NET-CENTRIC OPERATIONAL ENVIRONMENT JOINT INTEGRATING CONCEPT

Version 1.0

31 OCTOBER 2005

JOINT STAFF
WASHINGTON, D.C. 20318-6000

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In order to support a robust Capabilities-Based Assessment (CBA) and advance the development and application of net-centric capabilities for the future Joint Force, this *Joint Integrating Concept* (JIC) document presents the concept of a Net-Centric Operational Environment (NCOE). This NCOE JIC was developed as part of the broader NCOE implementation effort, the overall objective of which is seamless, integrated net-centric capabilities to the forward edge of the battlespace, enabling full spectrum dominance. This NCOE JIC addresses the following military problem: *The Joint Force and mission partners must have rapid access to relevant, accurate, and timely information, and also the ability to create and share the knowledge required to make superior decisions in an assured environment amid unprecedented quantities of operational data.*

By providing the Joint Force and mission partners with the technical connectivity and interoperability necessary to rapidly and dynamically share knowledge among decision-makers and others—while protecting information from those who should not have it—the NCOE will facilitate the coherent application of joint action. Indeed, the NCOE has the potential to revolutionize joint operations by optimizing and even transforming how information and knowledge are generated, presented, and used throughout the Joint Force and mission partners. The timeframe is 8 to 20 years in the future, with an illustrative focus on the year 2015.

The NCOE is more than a set of networked technical capabilities. *The concept's central idea is that, for the future Joint Force to achieve decisive levels of shared knowledge and technical connectivity, the NCOE must provide the Joint Force with pervasive knowledge through the full integration of knowledge management (KM), network management (NM), and information assurance (IA).*

- *Knowledge management*, or KM, is the process of discovering, selecting, organizing, distilling, sharing, developing and using information in a social-domain context to improve warfighter effectiveness.

- *Network management*, or NM, focuses on the people, technology, processes, policy and capabilities necessary to effectively operate the systems and networks, including their configuration, availability, performance, manageability, and enterprise connectivity.

- *Information assurance*, or IA, will provide the Joint Force and mission partners with assured mission management, assured information sharing, confidentiality, and integrity/non-repudiation capabilities.

The DoD Data Strategy is an acknowledged joint enabler, and data comprises the common currency of the NCOE, providing cross-cutting transactions for

each of the foregoing activities. In order for the NCOE concept to be realized and its goal of pervasive knowledge achieved, relevant data must be visible, accessible, understandable, and trusted. Data with context becomes information, whereas information with operational context becomes knowledge in the minds of its users.

This NCOE JIC builds upon the *Net-Centric Environment Joint Functional Concept* (NCE JFC) document, which defines baseline functional capabilities and attributes for future Joint Net-Centric Operations at all levels of command and across the range of military operations. This NCOE JIC extends the NCE JFC's integrating framework and articulates *how* net-centric tasks will be used to advantage by the future Joint Force. Eight examples provide detailed explanations of how specific tasks, described herein, will work together in the context of an integrated KM-NM-IA framework, thus providing the Joint Force with this new, potentially revolutionary capability. The NCOE is based upon an information-sharing risk management process to ensure that we move from a "risk avoidance" model of information-sharing to a true "risk management" model.

By focusing on the application of net-centric capabilities in major combat operations, this NCOE JIC also establishes the conditions, tasks, and standards needed to support the conduct of a Capabilities-Based Assessment, or CBA. Three *Enabling Constructs* and a classified Concept of Operations (CONOPS) are included as appendices for additional context and as "drill down" material for use in the CBA process. Over time, this NCOE JIC will be further harmonized with other key policy documents—i.e., the *Net-Centric Operations and Warfare Reference Model* (NCOW RM), Information Technology (IT) portfolios, documents for Joint Capabilities Areas (JCAs), etc.—in parallel with the CBA, in time to influence the resulting *Joint Capabilities Document* (JCD) taxonomy and standards.

1. PURPOSE

This document provides a conceptual look at how the Net-Centric Operational Environment, the NCOE, will enhance the overall performance of warfighters at every level. Its focus is supporting a Joint Task Force (JTF), including the JTF Commander, JTF mission partners, and warfighters at the "first tactical mile."[1] The goal is for the entire Joint Force and mission partners to have the technical connectivity and interoperability necessary to rapidly and dynamically share knowledge amongst decision-makers, communities of interest (COIs), and others, while protecting information from those who should not have it—all to facilitate the coherent application of joint action. The NCOE will translate information superiority into combat power by effectively linking (both horizontally and vertically) knowledgeable entities throughout the battlespace, thus making possible dramatically new ways of operating and, by extension, decisive advantages in warfighting. The timeframe is 8 to 20 years in the future, with an illustrative focus on the year 2015.

The NCOE is an operational subset of the Global Information Grid (GIG). The NCOE will use the GIG, and by incorporating other systems and organizational processes, will leverage the GIG for warfighting purposes. Most of the higher-level purposes of this *Net-Centric Operational Environment Joint Integrating Concept* (NCOE JIC) document are already described in concept development guidance and higher order concepts (CJCSI 3010.02B, CCJO) and therefore they are not repeated here. For example, the existing GIG architecture and the *Joint Concept of Operations for Global Information Grid NetOps (GIG NetOps CONOPS*) will be viewed as a basis to inform but does not bound this NCOE JIC. For example, the NCOE uses the NetOps framework but also expands it by incorporating the emerging field of expertise known as knowledge management. By including knowledge management, the NCOE is more than a networked set of technical capabilities.

2. MILITARY PROBLEM

The Joint Force and mission partners must have rapid access to relevant, accurate and timely information, and also the ability to create and share the knowledge required to make superior decisions in an assured environment amid unprecedented quantities of operational data.

The *Major Combat Operations Joint Operations Concept* (MCO JOC) document asserts that fundamental changes are needed in how we approach warfare and conflict resolution. People will remain the centerpiece, but changes within society, the global security environment, and the rapid advance and proliferation of information-age technologies all necessitate a continual

[1] The "first tactical mile" refers to the support which the NCOE will provide to warfighters directly involved in executing the mission. Those warfighters at the "tip of the spear" will receive perhaps the greatest benefit from the NCOE as it vastly improves their decision-making capabilities across the full spectrum of military operations.

transformation of the Joint Force. We must never assume that we will always enjoy material advantages over our adversaries. Instead, we must strive to be more effective at using whatever resources we have available—especially since, in the ordinary warfighting organization, latent power exists that is, by most standards, extraordinary. The exploitation of that potential may be one of the most profound revolutions in military affairs. The *Net-Centric Environment Joint Functional Concept*, or NCE JFC, argues that the Joint Force's current human and technical connectivity, its interoperability, and its ability to exploit those, are inadequate to leverage that latent power.

The difficulty in achieving a net-centric environment lies in two critical areas: knowledge management among humans, and technical connectivity and interoperability. *Knowledge management*, or KM, is the systematic process of discovering, selecting, organizing, distilling, sharing, developing and using information in a social-domain context to improve warfighter effectiveness. To better achieve a state of pervasive knowledge—ensuring that the right information is available to the right person, at the right time, in the right context—the Joint Force and mission partners require a paradigm shift from a "need to know" to a "need to share" orientation. The latter would support dynamic organizational constructs and decentralized decision-making in a fluid environment. Mission partners are expected to be from interagency, multinational, and coalition agencies, non-governmental organizations (NGOs), industry, and academia. To share knowledge among them and itself, the Joint Force currently lacks such a tailorable, dynamic KM capability.

The second critical area is technical connectivity and interoperability[2], two requirements of *network management* (NM). The Joint Force and mission partners require, but currently lack, a seamless sharing of required information and knowledge through an assured, protected network (referred to as *information assurance* or IA). This is required to connect not only command-and-control (C2) elements but also Joint Force users at the first tactical mile. Intelligence, surveillance and reconnaissance (ISR) platforms ("sensors") and weapon systems ("shooters") also need to be networked.

In most shooting engagements the winning force is that force which outpaces the other's decision-loop with decisive results, typically by outmaneuvering and destroying the adversary's asset(s) with effective fires faster than he can compensate for. As important as this capability is, however, satisfying our requirements will require more than the full networking of sensors to shooters. Future conflicts will likely be *contests in adaptability:* the winning force will be that force which adapts itself more effectively to the situation at hand, certainly faster and perhaps more thoroughly, whether for warfighting or for "winning the peace." Dynamic adaptation will be necessary because we cannot flawlessly predict every eventuality beforehand, nor even predict every possible

[2] See Glossary definition.

contingency to plan for. Instead, the Joint Force needs a capability that can leverage uncertainty—i.e., the capability of dynamic adaptability, via knowledge sharing and net-centric operations—to heighten our adversaries' fear and uncertainty that they can somehow prevail against us, even if they attempt to do so asymmetrically.

3. SCOPE

This NCOE JIC was developed as part of the broader NCOE development effort. The objective of the NCOE is "seamless, integrated net-centric capabilities to the forward edge of the battlespace, enabling full spectrum dominance." This document examines how the NCOE's capabilities will support the execution of Joint Net-Centric Operations (JNO)[3], particularly in a Major Combat Operations (MCO) context. Although this NCOE JIC focuses on MCO, it also captures many of the network needs described in other operating concepts, especially those pertaining to Stability Operations.

This NCOE JIC is accompanied by three (3) *Enabling Constructs* (ECs) and also articulates the critical integrating capabilities, tasks, and standards required to support MCO. It also illustrates, from an operational perspective, the NCOE's benefits to a Joint Task Force engaged in decisive actions.

In regard to JNO, the NCOE concept integrates knowledge management (and sharing), network management and information assurance capabilities directly into the Top level (Tier-1) framework, while, as appendices, its three ECs—*Information Transport, Enterprise Services,* and *Applications*—each provide a "drill down" to the sub-sub task layer for those tasks relevant to their described capability.[4] Future versions of the NCOE JIC will address additional ECs that may be needed, such as Computing Infrastructure.

3.1 Definition of Concept

The NCOE concept is defined as "the coherent application of Joint Net-Centric Operations (JNO) capabilities at the Joint Task Force-level and below in order to affect decisive outcomes in Major Combat Operations and related scenarios."

---

[3] JNO embodies the ability to exploit all human and technical elements of the Joint Force and our mission partners through the full integration of collected information, awareness, knowledge, experience, and decision-making, enabled by secure access and distribution, all to achieve agility and effectiveness in a dispersed, decentralized, dynamic and/or uncertain operational environment. JNO is a Tier-1 Joint Capability Area (JCA). Tier-1 JCAs are collections of similar capabilities, grouped at a high level to support decision-making, capability delegation, and analysis. Tier-2 capability areas capture the function and operational detail that either translate into Joint Force Commander-level operations/missions or which identify lower level activities.

[4] As of October 2005, the JNO structure lists IA as a Tier-2 capability. KM and NM are both listed as Tier-3. The JNO structure is anticipated to, at least in the near term, continue to evolve and reflect the understanding of these capabilities as described in this NCOE JIC.

While the framework for this NCOE JIC is derived from emerging JNO constructs, it is not limited by them.

Any *Joint Integrating Concept* document, or JIC, describes how future military commanders will, 8 to 20 years in the future, employ their capabilities to achieve desired effects and accomplish the mission. A JIC consists of a set of specific capabilities, tasks, and standards applicable to a range of scenarios, along with an illustrative Concept of Operations, or CONOPS, to show how leveraging those capabilities will increase our combat effectiveness. Of all the joint concept documents, the JIC has the narrowest focus, distilling capabilities from the Joint Operating and Functional Concepts (JOCs and JFCs) into the fundamental conditions, tasks, and standards required to conduct a Capabilities-Based Assessment, or CBA. The CBA process uses the JIC as a baseline to conduct rigorous analyses of capability gaps and overlaps, leading ultimately to appropriate material and non-material solutions as part of the broader Joint Capabilities Integration and Development System (JCIDS).

3.2 Timeframe

This NCOE JIC uses a timeframe of 8 to 20 years in the future (that is, from concept approval). For continuity, this document's illustrative CONOPS and *Enabling Constructs* are all focused on the year 2015.

3.3 Assumptions and Risks

Various assumptions are common to every joint concept. In addition to the particular assumptions listed in the NCE JFC document, three assumptions of this NCOE JIC are:

- That future U.S. Joint Force operations will occur in an environment wherein the United States is supported by various mission partners;

- That our adversaries will have access to advanced off-the-shelf technologies and to anti-access technologies that could threaten our ability to conduct combat operations; and

- That affordable technology will allow our coalition partners and other agencies to acquire net-centric capabilities.

Even with net-centric capabilities 8 to 20 years in the future, military leaders and planners will still need to employ prudent risk management strategies. Risks and mitigations concerning a net-centric environment can be found in the NCE JFC.

3.4 Applicable Military Operations or Functions and Activities

Every functional area of the Joint Force—such as personnel, intelligence, operations, logistics, and civil affairs—will be integrated, via the NCOE, into an all-inclusive, multi-Service, interoperable environment for enhanced warfighting. The NCOE will also integrate the network capabilities of mission partners, including non-governmental organizations and private businesses. These integrated capabilities will facilitate the fluid, coherent application of joint military action through pervasive knowledge.

3.4.1 Relationship to other Joint Concepts

This NCOE JIC is broadly defined by the NCE JFC and is strongly influenced by various *Joint Operations Concepts* (JOpsC) documents, especially the MCO JOC. This NCOE JIC is thus a cross-cutting document because the NCOE's capabilities, tasks, and standards are applicable to other Joint Operating, Functional and Integrating Concepts and also across multiple functional and operational mission-areas. However, for the purpose of bounding this NCOE JIC, Phase III-B ("Win Decisively") of the *Defense Planning Scenario Major Combat Operations #3* (MCO-3) has been chosen to illustrate the NCOE's capabilities. That phase poses the most challenging and dynamic environment, involving multiple units requiring integration across both functional areas and various levels of command, including allies, coalition partners, and non-combatant organizations.

4. CENTRAL AND SUPPORTING IDEAS

4.1 Central Idea

In order for the future Joint Force to achieve decisive levels of shared knowledge and technical connectivity, the Net-Centric Operational Environment (NCOE) must provide the Joint Force with pervasive knowledge through the full integration of knowledge management (KM), network management (NM), and information assurance (IA).

The NCE JFC document defines a net-centric environment as "a Joint Force framework for full human and technical connectivity that allows all DoD [Department of Defense] 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 NCOE is the operational implementation and manifestation of a net-centric environment, leveraged primarily by a Joint Task Force (JTF) and mission partners for warfighting and other purposes. The NCOE is not the Global Information Grid, although the NCOE will use the GIG and, by incorporating other systems and organizational processes, it will leverage the GIG for

warfighting purposes. By also incorporating the social domain aspects of knowledge management, the NCOE includes more than a networked set of technical capabilities. The NCOE can be thought of as a vastly improved synergy of DOTMLPF[5] and policy, energized by the advances of the information age—a synergy that will enable warfighters and other decision-makers, at every level, to make and execute superior decisions faster than adversaries. The NCOE will enable the Joint Force to outpace an adversary's decision-loop and be more adaptive to the situation at hand.

Since the NCOE will leverage the power inherent in networking, how networking works deserves some explanation. A network can be thought of as a collection of nodes connected by some means of communication. When something which one node would value, such as intelligence data, is acquired by another network entity, their connection enables them to transfer or share it. The more efficiently a network's nodes work together for their collective benefit, the more that network can leverage its collective resources—intelligence, fire support, logistics, etc.—to employ against an adversary.

In order for nodes to exchange information effectively, they must transact with each other using a common currency. Within the NCOE, the common currency is data. Although data is not an activity, per se, it is the enabler for all the other components. To provide this enabling function, data must be visible, accessible, understandable, and trusted.[6] Activities are required to accomplish each of the aforementioned data sharing goals. Implementation of the DoD Data Strategy is recognized as a fundamental premise and joint enabler for the full integration of KM, NM and IA, as well as for underpinning all of the enabling constructs associated with the NCOE. For example, data assets will be made visible by creating and associating metadata ("tagging"), including discovery metadata, for each asset. Discovery metadata will conform to the DoD Discovery Metadata Specification (DDMS).

All metadata will be discoverable, searchable and retrievable using DoD-wide capabilities that support JNO. Data assets will be made accessible by making data available in shared spaces. Data assets will be made understandable through the activities of communities of interest (COIs) and by publishing associated semantic and structural metadata in a federated DoD metadata registry. To enable trust, data assets will have associated IA and security metadata, and an authoritative source for the data will be identified as appropriate.

The NCOE will use an integrated set of knowledge-related (i.e., cognitive and social) processes enhanced by technical processes and systems. Integrating those knowledge and technical areas are three critical components used in

[5] DOTMLPF: Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities.
[6] See DOD Directive (8320.2) (Data Sharing Directive) for more information.

combination: knowledge management, network management, and information assurance. Although the physical technologies that enable KM, NM and IA reside in the technical area, that area alone is not the entirety of the NCOE and should not be treated as such. For whereas the NCOE's knowledge area is less tangible than its technical one, the two areas are wholly interdependent, as are the NCOE's KM, NM and IA components.

Figure 1 depicts a future transformation of the Joint Force's work-dynamics, coalescing from today's disjointed human-technical arrangement towards the future NCOE—when the Force's KM, NM and IA components will be fully integrated. At present, various communities throughout the Joint Force are trying to find ways to jointly accomplish their common mission objectives; but the human and technical separation of those communities causes their efforts to be, too often, exceptional, not as integrated as they should be, not easily repeatable, and rarely applicable to other scenarios. Such arrangements are woefully insufficient to meet the needs of the future Joint Force.

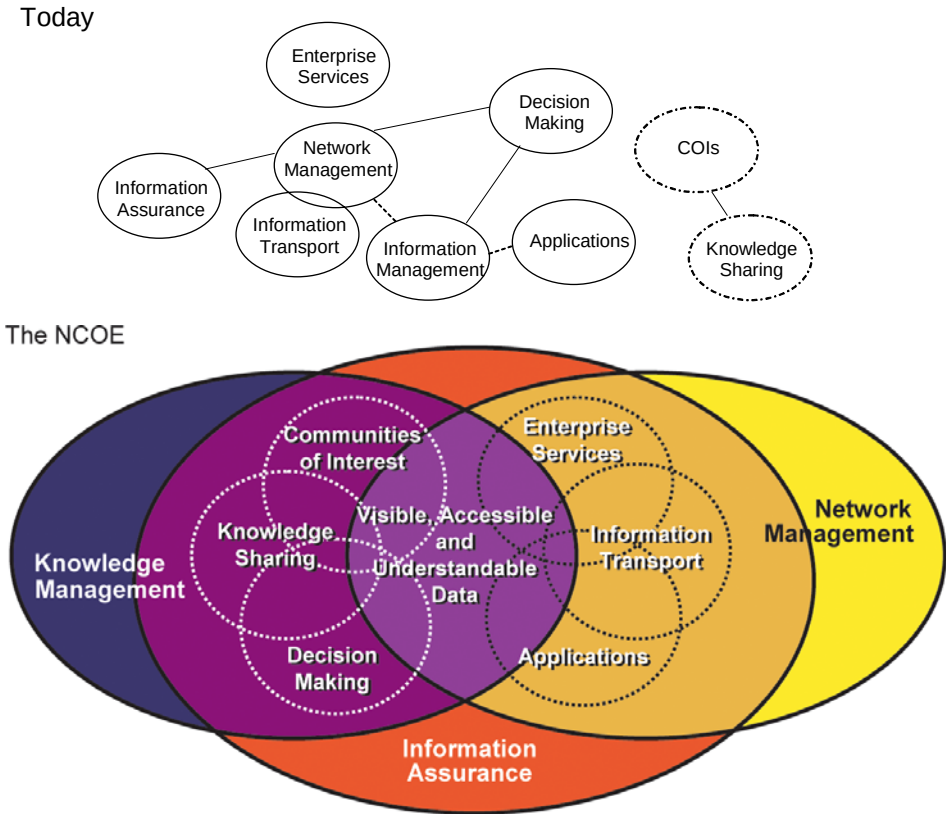


Figure 1. Transformation to the NCOE

The rest of this Central Idea section presents detailed descriptions of the NCOE's KM, NM and IA components, along with some subordinate concepts. A graphic depiction of the NCOE's operational context, Figure 2, appears in sub-section 4.1.5.

4.1.1 Knowledge Management (KM)

Knowledge management, or KM, is defined here as "the systematic process of discovering, selecting, organizing, distilling, sharing, developing and using information in a social domain context to improve warfighter effectiveness." Although other definitions of KM exist throughout the public and private sectors, they generally refer to similar processes.

KM stems from the premise that an organization's competitive advantage exists in how well, and how widely, that organization uses and enhances its own collective knowledge. A substantial portion of that knowledge is not written down because it exists only in the individual minds of people—as memories, as experiences, as each person's inner sense of what works and what does not. Whenever a widely experienced person retires from an organization, his departure may reduce that organization's collective knowledge more than if its internal training manuals were lost. For whereas training manuals have information, people have knowledge.

Knowledge (i.e., insights) can also be gained from an organization's various databases if those are networked and their data synthesized and analyzed for otherwise hidden cross-connections and patterns. In doing so, new efficiencies and opportunities can be revealed, many of them dependent upon short windows of time. To achieve and exploit them, however, more than computer processing and automated *information management* (IM) are required. KM, not IM, includes the crucial involvement of people who can realize the efficiencies and opportunities to be leveraged, who know their jobs well enough to know which information would enhance their performance and to ignore the rest, and who are empowered to organize their informational and work environments accordingly. Without that human involvement, better IM alone is insufficient.

The term *knowledge management* is sometimes criticized with the argument that if "knowledge" is something that exists only in the human mind, not in a book or a computer, then only the mind can "manage" knowledge. Therefore, this argument goes, organizations cannot manage knowledge but only data and information. Whatever the merits of this argument, however, the term *information management* is a poor substitute for KM since IM already refers to a specific technical process that does not include all of KM but, rather, is a sub-set of KM. Efforts to avoid using the KM term tend to sow confusion between those who have adopted the KM term versus those ignorant of it and of the substantial field of expertise that KM represents. The term is already accepted and used by many military institutions, including those of several allies (such as Britain's, Canada's, and Australia's) and throughout the U.S. Armed Forces.

In the terminology of KM, the terms *data*, *information*, and *knowledge* are not generally interchangeable because they refer to different categories:

- *Data* is a representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by human or by automatic means. A temperature reading of 50 degrees Fahrenheit is an example of data. When provided with registered discovery metadata, data sources can be effectively discovered and subscribed to or searched. However, data by themselves have no meaning because they lack context. A temperature of 50 degrees F. might feel cool in a jungle or warm in the Arctic, but without that climatic context the number is meaningless.

- *Information* is data placed in context, giving it meaning. Thus, 50 degrees F. becomes meaningful as the outdoors temperature of a particular environment. Content tagging (metadata) helps to provide the context for data.

- *Knowledge* is information with intrinsic value—because it has implications. If tomorrow's forecast is for weather suitable for most military activities, and if enemy forces typically exploit good weather to launch an attack, then the implication for a warfighter is that he should prepare to counter an enemy attack, possibly coming tomorrow. This is knowledge because it is based upon information, experience, reasoning, and the situation at hand.

For KM purposes, the above possibility of an enemy attack can be considered to be both information and knowledge. It is *information* when it appears as a report, in this case an urgent one. It is *knowledge* when it is understood by one or more people, they having made meaningful connections in their minds between the information they have received and, realizing its implications for their specific situation, what actions they can then take. What is called *actionable knowledge* is whatever information that, in a given situation, can be assimilated, integrated with other inputs, and then acted upon as the basis for a decision. When actionable knowledge is shared commonly across the Joint Force, it becomes pervasive knowledge and serves as the basis for coherent joint action.

