenario. (JCDRP 7/2004)
Criterion	A critical, threshold, or specified value of a measure. (JCDRP 7/2004)
Data	Information without context. (JC2FC v1.0)
Doctrine	Fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application. (JP 1-02)
Deconfliction	Preventing elements of the Joint Force from operating at cross-purposes. (NCE JFC)
Effect	An outcome (condition, behavior, or degree of freedom) resulting from tasked actions. (JCDRP 7/2004)
End state	The set of conditions, behaviors, and freedoms of action that defines achievement of the commander's objectives. (JCDRP 7/2004)
Expeditionary	Supporting a military operation conducted by an armed force to accomplish a specific objective in a foreign country. (JP1-02)
Friction	The amount of organizational effort required to bring a certain set of capabilities to bear in a specified amount of time. (NCE JFC)
Geo-spatial Information	The concept for collection, information extraction, storage, dissemination, and exploitation of geodetic, geomagnetic, imagery (both commercial and national source), gravimetric, aeronautical, topographic, hydrographic, littoral, cultural, and toponymic data accurately referenced to a precise location on the earth's surface. (JP 1-02)

Term	Definition
Information	Facts, data, or instructions in any medium or form with context that is comprehensible to the user. (JC2FC v1.0)
Information Resource	Information and related resources, such as personnel, equipment, funds, and information technology. (USC Title 44)
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (USC Title 44 [Paperwork Reduction Act])
Infrastructure	All building and permanent installations necessary for the support, redeployment, and military forces operations (e.g., barracks, headquarters, airfields, communications, facilities, stores, port installations, and maintenance stations). (JP 1-02)
Integrated	All functions and capabilities focused toward a unified purpose. (NCE JFC)
Interdependence	A mode of operations based upon a high degree of mutual trust, where diverse members make unique contributions toward common objectives and may rely on each other for certain essential capabilities rather than duplicating them organically. (JS J7 JTD)
Interoperability	The extent to which systems, units, or forces provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together. (DODD 4630.5)
Joint	Connotes activities, operations, organizations, etc., in which elements of two or more Military Departments participate with interagency and multinational partners. (JS J7 JTD)
Joint Force	The term "Joint Force" in its broadest sense refers to the Armed Forces of the United States. The term "joint force" (lower case) refers to an element of the Armed Forces that is organized for a particular mission or task. Because this could refer to a joint task force or a unified command, or some yet unnamed future joint organization, the more generic term "a joint force" will be used, similar in manner to the term "joint force commander" in reference to the commander of any joint force. (NCE JFC)
Joint Functional Concept (JFC)	An articulation of how a future joint force commander will integrate a set of related military tasks to attain capabilities required across the range of military operations. Although broadly described within the Joint Operations Concepts, they derive specific context from the joint operating concepts and promote common attributes in sufficient detail to conduct experimentation and measure effectiveness. (JCDRP 7/2004)
Joint Integrating Concept (JIC)	A JIC describes how a joint force commander integrates functional means to achieve operational ends. It includes a list of essential battlespace effects (including essential supporting tasks, measures of effectiveness, and measures of performance) and a CONOPS for integrating these effects together to achieve the desired end state. (JCDRP 7/2004)
Joint Operating Concept (JOC)	A description of how a future Joint Force Commander will plan, prepare, deploy, employ, and sustain a joint force against potential adversaries' capabilities or crisis situations specified within the range of military operations. Joint Operating Concepts serve as "engines of transformation" to guide the development and integration of joint functional and Service concepts to describe joint capabilities. They describe the measurable detail needed to conduct experimentation, permit the development of measures of effectiveness, and allow decisionmakers to compare alternatives and make programmatic decisions. (JCDRP 7/2004)

Term	Definition
Joint Operations Concepts (JOpsC)	An overarching description of how the future Joint Force will operate across the entire range of military operations. It is the unifying framework for developing subordinate joint operating concepts, joint functional concepts, enabling concepts, and integrated capabilities. It assists in structuring joint experimentation and assessment activities to validate subordinate concepts and capabilities-based requirements. (JCDRP 7/2004)
Knowledge	Data and information that have been analyzed to provide meaning and value. Knowledge is the collection of various pieces of processed data and information that have been integrated through the lens of understanding to begin building a picture of the situation. (NCE JFC)
Lethality	The capability to destroy or neutralize a target. (NCE JFC)
Material	All items (including ships, tanks, self-propelled weapons, aircraft, etc., and related spares, repair parts, and support equipment, but excluding real property, installations, and utilities) necessary to equip, operate, maintain, and support military activities without distinction as to its application for administrative or combat purposes. (JP1-02)
Manageable	Capable of being controlled, handled, or used with ease. (NCE JFC)
Measure	Quantitative or qualitative basis for describing the quality of task performance. (JCDRP 7/2004)
Measures of Performance	Measures designed to quantify the degree of perfection in accomplishing functions or tasks. (JCDRP 7/2004)
Measures of Effectiveness	Measures designed to correspond to accomplishment of mission objectives and achievement of desired effects. (JCDRP 7/2004)
Metadata	Information about information; more specifically, information about the meaning of other data. (JP 1-02)
Metric	A quantitative measure associated with an attribute. (JCDRP 7/2004)
Mission	The end state, purpose, and associated tasks assigned to a single commander. (JCDRP 7/2004)
Mission Partners	Includes allies, coalition partners, international organizations, civilian government agencies, non-government agencies, and other non-adversaries who are involved with the activities or operations of the Joint Force. (NCE JFC)
Multinational Organizations	A collective heading for intergovernmental and international organizations. (JP 3-16)
Net-Centric Environment	The Net-Centric Environment is a framework for full human and technical connectivity and interoperability that allows all DOD users and mission partners to share the information they need, when they need it, in a form they can understand and act on with confidence; and protects information from those who should not have it. (NCE JFC)
Net-Centric (network centric) Operations	The exploitation of the human and technical networking of all elements of an appropriately trained joint force by fully integrating collective capabilities, awareness, knowledge, experience, and superior decisionmaking to achieve a high level of agility and effectiveness in dispersed, decentralized, dynamic and uncertain operational environments. (NCE JFC)
Network Centric Warfare	An information superiority oriented concept of operations that generates increased combat power by networking sensors, decisionmakers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. (*Network Centric Warfare*) A sub-set of Net-Centric Operations, see above.
Objective	A desired end derived from guidance. (JCDRP 7/2004)
Quality	Lacking nothing essential or normal. (Roget's II)

Term	Definition
Risk	Probability and severity of loss linked to hazards. (JP 1-02)
Robust	Having or exhibiting strength or vigorous health. (Webster's)
Shared Understanding	A shared appreciation of the situation supported by common information to enable rapid collaborative joint engagement, maneuver, and support. (NCE JFC)
Standard	The minimum proficiency required in the performance of a task. For mission-essential tasks of joint forces, each task standard is defined by the joint force commander and consists of a measure and criterion. (JCDRP 7/2004)
Survivability	The capability of a system and its crew to avoid or withstand a man-made hostile environment without suffering an abortive impairment of its ability to accomplish its designated mission. (NCE JFC)
Synchronization	(1) The arrangement of military actions in time, space, and purpose to produce maximum relative combat power at a decisive place and time and (2) in the intelligence context, application of intelligence sources and methods in concert with the operation plan. (JP 2-0) (JP 1-02)
System	A regularly interacting group of items forming a unified whole. (Merriam-Webster Online)
Task	An action or activity defined within doctrine, standard procedures, or concepts that may be assigned to an individual or organization. (JCDRP 7/2004)
Transparency	Encourages open access to information, participation, and decisionmaking, which ultimately creates a high level of trust and collaboration among stakeholders. (NCE JFC)
Trustworthy	The extent to which confidence or assurance is held in information or decisions. (NCE JFC)
Understanding	Knowledge that has been synthesized and had judgments applied to it in the context of a specific situation. Understanding reveals the relationships among the critical factors in any situation. (NCE JFC)
User	Any individual, organization, or automated system that interfaces with the information environment as a consumer or producer. (NCOW Reference Model)
Vignette	A concise narrative description that illustrates and summarizes pertinent circumstances and events from a scenario. (JCDRP 7/2004)

Appendix C. List of Acronyms

BCT	Brigade Combat Team
C2	Command and Control
CBA	Capabilities Based Assessment
CBRNE	Chemical, Biological, Radiological, Nuclear, and High Yield Explosives
CJTF	Combined Joint Task Force
COA	Course of Action
COIs	Communities of Interest
CONUS	Continental United States
DOD	Department of Defense
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities
ERT	Emergency Response Team
EUCOM	European Command
HA/DR	Humanitarian Assistance/Disaster Relief
HUMINT	Human Intelligence
ICRC	International Community of the Red Cross
IHRN	International Human Relief Network
IRS	Internal Revenue Service
IS	Information System
IT	Information Technology
JCDRP	Joint Concept Development and Revision Plan
JCIDS	Joint Capabilities Integration and Development System
JFC	Joint Functional Concept
JIC	Joint Integrating Concept

JOA	Joint Operations Area
JOC	Joint Operating Concept
JOpsC	Joint Operations Concepts
JP	Joint Publication
JROC	Joint Requirements Oversight Council
JTF	Joint Task Force
MDPs	Military Decisionmaking Processes
NATO	North Atlantic Treaty Organization
NCE JFC	Net-Centric Environment Joint Functional Concept
NC FCB	Net-Centric Functional Capabilities Board
NCO CF	Network Centric Operations Conceptual Framework
NCO	Network Centric Operations
NCOW	Network Centric Operations and Warfare
NCW	Network Centric Warfare
NDS	National Defense Strategy
NGO	Non-Governmental Organization
NMS	National Military Strategy
NORTHCOM	Northern Command
NSS	National Security Strategy
OASD/NII	Office of the Assistant Secretary of Defense for Networks and Information Integration
OCONUS	Outside the Continental United States
OIRS	Organization for International Relief and Support
OPSEC	Operations Security
QDR	Quadrennial Defense Review
ROMO	Range of Military Operations

RRF	Rapid Reaction Force
SOCOM	Special Operations Command
SOP	Standards Operating Procedure
SOUTHCOM	Southern Command
TPG	Transformation Planning Guidance
TRANSCOM	Transportation Command
TTP	Tactics, Techniques, and Procedures
UAV	Unmanned Aerial Vehicle
UN	United Nations
USR	Urban Search and Rescue
WMD/E	Weapons of Mass Destruction/Effect

Appendix D. Table of Capabilities and Attributes

Table D-1. Knowledge Area Capabilities

Overarching Capabilities	Tasks (The Ability to…)
Ability to establish appropriate organizational relationships	Deal with flexible authority relations
	Maintain flexible attitudes towards power and authority
	Obtain and maintain an understanding of command intent
	Flexibly adapt to changing operational needs
Ability to collaborate	Effectively collaborate with other entities
	Overcome organizational/cultural limits to collaboration
	Establish trust in decisionmaking collaboration
Ability to synchronize actions	Flexibly adapt actions to take advantage of opportunities and minimize impact of threats
Ability to share situational awareness	Achieve situational awareness
	Communicate situational awareness to other decisionmakers
	Simultaneously process inputs from multiple sources and retain focus on the task at hand
Ability to share situational understanding	Use multiple methods to achieve situational understanding (e.g., inductive, deductive, adductive reasoning)
Ability to conduct collaborative decisionmaking/planning	Achieve higher quality situational understanding via multiple means (access to expert systems, etc.)
	Communicate understandings to other decisionmakers
	Utilize virtual reality training, wargaming, and exercises
	Make high quality decisions
Ability to operate interdependently	Know tasks and teams assigned to tasks
	Know available assets enterprise-wide
	Interact effectively with decision support tools in a collaborative environment
	Interact with and accept inputs from non-traditional communities of interest