Since information and knowledge are not necessarily tangible, they exist in four *domains*[7] that influence one another and, in some respects, overlap:

- The *information domain* is defined as "where information exists. [It] has a dual nature, consisting of the information itself and the medium by which we collect, process, and disseminate information. Characteristics

[7] Within the context of this NCOE JIC, a *domain* is defined as "a sphere of activity, concern, or function." The term is used both in a physical sense (air, land, and sea domains) and in a functional sense (information, physical, and cognitive domains)—interchangeably and without contradiction.

of the information domain include information quality (completeness, accuracy, timeliness, relevance, and consistency), distribution (range, sharing, and continuity), and interaction (exchange or flow of information)."

- The *physical domain* is the domain wherein military forces are moved through time and space. It spans the land, sea, air, and space environments because it is where physical military platforms, and where the communications-networks that connect those platforms, reside.

- The *social domain* is "shaped by the specifics of language and symbolic communication among human beings. It is the domain within which individuals interact and is strongly influenced by tacit knowledge..." In previous ages, whenever warfighters had to interact across considerable distances, they were limited to courier-delivered messages and, later, to voice-radio. Those methods were the best available, but their capacity for human expression was, and remains, rather limited in comparison to face-to-face communication. Since most face-to-face communication is actually non-verbal—relayed through facial expressions and other body language—the communicative importance of the social domain should not be discounted.

- The *cognitive domain* is perhaps the least tangible of the four domains because it "exists in the minds of human beings. This domain is influenced by individual intangibles such as training, experience, public opinion, and situational awareness. Most importantly, the cognitive domain is where we make decisions and is directly related to intellectual capabilities and developmental levels. Vital characteristics of this domain are those that affect individual and organizational decision-making, to include attitudes, opinions, beliefs, values, and understanding."

In the context of the NCOE, the information domain is wherever information exists, both on the network and outside it. The physical domain is the material environment wherein the NCOE operates. The social domain consists of the NCOE's many users—and likewise everyone else (besides the enemy) who can, for official purposes, interact with those users. The cognitive domain consists of the minds of the NCOE's users, especially that of the JTF Commander.

4.1.1.1 KM ensures coherent Knowledge Sharing

Knowledge sharing is the central purpose of KM (and likewise the NCOE). The outcome of effective knowledge sharing throughout the Joint Force is *pervasive knowledge*—that is, the realization of a common knowledge base with which decisions are made and actions taken. Knowledge sharing is vital because even actionable knowledge cannot be used if the format or medium used to share it is inadequate. Consider a seasoned warfighter whose intuition tells him that an enemy attack is imminent. To warn his superiors, he may send them a memorandum. However, that memo by itself cannot influence anyone until they become acquainted with it—in spite of their in-boxes full of other memos. If and when they do read it, they might not believe it in time if its content is not convincing enough, stating as its "evidence" of an imminent attack only the writer's personal feeling. Yet, that warfighter's intuition might be accurate.

Just as KM is more than IM alone, knowledge sharing includes but is also more than information sharing or management, since information sharing can include circulating a memo that nobody reads. Although individuals interpret and process knowledge differently, they share knowledge using a finite number of techniques, such as through agreed formats and by training to specific methods and standards. For instance, standardized taxonomies and interrelated ontologies are used within a semantic web, or a Service-Oriented Architecture (SOA), to enable a more efficient and effective sharing of knowledge amongst COIs. Within this NCOE JIC document, knowledge sharing is defined as:

> The ability of networked users to manage and make available relevant, accurate information, transform it into knowledge, and act upon it with confidence. This provides access to newly discovered or recurring information in a useable format and facilitates collaboration, distributed decision-making, adaptive organizations, and a greater unity of effort via synchronization and integration of force elements to the lowest levels.

Actionable knowledge is typically a combination of both *tacit* and *explicit* knowledge. An example of *tacit knowledge* is a warfighter's intuitive sense of a coming enemy attack. Since his intuition points to a specific implication, he might be able to express that implication very clearly, as in "I feel that an enemy attack is imminent and therefore we need to prepare." Yet, to articulate why, exactly, he knows what he knows might be remarkably difficult: "It's just a feeling I have," he might say. But his tacit knowledge is not an irrational mood: it is a cognitive combination of his experiences, "rules of thumb," and some deductions in his mind. It may enter his consciousness as a feeling, but

his tacit knowledge is based upon an inner logic that is probably quite reasonable and therefore collectively valuable. It should be shared.

What is called *explicit knowledge* can be more easily expressed and taught, typically as procedural steps specified in print. Yet, even some skills derived from training can include tacit knowledge. Consider how a firearms expert shoots (using tacit knowledge) as compared to a novice following an instruction manual (using explicit knowledge). The expert shooter, when aiming his weapon, tries to sense how different influences—the wind, the terrain, his stamina, the nuances of his weapon, the nature of his target—can be combined by some very subtle adjustments on his part to achieve a precise hit. He "feels" these factors more than he actively thinks about them. By contrast, the novice actively thinks the steps that the instruction manual specifies (i.e., "Okay, now that I'm in a good firing position, next I must control my breathing"). He performs what the manual specifies because he lacks any additional knowledge. Only with experience, preferably under a mentor, will the novice learn some personal techniques and intuitive ways that books cannot teach. Gradually his mind will assimilate the explicit knowledge he has received and combine it with his experiences, thereby creating tacit knowledge.

Knowledge sharing with KM tools seeks to make tacit knowledge explicit, such as through dialogue. Whether between a mentor and an apprentice, between equal colleagues, or between a superior and subordinates, these individuals can communicate their tacit knowledge by using discussions, metaphors, and analogies. By communicating face-to-face—even if their "faces" are seen via a video-link—they can share thoughts, exchange ideas, and learn to better explain their tacit knowledge by adjusting to the constant interpersonal feedback they receive. In KM terms, they leverage the social domain.

Interpersonal communication for official purposes is called c*ollaboration*. It is defined as "joint problem-solving for the purpose of achieving shared understanding, making a decision, or creating a product across the Joint Force and mission partners." It can be either formal or informal. Collaboration both shares and constructs knowledge, including actionable knowledge, by tapping into and combining various information sources and human perspectives.

A variety of KM technologies exist to facilitate collaboration, including video-conferencing, shared whiteboards, audio-conferencing (similar to telephone conference calls), chat rooms, shared documents, and email. Collaboration can occur simultaneously (called *synchronous)* or at different times *(asynchronous)*. Whereas video-conferencing can produce synchronous collaboration, email is a popular tool for asynchronous. No single collaborative tool is ideal for every situation; indeed, synchronous and asynchronous tools can be complementary. The NCOE will provide several such tools, perhaps including some whose enabling technology is, today, not yet mature.

To further facilitate knowledge sharing, KM tools accommodate each user's cognitive learning preferences. Thus, once an authorized user enters a network portal, typically via a desktop or laptop computer, he gains user-friendly access to whatever information he needs, when he needs it, in formats he can understand. Using a process called *individual information management* (I-IM), he can also tailor the audio-visual presentation, the formats, and some aspects of the content, all to better fit his personal preferences and professional needs, allowing him to cognitively grasp the needed information quickly, usually instantaneously. The NCOE will also provide real-time or near real-time map displays and other graphic representations, updated continuously, such as the Common Relevant Operating Picture (CROP) and the User Defined Operating Picture (UDOP). I-IM will enable users to develop their own individualized UDOP. Available, too, will be "information brokers" (online human assistants), "intelligent agents" (specialized search engines) and other I-IM tools. I-IM marks a greater emphasis upon the individual function, supporting knowledge sharing through automated agents that effectively provide and "pull" information (i.e., subscribing to information through automated agents that then populate the individual's UDOP).

To transition to a knowledge sharing environment, various internal and external barriers must be surmounted, including organizational and policy-based ones. Although KM tools can help overcome these barriers by facilitating the organization, elicitation, and discovery of knowledge, the needed cultural change will also necessitate effective training and education. Moreover, to facilitate the inclusion of mission partners, commanders must ensure that the relevant portions of KM plans are coordinated with those partners. Thereafter, subordinate knowledge managers/analysts must monitor the collection of the information and knowledge, synthesize those, and interpret and act upon the actionable knowledge as appropriate.

4.1.1.2 KM provides structure for Communities of Interest (COIs)

One collaborative method is called a *community of interest*, or COI, which consists of a group of people who interact for a common purpose and/or interests, typically because of interdependent tasks. KM tools enable a group of subject-matter experts (SMEs) and others—such as Joint/Multinational Force personnel, academics, interagency officials, representatives from NGOs and industry—to establish a virtual collaborative environment wherein, having a common purpose, they can leverage the right experience, expertise, and information to advise decision-makers and receive the decisions made. A COI is thus a means to advise, discuss, disseminate, and share knowledge.

Notionally there are two types of NCOE COIs: *institutional* and *expedient*. An institutional COI exists to address an enduring, established organizational responsibility, such as developing the procedures to analyze a specific intelligence problem-set, such as for Indications and Warning (I&W). Normally,

an institutional COI is established by and for its most important participant (process-owner), in this example the Joint Staff/Director of Intelligence (JS/J2). COIs can include whoever can usefully contribute, including one-time participants.

An expedient COI has a shorter life-cycle, created to help address the needs of a relatively temporary situation, such as the planning and execution of a military operation. As with an institutional COI, an expedient COI would probably be established by a process-owner with a task to resolve or complete. COIs will be encouraged to register themselves in a COI Registry to facilitate their visibility and collaboration. That registry will provide basic information about each COI, such as that COI's mission or objective, a list of its sponsors and members, and also links to COI-related products available via the NCOE. NCOE users will be encouraged to establish their public profiles as part of the I-IM process so that COIs can discover individuals according to their skills and experiences, and invite particular individuals to join the COI. Both the COI Registry and the public profiles are examples of enterprise capabilities available to help facilitate collaboration and to provide discoverable information for KM tools. Individuals who are not U.S. Government-affiliated (i.e., private business personnel, academicians, NGO representatives, foreign government officials, etc.) may participate through official sponsorship or as authorized individuals. However, that being said, uncertainties still exist as to when and how expedient COIs should be established and later dissolved.

Regardless of whether a COI is institutional or expedient, its processes, deliberations, and the decisions made as a result must be retained and archived to enhance the information-/knowledge-base. The COIs and their sponsoring organizations (i.e., domains, core missions) should establish the processes and capabilities needed to capture, manage, and share the COI products (i.e., COI services, reports, data schemas, recorded COI collaboration actions/decisions) in the sponsoring organization's information-/knowledge-base.

4.1.1.3 KM provides for distributed Decision-Making

Decision-making in a knowledge sharing environment will be heavily influenced by dynamic, self-defining patterns of collaboration. However, for exclusively military missions, collaboration is not—and must not be construed as—a form of decision-making that lacks individual accountability. Collaboration can inform a decision-maker but it does not make the decision. Leaders retain their decision-making responsibility.

Nevertheless, collaboration can facilitate better planning and execution—by enabling diverse mission partners to share mission objectives in ways which help synchronize the operation and task-organize it for optimal efficiency. By linking via the NCOE, partners can include groups and organizations that may

never have worked together before. Knowledge sharing 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.

Every authorized user, without necessarily being an expert in whatever mission he faces, can nevertheless act with the knowledge of a subject-matter expert or of several SMEs. This is because the NCOE will provide every authorized user with assured, robust access:

- to SMEs, via video-conferencing, email, and other means;
- to high-quality analyses and recommendations, in posted form; and
- to other relevant information, such as from synthesized databases and the mission-oriented "chat rooms" of colleagues.

Participation in the collaborative process is an important right and responsibility, necessitating training, experience, and the confidence to interact effectively. SMEs must also be made available to participate outside of formal organizational relationships. All Joint Force elements must be prepared to exploit the information and actionable knowledge made available. They must also post knowledge gained from previous experiences, their own and of others, as well as up-to-date information.

4.1.2 Network Management (NM)

Network management, or NM, focuses on the people, technology, processes, policy and capabilities necessary to effectively operate the systems and networks, including their configuration, availability, performance, manageability, and enterprise connectivity. Network management in the context of this NCOE JIC focuses upon the application of GIG enterprise management at the JTF-level and below. Network managers will oversee the establishment and implementation of Service-Level Agreements (SLAs) and ensure that such agreements support KM and IA needs.

Network managers will oversee and integrate the operation of the information transport, services, applications, computing infrastructure, spectrum, content staging, and other capabilities as necessary to ensure the proper functioning of the network at their respective levels of responsibility. Common tools, in the form of services, will be used by network managers at all levels to synchronize their actions. Smart tools, in the form of applications and services, will be used to speed and automate NM functions. Managers will put permissions in place to rapidly establish and dissolve networks in response to dynamic conditions. Well-articulated metadata descriptions and directories will be used for user-friendly advertisement, identification, and retrieval by authorized users.

Network management tools will be used to interface data-links of legacy systems with packet-switched Local Area Networks (LANs) and high-capacity Wide Area Networks (WANs) through network gateways. Radio frequency (RF) or wireless systems will probably interface directly with terrestrial optical fiber networks as part of much larger networks. At optical gateways, RF data-links or voice will converge with other terrestrial voice, data, and imagery traffic. Processed information from tactical data-link and voice systems could be converged on a multi-purpose, long-endurance relay aircraft and/or shared among spacecraft, airborne, maritime, and ground stations.

Since voice, data, and imagery sources will often converge over a single circuit, NM capabilities that prioritize network traffic in the theater will be essential. NM will thus require detailed planning and control—determining, *a priori*, how the operational traffic is to be prioritized and given precedence under what dynamic criteria. "Ruthless preemption"—as used in circuit-switched tele-communication—may not be available. A software-driven policy rule-set will be used to determine which traffic of what type gets access to which ports under what conditions.

NM must also provide visibility while anticipating and mitigating the effects of network degradation, outages, and attacks. If and when such problems arise, the global NM community must quickly and collaboratively determine how the information flow can be optimized and who must take action accordingly. To assess and respond rapidly, the NM personnel will employ shared situational awareness, along with the right technologies, procedures, and collaborative organizational structures.

4.1.3 Information Assurance (IA)

In Joint Net-Centric Operations, network information must be protected from attack and against unauthorized access, and yet remain continuously accessible by authorized users. *Information assurance*, or IA, will provide the Joint Force with assured mission management, assured information sharing, confidentiality, and integrity/non-repudiation capabilities in support of

enterprise network information and services during the conduct of joint actions.[8] As a critical component of the NCOE, IA will protect information from the time of its generation at network nodes, through its storage, processing, cataloging, and until its distribution (via posting, smart push, pull strategies, etc.) to individuals and groups (that is, to COIs and decision-makers). Non-repudiation will provide a timely, highly accurate ability to verify the identity of both the sender and the receiver of the information and also that information's authenticity.

Today, and likely in the future, information providers, processors, and consumers are targets for spoofing, masquerading, disclosure, data modification (integrity), system behavior modification (system integrity), and/or denial-of-service attacks. Similarly, information transactions between each of those nodes may be targeted for eavesdropping, service denial, modification of data in-transit, mis-routing of information, and traffic analysis-types of attacks. The NCOE must defend against all of these. Moreover, since new threats are emerging even as the old ones continue to evolve, the NCOE's IA strategy must be proactive in striving to understand how the NCOE's various facets, including its newest and emerging capabilities, could be exposed to disruption or manipulation.

Six (6) broad categories of IA capabilities are required for the NCOE:

- **Assured Information Sharing**—providing the JTF with the means to positively identify and authenticate entities on the network, share information between authorized entities, as well as form and manage dynamic COIs to support collaboration.

- **Highly Available Enterprise**—ensuring that computing and communication resources, net-centric services, and information are available to support the JTF. This capability provides an appropriate level of protection in the presence of attacks, degradation in bandwidth quality/quantity, and service availability, while maintaining key performance parameters.

- **Confidentiality**—enables the ability to validate and assure that network systems or information is provided to the correct party and not disclosed to unauthorized sources. Confidentiality also ensures that only trusted parties participate in the communication exchange.

- **Defend the GIG**—requiring the tools, processes, and means to detect unauthorized activity that may affect information sharing and collaboration. It also provides a means to maintain GIG services and

[8] DoD Directive 8000.1, "Management of DoD Information Resources and Information Technology," 27 February 2002.

access to information while the NCOE is under attack, and to prevent future attacks

- **Integrity and Non-Repudiation**—enabling technical capabilities that provide for storing, sharing, exchanging, and processing information with the assurance that it is correct and valid. This directly enables the JTF's abilities to share situational awareness and to understand information with confidence, knowing that what is communicated is what is intended. It also provides users with abilities to conduct collaborative decision-making and planning and to operate interdependently, confident that communication exchanges can be verified.

- **Assured Mission Management**—the ability to coordinate and de-conflict system configuration and resource changes, mission priority changes, and cyber-attack responses. It includes the ability to assign, prioritize, modify and revoke user-roles and system-roles, access rights, COI membership, and resources in a coordinated fashion using privileges, cryptographic keys, and IA configurations. Additionally, it ensures that attack responses do not adversely affect mission priorities. It must be automated, timely, and capable of reacting to changing priorities while under normal, degraded, and disconnected conditions.

An essential role for IA is Computer Network Defense (CND), protecting against a Computer Network Attack (CNA) and an Information Operations (IO) assault, whether by an outside adversary or possibly an insider threat. For the NCOE, CND means fully robust detection, investigation and response capabilities. The NCOE's CND must have the ability to rapidly identify, process, and integrate varied, dynamic, and often unanticipated IA threats, launched from anywhere in cyberspace or even from multiple locations in an asymmetric fashion.

Local NCOE IA efforts cannot be executed in isolation: they must be coordinated with the global IA effort since vulnerabilities in one part of the network can potentially affect all the others. Situational awareness is achieved through the collection, analysis, and correlation of sensor information from all GIG nodes, combined automatically with other intelligence and sources. CND functions are fully integrated with management and control activities, providing a seamless capability for near real-time views of the GIG and the capability to perform necessary management functions, thereby enabling proactive and responsive adjustments. Automated decision-support tools are integrated, helping to develop solutions that meet the security metrics, yet with the least impact on operational missions.

In order to achieve pervasive knowledge, the Joint Force requires a role-based access capability. This capability would allow JTF members and mission partners access to information based upon mission needs rather than upon

static policy decisions. This requirement implies the need to shift from a risk avoidance framework to a risk management framework. To support this, IA personnel will require the tools and training to execute IA functions in support of KM needs.

Currently, the inherent complexity of role-based access is problematic at the policy level—and this has significant implications when considering the shift from a "need to know" to a "need to share" paradigm. The shift to the NCOE is expected to create opportunities to review, refine, and change policy to ensure that NCOE capabilities can be fully utilized by the warfighter. One part of this shift is towards an international IA framework that would allow the JTF Commander to share information by utilizing Cross Domain Solutions (CDS). This would provide the ability to transfer data between differing security domains, thus enabling the secure sharing of information with allies, mission partners, and other organizations as necessary.

4.1.4 The Integration of KM, NM and IA

The NCOE's KM, NM and IA components will be integrated so thoroughly in conjunction with the DoD Data Strategy that, like an interwoven fabric, they will be interdependent. For example:

- The information that KM tools synthesize and display to users—which those users will convert into knowledge via their cognitive understanding and knowledge sharing—will be delivered by the technical means of NM, while IA protects that information's accuracy and completeness.

- NM will depend upon KM—and, by extension, upon the users utilizing KM tools—to help prioritize the content of the NCOE's information flow.

- KM will depend upon NM's processing capacity to help filter information flow.

- The continuous protection provided by IA will depend, for its ongoing maintenance, upon NM technologies and NM personnel.

- NM will depend upon IA to safeguard, as an essential minimum, the most basic of NM capabilities needed to restore network capacity after outages or attacks.

- KM will depend upon IA for operations security, including for role-based access and entry into COIs.

- KM will depend upon IM and NM to help balance mission objectives against the risks of participation in the NCOE, especially for foreign forces within the coalition, NGO partners, or potential SMEs for COIs.

4.1.5 The NCOE's Operational Context

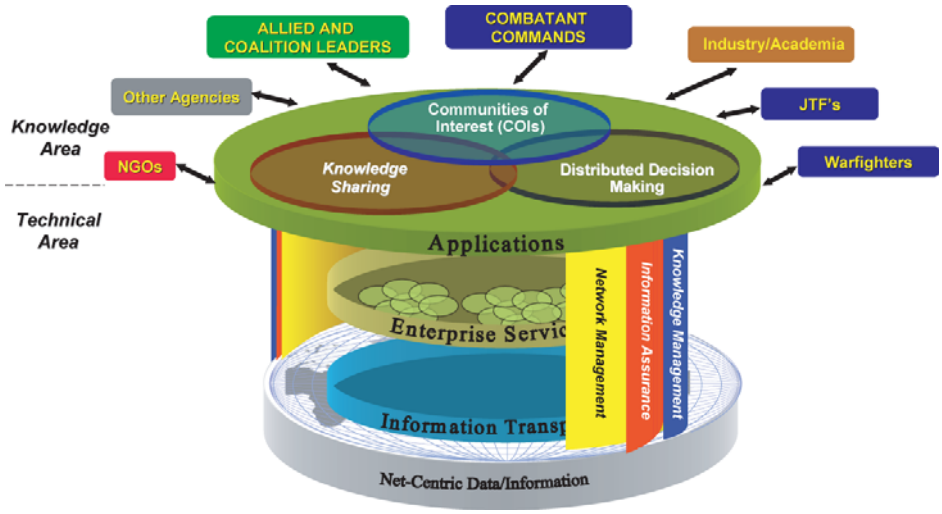


Figure 2. The NCOE's Operational Context

As depicted in figure 2, the NCOE's operational context is "built" upon a globally accessible platform of data and information. This access is provided through information transport mechanisms, which enable the processing of that data and information via enterprise services, interfaced to the users via the NCOE's applications. The functions of KM, NM and IA integrate the NCOE, providing the warfighter/user with a seamless capability to collect, create and use actionable knowledge in an operational context.

Applications from diverse COIs, Knowledge Sharing, and Decision-Making functions serve as the interface between the Knowledge Area capabilities and the enabling capabilities in the Technical Area. Integrated KM, IA, and NM provide assured user access to appropriate network resources in accordance with dynamic mission objectives.

4.2 Application of the Central Idea

NCOE users must have support throughout the full spectrum of the national, strategic, operational, and tactical environments, described in further detail below. NCOE capabilities must support a full spectrum of users, including deployed users operating in austere, hostile environments, often with minimal bandwidth and/or high latency. NCOE capabilities and mechanisms must also be able to operate under restrictive conditions, including in all phases of

deployment: mobilization, movement, employment, sustainment, and re-deployment. Deployed forces must contend with intermittent connectivity, be it intentional or unplanned. Their reconnection will require synchronization or re-synchronization with the core infrastructure.

The following eight examples demonstrate how new or improved warfighting capabilities can be achieved through the integration of KM, NM and IA within the NCOE. These examples are not exhaustive, showing only some of the many potential benefits that the NCOE will provide to the future Joint Force. Most of these examples can be easily extended to similar scenarios. For instance, the last example, transitioning to stability operations, can be easily applied to a humanitarian assistance/disaster relief scenario.