Table D-2. Technical Area Capabilities

Overarching Capabilities	Tasks (The Ability to…)
Ability to Create/ Produce Information	Collect Data
	Transform/Process data into information
Ability to Store/Share/Exchange	Tag information
	Post/publish information
	Share stored information
	Advertise information
	Stage content (smart store)
	Archive
	Collaborate
	Message
Ability to Establish an Information Environment	Establish criteria for storing and sharing
	Share across areas
	Support enterprise-wide and COI-specific applications
	Support dynamic, priority-based resource allocation
Ability to Process Data and Information	Support mediation/translation services
	Correlate and fuse information
	Process information
Ability to Employ Geo-Spatial Info	Link geographic information to underlying database
	Provide layering and drill down
Ability to Employ Information	Display information
	Enable machine to machine info-sharing
Ability to Find and Consume Information	Train using simulation and mission rehearsal
	Discover/search
	Pull/retrieve/access
	Subscribe
	Perform intelligent search/ smart pull
	Consume information
Ability to Provide User Access	Support role-based access control
	Support strong authentication
Ability to Access Information	Support multiple levels of security
	Share across security areas (Coalition, HLS)
Ability to Validate/Assure	Restore/recover
	Assure information
	Validate information
	Determine an information pedigree
	Develop trust in the information

Table D-2. Technical Area Capabilities (continued)

Overarching Capabilities	Tasks (The Ability to…)
Ability to Install/Deploy	Rapidly deploy/employ robust connectivity forward
	Tailor to specific capabilities
	Function under range of infrastructure and ROE constraints
	Dynamically plan network architecture development process
Ability to Operate/Maneuver	Dynamically allocate resources
	ID and maintain awareness of all nodes all the time
	"Wargame" the network
	Operate without geographic constraints
	Support all operations and transitional states along the ROMO
	Manage assured access/denial
	Provide ad hoc coalition connectivity
	Manage continuity and restoration of operations
	Provide timely and reliable delivery of information
Ability to Maintain/Survive	Detect and defend against logical attack
	Dynamically re-route services
	Degrade gracefully and contain cascade failures
	Continue essential operations in degraded environments (WMD/WME, Natural disasters)
	Prioritize data flows from key databases/backups (mirrors)
	Acquire additional network resources on demand
Ability to Provide Network Services	Connect with all assets
	Connect and share information among interagency/coalition/IO/commercial/NGO players
	Easily search, file, transfer, communicate, support network taxonomy
	Archive large volumes of data
	Inform/update chain of command of network status
	Support separate constellations of COIs
	Support geographically transitioning nodes

Table D-3. Knowledge Area Attributes

Attribute	Measure	Definition
Agile Moving quickly and easily	Flexible	The extent to which individuals or organizations dynamically meet evolving mission requirements.
	Innovative	The extent to which tasks are performed in novel ways
	Resilient	The extent to which recovery or adjustment is achieved given misfortune or change
	Responsive	The degree to which decisions and actions are relevant and timely
	Scalable	The extent to which organizations can seamlessly adjust size and scope to meet a given mission requirement.
Quality Lacking nothing essential or normal	Appropriate	The extent to which understandings and decisions are suitable and useful for the mission/situation at hand
	Relevant	The extent to which an understanding/decision is consistent with command intent and mission objectives
	Correct	The extent to which understandings agree with fact
	Consistent	Extent to which understandings and decisions are in line with prior understandings/decisions
	Accurate	The granularity and precision with respect to fact
	Complete	The extent to which all required elements are present
	Timely	The extent to which the currency of understandings or decisions are appropriate to the mission
Trustworthy The extent to which confidence or assurance is held in information or decisions.	Robust	The extent to which individuals or organizations exhibit strength or vigorous.
	Confident	The extent to which assurance is held in information or decisions.
	Willing	The extent to which a force entity possesses the desire to function in a shared information environment
	Competent	The extent to which one is able to perform a task and/or function

Table D-4. Technical Area Attributes

Attribute	Measure	Definition
Assured Grounds for confidence that an information-technology (IT) product or system meets its certainty or security objectives	Authentic	The extent security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information
	Confidential	The extent to which confidence or assurance is held in information or decisions
	Non-repudiated	The extent to which the senders/receivers of data are prevented from denying having processed data. Non-repudiation is measured by the extent to which senders are provided with proof of the sender's identity
	Available	The extent to which authorized users are provided with timely, reliable access to data and information services
	Integrity	The extent to which information is protected from unauthorized modification or destruction
Robust Having or exhibiting strength or vigorous health	Survivable	The extent of assurance provided a system, subsystem, equipment, process, or procedure that the named entity will continue to function during and after a natural or man-made disturbance, for example, a nuclear burst. (Note: For a given application, survivability must be qualified by specifying the range of conditions over which the entity will survive the minimum acceptable level or post-disturbance functionality, and the maximum acceptable outage duration.)
	Redundant	The extent to which surplus capability is provided to improve the reliability and quality of service
	Distributed	The extent to which the network resources, such as switching equipment and processors, are dispersed throughout the geographical area being served *Note:* Network control may be centralized or distributed
	Resilient	The extent to which recovery from or adjustment to malfunction (misfortune) or change is easily achieved
Agile Moving quickly and easily	Flexible	The extent to which success is achieved in different ways and the extent to which the network dynamically meets evolving mission requirements
	Responsive	The extent to which service is provided within required time
	Diverse	The extent to which the network is not dependent on a single element, media, or method
	Dynamic	The extent to which the network can adapt when there is a change in status
	Autonomous	The extent to which tasks are undertaken or carried on without outside control. It is the ability to exist independently; responding, reacting, or developing independently of the whole

Table D-4. Technical Area Attributes (continued)

Attribute	Measure	Definition
Manageable Capable of being controlled, handled, or used with ease	Scalable	The extent to which the network/system/organization can grow to accommodate additional users; hardware or software either co-located or globally distributed from the original system configuration
	Reconfigurable	The extent to which the network/system/organization can accommodate changes in hardware, software, features, or options
	Controllable	The extent to which a network manager has the ability to exercise restraint, direction over, or perform diagnosis to ensure optimal function and security; power or authority to guide, monitor, or manage
	Maintainable	The probability that an item will be retained in or restored to a specified condition within a given period of time, when the maintenance is performed in accordance with prescribed procedures and resources
	Upgradeable	The extent to which the network or system can accept new versions of software to meet changing requirements
	Repairable	The probability that the system/network can be restored to satisfactory operation by an action, including parts replacements or changes to adjustable settings
Expeditionary Supporting a military operation conducted by an armed force to accomplish a specific objective in a foreign country	Deployable	The extent of effort required to relocate personnel/systems to a Joint Operations Area (JOA)
	Maneuverable	The extent to which network elements support warfighters on the move
	Modular	The extent to which the network/system comprised of "plug-in" system/units/forces that can be added together in different combinations
	Transportable	The extent of mobility within the Joint Operations Area (JOA)
	Rugged	The extent to which the system/network can support operations in extreme environments and/or under conditions of high physical stress
	Reach	The extent to which the network/system can operate over extended distances to meet mission requirements
	Employable	The time and effort required to commence system operation upon arrival in the Joint Operations Area (JOA)
	Sustainable	The extent to which the network/system is able to maintain the necessary level and duration of operational activity to achieve military objectives. Sustainability is a function of providing for and maintaining those levels of ready forces, material, and consumables necessary to support military effort

Table D-4. Technical Area Attributes (continued)

Attribute	Measure	Definition
Quality Lacking nothing essential or normal	Accurate	The extent to which a transmission/data stream is error-free
	Traceable	The extent to which information is capable of being tracked or traced; the ability to follow, discover, or ascertain the course of development of something
	Complete	The extent to which all necessary parts, elements, or steps are present
	Consistent	The extent to which information is free from variation or contradiction
	Timely	The extent to which information is received in time to be useful
Integrated All functions and capabilities focused toward a unified purpose	Interoperable	The extent to which systems, units, or forces provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together
	Accessible	The extent to which all authorized users have the opportunity to make use of information capabilities
	Visible	The extent to which users and applications can discover the existence of data assets through catalogs, registries, and other search services. All data assets are advertised or "made visible" by providing metadata that describes the asset
	Usable	The extent of difficulty regarding the initial effort required to learn and the extent of recurring effort to use the functionality of the system and/or created by a information capability can be derived

Appendix E. Implications for Experimentation

The Net-Centric Environment Joint Functional Concept incorporates advanced and emerging concepts and technologies, and deals extensively with areas of endeavor that are not yet fully understood, particularly with regard to Knowledge Area issues. As a result, a robust campaign of experimentation will be necessary in order to develop, refine, test, and demonstrate net-centric concepts and methods.

As a starting point for thinking about this experimentation campaign, this Appendix captures a set of first-order hypotheses and issues for experimentation and research that surfaced during concept development.

E.1 First-Order Information Value Chain For The NCE JFC

A number of key ideas and postulated cause-effect relationships can be extracted from the main document[32] to allow one to construct a hypothesized "information value chain" for the NCE JFC. This value chain describes a process by which data is gathered from the operating environment, transformed into in-context information and actionable knowledge, and used in decision processes that lead to force action, which in turn affects the operating environment. At each stage in this process, force elements conduct activities to gather, process, fuse, and share information. How, whether, and under what conditions these processes add value to the force's mission effectiveness are appropriate subjects for a net-centric research and experimentation campaign. Figure E-1 shows one portrayal of an information value chain with a set of enablers that must be well understood to contribute effectively to net-centric function of the force.

[32] See, for example, the concept definition statement, the statement of the Central Idea of the functional concept, and the supporting hypotheses to that Central Idea.

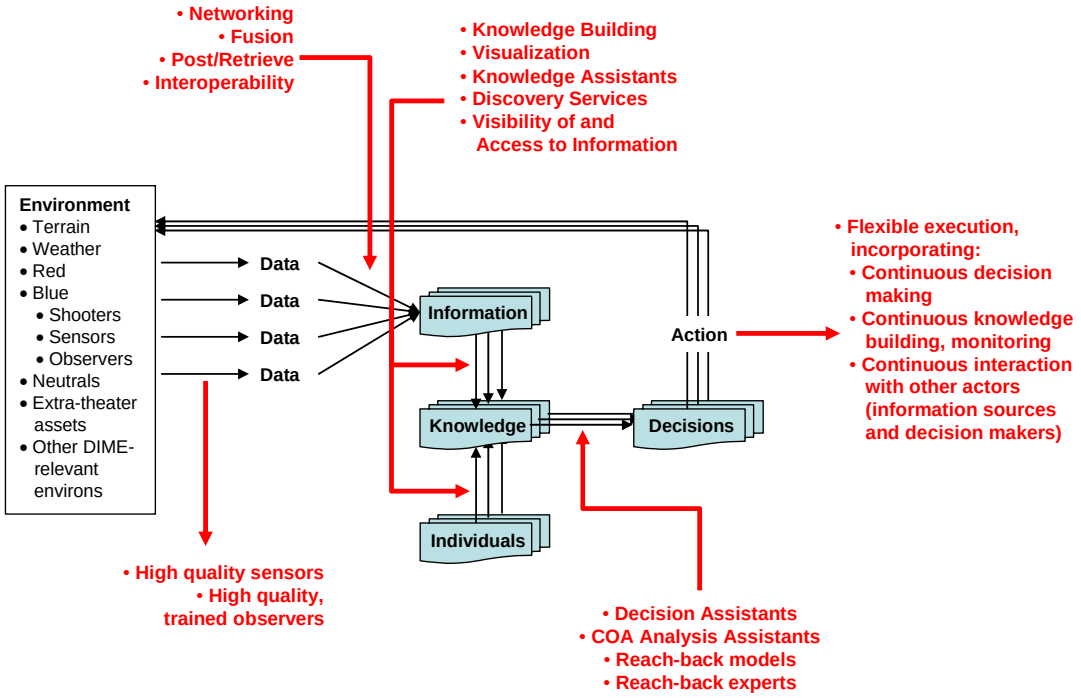

Figure E-1. Illustrative Information Value Chain for the NCE JFC, with enabling assets, technologies, and organizational capabilities