Each example contains italicized references to the specific tasks used within, showing how they help to fulfill the example. Accompanying figures 3-10 graphically show the tasks' interrelationships and, by extension, their interdependencies as KM (blue), NM (yellow), and IA (red) task-categories. Note that the tasks listed in these examples represent only the high order tasks. Additional development, modeling and simulation, experimentation, etc., can be employed to further develop these task threads. The eight examples are:

- Stand-up of a JTF-level COI;
- Establish a collaborative session with new multinational partners;
- Support dynamic targeting against time-sensitive targets (TSTs);
- User receives new task to produce actionable knowledge;
- Allocate additional resources to a unit on-the-move;
- Request by an NGO to access net-resources;
- Deploy network to forward location; and
- Reconfigure/Maintain network for transition to Stability Operations.

4.2.1 First Example: *Stand-up of a JTF-level COI*

Once a new Joint Task Force is established, JTF-level communities of interest will be needed quickly to ensure that the JTF Commander's operational requirements are pursued with superior decision-making. The participants will need to *obtain and maintain an understanding of command intent* and, through collaboration, *develop common understandings of* [the] *problems and goals* they have. With experience gained from using the NCOE, they will *establish trust in*

decision-making collaboration. In the case of broad COIs, they will be able to *share across security area*[s]: *coalitions, Homeland Security, etc. (cross domain information sharing).*

To stand-up a JTF-level COI, a list of prospective COI participants will be compiled by an intelligent tool-set that searches for and suggests participants based upon their backgrounds, the current situational awareness, and the mission. It will also help the COI leader to *know availability of knowledge assets.* Once the COI leader selects the members, the next task is to *establish a community vocabulary/lexicon* if one does not yet exist. That semantic foundation will help network mangers to *provide* [for a] *COI environment* and, for knowledge-sharing purposes, it will *support enterprise-wide, COI-specific applications.*

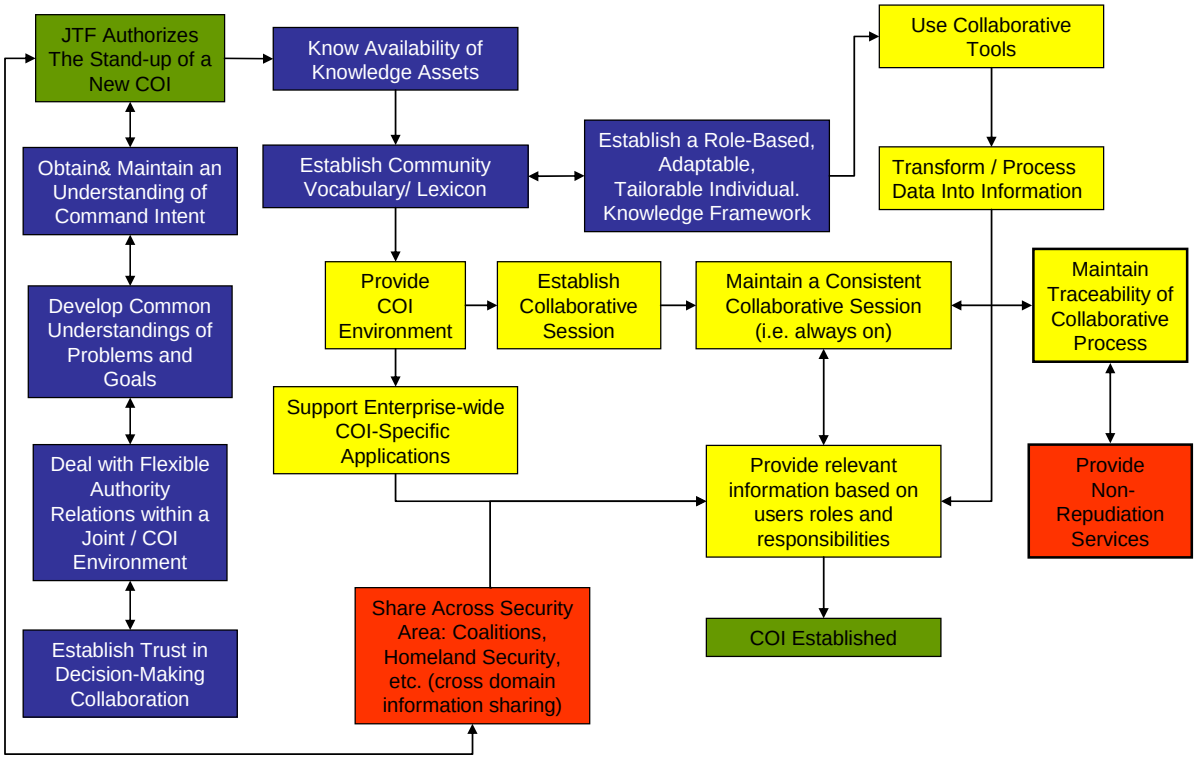


Figure 3. JTF-level COI Task Interdependencies

Each participant must, for KM purposes, *establish a role-based, adaptive, tailorable individual knowledge framework.* Every participant will then, within the COI, *use collaborative tools* to *transform/process data into information.*

For the overall group, NM will both *establish* [a] *collaborative session* and *maintain a consistent collaborative session (i.e., always on)*, the latter task aided by the requirement to *maintain traceability of* [the] *collaborative process.* Through the use of non-repudiation services, the COI members can quickly verify that other COI members have received the information distributed as

part of the collaborative session. The KM and NM operations, protected by IA, will ultimately combine to facilitate the participants' collaboration as they *provide relevant information based on users' roles and responsibilities.* Once this information is provided, the COI is considered established. If the operational requirements necessitate a change in the access level for one or more COI members, this can be done upon the JTF Commander's (or other COI leader's) approval.

4.2.2 Second Example: *Establish a collaborative session with new multinational partners*

As the probability of a military crisis increases, senior-level commanders will begin collaborating *with new multinational partners by way of an isolated Internet Protocol Video Teleconference (IP VTC) on a rigorously defended, shared separate network.* Through these sessions, the participants are able to *establish working relationships with potential partners,* which in this case depends upon their ability to *identify/establish appropriate relationships with JMMIs, NGOs, etc. (to build COIs).* Entry into the COI will be safeguarded by the NCOE's IA ability to *provide identity management.*

By having the ability to *know* [the] *availability of knowledge assets* and also the ability to *overcome organizational, cultural and language differences*, the mission partners are able to *establish* [a] *problem-solving framework*. Within that framework they can *adjust* [their] *procedures and/or organization as necessary, establish* [a] *schedule of recurring meetings*, and *set up expedient meetings based on the situation and events*.

The JTF's knowledge and network managers have primary responsibility for the session process from start to finish, although once the conference rule-sets are established the network can automatically duplicate others whenever required. Based on command guidance, the knowledge managers will determine the session parameters for the participants in terms of the assigned mission and the session's purpose. From a technical standpoint, it is the actual ability to *manage systems and networks* that links together the U.S. and multinational nodes—a network manager's responsibility. Based upon the session's priority, network rules will be adjusted to facilitate the most effective means of conducting the session, since the session is in competition with all other network traffic. A session-process checklist will include items such as: the attendees; their addresses; member and node attributes; security classification of the session; precedence and purpose; duration characteristics; permissions; and the creation and termination procedures. The network will also retain this information as part of an archived record of the VTC session.

The multinational mission partners will *establish* [a] *collaborative session* by using standardized international and common conference Internet Protocols (IP) for addresses. They will also have the ability to *determine/maintain an*

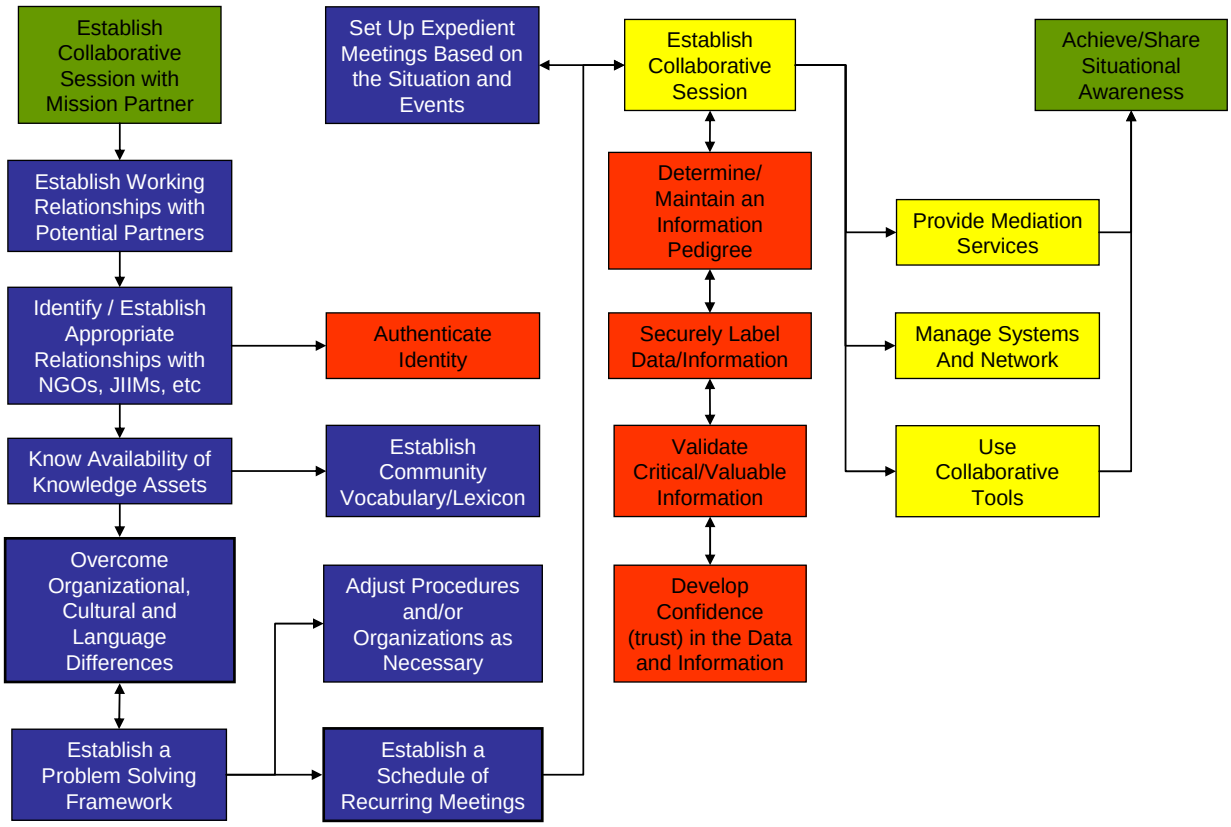


Figure 4. IP VTC Collaborative Session Task Interdependencies

information pedigree for archival and other purposes. IA capabilities will *securely label data/information consistent with IA guidelines*, as well as *validate critical/valuable information*, thus helping to *develop confidence (trust) in the data and information.*

In support of the session, the NCOE will *provide mediation services*; it will *manage systems and networks;* and it will enable the participants to *use collaborative tools* to *achieve/share situational awareness.*

4.2.3 Third Example: *Support dynamic targeting against time-sensitive targets (TSTs)*

Having identified a time-sensitive target, a reconnaissance team leader uses the NCOE's *ability to provide global information transport services*—via a secure data-link built into his multi-spectrum binoculars and laser range-finder. He identifies the enemy unit's range and bearing and, since he can *connect with all assets* on the net, he also auto-registers the target using a Global Positioning System (GPS) map displayed on his hand-held communications device. Once

he *transmit*[s the] *information*, the system automatically recognizes its importance (*control information flow and precedence)* and, to safeguard security, it *assure*[s the] *information* and *authenticate*[s the sender's] *identity*.

Depending on the mission, the system will *use collaborative tools* as either predominately man-to-machine or machine-to-machine. The system will *perform* [an] *intelligent search* using its *enable*[d] *smart push/pull of information*. The system has the ability to *manage data/ information into life-cycle and* [to] *optimize data/information handling*. It has the ability to *provide information publish/ subscribe services*. It will also *provide smart management and tasking of collection assets.*

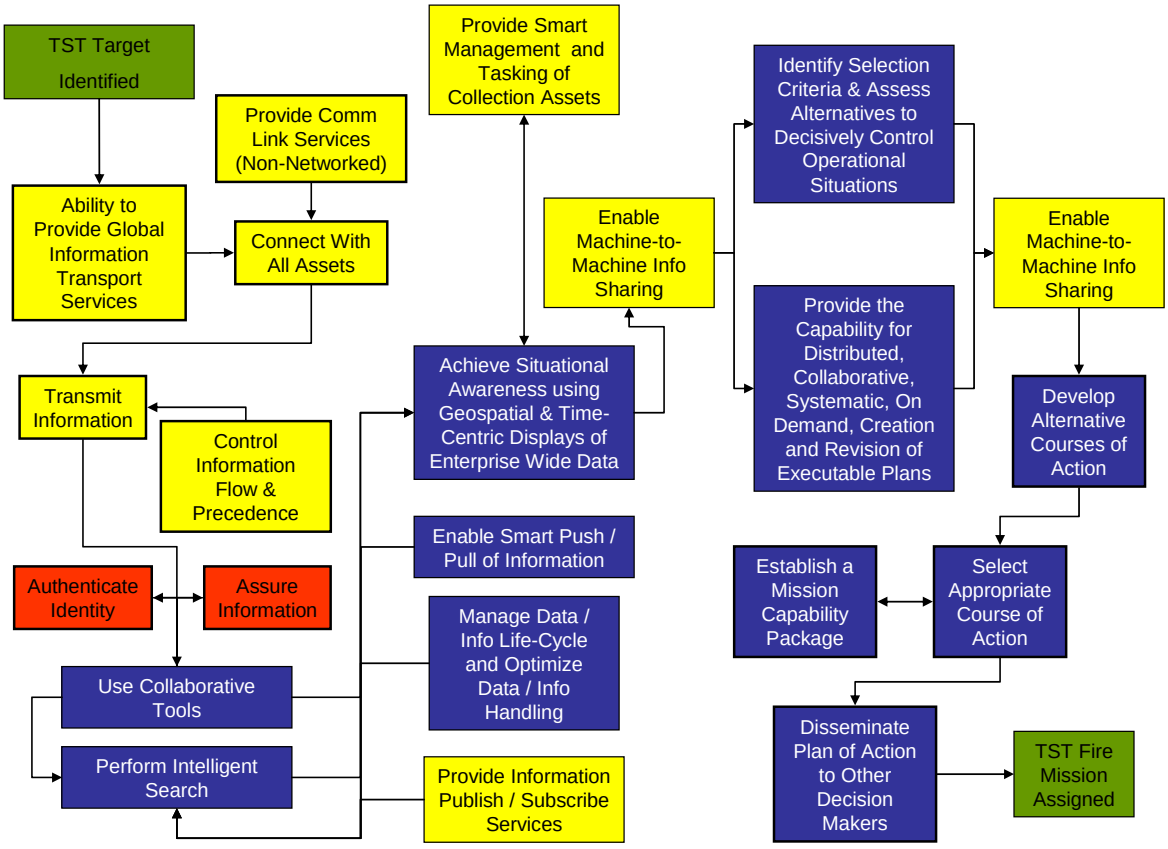


Figure 5. Support to TST Task Interdependencies

Among the transmission's recipients is an orbiting command-and-control aircraft. Viewing the processed information on a CROP, the aircrew will *achieve situational awareness using geospatial and time-centric displays of enterprise-wide data*. In this particular case, the new information's content and urgency are automatically "flagged" for priority. This "flag" also appears on the CROP display as an item of potentially high interest. Since the system *enable*[s] *machine-to-machine information sharing*, an intelligent search occurs automatically, scanning for which fire-support assets throughout the JTF are

capable of destroying the target within ten minutes. Applications are used to *identify selection criteria and assess alternatives to decisively control operational situations.* It can also *provide the capability for distributed, collaborative, systematic, on-demand creation and revision of executable plans.* The process occurs extremely quickly through *machine-to-machine information sharing.* Applications automatically *develop alternative courses of action.*

The collaborative ability to *select* [an] *appropriate course of action* is achieved when the C2 aircraft's controller acknowledges, validates and approves the targeting request, which is then automatically passed to the Fire Support Coordination Element (FSCE). To *establish a mission capability package,* automated tools immediately prioritize the pending mission requests and assign fire or strike missions accordingly. Other networked tools in the FSCE include: airspace de-confliction for transiting aircraft, artillery, and missiles; the range and bearing of the assigned target; and a firing window to avoid any fratricide of nearby friendly forces. These tools accompany the already fulfilled requirement to *disseminate* [the] *plan of action to other decision-makers.* It includes returning information to the requestor to confirm mission acceptance and to provide a Time on Target (TOT) for the fire mission.

4.2.4 Fourth Example: *User receives new task to produce actionable knowledge*

NCOE system capabilities will provide the ability to *flexibly adapt to changing operational needs.* For example, to support a new tasking to produce actionable intelligence based upon the events of the previous 24 hours, a briefer can *change information search and retrieval patterns* to query the information sources (i.e., COI data services, metadata catalogs, COI collaborative shared spaces, COI Directory) in the NCOE for available data assets (i.e., reports, video and audio recordings) using a tool that provides *context-relevant search & retrieval services* based upon the briefer's specific request.

That search will *capture timely, relevant, interoperable source data from sensors and other input areas.* Meanwhile, IA functions, consistent with the GIG Data Strategy, will *maintain an information pedigree* of that data. As the data is retrieved, the system will automatically *transform/process* [that] *data into information* which, in turn, will *become validated critical/valuable information* that is delivered into folders the briefer has created to support the relevant tasks. The data will also have a header that *determines an information pedigree*, i.e., how old the data is, who interpreted or analyzed it, who may have updated or changed the data based upon other analyses, and how it compares to other data within the same area.

The system will *provide information publish/subscribe services*; it will *enable smart push/pull of* [the needed] *information*; it will *provide mediation services*; and it will *provide discovery services.* Throughout this process, protection against enemy CNA is continually performed by IA functions designed to *deter, detect,* [and] *deny unauthorized intrusions* into the network.

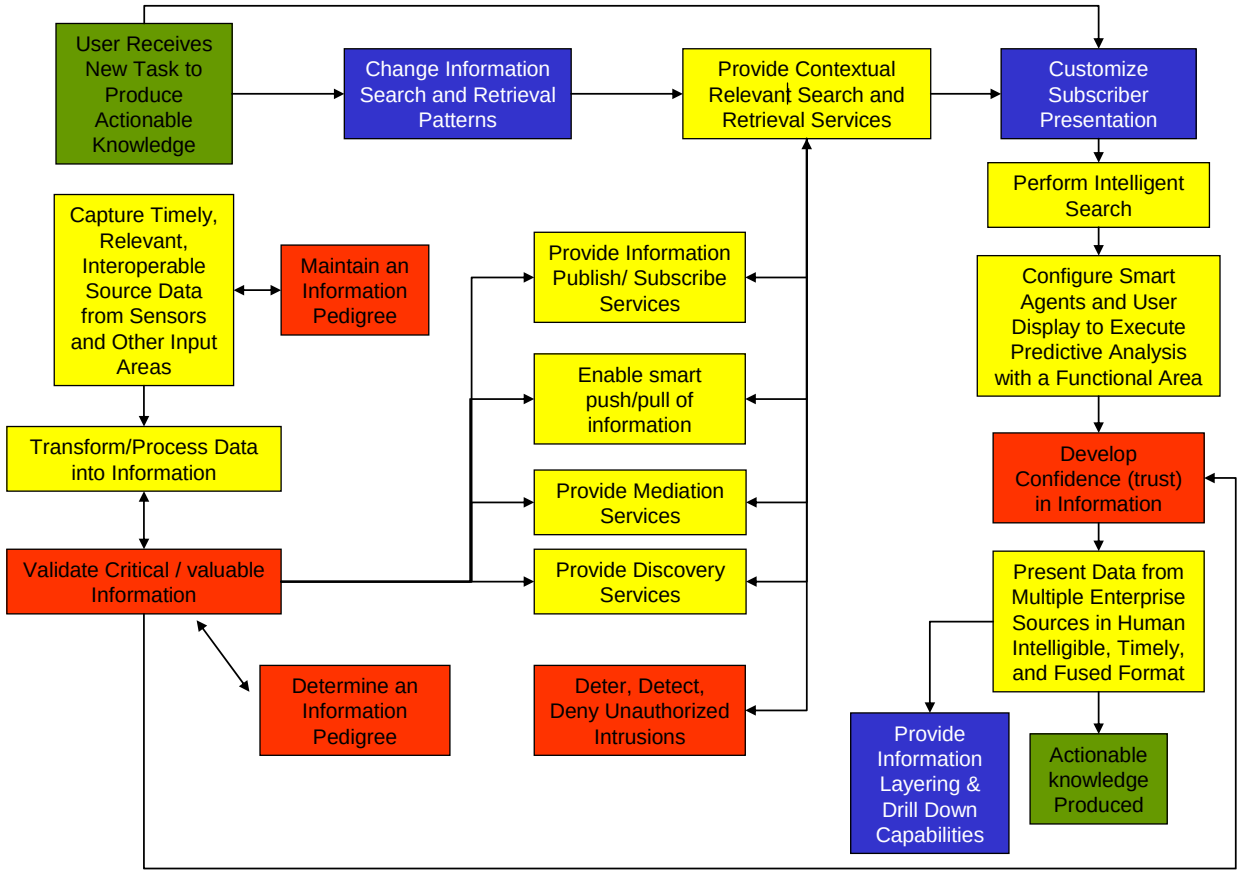


Figure 6. I-IM Task Interdependencies

With the automatic arrangement of the information into a visual briefing format, this ability to *customize* [the] *subscriber presentation*—thereby providing a UDOP function—is further enhanced by abilities to *perform intelligent search* and to *configure smart agents and user display to execute predictive analysis within a functional area.* The latter helps the user to *develop confidence in information* received.

For the finalized presentation, the user has the ability to *present data from multiple enterprise sources in* [a] *human intelligible, timely and fused format.* The NCOE will also *provide information layering and drill down capabilities*, allowing a briefer to present the same basic briefing to different audiences and levels of decision-makers, with instant modification as desired. Finally, the

brief will be "posted" and thereby be capable of being shared with, and used by, any unanticipated (but authorized) user, resulting in actionable knowledge.

4.2.5 Fifth Example: *Allocate additional resources to a unit on-the-move*

As JTF units move forward, each unit possesses a wireless capability that can *operate without geographic constraints*. This capability for communications-on-the-move means that, no matter where the unit moves to, the NCOE will automatically and continuously *manage systems and networks* to ensure optimal performance. Included is the ability to *rapidly deploy/employ robust connectivity forward*, the ability to *maintain network capabilities and ensure survivability*, the ability to *ensure spectrum availability*, and the ability to *establish controllable communication relays*—all of which contribute to *maintaining information and knowledge connectivity in* [a] *limited bandwidth environment*.