Following Figure E-1, sensors (human *and* machine) gather data to characterize the environment along dimensions relevant to the activity and mission of the force. The quality of this data extraction process, determined by the technical capability of sensing equipment and the capability and training of human sensors/observers, is the foundation for building high-quality situational awareness. Extracted data is transported to various points in the force via the force's human and technical networks, where it can be processed, fused, correlated, and placed into context. This allows individuals in the force to have access to information gathered by other force elements; further, it contributes to consistency in the information representations of individuals across the force (as those representations are drawn from a common, global set of information sources); and importantly, it provides for the representation and visualization of information in ways that are comprehensible and relevant for how it will subsequently be used by force elements.

High quality information sets allow individuals to transform information resident in systems and transported across networks in order to be incorporated into individuals' knowledge sets. The NCE JFC characterizes these processes as gaining *awareness* and *understanding* of the situation. Just as networking allows information sets to be correlated and consistent, networking does the same for knowledge sets. While consistent information bases facilitate common perceptions of the situation, it is well known that different individuals have different sets of experiences and different ways of thinking, and can draw different conclusions when presented with common information.

Networking allows individuals to synchronize their perceptions, or at least to become aware of the different perceptions that exist in different parts of the force.

With knowledge and information sets correlated (and when not correlated, with well understood differences), activities and decision processes undertaken by individuals can be correlated in ways that contribute to the agility and mission effectiveness of the force. This activity and decision coordination can be direct (taking place through explicit collaboration) or indirect (occurring through common ties to the environment, and because individuals are commonly trained and have access to relevant and consistent pictures of the mission space).

Importantly, decisions in this context refer to both formal planning and decision processes involved in command and control and instantiated in doctrine via military decisionmaking processes (MDPs), as well as informal decisions made at all levels of warfighting and at all echelons of the force. Indeed, the decision by a force member to stop his vehicle or to switch display modes on a screen can be considered decisions in this framework. The central point is that the kinds of decisions broadly impacted by this information- and network-enabled capability go beyond those of formal command and control of forces.

E.2 The Net-Centric Environment Joint Functional Concept Value Proposition

Figure E-2 illustrates the hypothesized NCE JFC "value proposition," extracting from the NCE JFC text several important elements of the functional concept and how they interrelate and follow from one another.

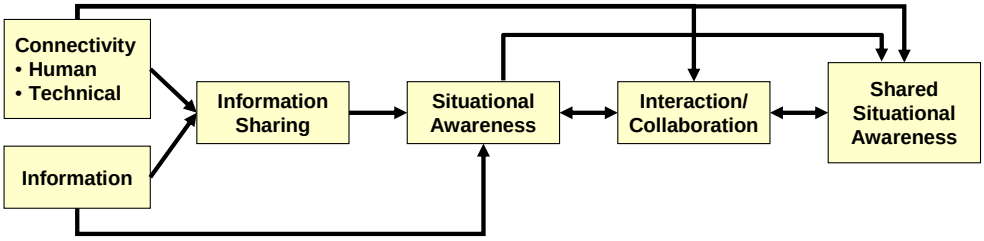

Figure E-2. Network- and Information-enabled Situational Awareness, Interaction/Collaboration, and Shared Situational Awareness

As a network- and information-enabled concept, the NCE JFC uses its Knowledge and Technical networking to create the conditions for information sharing in the force. This sharing of information, along with the collection of high-quality and relevant information from the force's Knowledge and machine sensors, improves the level of situational awareness possessed by each element in the force. With better situational awareness and appropriate DOTMLPF, force elements can interact and collaborate more effectively (they know more about what they need to know, where that information is likely to be found, and with what other force elements their capabilities need to combine, and they are interacting and collaborating in a policy, cultural, and technical environment suitable for that interaction). This in turn permits force elements to further refine their situational

awareness, as well as achieve consistency at appropriate levels among their individual pictures of the mission space. Thus, not only is situational awareness improved, but high-quality shared situational awareness is achieved as well. High quality shared situational awareness allows for the development of situational understanding because the parties are working from the same or comparable sets of facts. They can then work at sharing their deeper cognitive understanding of the unfolding situation. Enhanced shared situational awareness and shared understanding allow the Joint Force and its mission partners to engage in value-added activities such as effects-based planning, rapid course of action analysis, and wargaming of potential options.

The value chain just described, while logical, requires research and experimentation in order to be verified and operationalized. Topics for an experimentation campaign to investigate and instantiate this value chain include:

- Knowledge networking;
- Technical networking;
- Coevolution of knowledge and technical networking;
- Information sharing;
- Situational awareness;
- Collaboration/interaction; and
- Shared situational awareness.