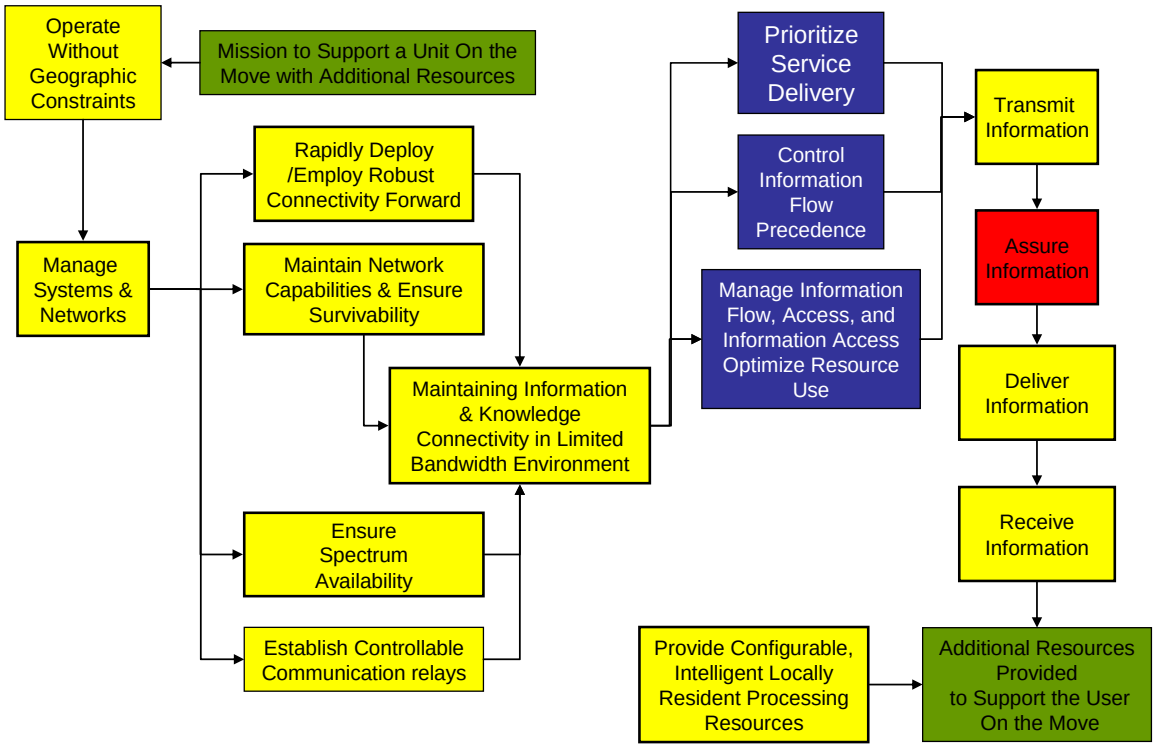


Figure 7. Task Interdependencies for Additional Resources for Comms-on-the-Move

In some mountainous or heavily urbanized areas, the unit's level of connectivity may deteriorate unavoidably and become sporadic. However, the system will utilize advanced wireless technologies that continually seek to re-establish and reroute its communications links back to the primary server. In support, the NCOE will *provide configurable, intelligent locally resident processing resources*. Once re-connected, other capabilities will ensure that

the latest and most critical information is received and processed first, using preemptive and precedence technology. For example, critical information on the movement of hostile chemical weapons into the battle area would take precedence over logistical re-supply information, which would take precedence over minor personnel and manning issues. The relevant tasks include the ability to *prioritize service delivery*, to *control information flow precedence*, and to *manage information flow, access, and…resource use*.

The final tasks in the process include abilities to transmit, deliver, and receive information, protected by IA capabilities. The net result of this series of tasks is that additional resources are provided to the user on the move.

4.2.6 Sixth Example: *Request by an NGO to access net-resources*

A civilian-run humanitarian relief organization reports a potential disease outbreak near the forward edge of the battlespace to the JTF. Having recognized the need to *identify/establish appropriate relationships with NGOs, JIIMs, etc.*, that relief effort is facilitated by the NCOE and interfaces with the JTF. Using that connection, some members of the relief-oriented COI want to subscribe to the military network to get data regarding Red Forces in the region. The JTF Commander agrees that at least some current Red Force information can be released accordingly.

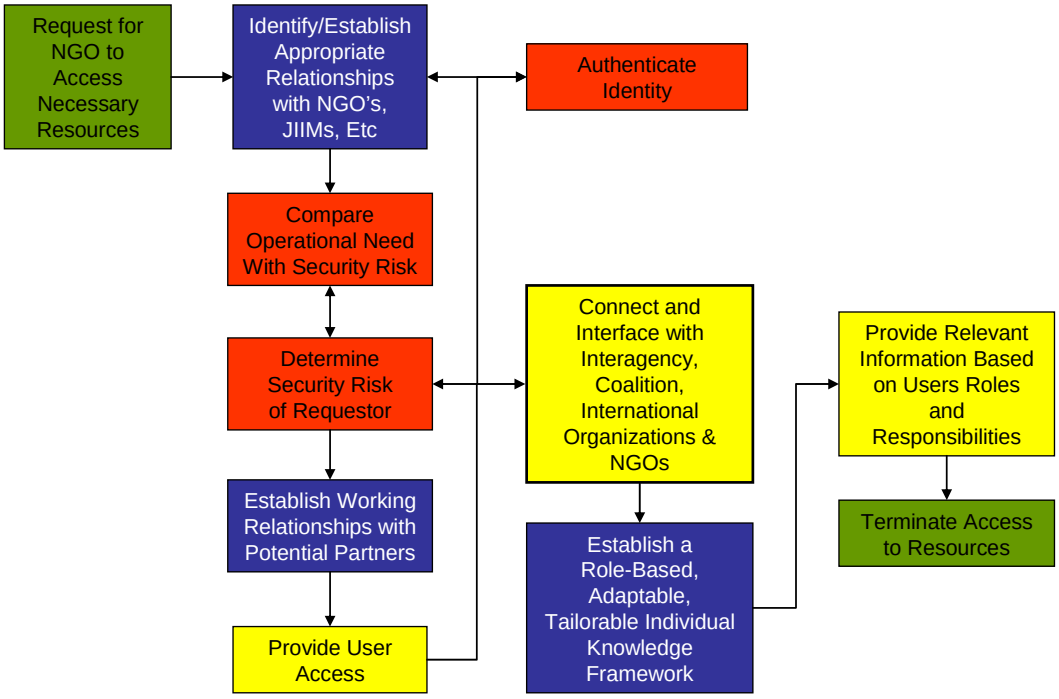


Figure 8. Task Interdependencies to support an NGO

Whenever the COI requests access to the latest Red Force information, the JTF system *authenticate*[s the] *identity* of the requestor. Depending upon the information's sensitivity and the security clearance-level of the requestor, either a man-to-machine or a machine-to-machine interface first *compare*[s the] *operational need with* [the] *security risk* involved and then *determine*[s the] *security risk of* [the] *requestor.* Such steps become increasingly important as the JTF *establish*[es and deepens its] *working relationships with potential partners*.

The collaborative preference is to *provide user access* and thus *connect and interface with interagency, coalition, international organizations and NGOs.* Yet, this preference will necessitate various KM, NM and IA requirements, such as the KM requirement to *establish a role-based, adaptable, tailorable, individual knowledge framework* to receive and present the Red Force information in ways which make sense to the civilian users. Different users may request—and either may or may not need—different levels and degrees of detail; therefore, NM and IA personnel must find ways to provide the relevant information based on the users' roles and responsibilities

Once Red Force units in the area are neutralized, IA tools prompt the knowledge and network managers to consider that the JTF *terminate* [NGO] *access to resources.*

4.2.7 Seventh Example: *Deploy network to forward location*

As JTF units advance quickly in response to the enemy's collapse, they must *flexibly adapt to changes in operational needs* and *modify/revise* [their] *procedures* as the situation evolves. For that, the NCOE *provide*[s for] *collaborative mission planning and rehearsal*.

Since the JTF units have the ability to *operate without geographic constraints*, they can *rapidly deploy/employ robust connectivity forward*.

The enemy's collapse leaves the civil functions chaotic. A new network must be established, one able to connect and interface with various mission partners including civilian agencies and NGOs. The JTF's NM personnel begin by *executing a network configuration plan* whose precepts guide them as they *manage systems and networks*.

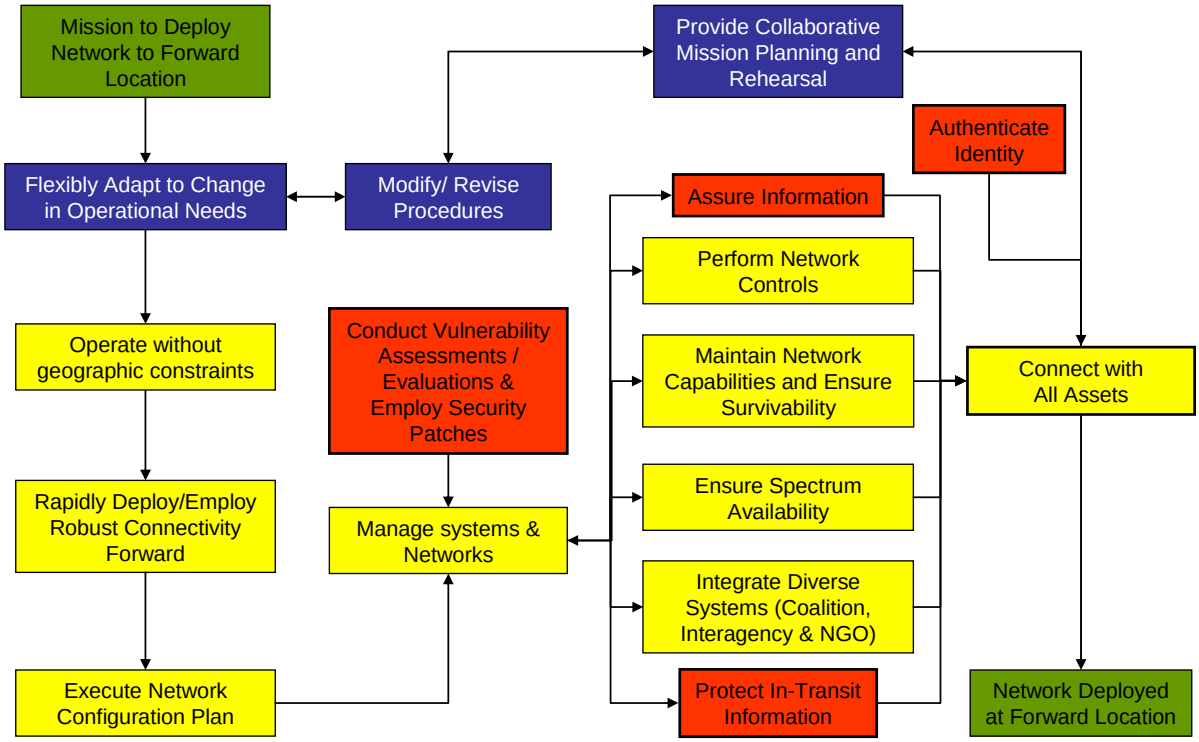


Figure 9. Task Interdependencies for Deploying and Establishing a Network in a forward area

They have the ability to *perform network controls*, such as fault, configuration, accounting, performance and security (FCAPS) management. They can *maintain network capabilities and ensure survivability*, and they can *ensure spectrum availability*, despite the increased demand, as they *integrate diverse systems (coalition, interagency, and NGO).* They can *connect with all assets* they require and can successfully deploy the network in the forward area.

4.2.8 Eighth Example: *Reconfigure/Maintain network for transition to Stability Operations*

Even during ongoing major combat operations, some areas of the battlespace transition to stability operations, a transition which necessitates changes to the local network configuration. To *flexibly adapt to changing operational needs*—informed by their *common understanding of problems and goals*—the participants must collaboratively *establish* [a] *problem-solving framework* and also *establish* [a] *community vocabulary/lexicon.*

For the network to adapt effectively, network managers must *identify* [the] *mission criticality of friendly systems and nodes* as those personnel, and others, *adjust* [their] *procedures and/or organization as necessary* to suit the new situation. IA personnel must *conduct vulnerability assessments,* as well as *maintain network capabilities and ensure survivability.* Meanwhile, KM

personnel must *define and implement a knowledge dissemination strategy* to *support all operations and transitional states along the ROMO* [Range Of Military Operations]. Accordingly, they may need to *modify/revise procedures and schedules*.

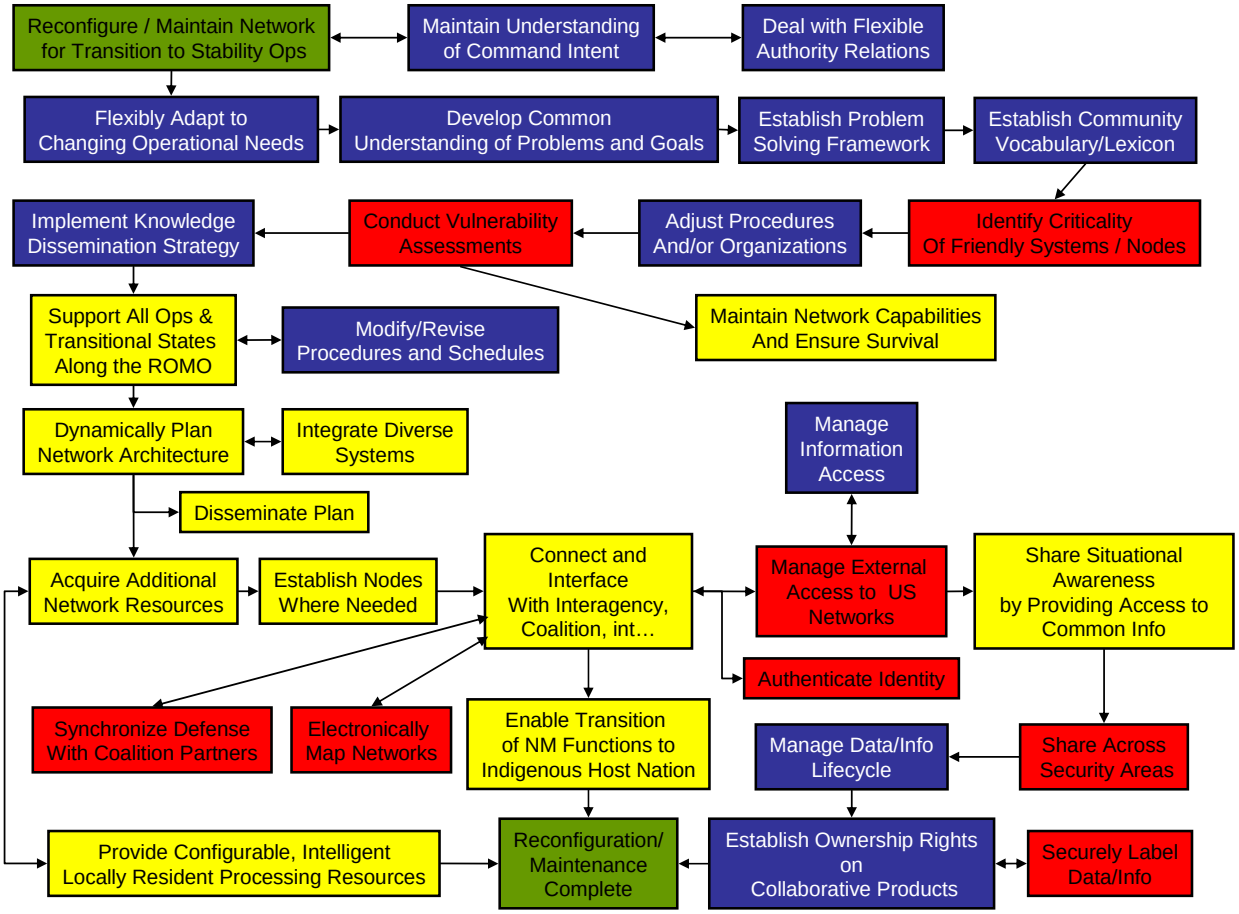


Figure 10. Task Interdependencies for Transitioning the Network for Stability Operations

To dynamically plan the network architecture, the participants and their support personnel need to *integrate diverse systems,* disseminate the plan, *acquire additional network resources on demand*, and *establish nodes where needed.* The aim is to *connect and interface with interagency, coalition, international organizations, commercial and NGOs*—a task which could require that they synchronize the network's defense with coalition partners, as well as *electronically map* [their added] *networks in which DoD information traverses*.

As new participants and organizations enter the network, they and the network will need to *provide identity management* and even *manage external access to U.S. networks* to safeguard legitimate entry and use of the network. Their participation will help *share situational awareness by providing access to*

common information, information which is *share*[d] *across security areas*, along with the requirement to *manage* [the] *data/information life-cycle*. As they collaborate, they will *establish ownership rights on collaborative products* and *securely label data/information.* Those products, combined with *locally resident processing resources* and the *transition of NM capabilities to host nation control,* provide the final steps for reconfiguration/maintenance of the network for follow-on use.

4.3 Benefits for the Warfighter

The preceding examples demonstrate the power of fully integrated KM, NM and IA. The pervasive knowledge generated by using the NCOE will thus produce many warfighting advantages. Some of those are:

- ***Efficiency***—increased in terms of time, economy of force, and cognitive learning. Time efficiency is increased because ubiquitous network connectivity and good IM will reduce or eliminate the need to manually convert data and information. Also, automated machine-to-machine information sharing, and data translation through data services, will allow humans to concentrate on less mundane tasks. To optimize economy of force, every JTF element can call upon the capabilities of other JTF elements as appropriate. For quicker cognitive learning, KM and I-IM tools will enable each user to receive and focus on whatever information is needed, in a format tailored to best fit his/her professional and personal preferences.

- ***Cross Functional Synergy***—achieved by networking and synthesizing the Joint Force's data, including the traditionally separate staff functions of personnel (1), intelligence (2), operations (3), logistics (4), and military-civil/international affairs (5). These cross-connections can be leveraged to reveal new insights. For example, in preparing for an aerial strike mission, the NCOE will anticipate and retrieve essential planning information from known and trusted sources, augmented by event-driven alternate inputs. It will also provide warnings of in-process threats to the operation, followed by near real-time bomb damage assessments.

- ***Joint Cohesion***—enhanced by promoting technical connectivity and IM, while KM and NM tools will spread and improve ever-developing knowledge of how best to conduct cohesive Joint Net-Centric Operations. The NCOE will link every Joint Force element to help find, disseminate, and implement "lessons learned" throughout the Force, continuously. It will also leverage various Joint Force capabilities heretofore latent. Called *constructive interdependence,* this depends upon a high degree of mutual trust as the Force's diverse members make unique contributions toward common objectives and rely upon each other for various essential

capabilities instead of duplicating those capabilities organically (i.e., economy of force). The NCOE will achieve this by employing intelligent agents to search inventory databases and match requirements to individual unit capabilities. The NCOE will thus facilitate an almost limitless combination of Service and component capabilities in ways not previously achievable.

- ***Collaboration with Mission Partners***. Constructive interdependence is not limited to the Joint Force alone. The NCOE-enabled integration of mission partners via their networks will enable the JTF to share mission objectives, synchronize the operation, task-organize it for optimal efficiency, and enhance its effectiveness.

- ***Decision Superiority***—facilitated by providing every decision-maker with access to a wealth of relevant information and knowledge, including the very latest ISR reports, the current operational picture, and the insights and advice of SMEs and/or COIs. Advanced visualization techniques will show unprecedented quantities of information, individually tailored to specific needs. Although the proverbial "fog and friction" of war can never be eliminated entirely, KM and I-IM tools will reduce its uncertainties and risks by promoting a higher level of situational awareness, further enhanced by applied analytical confidence factors, embedded modeling and simulation algorithms, and expanded knowledge sharing opportunities. Confidence weightings will be determined by a group of automated smart tools and programs designed to correlate data from various sources into a coherent information object.

- ***Rapid Adaptability at the Tactical, Operational and Strategic levels***—facilitated by the NCOE's comprehensive reach throughout the Joint Force and mission partners, enabling the near instantaneous dissemination of information, knowledge, and command guidance. Commanders at multiple levels can "drill down" to see any aspect of the tactical or operational picture they desire. Vital "lessons learned" will be acquired rapidly, improving the JTF knowledge-base and ensuring that the Force becomes better prepared to address recurring situations. If any Force elements require additional training or re-training to more effectively counter an adversary's asymmetric ways, various instructional aids will accelerate that needed training, such as audio-visual briefings, virtual reality simulators, and interactive software programs. Such training will be especially valuable for personnel who must perform unexpected missions, such as artillery personnel compelled to perform counter-insurgency and military police missions.

In sum, by fully integrating KM, NM and IA to achieve decisive levels of pervasive knowledge and technical connectivity, the NCOE is optimizing and

even transforming how data, information, and knowledge are generated, presented, and used throughout the Joint Force. This integration brings coherency to the Force's knowledge and technical capabilities, leveraging power heretofore latent. The NCOE also provides an enhanced framework for tying-in mission partners, including non-governmental organizations and private businesses, enabling their access to the mission-oriented information and knowledge they need when they need it—while prudently limiting their access otherwise, and denying access to adversaries. The NCOE, by leveraging non-material advantages such as human knowledge as much as technical network advances, dramatically improves how major combat operations can be planned and conducted as effects-based—with every echelon supported dynamically, especially warfighters at the first tactical mile.

4.4 Conditions

Conditions are variables of the operational environment that may affect task performance. For the purposes of this NCOE JIC's illustrative CONOPS, what are called *physical* conditions pertain to the material environment: weather, climate, geography and terrain, including man-made terrain such as urbanization. *Military* conditions are those characteristics of equipment upon which the performance of desired military functions depend; these include physical and operational characteristics, but not technical characteristics.[9] *Civil* conditions are those characteristics that describe the political and civilian conditions: cultural identities, religious influences, and governmental characteristics, such as the form of government. Whereas the CONOPS should be referred to for detailed conditions for various phases and levels of execution, the following general conditions are applicable to the tasks contained in this NCOE JIC:

4.4.1 Physical

- The majority of the scenario's terrain is mountainous and non-arable, with the mountain ranges having a general north-south orientation with few lateral east-west routes.

- The mountainous lay of the land canalizes the road and rail links in the general orientation of the mountain ranges. In large parts of the Joint Operating Area (JOA), the transportation network consists of unpaved and poorly maintained paved roads and aging rail links.

- Ground flora is plentiful during the growing season, but there are few virgin forests. The winters are devoid of most natural plant cover.

[9] Joint Publication 1-02, *Department of Defense Definition of Military and Associated Terms*, 12 April 2002, p. 33.

- The area's high population density is limited to the arable land and concentrated in several major urban areas. The remainder of the population follows the Lines Of Communication (LOC) network that links the urban areas. There is no significant population in the high elevations.

- The weather patterns follow four distinct seasons. The winters are cold. At the lower elevations the precipitation is only moderate.

- The area's long coastlines facilitate access from the sea.

4.4.2 Military

- The Joint Task Force (JTF) Headquarters (HQ) is the level of command directing the mission. The JTFHQ is combined and multinational. The subordinate ground, sea, and air component HQs are likewise combined. Subordinate component formations (i.e., at the echelon-level of the Unit of Action/UA) are task-organized as Joint but not combined (that is, they are not multinational).

- At the JTFHQ-level, there is a mature combined doctrine that guides JTF planning development, but which attenuates or diminishes in operational execution at the UA echelon-level.

- English is the predominant "working" language of the JTFHQ and of the component HQs. Various national languages predominate at the UA echelon-level.

- There are fully developed combined command relationships that meet the requirements for combined military operations, but which are influenced by the multinational partners' domestic political considerations.

- The Joint Task Force's Rules of Engagement (ROE) diverge from the Standing Rules of Engagement, CJCSI 3121.01, to accommodate multinational ROE as agreed upon by the coalition's members. Those ROE are fully developed and combined.

- Communications systems and processes are interoperable within and between the JTFHQ and the component HQs, but not between the separate national formations at the UA echelon-level. Multiple levels of security are in place for effective information flow across functional boundaries (i.e., logistics, intelligence, operations, etc.) at the JTFHQ- and component HQ-levels, but not between separate national formations at the UA echelon-level.