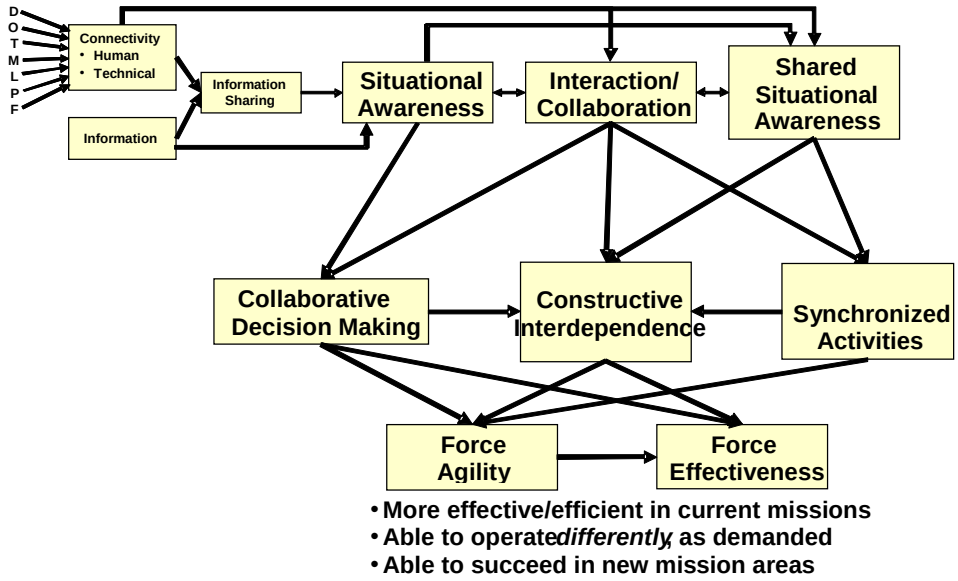

Figure E-3. Value Proposition Hypothesis: Force Agility and Effectiveness Enabled by Situational Awareness, Interaction/Collaboration, and Shared Situational Awareness

Figure E-3 suggests how the situational awareness, interaction/collaboration, and shared situational awareness created by the above-described processes lead to the ultimate objective of the Net-Centric Environment Joint Functional Concept: a joint force that is unparalleled in its effectiveness, and is effective across a broad spectrum of missions and mission conditions (i.e., is *agile*). Components of this value chain include:

- Superior decisionmaking;
- Constructive interdependence; and
- Synchronized activities (including self-synchronization).

Experimental testing of this set of hypotheses is critical, not only to establishing the value and validity of net-centric concepts, but also to understanding the factors that bear on how such value is created, and what capabilities and actions are necessary in order to attain its creation. Better understanding of how information and networking is and can be used by commanders and other force elements, how complex military organizations operate and adapt in complex environments, how evolving military and information technology is affecting the conduct of operations, how that technology can best be brought to bear in the Joint Force, and how the mind turns information into knowledge, and ultimately action, is needed to ensure the successful implementation of the NCE JFC.

Specific implications for a research and experimentation campaign involve research in the following areas:

- Cognitive processes involved in Knowledge collaboration;
- Knowledge creation from information;
- Knowledge decisionmaking processes;
- Effects of distance and networking on collaboration;
- Developing adaptive learning organizations;
- Impact of human factors on net-centric operations; and
- Others.

E.3 Other Recommendations for Experimentation

In addition to these overarching experimentation issues that relate to how cognitive and operational capabilities are created from information and networking capabilities, there are research issues associated with how to best field a particular capability in the force. For example, suppose it is established that less rigid organizational structures (one interpretation of an agile Knowledge network) and a robust Technical network that allows for rich communications and information exchange lead to enhanced situational awareness, force element interaction, and ultimately to unparalleled force effectiveness. The question remains as to which is the best *instantiation* of that organizational structure, and which is the best technical *implementation* of communications and information networks to achieve the needed awareness and interaction.

In the ultimate end state, where there are ubiquitous sensor networks, perfect fusion tools, no restrictions on bandwidth availability and high-resolution, real-time, 3-dimensional visualization, any collectable information in any force would be available to any force element, and virtual collaboration environments would be indistinguishable in terms of quality from physical “same room” collaborations. But how close to this end state does one have to come in order to achieve effective distance collaboration, make effective decisions, or be dominantly effective as a force across the range of military operations? Answering such questions requires research in fields of organizational behavior, complex

organizational analysis, Knowledge-computer interaction, and others. What follows is a suggested list of topics relevant to creating effective Net-Centric Environments, processes, individuals, and organizations. These topics are an important part of the NCE JFC research and experimentation campaign; referencing Figures E-2 and E-3, they deal with making each concept and each arrow in the Figures as value-adding as they can be.

- Effects of alternative organizational/command structures and doctrine/policy/TTP sets on information sharing, collaboration, and synergistic and synchronized activity.
- Determination of effective education and training activities to ensure force elements have knowledge required to successfully operate in a Net-Centric Environment (i.e., what does a net-centric warrior need to know in order to exploit this environment?).
- Effects of various technical networking architectures on ability to share information and collaborate.
- Correlated effects of knowledge and technical networking capabilities on operations. Effects of alignment/misalignment of Knowledge and Technical networks.
- Research in Knowledge-machine systems to explore concepts of trust (Knowledge-Knowledge trust, Knowledge-machine trust, machine-Knowledge trust, and machine-machine trust).
- Technical research into creating high-capacity, survivable, flexible, manageable, deployable, etc. networks.
- Technical research into creating effective applications to facilitate information sharing, fusion, discovery, and visualization.
- Technical research into creating effective distributed collaborative environments.

E.4 Phases of a Research and Experimentation Campaign

A suitable framework for planning and executing such an experimentation campaign is described in the *Code of Best Practice for Experimentation*,[33] which describes the execution of methodologically-sound experimentation in complex issue spaces, such as that of the Net-Centric Environment Joint Functional Concept. A complete and well-designed experimentation campaign will involve experiments and research projects variously geared towards discovery of underlying and important phenomena, testing of hypotheses, and concept demonstration, all of which are critical to getting the theory right, understanding its application, and demonstrating its value and limitations to users and decisionmakers.

[33] Alberts, David S. *Code of Best Practice for Experimentation*. Washington, D.C.: CCRP Publication Series, 2002.

E.5 Elements and Tools for NCE JFC Research and Experimentation

A diverse set of analytic, research, and experimentation tools and methods is required for thorough investigation and validation of net-centric concepts. These tools and methods include large-scale live military experiments, tabletop or sand table exercises, analytic studies, modeling and simulation at many levels of resolution, and combinations of the above, and others. Each of these elements has advantages and disadvantages. For example, large-scale live experiments often have the highest level of credibility and realistic representation of military decisionmaking processes and their impact on operational effectiveness, but are expensive, difficult to conduct scientifically, and are not repeatable. Modeling and simulation studies are generally repeatable, and may or may not be inexpensive, but it is difficult to capture faithfully, even in the most sophisticated software agents, the knowledge and decision processes whose enhancement is a focus of net-centric systems and processes. As is usually the case when studying complex problems, a family of approaches is required.

In designing and implementing a research and experimentation campaign, the full complement of analytic and research capabilities available should be brought to bear. Some of these elements (inclusive of those discussed above) are:

- Large-scale live experimentation
- Mixed live-virtual force experimentation
- Modeling and simulation studies at various levels of resolution
- Modeling and simulation-facilitated Knowledge experimentation, including man-in-the-loop and hardware-in-the-loop capabilities to examine effects of real systems on real decisionmakers.
- Analytical studies of the value of information and collaboration, including the development of mathematical representations of information and collaboration effects.
- Reviews and integration into experimentation of related research from business and academia, especially where cognitive and social issues are explored in venues such as distance learning, knowledge management, and distributed work environments.
- Multiple levels of security technical, policy, procedures, and organizational issues.
- Data fusion, both automated and human directed, including algorithms and value-added for each level of fusion.

E.6 Other Research Topics for an Experimentation Campaign

- Testing interdependency.
- Testing the concept and implementation of Communities of Interest.
- Testing Communities of Action.
- Testing external to DOD (e.g., IRS, NATO, IOs, NGOs,).
- Man-in-the-loop scenarios to test trust.
- Testing of machine-to-machine interface.
- Leverage off non-DOD experimentation (testing, e.g., Touring).

- Testing Knowledge dynamics to recruit towards.
- Realistic aptitude testing.
- Dealing with self-organizing entities.
- Cross-portal access.
- Measuring for cultural and social change.
- Get inside the asymmetric threat process.
- Compartmented Activity Data Sharing Process.
- Rapid database generation.
- Rapid data mining and analysis tools and techniques.
- Correlation of multiple resolution M&S and geospatial information.
- Web-enabled network services for M&S and analysis.
- Social and cultural impacts on decisionmaking and shared understanding.
- Artificial intelligence aids for fusion and decisionmaking.

E.7 Areas for Developing Future Hypotheses

- Ability to establish effective force arrangements.
- Ability to support enterprise-wide and COI-specific applications.
- Ability to perform Network Operations.
- Ability to dynamically plan network architecture development process.
- Ability to dynamically allocate network resources.
- Ability to support separate constellations of COIs.
- Ability to tailor to specific capabilities.
- Ability to acquire additional resources on demand.
- Ability to support geographically transitioning nodes.
- Ability to support dynamic, priority-based resource allocation.
- Ability to dynamically re-route services.
- Ability to implement information assurance.
- Ability to achieve shared situational understanding.
- Ability to achieve shared situational awareness.
- Ability to connect and share information among interagency/coalition/IO/commercial/NGO players.
- Ability to share across areas.
- Ability to collaborate.
- Ability to perform intelligent search/smart pull.
- Ability to develop trust in the information.
- Ability to share stored information.
- Ability to archive large volumes of data.
- Ability to establish rules for machine-to-machine processes.
- Ability to effectively trust and employ intelligent agents, processes, hardware, weapons, systems, and decision-aids.

Appendix F. Mapping Capabilities to Attributes

ATTRIBUTES	Ability to Create/Produce Info	Ability to Store, Share, and Exchange Information & Data	Ability to Establish Info Environment	Ability to Process Data and Information	Ability to Employ Geospatial Info	Ability to Employ Information	Ability to Find and Consume Information	Ability to Provide User Access	Ability to Access Information	Ability to Validate/Assure	Ability to Install/Deploy	Ability Operate/Maneuver	Ability to Maintain/Survive	Ability to Provide Network Services
Assured	X	X	X	X	X	X	X	X	X	X		X	X	X
Robust		X	X			X	X		X	X	X	X	X	X
Agile		X	X	X		X	X	X			X	X	X	
Manageable		X	X	X	X	X	X	X	X		X	X	X	X
Expeditionary			X		X			X			X	X	X	X
Quality	X	X	X	X		X	X		X	X		X		X
Integrated	X	X	X	X	X	X	X	X	X		X	X	X	X

Figure F–1. Mapping Capabilities to Attributes: Technical Area

ATTRIBUTES	Ability to establish appropriate organizational relationships	Ability to collaborate	Ability to synchronize actions	Ability to share situational awareness	Ability to share situational understanding	Ability to conduct collaborative decisionmaking/planning	Ability to achieve constructive interdependence
Agile	X	X	X		X		X
Quality	X	X	X	X	X	X	X
Trustworthy	X	X		X	X	X	X