- Multinational partners in the JTFHQ and in the component HQs have comparable information-age cultures, but not necessarily the same degree of cross-cultural understanding due to different national languages and word-meanings.

- In support of the JTF are various COIs worldwide, composed of experts in the fields of international relations, host nation domestic politics, emergency humanitarian relief-aid, international civilian police (CIVPOL), civil reconstruction, as well as representatives from non-governmental organizations and private businesses. All of these COIs are properly networked into the NCOE and can be accessed virtually by the JTF Commander and by levels below and above him.

- The adversary has armed forces with conventional and unconventional formations capable of launching direct and indirect fires from land, sea and air.

- The adversary possesses anti-access systems, including advanced mobile surface-to-air missiles (SAMs).

- The adversary possesses the capability for Chemical, Biological, Radiological, Nuclear, and/or high-yield Explosive (CBRNE) effects with delivery-means sufficient to reach outside the JOA and the theater-region.

- The adversary possesses capabilities to conduct computer network attacks, Signals Intelligence (SIGINT), special operations, and electronic warfare (EW) attacks to exploit, deny, disrupt, degrade or destroy GIG security services and information.

4.4.3 Civil

- The population of the adversary's territory is non-Western in history, culture, customs, language, economy, and government.

- Populations of the multinational partners come from Western societies and/or from those societies which, while non-Western in history, culture, customs and language, nevertheless have a recent history of Western political and economic traditions.

4.5 Illustrative Concept of Operations (CONOPS)

To best illustrate the capability improvements which the NCOE will provide to the JTF Commander, a classified illustrative Concept of Operations is included as Appendix G. This illustrative CONOPS is tied to a specific *Defense Planning*

Scenario set in the year 2015 and provides a series of operationally-based vignettes depicting how military commanders and civilian leaders of the future could use the NCOE to conduct operations.

5. CAPABILITIES, TASKS, AND STANDARDS

In this NCOE JIC:

- *Capabilities* are discussed in narrative form. The NCE JFC divides them into Knowledge and Technical areas, a categorization retained here.

- *Tasks* are discrete events or actions that enable a mission or function to be accomplished by individuals or organizations.[10] Herein, the tasks are discussed collectively to illustrate their interdependence.

- *Standards* are the minimally acceptable proficiencies required to perform a task; they consist of measures and criterion. The types of standards, and the new standards postulated, are considered here at every level as they pertain to the Joint Force's interoperability, circa 2015.[11]

The NCE JFC document defines *what* capabilities and attributes are required for the future Joint Force across all the operating and functional concepts. This NCOE JIC builds upon the NCE JFC by establishing the integrated KM, NM and IA idea to demonstrate *how* net-centric capabilities might be applied to a particular set of operations.

Some tasks listed in this NCOE JIC but not found in the NCE JFC were derived from a comprehensive review of other JFC documents (such as for Battlespace Awareness and Focused Logistics) or from the NCOE JIC analysis process, including a Defense Assessment Review Team (DART) review, an O-6 level coordination, and a Limited Objective Experiment (LOE) "war-game." To better align the capabilities framework with the knowledge gained since the publication of the NCE JFC document, the set of capabilities has been decreased from twenty-one (21) to thirteen (13).

A comprehensive Capabilities/Task/Standards Matrix, found in Appendix A, shows how closely the NCOE is supported by its *Enabling Constructs* and how the KM, NM and IA components help to integrate it.

[10] CJCSM 3500.04C, *Universal Joint Task List*, July 1, 2002 (Current as of May 13, 2003), p. GL-II-3.
[11] Ibid, pp. GL-II-1 to GL-II-3.

5.1 Capabilities

A capability is the ability to achieve an effect to a standard under specified conditions using multiple combinations of means and ways to perform a set of tasks.[12]

The Joint Force must have the ability to exchange information, cross-domain, in near real-time, with allied, coalition, and non-DoD partners via automated means that do not require the burden of having technically trained personnel with special security clearances. Systems must prevent access to information and network communications by adversaries during and after an overrun or capture, while retaining the capability to restore systems to normal operations after repatriation. Size, weight and power (SWAP) attributes for NCOE equipment must be appropriate to the tactical environment.

The NCOE also must perform across the full range of military operations and under all national, strategic, operational and tactical environments, including amid electromagnetic pulse (EMP) and CBRNE-contaminated environments. The capabilities specified in this section apply to terrestrial, airborne, maritime, surface/sub-surface and space-based networks. NCOE capabilities must have fail-safe measures in-place to ensure that vulnerabilities are not created when tactical personnel or equipment fall into the hands of adversaries. NCOE material and non-materiel approaches need to address the unique challenges associated with self-forming, self-healing, and ad hoc networks.

Capabilities do not exist in isolation: they remain closely interrelated to both attributes and tasks. The NCE JFC document bins the NCOE's capabilities into two areas: knowledge and technical. The knowledge area comprises the cognitive and social properties required to function effectively within a net-centric environment.[13] The technical area comprises the physical infra-structure and information properties of the network.[14] The knowledge area depends on the data and information which the technical means provide, later to turn that data and information into knowledge.

Many capabilities originally found in the NCE JFC do not appear as such in this NCOE JIC. The preponderance of those originals were not deleted but, rather, absorbed, either into a modified capability or into a new capability—subsequently becoming either a task or a sub-task. For example, the original "ability to share situational awareness" consists of two different undertakings: to achieve situational understanding and then to share it. Other original capabilities—such as the ability to "employ geo-spatial information," and "employ information," and "provide user access," and "access information," and "operate/maneuver," and "provide network services"—were all deemed to be

[12] CJCS, *Joint Concept Development and Revision Plan* (JCDRP), July 2004, p. 15.
[13] CJCS, *Net-Centric Environment Joint Functional Concept* (NCE JFC), 7 April 2005, p. 21.
[14] Ibid.

either too vague or too detailed. A few originals, such as the "ability to synchronize actions" and the "ability to operate interdependently," were deemed to be too C2-focused and thus inappropriate for this NCOE JIC.

In section 5.1.1 and 5.1.2, the NCOE JIC capabilities are divided into two or three categories: NCE JFC capabilities; modified NCE JFC capabilities; and new capabilities without a reference in the NCE JFC.

5.1.1 Knowledge Capabilities

NCE JFC capabilities:

- **Ability to establish appropriate organizational relationships.** This is the ability to set-up and change formal organizational and command relationships according to mission and task needs. The NCOE supports existing frameworks and provides a new COI framework for formal and informal organizational needs.

- **Ability to share situational understanding.** Sharing understanding with an array of participants will lead to better collective understanding and contribute to higher quality decision-making. Through the use of KM tools, sharing situational understanding will be enhanced.

- **Ability to collaborate.** Collaboration must be continuous and include geographically separated participants, involving all relevant parties in a virtual space that utilizes collaboration tools and visualization techniques to share knowledge. This will enhance the decision-making of the JTF Commander and of others.

Modified NCE JFC capabilities:

- **Ability to provide adaptive, distributed, cooperative, and collaborative decision-making and planning.** Many elements will be involved in decision-making. Therefore, decision-makers will need collaboration tools and sophisticated decision-support tools.

  To capture the complex nature of decision-making and of the technical means for sharing knowledge among COIs or others, this capability recognizes that a variety of different methods could be needed, especially for a variety of environments, circumstances, and missions.

- **Ability to continuously develop knowledge, skills, and abilities of individuals and teams.** Knowledge, skills, and abilities can be enhanced through effective collaborative training methods. The dynamic nature of the future environment will require that teams be established with little

or no previous working relationships. As a result, training will need to be conducted en route to the operating area. The use of collaborative and interactive training will enable effective training to be accomplished in minimal time.

5.1.2 Technical Capabilities

NCE JFC capabilities:

- **Ability to establish an information environment.** This capability includes the establishment of criteria processes and procedures to store and share data/information, including across different environments and functional areas, along with support for multiple and sometimes changing COIs.

- **Ability to identify, store, share, and exchange data and information.** 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).

- **Ability to process data and information.** To be useful, data and information must be filtered, fused, and correlated into useful forms.

- **Ability to maintain and survive.** The network must be able to maintain service under both physical and information attack. It should degrade gracefully, dynamically rerouting services as nodes are incapacitated and/or as information flow requirements change.

Modified NCE JFC capabilities:

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

  Currently, more data and information is collected than can be exploited. This capability addresses the problem by employing KM and NM tools to identify and distribute timely and relevant information to the warfighter.

- **Ability to provide end-to-end assurance and validation of information and information systems.** That is, the ability to restore and recover data, assure the availability of information, validate that information's integrity, determine its origin, and maintain an audit trail (i.e., the pedigree of that information).

- **Ability to install and deploy a scalable and modular network.** The net-centric model depends upon connectivity where and when required, capable of forward deployment, and tailorable to mission requirements. Also, the network must be capable of dynamic reconfiguration as missions/tasks change and be functional in harsh and/or unimproved infrastructure environments.

- **Ability to create and produce information in an assured environment.** The ability to collect data and transform it into information, while also providing end-to-end protection to assure the availability of information, validating that information's integrity.

New capabilities:

Ability to defend systems and network. That is, capable of monitoring situational awareness of the network and identifying when unauthorized users attempt to gain access, especially by hostile means. It must also provide network security measures to ensure network integrity. This capability was added to emphasize the role of information assurance in defending information systems and the network.

- **Ability to optimize network functions and resources.** To maximize the impact of a desired effect, the NCOE must provide the warfighter with the connectivity and information/knowledge he needs. The NCOE must recognize economies of scale and prioritize network functions and resources, providing access based upon the roles and responsibilities of each user.

  This capability addresses the need for a flexible infrastructure and ensures that the most important users, from the JTF Commander out to warfighters at the "first tactical mile," have the access and resources they need in combat situations.

- **Ability to transport information end-to-end.** That is, having built and optimized a survival data network infrastructure, then putting into action the transport of information into, out of, and throughout this dynamically changing network.

5.2 Tasks

A task is an action or activity, derived from doctrine, standard procedures, and mission analysis of concepts that may be assigned to an individual or to an organization.[15]

[15] JCDRP, p. 16.

The NCOE's baseline tasks were derived from the NCE JFC and refined through several workshops and conferences with SMEs, the Services, and private industry—including a "capabilities" workshop, a JIC/EC Task Integrating Working Group, and a Limited Objective Experiment (LOE) led by JFCOM for Joint Experimentation (J9). All of these tasks are essential to the integration of KM, NM, and IA, ensuring an efficient and effective interface between the NCOE's knowledge and technical areas.

5.3 Standards

A standard is the minimum proficiency required in the performance of a task. For the mission-essential tasks of joint forces, each task standard is defined by the Joint Force Commander and consists of a measure and criterion.[16]

Appendix A provides a table of standards associated with tasks. The standards were developed and subjected to a vetting process by operational experts in their respective fields, including from some U.S allies. Conferences, "workshops," comment-and-coordination processes, and war-gaming were all employed. Many of the knowledge area tasks involve cognitive processes, such as measuring understanding and trustworthiness, which the scientific and KM communities acknowledge are very difficult to measure; however, because these knowledge area tasks are vital to achieving success in the NCOE, they have been incorporated into this NCOE JIC with a nascent set of standards. These standards will be improved during the CBA process and will include emerging metrics produced by the scientific and KM communities.

Other standards have been derived, in whole or in part, from previously developed concept and capabilities documents. While currently still notional, these operational standards provide a baseline for the CBA process. The CBA process will use extensive modeling and simulation (M&S) and other analytical techniques to refine the standards into a set, or sets, of technical standards suitable for material and non-material capabilities analysis. Validation of these standards will be conducted in conjunction with the CBA review and approval process as outlined in CJCSI 3170.01E. M&S sensitivity analysis will also be employed to determine potential shortfalls at various force levels (i.e., JTF and below).

One of the standards shown in Appendix A utilizes a *Quality of Protection* (QoP) framework for information assurance tasks. The QoP measurement framework uses five levels of protection: level 0 through level 4. Level 0 denotes that no IA protection is required or applied against the indicated class of IA attacks or threats. Conversely, level 4 protection (or L-4) denotes that IA protection, commensurate with defending against IA attacks expected from well-funded, highly aggressive and determined "nation-state" adversaries, is desired and/or

[16] Ibid.

provided. Protection assurances and mechanisms along the continuum from L-0 thru L-4 should be viewed as additive. Therefore, it is conceivable that components "rated" at lower QoP protection levels (i.e., L-1 thru L-3) could be combined using good system engineering techniques (i.e., defense-in-depth) to achieve, synergistically, higher effective QoP values for a particular operation or mission. For example, commercial products may, by themselves, provide only L-1 or L-2 levels of IA protection; yet, they may still play an integral part in contributing towards achieving the L-4 protection necessary for particular NCOE missions and operations.

6. IMPLICATIONS

The NCE JFC document provides a comprehensive list of implications associated with transitioning to a net-centric environment. That list is applicable to this NCOE JIC as well. Since this NCOE JIC extends the framework found in the NCE JFC by proposing an integrated KM, NM, and IA strategy, joint training must be developed and implemented to specifically address this detailed integration. This NCOE JIC also extends the scope of IA from that described by the NCE JFC, in specifically calling for role-based, risk-managed user access. This requires not only policy changes, it implies an increased responsibility set for IA personnel. Emerging technology, such as distributed key management, as well as enterprise-wide security updates, will likely reduce or eliminate some of the current primary IA tasks. Accordingly, the organization, training, and certification of IA personnel will need to evolve to support the IA requirements articulated in this NCOE JIC.

7. CONCEPT DEVELOPMENT AND EXPERIMENTATION

Among the family of joint concept documents, the JIC has the narrowest focus, distilling capabilities from the JOCs, JFCs, and other JCIDS documents into the fundamental conditions, tasks, and standards required for a Capabilities-Based Assessment. The CBA process will use the JIC as a baseline to conduct rigorous analyses of capability gaps and overlaps, leading ultimately to appropriate material and non-material solutions as part of the broader JCIDS effort. To accomplish this, the JIC taxonomy and standards will be harmonized with related efforts, such as the GIG taxonomies, JCA efforts, the *Net-Centric Operations and Warfare Reference Model* (NCOW RM), the *Net-Centric Implementation Documents* (NCIDS), and Information Technology (IT) portfolios.

The CBA process will further review, refine, and validate the conditions, tasks, and standards discussed in this NCOE JIC through the extensive use of M&S and other analytical techniques. The outcome of this analysis will likely cause various standards to be modified and others to be added or eliminated accordingly; for example, the process will address areas such as computing infrastructure capabilities and standards. Over time, this NCOE JIC will be further harmonized with other key policy documents—such as for the JCAs,

the NCOW RM, the NCIDS, etc.—in parallel with the CBA, in time to influence the resulting *Joint Capabilities Document* (JCD) taxonomy and standards.

The JIC also has a role within the larger context of the DoD Acquisition process and IT portfolio management. Specifically, the capabilities identified in this NCOE JIC and its associated *Enabling Constructs*, once coordinated and validated through a rigorous CBA and JCIDS process, will be provided through a range of DOTMLPF initiatives and solutions. Material solutions—whether legacy transformed, under development at present, or newly started between now and the period of effectiveness of this NCOE JIC—will be implemented under the governance of the various IT portfolios established by the Deputy Secretary of Defense.

APPENDIX A. NCOE JIC Capabilities/Tasks/Standards

Knowledge Area

Discussion Located in		Knowledge Capability	Operational Task	Standard	
				Measure	Criterion
NCE JFC	**1.0**	**Ability to Establish Appropriate Organizational Relationships**			
NCE JFC	1.1		Obtain and maintain an understanding of command intent	Time to disseminate and synchronize command intent. Percentage of COI which has and understands command/COI intent.	TBD TBD
NCOE JIC	1.2		Establish working relationships with potential partners	Time to establish working relationships	TBD
Enterprise Serv. EC	1.3		Provide COI environment	Time for information change to be posted and/or subscribers notified. Percentage of uptime of required service.	<1 min[17] 99.9%[18]
NCOE JIC	1.4		Define and implement a knowledge dissemination strategy	Time to define and implement strategy. Knowledge dissemination strategy passed on to potential COI members. COI partners participating in strategy formulation.	6 hrs <1 hr 95%
NCOE JIC	1.5		Identify / Establish appropriate relationships with NGOs, JIIMs, etc. (Build COIs)	Percentage of entities registered. Time to register participants.	90% 2 hrs
NCOE JIC	1.6		Modify formal and informal collaboration patterns	Time to establish coordination process with coalition, NGOs, etc.	30 min
NCOE JIC	1.7		Deal with flexible authority relations within a Joint/COI environment	Trustworthiness measured in degree of confidence.	High/Full
NCOE JIC	1.8		Maintain flexible attitudes towards power and authority within a Joint/COI Environment	Trustworthiness measured in degree of confidence.	High/full
NCOE JIC	1.9		Adjust procedures and/or organization as necessary	Time to recognize entity disconnects in COI and to adjust procedures.	TBD
NCE JFC	1.10		Flexibly adapt to changing operational needs	Time to adapt to changing operational needs. Newly connected users are discovered. Machine time should be minutes. Timeframe for COI to adjust. Time for COI to gather necessary information.	6 hrs/ 2 hrs <30 sec 5/10 min 1-3 min Information available < 1 min Information

[17] CJCS, *Enterprise Services Enabling Construct*, 1 November 2005. Appendix E of the NCOE JIC.
[18] Ibid.

Discussion Located in		Knowledge Capability	Operational Task	Standard	
				Measure	Criterion
					derived from outside sources -- longer
NCOE JIC	1.11		Support enterprise-wide and COI-specific applications	Time for service to adapt requirements. Time to assure applications and services. Machine-to-machine: Man-to-machine:	TBD TBD x<3 min x<=10 min
NCOE JIC	1.12		Ensure that hostile entities are not inadvertently included as part of the organizational constructs.	Percentage of non-validated (untrusted) information/services utilized for organizational interactions. Confidence that each individual in each organization possesses the appropriate authority (i.e. rights and responsibilities) to execute their respective role in the organization. Confidence that no hostile individuals or groups are included in the established organizational relationships.	< 10% 90% 90%
NCE JFC	**2.0**	**Ability to collaborate**			
Enterprise Serv. EC	2.1		Establish a collaborative session	Time to establish collaboration sessions. Percent of desired participants able to participate. Percent decrease in time to conduct planning tasks.	Minutes[19] TBD[20] x%
Enterprise Serv. EC	2.2		Maintain a consistent collaborative session (i.e. always on)	Percent commonality between different COIs in form and function. Time to establish collaboration sessions Percent desired participants able to participate Percent decrease in time to conduct planning tasks	80% Minutes[21] 95%[22] x%[23]
Applications EC	2.3		Utilize the collaborative tools through custom user interface	Time to display CROP information received using standard message formats Percentage of information exchange agreed-to by the parties	< 15 sec >90%

[19] CJCS, *Applications Enabling Construct*, 1 November 2005. Appendix F of the NCOE JIC.
[20] Ibid.
[21] Ibid.
[22] Ibid.
[23] Ibid.

Discussion Located in		Knowledge Capability	Operational Task	Standard	
				Measure	Criterion
Applications EC	2.4		Provide synchronization between multiple applications with simultaneous user interaction	Time to synchronize applications. Number (applications multiplied by users) simultaneously supported.	<1 second >100
NCOE JIC	2.5		Establish community vocabulary, lexicon	Percentage of COI members that are able to understand COI goals and missions. Percentage of COI has and understands command/COI intent . Lexicon developed and agreed to. Lexicon published to COI members. No semantic ambiguity in lexicon. Lexicon can be easily and quickly updated.	99% 95% 99% per COI
Enterprise Serv. EC	2.6		Establish schedule of recurring meetings	Time to establish schedule of recurring meetings.	TBD
NCOE JIC	2.7		Notify participants of a meeting	Percent notified	95%
NCOE JIC	2.8		Deconflict schedules	Time to de-conflict schedules	30 min
NCOE JIC	2.9		Overcome organizational/cultural/language limits to collaboration to support Joint/Coalition operations	Time to overcome organizational/cultural/language barriers.	N/A
NCOE JIC	2.10		Establish a role-based, adaptable, tailorable individual knowledge framework	Time to establish.	Minutes
Enterprise Serv. EC	2.11		Know availability of knowledge assets	Percent of available assets correctly identified.	TBD
Enterprise Serv. EC	2.12		Set up expedient meetings based on the situation and events	Time to set up expedient meetings.	TBD
Enterprise Serv. EC	2.13		Establish collaborative sessions "on the fly" during operations	Time to establish collaboration sessions. Percent of desired participants able to participate. Percent of critical information disseminated to collaboration partners.	<5 min[24] 95%[25] 99%[26]
Enterprise Serv. EC	2.14		Maintain traceability of collaborative process	Time to establish collaboration sessions. Percent of desired participants able to participate.	Minutes[27] x%[28]

[24] CJCS, *Applications Enabling Construct*, 1 November 2005. Appendix F of the NCOE JIC.
[25] Ibid.
[26] Ibid.
[27] Ibid.
[28] Ibid.

Discussion Located in		Knowledge Capability	Operational Task	Standard	
				Measure	Criterion
Enterprise Serv. EC	2.15		Establish ownership rights on collaborative products	Time to establish collaboration sessions. Percent of desired participants able to participate. Percent of critical information disseminated to collaboration partners. Percent decrease in time to conduct planning tas.	Minutes[29] x%[30] x%[31] x%[32]
NCOE JIC	2.16		Limit collaboration to authorized participants.	Percentage of collaboration that must occur outside of the Assured Information Environment.	TBD
Enterprise Serv. EC	3.17		Discover organizational structure	TBD	TBD
NCOE JIC	**3.0**	**Ability to provide adaptive, distributed, cooperative, and collaborative decision-making and planning**			
NCOE JIC	3.1		Establish trust in decision-making collaboration	Percent of information tagged appropriately.	99.99%
NCOE JIC	3.2		Interact effectively with collaborative tools in a cooperative environment	Percent of participants that use tools effectively.	90%x%
NCOE JIC	3.3		Establish problem-solving framework	Percent of decisions untimely due to excessive deliberation. Percent of decisions made with too little deliberation	5x% 10%x%
App	3.4		Use multiple authoritative applications in parallel for course of action or functional alternative development in a distributed environment	Percent of COI which must be contributors to network environment. Percent of time en-route users supported.	95% 95%
App	3.5		Develop a parallel process for monitoring and understanding the operational environment and synchronizing actions of assigned forces	Web-based architecture established and installed. Time to display CROP information received using standard message formats. Time to receive acknowledgement of understanding from receiver of intent back to sender.	TBD <15 sec TBD
NCOE JIC	3.6		Establish a Mission Capability Package	Time to establish Mission Capability Package.	Hours
Applications EC	3.7		Provide visualizations of non-visible phenomena by synthetic means for COI purposes and threat awareness	Develop plausible visualizations.	Three simultaneous alternatives
NCOE JIC	3.8		Develop Alternative Courses of Action	TBD	TBD
NCOE JIC	3.9		Select Appropriate Course of Action	TBD	TBD
Applications EC	3.10		Provide collaborative mission planning and rehearsal en route	TBD	TBD

[29] Ibid.
[30] Ibid.
[31] Ibid.
[32] Ibid.

Discussion Located in		Knowledge Capability	Operational Task	Standard	
				Measure	Criterion
Applications EC	3.11		Present data from multiple enterprise sources in a humanly intelligible, timely, and fused format	Percent of COI median time required for a COI member to configure display for new planning task	5 min
Applications EC	3.12		Provide the capability for distributed, collaborative, systematic, on-demand, creation and revision of executable plans, with up-to-date options, as circumstances require.	Time to complete adaptive campaign planning upon receipt of a planning directive.	8-12 hrs
Applications EC	3.13		Identify selection criteria, & assess alternatives to decisively control operational situations, through automation in exchange, fusion, & understanding of information	Time to complete an adaptive campaign planning upon receipt of a planning directive.	<96 hrs
Applications EC	3.14		Configure smart agents and user display to execute predictive analysis within a functional area	Time to configure smart agents for new information search. Time to compute and display search results on user interface.	>1 min >10 sec
NCOE JIC	3.15		Change information search and retrieval patterns	Time to accomplish search and retrieval patterns.	10 min
NCOE JIC	3.16		Modify/revise procedures and schedules	Time to establish new procedures.	20 min
NCOE JIC	3.17		Adapt info sharing to accommodate evolving needs	TBD	TBD
NCOE JIC	3.18		Assure adequate control, tracking and management of plans and decisions.	Percent utilization of services outside of those offered by the NCOE Assured Information Environment.	<1%
Applications EC	3.19		Conduct simulation on COA	TBD	TBD
NCOE JIC	**4.0**	**Ability to share situational understanding**			
NCOE JIC	4.1		Develop common understanding of problems and goals	Time to develop common understanding of problems and goals.	15 min
Applications EC	4.2		Achieve situational awareness using geospatial and time-centric displays of enterprise-wide data to relate information with similar characteristics	Display CROP information at the level of accuracy received, using standard message formats.	<15 sec[33]
NCOE JIC	4.3		Use knowledge to influence not connected to the physical network	Percent of units that need to process information in order to understand it. Time to distribute. Percent of information released to unauthorized users.	15% 2 hrs 1%
Applications EC	4.4		Provide access, collation, and display of CROP information at source-level accuracy for first tactical mile users	Process and display information from standard message formats.	< 15 sec[34]
Applications EC	4.5		Share situational awareness by providing access to common information with specific indication of contextual relevance	Percent of COI information with contextual relevance tagging.	90%
Applications EC	4.6		Disseminate plan of action to other decision makers	Time to communicate all approved orders and plans to subordinate and adjacent units.	x<=1 min

[33] CJCS, *Applications Enabling Construct*, 1 November 2005. Appendix F of the NCOE JIC.
[34] Ibid.

Discussion Located in		Knowledge Capability	Operational Task	Standard	
				Measure	Criterion
NCOE JIC	4.7		Achieve shared understanding	Time to display CROP information received using standard message formats. Connectivity and capacity to transport understanding. Service databases/information sources available on the web.	<15 sec[35] TBD TBD
NCOE JIC	4.8		Limit the sharing of situational understanding to authorized individuals and to only accept situation updates from authoritative sources.	Percent utilization of services outside of those offered by the NCOE Assured Information Environment.	<1%
NCOE JIC	5.0	**Ability to continuously develop knowledge, skills, and abilities of individuals and teams**			
NCOE JIC	5.1		Develop high-performing teams	Time to establish.	1 hrs
NCOE JIC	5.2		Support rehearsal with live, virtual constructive simulations and training	Percent of rehearsal with live, virtual constructive simulations.	90%
NCOE JIC	5.3		Capture, obtain, and distribute "lessons learned"	Time to distribute.	2 hrs

Technical Area

Discussion Located In		Technical Capability	Operational Task	Standard	
				Measure	Criterion
NCOE JIC	**6.0**	**Ability to Create/ Produce Information In An Assured Environment**			
NCOE JIC	6.1		Provide smart management / tasking of collections assets	Time to set-up an information exchange. Time for information change to be posted and/or subscribers notified.	<1 min[36] <1 min
NCOE JIC	6.2		Capture timely, relevant, interoperable source data from sensors and other input areas	Time for information change to be posted and/or subscribers notified. Percent of accuracy information; level of confidence.	<1 min TBD
Applications EC	6.3		Transform/ Process data into information	Time for information change to be posted and/or subscribers notified.	<1 min
Applications EC	6.4		Capture, create and display information with local tools while disconnected from the enterprise	Time supported between synchronization with networked resources.	48 hrs
NCOE JIC	6.5		Prevent the injection of malicious	Percent utilization of	<1%

[35] Ibid.
[36] Dependent upon complexities of the operational environment and medium employed.

			functionality or other malfeasance within the Smart Environment.	services outside those offered by the NCOE Assured Information Environment.	
NCOE JIC	6.6		Ensure that only authorized entities and valid information/services are used within the Smart Environment.	Percent of non-validated (untrusted) information/services utilized for the Smart Environment..	< 10%
NCOE JIC	**7.0**	**Ability to Identify/Store/Share/Exchange data/information**			
NCOE JIC	7.1		Connect and interface with interagency, coalition, international organizations, commercial and NGOs	Percent of critical information available to individuals responsible for action within time to react. Percent of allied/coalition access that can be managed Response time to provide connection to US and non-US networks. Percent of interested entities registered participants in the COI. Time to register interested participants to a COI. Time to establish collaboration sessions. Within 15 minutes of notification effect physical connection	95/99 >97/>98 US 30 sec; non-US 60 sec 90% <2 hrs 30 min/20 min >64K for text/voice; >256K for video
NCOE JIC	7.2		Share across security areas such as coalitions, Homeland Security, etc. (cross-domain information sharing)	TBD	TBD
NCOE JIC	7.3		Enable machine-to-machine info-sharing	Time to set-up an information exchange Time to select	<1 min <5 sec/<1 sec
NCOE JIC	7.4		Provide relevant information based on users roles and responsibilities	Percentage of critical information available to individuals responsible for action within time to react: Accuracy necessary to identify changing roles and responsibilities and match them to critical information	95/99 99%
NCOE JIC	7.5		Manage data/information life cycle and optimize data/info handling	Eliminate a percentage of unnecessary redundancy Percentage of time data/information is available	TBD 99%

Enterprise Serv. EC	7.6		Provide Discovery Services	Network availability Percentage of correct service binding to deliver requested transactions Percentage of services implementation that can be reused in the generation of related services/new versions	>99% under routine conditions and 99% under override conditions >95% >60%
NCOE JIC	7.7		Provide information publish/subscribe services	Availability of services Percent of information posted and published	> or = 99.9% 95% threshold/ 99% objective
NCOE JIC	7.8		Enable smart pull/push information	Response time to user requests or demand Responsiveness available Time to establish connectivity Network availability	< 1 sec > or = 99.9% N/A >99% under routine conditions and 99% under override conditions
NCOE JIC	7.9		Perform intelligent search	Time to Push/Pull Time to establish comms with needed experts	7/3 min 5/2 min
Enterprise Serv. EC	7.10		Provide Messaging Services	Time to display shared information Network availability Percentage of correct service binding to deliver requested transactions	<1 sec >99% under routine conditions and 99% under override conditions >97% ** Special Category messages 100%

NCOE JIC	7.11		Provide Risk Adaptive Access Control (RAdAC) based on Dynamic Operational Needs	Confidence that the operational need and the security risk were adequately considered in the Risk Adaptive Decision. Time required to render a Risk Adaptive access decision.	Moderate 60 sec ==> initial response (Automated) + 30 min ==> adjudicated response
NCOE JIC	7.12		Use assured services in conjunction with validated sources	Percent utilization of services outside of those offered by the NCOE Assured Information Environment Percent of non-validated (untrusted) information/services utilized for data/information transactions	<1% < 10%
NCOE JIC	**8.0**	**Ability to Establish a Smart, Assured Information Environment**			
Enterprise Serv. EC	8.1		Provide Application Hosting Environment	Number of allowable service bindings within the required timeframe Time to effect the service contract modification	>10,000 <1 min
Enterprise Serv. EC	8.2		Provide Subscriber Service Provider Interface	Time to establish access and implement subscriber authentication Accurately identify changing roles and responsibilities and match them to critical information	1 min/ 10 sec 99%
Enterprise Serv. EC	8.3		Customize Subscriber Presentation	Percent of content that can be tailored to meet user needs	>90%
Enterprise Serv. EC	8.4		Maintain information and knowledge connectivity in limited bandwidth environment	Network availability	>99% under routine conditions and 99% under override conditions
NCOE JIC	8.5		Provide Information Confidentiality Services	Confidence that only authorized groups and individuals can access information protected by the NCOE	99%
NCOE JIC	8.6		Provide Non-Repudiation Services	Confidence that authorized users can justifiably/legally prove that information transactions occurred.	99%

				Service returns confirmation that transaction occurred.	1 min
NCOE JIC	8.7		Ensure that hostile attacks to the environment (and within the environment) are detected, investigated, and dealt with appropriately.	Percent coverage of the Assured Information Environment that is defended by the NCOE Network Defense capability	>80%
NCOE JIC	8.8		Ensure that the information and information services are authoritative.	Percentage of non-validated (untrusted) information/services utilized for data/information transactions.	< 10%
NCOE JIC	**9.0**	**Ability to Process Data and Information**			
Enterprise Serv. EC	9.1		Provide Mediation Services	The percent of correct service bindings to deliver requested transactions within the NCOE Network availability Time to set-up an information exchange	>99.99% and external to the NCOE (non-DOD) >95%. >99% under routine conditions and 99% under override conditions < 1min
Applications EC	9.2		Integrate/Fuse Data	Percentage of accuracy depicted information ; level of confidence Time for information to be posted and/or subscribers notified and integrated	95 <1 min
Applications EC	9.3		Provide configurable, intelligent locally resident processing resources	Percent of data and information which can be processed while disconnected from enterprise resources	>90%
NCOE JIC	9.4		Maintain confidence in the authority of the information/services received and the authorization of the consumers of those information/services.	Percent utilization of services outside of those offered by the NCOE Assured Information Environment	<1%
Applications EC	9.5		Enable sharing of enterprise information resources and enterprise process and applications.	TBD	TBD
Applications EC	9.6		Enable rapid configuration and modification of new and existing applications	TBD	TBD
NCOE JIC	**10.0**	**Ability to Find Useful Information**			
Enterprise Serv. EC	10.1		Provide context relevant Search and Retrieval Services	Percentage of information search and retrieval services provide accurate and relevant data	99.99%

NCOE JIC	10.2		Provide information layering and drill down capabilities	Percentage of accuracy of viewing information; level of confidence Percentage of information object that accurately can be traced to source	95% >99%
NCOE JIC	10.3		Ensure that only authoritative information/sources are provided to users.	Percentage of non-validated (un-trusted) information/services utilized for data/information transactions.	< 10%
NCOE JIC	**11.0**	**Ability to provide end-to-end assurance and validation of information and information systems**			
NCOE JIC	11.1		Assure information	Percentage of information not corrupted QoP: Defend Data Modification QoP: Defend Re-Direct (Misdirected) Traffic/ Transmission QoP: Defend Transmission Eavesdropping QoP: Defend Unauthorized Data Disclosure QoP: Unauthorized Service Access Time to restore or recover information/data from backups.	<99.999% L-4: Nation-State Hours
NCOE JIC	11.2		Validate critical/valuable information	Percentage of critical information needs to be validated Time to determine information pedigree Percentage of pedigree accurate Time to validate authoritative source of information	99% <1 sec 99.9% <1 sec
NCOE JIC	11.3		Determine/Maintain an information pedigree	Time to determine information pedigree	<1 sec
NCOE JIC	11.4		Securely label data/information consistent with IA guidelines	Percentage of data/information labeled with data-authority (e.g. owner/manager/source (e.g. group, COI, etc.) of data element. Percentage of data/information	99.99% 80%

				labeled with pertinent access decision fields Binding of labels to data Integrity of security labels	 Strong High
NCOE JIC	11.5		Develop (confidence) trust in information	Percentage of critical information needs to be validated QoP: Defend Data Modification	99.99% L-4: Nation-State
NCOE JIC	11.6		Compare Operational Need With Security Risk	TBD	TBD
NCOE JIC	11.7		Determine Security Risk of Requestor	TBD	TBD
NCOE JIC	11.8		Authenticate Identity	QoP: Defend Identity Masquerading QoP: Defend Service Spoofing	L-4: Nation-State
NCOE JIC	11.9		Verify Identity of information/service provider or requestor	Confidence that the asserted identity matches the actual identity Confidence that the asserted identity posses the authority to provide or consume the specific information or service	80% certainty 80%
NCOE JIC	11.10		Manage execution of authorities.	Degree to which the rights and responsibilities of individuals and groups can be supported/enforced within the Net-Centric environment. Time required to validate the authority of an information/service provider or consumer to perform an activity.	75% Seconds
NCOE JIC	11.11		Manage Resources	Degree to which resources can be provided to the highest priority authorized user when required. Time required to provide/allocate resources to authorized consumers.	TBD TBD

NCOE JIC	11.12		Perform assured information dissemination.[37]	Percent of coverage regarding the appropriate (authorized) individuals receive the provided information/services. Confidence that consumers of information/services have the information they need, commensurate with their specific authorities for that information.	75% Moderate
NCOE JIC	**12.0**	**The Ability to Defend Systems and Network**			
NCOE JIC	12.1		Protect In-Transit Information	Time to isolate compromised network QoP: Defend Data Modification QoP: Defend Re-Direct Traffic/Transmission QoP: Defend Traffic Analysis QoP: Defend Traffic/Transmission Detection QoP: Defend Transmission Eavesdropping	<30 sec L-4: Nation-State
NCOE JIC	12.2		Identify mission criticality of friendly systems and nodes	Formal Identification and management/tracking of mission critical nodes/systems Formal identification of mission support nodes and systems	99.99% Receive status reporting
NCOE JIC	12.3		Track DoD information flow	Confidence in information paths between (critical) nodes	High
NCOE JIC	12.4		Electronically map networks in which DoD information traverses	Accuracy of electronic map Currency of Network Map	90% <30 days

[37] This task includes, but is not limited to, information dissemination strategies such as "content staging," "persistent file management," and assured delivery.

NCOE JIC	12.5		Perform continuous network defense	Continuously maintain full spectrum awareness of network events	24 hrs/7 days
				Coverage of status-monitoring of critical nodes	99.99%
				Time to detect Security Events	Minutes
				Time to identify Security Events	Minutes/ Hours[38]
				Accuracy of Incident Reporting	90%
				Time to investigate Security Incidents	Hours[39]
				Time to "appropriately" respond to security incidents	Hours[40]
NCOE JIC	12.6		Employ tiered, defense in depth protection across the NCOE	QoP: Defend Data Modification QoP: Defend Identity Masquerading QoP: Defend Re-Direct Traffic/Transmission QoP: Defend Service Disruption QoP: Defend Service Modification QoP: Defend Service Spoofing QoP: Defend Traffic Analysis QoP: Defend Traffic/Transmission Detection QoP: Defend Transaction Repudiation QoP: Defend Transmission Eavesdropping QoP: Defend Unauthorized Data Disclosure QoP: Unauthorized Service Access	L-4: Nation-State

[38] May vary depending on the information operations condition (INFOCON) level.
[39] Situation-dependent.
[40] Situation-dependent.

NCOE JIC	12.7		Deter, detect, and deny unauthorized intrusions to the NCOE	Response time to detect and assess unauthorized intrusion	15 min
NCOE JIC	12.8		Deter, detect, and deny unauthorized insider access to the NCOE	Time to detect nefarious activity Time to appropriately respond to unauthorized activity	15 min
NCOE JIC	12.9		Identify network intrusions/probing attempts	Awareness of network functions Network availability	99.99% >99% under routine conditions and 99% under override conditions
NCOE JIC	12.10		Provide cyber situational awareness and network defense	Time to assess readiness of critical systems/services Time to report security situations	10 min
NCOE JIC	12.11		Investigate security events/incidents to determine cause, impacts, and response options	Network Availability	0.988% availability
NCOE JIC	12.12		Assess Operational impact of attacks	Time to report impacts Confidence in accuracy of assessment	Consistent with Network Defense Strategy
NCOE JIC	12.13		Characterize the current (active) threat to network environment	Confidence in characterization of network threat conditions	Consistent with NetOps CONOP
NCOE JIC	12.14		Report on characterization of attack elements	Confidence in our understanding of the nature and objective of discrete/collective attacks	Consistent with Network Defense Strategy
NCOE JIC	12.15		Respond to network attacks/intrusions with appropriate actions	Time to provide response Time to re-establish critical services from disruption	< 60 min < 60 min
NCOE JIC	12.16		Share IA/CND situational awareness information with authorized users	Time to alert authorized users of cyber situations	TBD[41]
NCOE JIC	12.17		Conduct vulnerability assessments/evaluations	Time to report compliance with IAVA	TBD[42]
NCOE JIC	12.18		Employ security patches	Time to report compliance with IAVA	TBD[43]
NCOE JIC	12.19		Channel the attacker	Time to detect attack Time to isolate the attacker Degree of isolation applied to attacker	15 min 15 min 90%

[41] INFOCON-dependent.
[42] INFOCON-dependent.
[43] INFOCON-dependent.

NCOE JIC	12.20		Isolate compromised network nodes	Response time to isolate a compromised network	< 30 sec
NCOE JIC	12.21		Synchronize defense operation across DoD and with coalition partners	Effectiveness of DIO OPLAN[44]	99.99%
NCOE JIC	12.22		Replicate information systems and information infrastructures (both friendly and adversary) through modeling and simulation	Percent Coverage	80%
NCOE JIC	12.23		Establish and maintain Continuity of Operations (COOP) plan/activity	Percent effectiveness of COOP plan (ability to meet plan goals and objectives)	90%
NCOE JIC	12.24		Perform forensic analysis to establish the facts or evidence surrounding security events/incidents.	Time required to perform forensic analysis. Degree to which the established facts/evidence can be used in legal proceedings (e.g. court martial or other legal prosecution.)	Days or weeks 80%
NCOE JIC	**13.0**	**Ability to install and deploy a scalable and modular network**			
Information Trans. EC	13.1		Rapidly deploy/employ robust connectivity forward	Percentage of availability/persistence Total time to establish connectivity	> 99% < 60 min
Information Trans. EC	13.2		Provide global information transport services	Time to establish and deliver services	<60 min
Information Trans. EC	13.3		Acquire additional network resources on demand	TBD	TBD
Information Trans. EC	13.4		Inform/Update chain of command of network status	TBD	TBD
Information Trans. EC	13.5		Provide Comm Link Services (Non-Networked)	TBD	TBD
Information Trans. EC	13.6		Tailor to specific capabilities	Time to establish connection	30 sec/5 sec
Information Trans. EC	13.7		Function under range of infrastructure and ROE constraints	Time to re-establish disrupted service	60 min
Information Trans. EC	13.8		Dynamically plan network architecture development processes	TBD	TBD
Information Trans. EC	13.9		Integrate diverse systems (coalition, interagency, and NGOs)	TBD	TBD
Information Trans. EC	13.10		Establish nodes where needed	TBD	TBD
Information Trans. EC	13.11		Design for rapid insertion of new technology	TBD	TBD
Information Trans. EC	13.12		Operate without geographic constraints	TBD	TBD
Information Trans. EC	13.13		Provide ad hoc coalition connectivity	TBD	TBD
Information Trans. EC	13.14		Connect with all assets	TBD	TBD
NCOE JIC	13.15		Establish controllable communications relay	TBD	TBD
NCOE JIC	**14.0**	**Ability to optimize network functions and resources**			

[44] DIO OPLAN – Defensive Operations Plan.

Enterprise Serv. EC	14.1		Provide IM services	Network administrators can optimize network functions	97%
Information Trans. EC	14.2		Ensure spectrum availability to satisfy operational requirements	Percentage of spectrum available for DOD use that is actually accessible to DOD users	Criterion: >85%/>95%
Information Trans. EC	14.3		Execute Network Configuration Plan	Time to reconfigure network	10 min/1 min
Information Trans. EC	14.4		Manage and Configure Systems and Networks	Time to set-up network and configure	4 hrs/1 hr
Information Trans. EC	14.5		Perform network control (FCAPS)	Time to establish network organization	<10 min/<3 min
NCE JFC	**15.0**	**Ability to maintain and survive**			
Enterprise Serv. EC	15.1		Manage Enterprise Services	Enterprise services prioritized by mission	>98% of supported platforms
Information Trans. EC	15.2		Provide network situational awareness	TBD	TBD
Information Trans. EC	15.3		Support all operations and transitional states along the ROMO	Percentage of allied/ coalition access that can be managed	98%
Information Trans. EC	15.4		Maintain network capabilities and ensure survivability	Re-establish Enterprise Network from catastrophic failure	60 min
NCOE JIC	15.5		Minimize Packet loss in a hostile environment	Percent Packet Loss Relieve network congestions points caused by component failures and/or attacks	< 20% Norm: 60 min Degr: 30 min Attack: 10 min
NCOE JIC	**16.0**	**Transport Information end-to-end**			
Information Trans. EC	16.1		Transmit Information[45]	Time to transmit traffic/ information	TBD
Information Trans. EC	16.2		Perform Retransmission/ Relay/ Gateway Services	Latency of retransmission	<0.1 sec / none
Information Trans. EC	16.3		Receive information	Information reception rate	>10 Mbs (First tactical Mile User) / >100 Gbs (Core Infrastructure)
Information Trans. EC	16.4		Manage Services Delivery	Percentage of available services that can be remotely managed	>95% / >98%
Information Trans. EC	16.5		Prioritize Service Delivery	Time to automatically implement service prioritization	<3 min / < 1min
Information Trans. EC	16.6		Control Information Flow Precedence	Percentage of information that can be controlled using pre-agreed precedence	>90% / > 98%
Information Trans. EC	16.7		Manage information flow, access, and information access Optimize Resource Use	Time to establish network organization	<10 min / < 3 min
Information Trans. EC	16.8		Monitor Resource Use	Latency in monitoring resource usage	<1 min / <10 sec
Information Trans. EC	16.9		Deliver Information	Time	<1 min / <10 sec
Information	16.10		Select Distribution Channel	Time to select a	<2 sec / <.5 sec

[45] Media-dependent.