Figure F-2. Mapping Capabilities to Attributes: Knowledge Area

Appendix G. Contributors

Last Name	First Name	Rank/Pos	Organization
Ables	Jimmy D.	Mr.	NCI Info Sys. Inc./USTRANSCOM/TCJ6-OP
Atkinson	Kenn	Mr.	DMSO/SAIC
Bankert	Brian	MAJ	HQ USAF/XIII
Beasley	William	Mr.	OUSD (AT&L)/Joint Force Integration
Bell	Michael	Dr.	CNO N61F
Benham	Barry	Mr.	Battle Command and Awareness Division, Future Center, TRADOC
Bodiford	Kurt	MAJ (P)	U.S. Army G8-FDJ
Boeckman	Chuck	Mr.	MITRE Corporation
Boggs	Steve	Mr.	SAIC, Systems Study Integrator, JS/J6-A
Boyd	Bobby	Mr.	Futures Center, Architecture Integration and Management Directorate
Bryant	Louis	Mr.	Evidence Based Research, Inc.
Burris	Craig	Lt Col	NC FCB/JS J6A
Cagle	Joseph	Lt Col	HQ USAF/XIII
Cameron	Andrew	LCDR	CNO-N6IC
Carroll	Rick	Mr.	NC FCB/JS J6A /SAIC
Carter	David	MAJOR	HHC G3 HQDA
Cartier	Joanna	Dr.	IDA
Centola	Joanna	Ms.	Evidence Based Research, Inc.
Conrad	Walter	Mr.	SAIC/J6A
Cordray	Elisabeth	Mrs.	Office of the Secretary of Defense for Policy (Resources and Plan)
Corey	Shannon	Ms.	Evidence Based Research, Inc.
Cranford	Steven	Mr.	Simulation Technologies, Inc/HQ USAF/XIII
Creighton	Kathleen	CDR	NC FCB/JS J6A
Davis	Brian	Mr.	Evidence Based Research, Inc.
Dunning	Regina	Ms.	USTRANSCOM/TCJ6-A
Faltum	Andrew	Mr.	Alion Science and Technology/Joint Staff J6I
Fields	Evelyn	RADM (Ret.)	Evidence Based Research, Inc.
Flournoy	Horace	Lt Col	JFCOM J8/JI&I
Garstka	John	Mr.	Office of Force Transformation, OSD
Grimsley	Russ	Mr.	SAIC/C2FCB
Haney	Scott	Lt Col	J8 WCAID
Harvey	Tina	Lt Col	AF/XIWS
Hayes	Richard	Dr.	Evidence Based Research, Inc.

Last Name	First Name	Rank/Pos	Organization
Hintz	Willis	Mr.	Futures Center, TRADOC
Holloman	Kimberly	Dr.	Evidence Based Research, Inc.
Horan	John	Mr.	HQ USAF/XORI (TITAN)
Jakubek	David	Mr.	ODUSD (S&T)
Jones	Ernest	Mr.	U.S. Army TRADOC
Joyce	Daniel	Mr.	NSR, Inc./Joint Staff/J6I
Jurinko	Stephen	LTC (P)	AAIC, Army CIO/G6
Keane	Sheyla	Ms.	Evidence Based Research, Inc.
Kennamer	Celeste	Ms.	HQDA G3/Alion Sciences & Technology
Kettler	Thomas	LT COL	HQ AF/XOXR
Kinny	Rory	COL	AF/XOR-NC
Kirzl	John	Mr.	Evidence Based Research, Inc.
Kropp	Wayne	Mr.	Army TRADOC Future, AIMD
Leber	Grant	Mr.	LMIT/ASD (NII)
Lee	Richard	Mr.	OSD/AT&L/AS&C
Leedom	Dennis	Dr.	Evidence Based Research, Inc.
Leidy	Charlotte	CAPT	Lead, NC FCB/JS J6A
Little	Laura	LtCol	JS/J6 Director's Action Group
Maddox	Alice	Mrs.	HQ USAF/XIWA
Malburg	Ronald	Mr.	CSC/USTRANSCOM J6
Martin	Jo-Anne	Ms.	The Boeing Company
Maxwell	Daniel	Dr.	Evidence Based Research, Inc.
McArdle	Kim C.	Mr.	AF/XICC (Scitor Corp.)
McCreedy	Kenneth h	LTC	Office of Force Transformation, OSD
McEver	Jimmie	Dr.	Evidence Based Research, Inc.
McKee	Robert	Mr.	MITRE
Mertz	Don	Lt Col	NC FCB/JS J6A
Miller	Lynn	Ms.	DISA
Miner	Patrick	LTC	USCENTCOM, CCJ6
Mottram	Bonnie	Ms.	Evidence Based Research, Inc.
Mullen	Edward	CDR	NC FCB
Nickson	Mark	Lt Col	Joint Staff/J6
Ouellette	Roger	Major	USSTRATCOM/CL13
Powers	James	MAJ	USSOUTHCOM
Quigley	John	Mr.	Boeing (Washington, DC Naval Systems)
Quinton	Keith	Lt Col	JS J-7
Robinson	Louray	Ms.	AF/XICS - Sumaria

Last Name	First Name	Rank/Pos	Organization
Rohatgi	Mukesh	Mr.	Old Dominions University Research Foundation
Sadauskas	Leonard	Mr.	DASD (DCIO) CP/O
Schuller	Jeffrey	Mr.	Joint Staff/J8 WCAID
Seitz	Gregory	Mr.	Binary Consulting/Army CIO/G6 FCS
Shanley	William	Mr.	USJFCOM J-61
Signori	David	Dr.	Evidence Based Research, Inc.
Siomacco	Edward	COL, O-6	Army C10/G-6
Smith	Brian	Mr.	Evidence Based Research, Inc.
Sobers	Arthur	Mr.	CSC/J-8 Protection Assessment Division
Spencer	Jay	CDR	Joint Staff/J8/Force Application
Stephens	Vincent	Lt	USSTRATCOM/CL132
Stockland	Orville	Mr.	NSA/123
Tabacchi	Len	Mr.	ASD NII
Taylor	Bridgette	Ms.	CSC J8-PAD/DDFP
Valent	Oscar	Mr.	Executive Assistant to Defense S&T Reliance Executive Staff Chair
Van Dine	Wayne	Mr.	DOD/IAA SPO
Veneeri	Janice	Ms.	DISA
Watson	Ian	Mr.	NORTHCOM J5
Whaley	Steven	MAJ	U.S. Marine Corps
Williams	Gary	Mr.	SYColeman/Army G-35
Wilson	Anhtuan	LCDR	PACOM/J622
Young	David	Mr.	USJFCOM/Old Dominion University
Zavin	Jack	Mr.	ASD(NII)/DOD CIO