Trans. EC				distribution channel	

A.1 Knowledge-Sharing Subordinate Task Mapping

Discussion Located in		Knowledge Capability	Operational Task	Sub-Task	Sub-Sub-Task	Sub-Sub-Sub-Task	Standard	
							Measure	Criterion
NCE JFC	**2.0**	**Ability to collaborate**						
NCOE JIC	2.7		Notify participants of a meeting				Percent notified	95%
NCOE JIC	2.8		Deconflict schedules				Time to de-conflict schedules	30 min
NCOE JIC	2.9		Overcome organizational/cultural/language limits to collaboration to support Joint/Coalition Operations				Time to overcome organizational/cultural/language barriers	N/A
NCOE JIC	2.10		Establish a role-based, adaptable, tailorable individual knowledge framework				Time to establish	Minutes
NCOE JIC	**3.0**	**Ability to provide adaptive, distributed, cooperative, and collaborative decision-making and planning**						
NCOE JIC	3.2		Interact effectively with collaborative tools in a cooperative environment				Percent of participants that use tools effectively	90%
NCOE JIC	3.3		Establish problem-solving framework				Percent of decisions untimely due to excessive deliberation Percent of decisions made with too little deliberation	5% 10%
NCOE JIC	3.6		Establish a Mission Capability Package				Time to establish Mission Capability Package	Hours
Applications EC	3.7		Provide visualizations of non-visible phenomena by synthetic means for COI purposes and threat awareness				Develop plausible visualizations	Three simultaneous alternatives
NCOE JIC	3.7.1			Identify objectives, constraints, and measures of success			Percent objectives, constraints, and measure of success correctly identified	95%
NCOE JIC	3.7.2			Develop and evaluate alternative solutions			Time to evaluate each alternative	5 min
NCOE JIC	3.7.3			Understand plans being developed by other assets			Time lag in currency of information on plans for other military forces or non-DOD agencies	25 min
NCOE JIC	3.15		Change information search and retrieval patterns				Time to accomplish search and retrieval patterns	10 min
NCOE JIC	3.16		Modify/revise procedures and schedules				Time to establish new procedures	TBD
NCOE JIC	**4.0**	**Ability to share situational understanding**						
NCOE JIC	4.1		Develop common understanding of problems and goals				Time to develop common understanding of problems and goals	15 min
NCOE JIC	4.1.1			Understand other participants perceptions of the situation			Percent of understanding of perceptions	95%
NCOE JIC	4.1.2			Understand other			Percent of cultural backgrounds	85%

			participants' cultural backgrounds	present which are recognized by the group	
NCOE JIC	4.1.3		Develop common understanding of roles, responsibilities, and taskings	Time to develop common understanding of roles, responsibilities, and tasking	30 min
NCOE JIC	4.1.4		Use multiple methods to achieve situational understanding via multiple means (i.e., inductive, deductive, adductive reasoning)	Percent of time COI detected invalid assumptions	85%
NCOE JIC	4.1.5		Develop high performing teams	Time to establish	2 hrs
NCOE JIC	4.1.6		Communicate preferred solutions and underlying rationale to other decision-makers	Instances of organization/unit aware of others objectives/plans	95%
NCOE JIC	4.1.7		Post knowledge products	Percent posted	90
Applications EC	4.2		Achieve situational awareness using geospatial and time-centric displays of enterprise wide data to relate information with similar characteristics	Display CROP information at the level of accuracy received using standard message formats	<15 sec
NCOE JIC	4.2.1		Communicate situational awareness to other decision makers	Percent of critical information reaching person responsible for action in time to react	99%
NCOE JIC	4.2.2		Simultaneously process inputs from multiple sources and retain focus on the task at hand	Time lag between COP and the real world situation	1-2 min
NCOE JIC	4.2.3		Establish a common individual knowledge framework	Time to establish	5 min
NCOE JIC	4.2.4		Request for information	Time to process and disseminate status information Percent of critical information acquired and disseminated	1-2 min 99%
NCOE JIC	4.2.5		Assess validity/currency of information	Time lag between information and real world situation	1-2 min
NCOE JIC	4.2.6		Achieve higher quality situational understanding via multiple means (access to expert systems, etc.)	TBD	TBD
NCOE JIC	4.2.7		Communicate understandings to other decision-makers	Percent of critical information reaching person responsible for action in time to react	99%
NCOE JIC	4.2.17		Provide public information		
NCOE JIC	4.2.18		Provide private information		
NCOE JIC	4.3		Use knowledge to influence	Percent of units that need to	15%

			groups/individuals not connected to the physical network	process information in order to understand it Time to distribute Percent of information released to unauthorized users	 2 hrs 1%
NCOE JIC	4.7		Achieve Shared Understanding	Time to display CROP information received using standard message formats Connectivity and capacity to transport understanding Service databases/information sources available on the web	<15 sec TBD TBD
NCOE JIC	4.7.6		Provide information in a useful format	Time to distribute	2 hrs
NCOE JIC	**5.0**	**Ability to continuously develop knowledge, skill, and abilities of individuals and teams**			
NCOE JIC	5.1		Develop high-performing teams	Time to establish	1 hrs
NCOE JIC	5.2		Support rehearsal with live, virtual constructive simulations and training	Percent of rehearsal with live, virtual constructive simulations	90%
NCOE JIC	5.3		Capture, obtain, and distribute "lessons learned"	Time to distribute	2 hrs

1
2

Discussion Located in		Technical Capability	Operational Task	Sub-Task	Standard	
					Measure	Criterion
NCOE JIC	**7.0**	**Ability to Identify/Store/Share/Exchange data/information**				
NCOE JIC	7.8		Enable smart pull/push information		Response time to user requests or demand Responsiveness available Time to establish connectivity Network availability	< 1 sec > or = 99.9% N/A >99% under routine conditions and 99% under override conditions
NCOE JIC	7.8.1		Push information to required entities		Time for Joint staff sections and boards to establish communications with needed experts	2 min
NCOE JIC	7.8.2		Pull information to required entities		Time for Joint staff sections and boards to	3 min

Discussion Located in		Technical Capability	Operational Task	Sub-Task	Standard	
					establish communications with needed experts	

A.2 Information Assurance Subordinate Task Mapping

Discussion Located in		Knowledge Capability	Operational Task	Sub-Task	Sub-Sub Task	Sub-Sub-Sub Task	Standard	
							Measures	Criterion
NCE JFC	**1.0**	**Ability to Establish Appropriate Organizational Relationships**						
NCOE JIC	1.12		Ensure that hostile entities are not inadvertently included as part of the organizational constructs.				Percentage of non-validated (untrusted) information/services utilized for organizational interactions. Confidence that each individual in each organization posses the appropriate authority (i.e. rights and responsibilities) to execute their respective role in the organization. Confidence that no hostile individuals or groups are included in the established organizational relationships.	< 10% 90% 90%
NCE JFC	**2.0**	**Ability to collaborate**						
Enterprise Serv. EC	2.1		Establish a collaborative session				Time to establish collaboration sessions Percent desired participants able to participate Percent decrease in time to conduct planning tasks	Minutes TBD x%
Enterprise Serv. EC	2.1.2			Provide collaboration management			TBD	TBD
NCOE JIC	2.1.2.2				Perform Identity verification		TBD	TBD
NCOE JIC	2.16		Limit collaboration to authorized participants.				Percentage of collaboration that must occur outside of the Assured Information Environment.	
NCOE JIC	**3.0**	**Ability to provide adaptive, distributed, cooperative, and collaborative decision-making and planning**						
NCOE JIC	3.18		Assure adequate control, tracking and management of plans and decisions.				Percent utilization of services outside of those offered by the NCOE Assured Information Environment	<1%
NCOE JIC	**4.0**	**Ability to share situational understanding**						

Discussion Located in		Knowledge Capability	Operational Task	Sub-Task	Sub-Sub Task	Sub-Sub-Sub Task	Standard	
							Measures	Criterion
NCOE JIC	4.8		Limit the sharing of situational understanding to authorized individuals and to only accept situation updates from authoritative sources.				Percent utilization of services outside of those offered by the NCOE Assured Information Environment	<1%

1
2

Discussion Located in	Technical Capability		Operational Task	Sub-Task	Sub-Sub-Task	Sub-Sub-Sub Task	Standard	
							Measure	Criterion
NCOE JIC	**6.0**	**Ability to Create/ Produce Information In An Assured Environment**						
NCOE JIC	6.5		Prevent the injection of malicious functionality or other malfeasance within the Smart Environment.				Percent utilization of services outside of those offered by the NCOE Assured Information Environment	<1%
NCOE JIC	6.6		Ensure that only authorized entities and valid information/services are used within the Smart Environment.				Percentage of non-validated (untrusted) information/services utilized for the Smart Environment	< 10%
NCOE JIC	**7.0**	**Ability to Identify/Store/Share/Exchange data/information**						
NCOE JIC	7.11		Provide Risk Adaptive Access Control (RAdAC) based on Dynamic Operational Needs				Confidence that the operational need and the security risk were adequately considered in the Risk Adaptive Decision. Time required to render a Risk Adaptive access decision.	Moderate 60 sec ==> initial response (Automated) + 30 min ==> adjudicated response
NCOE JIC	7.11.1			Determine Probablistic Security Risk (vector) associated with Access Request			Confidence that the security risk vector accurately reflects the appropriate risk factors Time required to generate the Security Risk vector for an access request.	Moderate 30 sec

Discussion Located in	Technical Capability		Operational Task	Sub-Task	Sub-Sub-Task	Sub-Sub-Sub Task	Standard	
							Measure	Criterion
NCOE JIC	7.11.1.1					Determine the relative "Trust" factor of individual requesting access	Confidence	Certified and Accredited by responsible DAA (Designated Accreditation Authority)
NCOE JIC	7.11.1.2					Determine the Quality of Protection (QoP) associated with the IT Components hosting the provide, process, and consume functions of the requested information transaction.	Confidence	Certified and Accredited by responsible DAA
NCOE JIC	7.11.1.3					Determine the sensitivity of the information being requested.	Confidence	Certified and Accredited by responsible DAA
NCOE JIC	7.11.1.4					Determine the Environmental Factors of the associated IT Components	Confidence	Certified and Accredited by responsible DAA
NCOE JIC	7.11.1.5					Determine the Situational Factors of the associated IT Components	Confidence	Certified and Accredited by responsible DAA
NCOE JIC	7.11.1.6					Apply the current set of Heuristic "Rules/Principles" associated with Risk factors	Confidence	Certified and Accredited by responsible DAA
NCOE JIC	7.11.1.7					Determine the Applicable Access Control Policies based on requestor trust, QoP, information sensitivity, environment, and situation, and heuristic factors.	Confidence	Certified and Accredited by responsible DAA
NCOE JIC	7.11.1.8					Calculate the Security Risk Vector for the access request.	Confidence	Certified and Accredited by responsible DAA

Discussion Located in	Technical Capability		Operational Task	Sub-Task	Sub-Sub-Task	Sub-Sub-Sub Task	Standard	
							Measure	Criterion
NCOE JIC	7.11.2			Determine Criticality of Operational Need associated with Access Request			Confidence that the calculated operational need vector accurately reflects the appropriate operational considerations. Time required to generate the operational need vector for an access request.	Moderate 30 sec
NCOE JIC	7.11.2.1				Determine the authority of the individual requesting access.		Confidence	Certified and Accredited by responsible DAA
NCOE JIC	7.11.2.2				Determine the Situational Factors or current operational (e.g. battle) conditions		Confidence	Certified and Accredited by responsible DAA
NCOE JIC	7.11.2.3				Determine the Heuristic "Rules/Principles" associated with Operational impacts to the mission of requestor		Confidence	Certified and Accredited by responsible DAA
NCOE JIC	7.11.2.4				Determine the Applicable Operational Access Policies based on requestor's authority, situation, and heuristic factors.		Confidence	Certified and Accredited by responsible DAA
NCOE JIC	7.11.2.5				Calculate the Operational Need Vector for the Access Decision		Confidence	Certified and Accredited by responsible DAA
NCOE JIC	7.11.3			Perform Risk Adaptive Access Decision based on Digital Access Policy			Confidence that the Risk Adaptive Access decision/rationale reflects the trade-off between the operational need and the security risk. Time required to generate the Risk Adaptive Access Recommendation with Rationale.	Moderate 30 sec

Discussion Located in	Technical Capability		Operational Task	Sub-Task	Sub-Sub-Task	Sub-Sub-Sub Task	Standard	
							Measure	Criterion
NCOE JIC	7.11.3.1					Obtain the Security Risk Vector	Confidence	Certified and Accredited by responsible DAA
NCOE JIC	7.11.3.2					Obtain the Mission/Operation Need of the Request	Confidence	Certified and Accredited by responsible DAA
NCOE JIC	7.11.3.3					Calculate the Risk Adaptive Access Decision with Rationale	Confidence	Certified and Accredited by responsible DAA
NCOE JIC	7.12		Use assured services in conjunction with validated sources				Percent utilization of services outside of those offered by the NCOE Assured Information Environment Percentage of non-validated (untrusted) information/services utilized for data/information transactions	< 1% < 10%
NCOE JIC	**8.0**	**Ability to Establish an Information Environment**						
NCOE JIC	8.5		Provide Information Confidentiality Services				Confidence that only authorized groups and individuals can access information protected by the NCOE	99%
NCOE JIC	8.6		Provide Non-Repudiation Services				Confidence that authorized users can justifiably/legally prove that information transactions occurred	99%
NCOE JIC	8.7		Ensure that hostile attacks to the environment (and within the environment) are detected, investigated, and dealt with appropriately.				Percent coverage of the Assured Information Environment that is defended by the NCOE Network Defense capability	>80%
NCOE JIC	8.8		Ensure that the information and information services are authoritative.				Percentage of non-validated (untrusted) information/services utilized for data/information transactions.	< 10%
NCOE JIC	**9.0**	**Ability to Process Data and Information**						

Discussion Located in	Technical Capability		Operational Task	Sub-Task	Sub-Sub-Task	Sub-Sub-Sub Task	Standard	
							Measure	Criterion
NCOE JIC	9.4		Maintain confidence in the authority of the information/services received and the authorization of the consumers of those information/services.				Percent utilization of services outside of those offered by the NCOE Assured Information Environment	<1%
NCOE JIC	**10.0**	**Ability to Find Useful Information**						
NCOE JIC	10.3		Ensure that only authoritative information/sources are provided to users.				Percentage of non-validated (un-trusted) information/services utilized for data/information transactions.	< 10%
NCOE JIC	**11.0**	**Ability to provide end-to-end assurance and validation of information and information systems**						
NCOE JIC	11.1		Assure information				Percentage of information not corrupted Time to restore or recover information/data from backups	<99.999% Hours
NCOE JIC	11.2		Validate critical/valuable information				Percentage of critical information needs to be validated Time to determine information pedigree Percentage of pedigree accurate	99% <1 sec 99.9%
NCOE JIC	11.3		Determine/Maintain an information pedigree				Time to determine information pedigree	<1 sec
NCOE JIC	11.4		Securely label data/information consistent with IA guidelines				TBD	TBD
NCOE JIC	11.5		Develop (confidence) trust in information				Percentage of critical information needs to be validated	99.99%
NCOE JIC	11.6		Compare Operational Need With Security Risk				TBD	TBD
NCOE JIC	11.7		Determine Security Risk of Requestor				TBD	TBD
NCOE JIC	11.8		Authenticate Identity				TBD	TBD
NCOE JIC	11.8.1		Provide unique ID				TBD	TBD
NCOE JIC	11.8.2		Provide persistent ID				TBD	TBD

Discussion Located in	Technical Capability		Operational Task	Sub-Task	Sub-Sub-Task	Sub-Sub-Sub Task	Standard	
							Measure	Criterion
NCOE JIC	11.9		Verify Identity of information/service provider or requestor				Confidence that the asserted identity matches the actual identity Confidence that the asserted identity posses the authority to provide or consume the specific information or service	TBD TBD
NCOE JIC	11.10		Manage execution of authorities.				Degree to which the rights and responsibilities of individuals and groups can be supported/enforced within the Net-Centric environment. Time required to validate the authority of an information/service provider or consumer to perform an activity.	75% seconds
NCOE JIC	11.11		Manage Resources				Degree to which resources can be provided to the highest priority authorized user when required. Time required to provide/allocate resources to authorized consumers.	TBD TBD
NCOE JIC	11.12		Perform assured information dissemination.[46]				Percent of coverage regarding the appropriate (authorized) individuals receive the provided information/services. Confidence that consumers of information/services have the information they need, commensurate with their specific authorities for that information.	75% moderate
NCOE JIC	**12.0**	**The Ability to Defend Systems and Network**						

[46] This task includes, but is not limited to, information dissemination strategies such as "content staging," "persistent file management," and assured delivery.

Discussion Located in	Technical Capability		Operational Task	Sub-Task	Sub-Sub-Task	Sub-Sub-Sub Task	Standard	
							Measure	Criterion
NCOE JIC	12.1		Protect In-Transit Information				Time to isolate compromised network	<30 sec
NCOE JIC	12.2		Identify mission criticality of friendly systems and nodes				Formal Identification and management/tracking of mission critical nodes/systems Formal identification of mission support nodes and systems	99.99% Receive status reporting
NCOE JIC	12.3		Track DoD information flow				Confidence in information paths between (critical) nodes	High
NCOE JIC	12.4		Electronically map networks in which DoD information traverses				Accuracy of electronic map Currency of Network Map	90% <30 days
NCOE JIC	12.5		Perform continuous network defense				Continuously maintain full spectrum awareness of network events Coverage of status-monitoring of critical nodes Time to detect Security Events Time to identify Security Events Accuracy of Incident Reporting Time to investigate Security Incidents Time to "appropriately" respond to security incidents	24 hrs/7 days 99.99% Minutes Minutes/ Hours 90% Hours Hours
NCOE JIC	12.5.1		Monitor CND activities				TBD	TBD
NCOE JIC	12.5.1.1		Capability to monitor network traffic				TBD	TBD
NCOE JIC	12.5.1.2		Capability to receive external alerts and advisories				TBD	TBD
NCOE JIC	12.5.1.3		Capability to monitor host activities				TBD	TBD
NCOE JIC	12.5.1.4		Capability to monitor IDS and firewall activity				TBD	TBD
NCOE JIC	12.5.2		Detect unauthorized network activity				TBD	TBD

Discussion Located in	Technical Capability		Operational Task	Sub-Task	Sub-Sub-Task	Sub-Sub-Sub Task	Standard	
							Measure	Criterion
NCOE JIC	12.5.3		Analyze unauthorized activity				TBD	TBD
NCOE JIC	12.5.4		Perform response actions				TBD	TBD
NCOE JIC	12.5.4.1			Provide tools to track and manage response events			TBD	TBD
NCOE JIC	12.5.4.1.1					Provide security event correlation	TBD	TBD
NCOE JIC	12.5.4.1.2					Provide IT trending analysis	TBD	TBD
NCOE JIC	12.5.4.1.3					Provide auto-discovery capability	TBD	TBD
NCOE JIC	12.5.4.2			Provide tools to implement response actions to support network/host configurations			TBD	TBD
NCOE JIC	12.5.4.3			Provide tools to capture and safeguard forensic data			TBD	TBD
NCOE JIC	12.5.4.4			Provide automated response procedures			TBD	TBD
NCOE JIC	12.6		Employ tiered, defense in depth protection across the NCOE				QoP: Defend Data Modification QoP: Defend Identity Masquerading QoP: Defend Re-Direct Traffic/Transmission QoP: Defend Service Disruption QoP: Defend Service Modification QoP: Defend Service Spoofing QoP: Defend Traffic Analysis QoP: Defend Traffic/Transmission Detection QoP: Defend Transaction Repudiation QoP: Defend Transmission Eavesdropping QoP: Defend Unauthorized Data Disclosure QoP: Unauthorized	L-4 Protection Level (Commensurate with Nation-state level attacks)

Discussion Located in	Technical Capability		Operational Task	Sub-Task	Sub-Sub-Task	Sub-Sub-Sub Task	Standard	
							Measure	Criterion
							Service Access	
NCOE JIC	12.7		Deter, detect, and deny unauthorized intrusions to the NCOE				Response time to detect and assess unauthorized intrusion	15 min
NCOE JIC	12.8		Deter, detect, and deny unauthorized insider access to the NCOE				Time to appropriately respond to unauthorized activity	15 min
NCOE JIC	12.9		Identify network intrusions/probing attempts				Awareness of network functions Network availability	99.99% >99% under routine conditions and 99% under override conditions
NCOE JIC	12.10		Provide cyber situational awareness and network defense				Time to assess readiness of critical systems/services Time to report security situations	10 min
NCOE JIC	12.10.1			Computer Enterprise Protection Capabilities			TBD	TBD
NCOE JIC	12.10.1.1				Capabilities to analyze network vulnerabilities		TBD	TBD
NCOE JIC	12.10.1.2				Capabilities to analyze Enterprise threats		TBD	TBD
NCOE JIC	12.10.1.3				Capabilities for enterprise defense mechanisms		TBD	TBD
NCOE JIC	12.10.1.3.1					System firewalls and premise routers	TBD	TBD
NCOE JIC	12.10.1.3.2					Intrusion detection systems (IDS)	TBD	TBD
NCOE JIC	12.10.1.3.3					Host anti-virus (Host-AV)	TBD	TBD
NCOE JIC	12.10.1.3.4					Maintain network confidentiality	TBD	TBD
NCOE JIC	12.11		Investigate security events/incidents to determine cause, impacts, and response options				Network Availability	0.988% availability
NCOE JIC	12.12		Assess Operational impact of attacks				Time to report impacts Confidence in accuracy of assessment	Consistent with Network Defense Strategy
NCOE JIC	12.13		Characterize the current (active) threat to network environment				Confidence in characterization of network threat conditions	Consistent with NetOps CONOP

Discussion Located in	Technical Capability		Operational Task	Sub-Task	Sub-Sub-Task	Sub-Sub-Sub Task	Standard	
							Measure	Criterion
NCOE JIC	12.14		Report on characterization of attack elements				Confidence in our understanding of the nature and objective of discrete/collective attacks	Consistent with Network Defense Strategy
NCOE JIC	12.15		Respond to network attacks/intrusions with appropriate actions				Time to provide response Time to re-establish critical services from disruption	< 60 min < 60 min
NCOE JIC	12.16		Share IA/CND situational awareness information with authorized users				Time to alert authorized users of cyber situations	TBD
NCOE JIC	12.17		Conduct vulnerability assessments/evaluations and employ security patches				Time to report compliance with IAVA	TBD
NCOE JIC	12.18		Channel the attacker				Time to detect attack Time to isolate the attacker Degree of isolation applied to attacker	15 min 15 min 90%
NCOE JIC	12.19		Isolate compromised network nodes				Response time to isolate a compromised network	< 30 sec
NCOE JIC	12.20		Provide the capability for the infrastructure to withstand information operations/ information warfare attacks				Continuously maintain full spectrum awareness of network events Percentage of system compromised Ability to isolate attack (impacts) Ability to isolate (protect/maintain) critical services between critical nodes	24 hrs/7 days <=1% within a theater/ region/ domain/ network/ sub-net 99.99% per COOP
NCOE JIC	12.21		Synchronize defense operation across DoD and with coalition partners				Effectiveness of DIO OPLAN	99.99%
NCOE JIC	12.22		Replicate information systems and information infrastructures (both friendly and adversary) through modeling and simulation				Percent Coverage	80%

Discussion Located in	Technical Capability		Operational Task	Sub-Task	Sub-Sub-Task	Sub-Sub-Sub Task	Standard	
							Measure	Criterion
NCOE JIC	12.23		Establish and maintain Continuity of Operations (COOP) plan/activity				Percent effectiveness of COOP plan (ability to meet plan goals and objectives)	90%
NCOE JIC	12.24		Perform forensic analysis to establish the facts or evidence surrounding security events/incidents.				Time required to perform forensic analysis. Degree to which the established facts/evidence can be used in legal proceedings (e.g. court martial or other legal prosecution.)	Days or weeks 80%
NCE JFC	**15.0**	**Ability to maintain and survive**						
NCOE JIC	15.5		Minimize Packet loss in a hostile environment				Percent Packet Loss Relieve network congestions points caused by component failures and/or attacks	< 20% Norm: 60 min Degr: 30 min Attack: 10 min

APPENDIX B. Glossary and Acronyms

B.1 Glossary

Term	Definition
Accessible	The extent to which users can find and use an information-system resource.
Action	A structured behavior of limited duration. (JCDRP 7/2004)
Actionable Knowledge	Information that enables the decision maker to understand the situation and make use of opportunities for effective action. It is information placed in the context of the situation that includes objectives, constraints, courses of action, uncertainties, and cultural influences.
Accurate	The extent to which a transmission/data stream is error free.
Activity	A structured behavior of continuous duration. (JCDRP 7/2004)
Agility	The ability to move quickly and easily. (*Power to the Edge*)
Applications	The ability to provide a locally resident software program or group of programs that interfaces directly with Joint Force decision-makers and Communities of Interest, which carries out generalized or mission-specific tasks or processes for which a computer is used, i.e., word processing, spreadsheets, graphics, database management, and communications packages.
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)
Authentic	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. (binary)
Autonomous	Undertaken or carried on without outside control; existing or capable of existing independently; responding, reacting, or developing independently of the whole
Available	Timely, reliable access to data and information services for authorized users (percentage)
Battlespace Awareness	Situational information resulting from the processing and presentation of time sensitive and perishable data relating to the operational environment, including the status and dispositions of friendly, adversary, and non-aligned actors.
Battlespace Knowledge	Data and information gathered from the battlespace that has been analyzed and integrated through the lens of understanding including the impacts of physical, cultural, social, political, and economic factors on military operations.
Capability	The ability to achieve a desired effect under specified standards and conditions through combinations of ways and means to perform a set of tasks. (CJCSI 3170.01E)

Term	**Definition**
Cognitive Domain	This domain exists in the minds of human beings. This domain is influenced by individual intangibles such as training, experience, public opinion, and situational awareness. Most importantly, the Cognitive Domain is where we make decisions and is directly related to intellectual capabilities and developmental levels. Vital characteristics of this domain are those that affect individual and organizational decision-making, to include attitudes, opinions, beliefs, and values, and understanding.
Collaboration	Working together in a joint effort for the purpose of achieving a shared understanding, making a decision, or creating a product. (NCE JFC)
Command and Control (C2)	The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.
Community of Interest (COI)	A collaborative group of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes. (*DoD Net-Centric Data Strategy*)
Complete	Having all necessary parts, elements, or steps
Condition	A variable of the environment that affects performance of a task. (JCDRP 7/2004)
Confidential	Assurance that information is not disclosed to unauthorized persons, processes, or devices (binary)
CONOPS (Concept of Operations)	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)
Consistent	Free from variation or contradiction
Control Information	Information required by the Joint Force to regulate personnel and functions in the execution of command intent. It provides the means to measure, report and correct performance. Tactical control information is required in near-real time to support forces engaged in on-going operations. Operational control information is used to direct assigned forces to accomplish specific missions or tasks that are usually limited by function, time, or location. (derived from JP 3.0)
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
Construct	A concept or theory devised to integrate in an orderly way the diverse data on a phenomenon. (Webster's)
Constructive Interdependence	The creation of new capabilities from the connection of latent capabilities within the Joint Force dependent 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.
Criterion	A critical, threshold, or specified value of a measure. (JCDRP 7/2004)

Term	**Definition**
Current	In progress or contemporary. (Webster's)
Cyber-Situational Awareness	Continuously access threats and vulnerabilities to the information domain in order to provide assured information and confidence. Cyber-situational awareness is usually used in conjunction with automated computer defense.
Data	Information without context. (JC2FC v1.0)
De-confliction	Preventing elements of the Joint Force from operating at cross-purposes. (NCE JFC)
Decision Support Tools	Tools intended to help decision makers utilize data and models to identify and solve problems and make decisions
Deployable	Effort required to relocate system to Joint Operations Area (JOA)
Dislocated Civilian Support Mission	Specific humanitarian missions designed to support the resettlement of refugees, stateless persons, evacuees, expellees, and displaced persons. These missions include camp organization, basic construction, and administration; provision of care (food, supplies, medical attention, and protection); and placement (movement or relocation to other countries, camps, and locations). They are often long-term and require enormous resourcing normally not available through DOD sources. (JP 3-07.6)
Distributed	A structure in 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
Diverse	Not dependent on a single element or media
Doctrine	Fundamental principles by which the military forces guide their actions in support of national objectives. It is authoritative but requires judgment in application. (JP 1-02)
Dynamic	Reacts appropriately to change in system status.
Effect	An outcome (condition, behavior, or degree of freedom) resulting from tasked actions. (JCDRP 7/2004)
Employable	Effort required to commence system operation upon arrival in the Joint Operations Area (JOA)
End-state	The set of conditions, behaviors, and freedoms of action that defines achievement of the commander's objectives. (JCDRP 7/2004)
Enterprise Services	The ability to provide well-defined, enterprise network functions that accept a request and return a response through an interface with a user or another service, such as collaboration, messaging, or information discovery and storage.
Expeditionary	Supporting a military operation conducted by an armed force to accomplish a specific objective in a foreign country. (JP1-02)
Flexible	Dynamically meets evolving mission requirements. (Scenario/Condition dependent)
Focused Logistics (FL)	The planning and execution out logistic operations to support the protection, movement, maneuver, firepower, and sustainment of operating forces
Force Application	The integrated use of maneuver and engagement to create the effects necessary to achieve assigned mission objectives

Term	**Definition**
Foreign Humanitarian Assistance	(DOD) Programs conducted to relieve or reduce the results of natural or manmade disasters or other endemic conditions such as human pain, disease, hunger, or privation that might present a serious threat to life or that can result in great damage to or loss of property. Foreign humanitarian assistance (FHA) provided by US forces is limited in scope and duration. The foreign assistance provided is designed to supplement or complement the efforts of the host nation civil authorities or agencies that may have the primary responsibility for providing FHA. FHA operations are those conducted outside the United States, its territories, and possessions. Also called FHA. See also foreign assistance. (JP 3-07.6)
Friction	The amount of organization 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)
Information	Any communication or representation of knowledge such as facts, data, or opinion in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms. (DoD Directive 8000.1)
Information Assurance (IA)	The ability to provide the measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities. (DoD Directive 8500.1, “Information Assurance”)
Information Domain	Where information exists. The Information Domain has a dual nature, consisting of the information itself and the medium by which we collect, process, and disseminate the information. Characteristics of the Information Domain include information quality (completeness, accuracy, timeliness, relevance, and consistency), distribution (range, sharing, and continuity), and interaction (exchange or flow of information).
Information Management (IM)	The planning, budgeting, manipulating, and controlling of information throughout its life cycle. (DoD Directive 8000.1)
Information Transport	The ability to provide the physical communications media over which assured connectivity takes place, supported by switching and routing systems.
Infrastructure	All building and permanent installations necessary for the support, redeployment, and military forces operations (i.e., 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)
Integrity	Protection against unauthorized modification or destruction of information
Interdependence	A mode of operations based on 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)
Internally Displaced Person	Any person who has left their residence by reason of real or imagined danger but has not left the territory of their own country. (JP 3-07.6)

Term	**Definition**
Interoperability	A spectrum of compatibility and connectedness that ranges from isolation to integration. (JS J7 JTD)
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 Net-Centric Operation (JNO)	The ability to exploit all human and technical elements of the Joint Force and its mission partners by fully integrating collected information, awareness, knowledge, experience, and decision-making, enabled by secure access and distribution, to achieve a high level of agility and effectiveness in a dispersed, decentralized, dynamic and/or uncertain operational environment.
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 decision makers to compare alternatives and make programmatic decisions. (JCDRP 7/2004)
Joint Operations Concepts (JOpsC)	The JOpsC is the overarching concept that guides the development of future joint force capabilities. It broadly describes how the Joint Force is expected to operate 10-20 years in the future in all domains across the range of military operations within a multilateral environment in collaboration with interagency and multinational partners. The JOpsC describes the proposed end-states derived from strategy as military problems and the key characteristics of the future Joint Force. (CJCSI 3170.01E 05/2005)
Knowledge	Data and information that have been analyzed to provide meaning and value. Knowledge is various pieces of the processed data and information that have been integrated through the lens of understanding to begin building a picture of the situation. (NCE JFC)

Term	**Definition**
Knowledge Management (KM)	The systematic process of discovering, selecting, organizing, distilling, sharing, developing and using information in a social domain context to improve warfighter effectiveness. (NCE JFC)
Knowledge Sharing	The ability of networked users to manage and make available relevant, accurate information, transform it into knowledge, and act upon it with confidence. This provides access to newly discovered or recurring information in a usable format and facilitates collaboration, distributed decision-making, adaptive organizations, and a greater unity of effort via synchronization and integration of force elements to the lowest levels.
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)
Net-Centric Environment (NCE)	A Joint Force framework for full human and technical connectivity 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 Operations (NCO)	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 decision-making to achieve a high level of agility and effectiveness in dispersed, decentralized, dynamic and uncertain operational environments. (NCE JFC)
Net-Centric Operational Environment (NCOE)	The coherent application of seamless, integrated net-centric capabilities to the forward edge of the battlespace enabling full spectrum dominance.
Net-Centric Warfare (NCW)	An information superiority-oriented concept of operations that generates increased combat power by networking sensors, decision-makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. A sub-set of Net-Centric Operations. (*Network Centric Warfare*)

Term	**Definition**
NetOps (also spelled as NETOPS)	Provides assured and timely net-centric services across strategic, operational and tactical boundaries in support of DoD's full spectrum of warfighting, intelligence and business missions. NetOps provides an integrated approach to accomplishing three interdependent tasks necessary to operate the GIG: GIG Enterprise Management (GEM), GIG Network Defense (GND), and Information Dissemination Management/Content Staging (IDM/CS). *(Joint Concept of Operations for Global Information Grid NetOps)*
Network	Two or more computers connected to each other. The purpose of a network is to enable the sharing of files and information between multiple systems. The Internet can be described as a global network of networks. Computer networks can be connected through cables (Ethernet cables or phone lines) or wirelessly, using wireless networking cards that send and receive data through the air.
Network Management (NM)	Provides the network with the desired level of quality, agility, and trustworthiness. NM focuses on the configuration, availability, performance and manageability of network services and the underlying physical assets that provide end-user services, as well as connectivity to enterprise application services.
Objective	A desired end derived from guidance. (JCDRP 7/2004)
Planning Information	Information used by the Joint Force for developing courses of action. Since the information is used prior to execution, it is normally not as time critical as the information used in current or on-going operations (see situational awareness information). However, such information increases Joint Force knowledge by linking situational awareness with an understanding of the capabilities, training level, experience, and morale of both friendly and enemy forces.
Predictive Information	Information that allows for proactive decisions by the Joint Force. It consists of past observations and historical data used by the Joint Force in future planning, and prevents a "reaction" to a situation. It is the least time critical of the information types.
Quality	Lacking nothing essential or normal. (Roget's II)
Risk	Probability and severity of loss linked to hazards. (JP 1-02)
Robust	Having or exhibiting strength or vigorous health. (Webster's Dictionary)
Shared Understanding	A shared appreciation of the situation supported by common information to enable rapid collaborative joint engagement, maneuver, and support. (NCE JFC)
Situational Awareness (SA) Information	An information category depicting individual Joint Force members' perceptions of the current environment. Based upon gathered, accessible, and provided data, it allows individuals to identify where friendly forces are in relation to each other. Additionally, SA includes the location of enemy and neutral forces within the battlespace and what those forces are doing. The SA information timing is near instantaneous, allowing the Joint Force the ability to make rapid and decisive decisions based upon that information.

Term	**Definition**
Social Domain	The Social Domain is shaped by the specifics of language and symbolic communication among human beings. It is the domain within which individuals interact and is strongly influenced by tacit knowledge including elements of culture, education, collective experience, and morale.
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, subsystem, equipment and its crew to avoid or withstand a hostile environment without suffering an abortive impairment of its ability to accomplish its designated mission. 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 (condition dependent) (NCE JFC-Modified)
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)
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)
Vignette	A concise narrative description that illustrates and summarizes pertinent circumstances and events from a scenario. (JCDRP 7/2004)

B.2 Acronyms

ASD-NII	Assistant Secretary of Defense for Networks and Information Integration
BA	Battlespace Awareness
BCT	Brigade Combat Team
C2	Command and Control
C4	Command, Control, Communications, and Computers
CBA	Capabilities-Based Assessment
CBRNE	Chemical, Biological, Radiological, Nuclear, and High Yield Explosive
CD	Compact Disc
CDD	Capabilities Development Document
CDS	Cross Domain System
CERT	Computer Emergency Response Team
CIC	Combat Information Center
CIVPOL	Civilian Police
CJTF	Commander, Joint Task Force
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
CNO	Computer Network Operation
COA	Course of Action
COCOM	Combatant Command
COI	Community of Interest
COMSEC	Communications Security
CONOPS	Concept of Operations
CONUS	Continental United States
CPD	Capabilities Production Document
CRD	Capabilities Requirements Document
DDMS	DoD Discovery Metadata Standard
DECC	DISA Enterprise Computing Center
DISA	Defense Information Systems Agency
DoD	Department of Defense
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities
DRB	Division Ready Brigade
EA	Electronic Attack
ECM	Evaluation Capability Module
EMP	Electromagnetic Pulse
EW	Electronic Warfare
FL	Focused Logistics
Gbs	Billion bits per second
GCCC	Global C4S Coordination Center
GEMS	Ground Element MEECN Systems
GIG	Global Information Grid
GIG-BE	GIG-Bandwidth Expansion

GMT	Ground Multi-band Terminal
GNCC	Global Network Control Center
GNO	Global Network Operation
GPS	Global Positioning System
HA/DR	Humanitarian Assistance/Disaster Relief
HAIPIS	High assurance Internet Protocol Interoperability Specification
HQ	Headquarters
HUMINT	Human Intelligence
I&W	Indications and Warning
IA	Information Assurance
IC	Intelligence Community
ICD	Initial Capabilities Document
IDP	Internally Displaced Person
IM	Information Management
IO	Information Operation, International Organization
IP	Internet Protocol
IPv6	Internet Protocol version 6
IPB	Intelligence Preparation of the Battlespace
ISR	Intelligence, Surveillance and Reconnaissance
IT	Information Technology / Transport
JAO	Joint Action Officer
JCA	Joint Capabilities Area
JCDRP	Joint Concept Development and Revision Plan
JCIDS	Joint Capabilities Integration and Development System
JEC	Joint Enabling Construct
JFC	Joint Functional Concept
JIACG	Joint Interagency Coordinating Group
JIC	Joint Integrating Concept
JNMS	Joint Network Management System
JNO	Joint Net-Centric Operation
JOC	Joint Operating Concept
JOpsC	Joint Operations Concepts
JP	Joint Publication
JS	Joint Staff
JTF	Joint Task Force
JTFHQ	Joint Task Force Headquarters
JTRS	Joint Tactical Radio System
Kbs	Thousand bits per second
KM	Knowledge Management
LAN	Local Area Network
LOC	Line of Communication
Mbs	Million bits per second
MCEITS	Marine Corps Enterprise Information Technology System
MCEN	Marine Corps Enterprise Network
MCO	Major Combat Operations
MCO-3	Major Combat Operation (Defense Planning Scenario) # 3

MEECN	Minimum Essential Emergency Communications
MEU	Marine Expeditionary Unit
MP	Military Police
NCE	Net-Centric Environment
NCE JFC	Net-Centric Environment Joint Functional Concept
NCES	Net-Centric Enterprise Services
NCO	Network-Centric Operations
NCO CF	Network-Centric Operations Conceptual Framework
NCOE	Net-Centric Operational Environment
NCW	Net-Centric Warfare
NDS	National Defense Strategy
NeMaC	Network Management and Control
NGA	National Geo-spatial Intelligence Agency
NGO	Non-Governmental Organization
NM	Network Management
NMS	National Military Strategy
NOC	Network Operations Center
NOSC	Network Operation and Support Center
NCOW	Net-Centric Operations and Warfare
NSA	National Security Agency
NSS	National Security Strategy
OCONUS	Outside the Continental United States
OPCON	Operational Control
OPTEMPO	Operational Tempo
PKI	Public Key Infrastructure
POTUS	President of the United States
PVO	Private Voluntary Organization
RAPID	Relocateable Army Processors for Intelligence Data
RCT	Regimental Combat Team
RFS	Request for Service
ROE	Rules of Engagement
ROMO	Range Of Military Operations
SAM	Surface-to-Air Missile
SATCOM	Satellite Communications
SCI	Sensitive Compartmented Information
SIGINT	Signals Intelligence
SLA	Service Level Agreement
SME	Subject-Matter Expert
SMI	Security Management Infrastructure
SOA	Service-Oriented Architecture
SOF	Special Operations Force(s)
SOP	Standard Operating Procedure
SPAWAR	Space and Naval Warfare
TBD	To Be Determined
TCCC	Theater Communications Control Center

TNCC	Theater Network Control Center
TNOSC	Theater Network Operations and Security Center
TPG	Transformation Planning Guidance
TPPU	Task, Post, Process, Use
T-SAT	Transformational Satellite
TSO	Telecommunication Service Order
TSR	Telecommunication Service Request
TTP	Tactics, Techniques, and Procedures
UDOP	User Defined Operational Picture
UN	United Nations
US	United States
USJFCOM	United States Joint Forces Command
USSTRATCOM	United States Strategic Command
WAN	Wide Area Network
WIN-T	Warfighter Information Network-Tactical
WMD/E	Weapon(s) of Mass Destruction or Effect

APPENDIX C. List of Contributors

Name	Agency
Anderson, Mr. Derrick	HQDA/G6/CIO
Anderson, Ms. Mary Ann	NSA/CSS/SO1A
Angle, Mr. Charles	SOCOM
Arrendale, Lt Col Frederic	AF/XCIE
Bacharach, Mr. Mark	HQ USMC
Baier, Mr. Michael	SAIC
Banghart, Mr. Stephen	Joint Staff/J6A
Barry, Mr. Philip	MITRE
Batista, Lt Col Tony	JFCOM
Beavers, Mr. William	
Bedford, Mr. John	SAIC
Bednar, Ms. Judy	ASD/NII/DCIO/A&I
Bell, Mr. Randy	JFCOM
Benoit, Mr. Russell	USASC&FG
Bilmanis, Mr. John	HQDA G-3/5/7 DAMO-SSB
Bohn, Mr. Peter	Joint Staff/J6A
Bosley, LTC Jesse	SOCOM/J6M
Brown, Lt Col Jonathan	DISA
Brown, Mr. Gregory	SAIC
Bruning, Lt Col Terry	HQ USMC
Buder, Lt Col Beau	NORTHCOM/J6 N-NC
Burris, LtCol Craig	Joint Staff/J6A
Byers, Ms. Pamela	DISA
Cake, Mr. Spencer	Joint Staff/J6A
Capps, Mr. Steve	NSA/CISSP
Carey, Mr. Paul	JFCOM
Cavaliero, Mr. Mark	HQ USMC/C4/IMA
Condra, Maj Jerome	JFCOM
Cook, Mr. Allen	JFCOM/J84
Creighton, Mr. William	SAIC
Crist, Mr. Charles	
Daily, Mr. John	Booze Allen Hamilton
Damashek, Mr. Robert	Binary Consulting Inc.
Damiens, Mr. Dennis	Joint Staff/J6
Davis, CDR Larry	Joint Staff/J6A

Dean, Mr. Keith	OSD
Delporto-Lee, Ms. Leanne	ASD/NII/DCIO
Dettling, Ms. Jean	JFCOM
Earle, Mr. Hilton	General Dynamics
Edwards, CDR Gary	Joint Staff/J6I
Eger, MAJ Bill	Joint Staff/J3 DDGO CSDO
Emrick, Ms. Brooks	NSA/CSS/S01A
Faltum, Mr. Andrew	Joint Staff/J6X
Fielden, Maj Don	CENTCOM
Forrer, Mr. Don	AF/XOX
Gardner, MAJ David	HQDA/G-35/DAMO-SSP
Garstka, Mr. John	OSD/Force Transformation
Gelenter, Mr. David	STRATCOM/J88G
Gentry, Col Brad	DISA
Gill, Lt Col Andrew	HQ USMC
Gilman, Mr. Michael	JFCOM/J87
Godfrey, Maj Patrick	AF/XIWA
Goode, Mr. Brendan	Booze Allen Hamilton
Gordon, Mr. John	SRA International
Graham, Mr. Douglas	
Graham, Mr. Jack	USASMDC
Grant, Ms. Rosenell	TRADOC
Greene, Ms. Traci	
Grzybowski, MAJ Greg	
Haas, Lt Col Richard	AF/XOXS
Hackman, Mr. Jeffrey	AF/XORI
Harris, Mr. Ronald, Jr.	HQ USMC
Hartline, Mr. Gregory	
Heidenrich, Mr. John G.	SAIC
Hernddon, Mr. Charles	Anteon
Hignett, Mr. Gary	HQDA/CIO/G6 SAIS-GKM
Hintz, Mr. Willis	TRADOC
Hongfong, Mr. Ken	OSD/AT&L
Hostetler, Maj William	STRATCOM/J88G
Houston, Mr. Chuck	SAF/AQI
Hurley, COL Brian	Joint Staff/J6A
Hutchins, Mr. Lee	HAF/XOX
Jackson, Mr. Patrick	AF/HAF
Johnson, Mr. Darrel	

Johnston, Mr. Scott	SOUTHCOM/SCJ6
Jones, Mr. Earnest	TRADOC
Juul, Mr. Kenneth	
Kavanaugh, Ms. Theresa	DISA
Kendrick, Mr. David	General Dynamics
Kern, Mr. Patrick	ASD/NII
Kilborn, Mr. Scott	JFCOM/J9
Kirzl, Mr. John	Evidence-Based Research Inc
Kobiela, Mr. Steven	JFCOM/J9
Kraus, Ms. Marilyn	DCIO/A&I
Kubow, Col Lee	OPNAV
Lasher, Mr. Kevin	OPNAV/N711
Lauver, Mr. Mark	SAIC
Leidy, CAPT Charlotte	Joint Staff/J6
Lee, CDR Daniel	JFCOM
Lewis, Ariapong	
Lind, Mr. Carl	SAIC
Lisi, Mr. Steve	AF/XCIES
Little, LtCol Laura	Joint Staff/J6
Luchs, Lt Col Mark	Joint Staff/J6
Maggiano, Mr. Michael	SAIC
Marcinczyk, Dr. Robert	OSD PA&E
Matzner, Mr. John	HQDA/G3/DAMO-SBB
McHale, Mr. Kevin	MCCDC
McCabe, Ms. Linda	SAIC
McCain, Maj Charles	JFCOM/J68
McKinzie, Lt Col Edward	Joint Staff/J7
McMillan, LCDR Michael, Jr.	JFCOM/J9
Mertz, Lt Col Don	Joint Staff/J6
Miller, Mr. Jeff	ASD/NII/DCIO
Minor, Mr. Philip	ASD/NII
Moore, Dr. Louis, III	RAND Corporation
Moore, Mr. Kyle	General Dynamics
Moose, Mr. Robert	MITRE
Murdock, Mr. Brad	STRATCOM/J856
Myers, Mr. Jack	JFCOM/J9
Newberry, Maj Brian	AF/XOXS
Niezgoda, Col Michael	TRANSCOM/TCJ6-O
Noehl, Mr. Michael	SyColement

Ouellette, Mr. David	
Ouyang, Mr. Wilson	ASD/NII/DCIO
Owen, Mr. Donald	Evidence-Based Research Inc
Parrott, CDR Neil	OSD
Perera, CPT Kevin J.	HQDA/G-35/DAMO-SSP
Petit, LTC Tim	Joint Staff/J6
Place, Mr. Scott	
Porche, Dr. Isaac, III	RAND Corporation
Porter, LTC Carl	Joint Staff/J3/DDGO
Prantl, Mr. Carl	MITRE
Purnell, LTC Lavon	Joint Staff/J6
Redman, Mr. Michael	AF/XOS-H
Richardson, Col Eddie	JFCOM
Risher, BG Paulette M.	SOCOM
Roberts, Mr. Gary	Booze Allen Hamilton
Russell, Mr. Troy	
Salvato, CAPT Michael	JFCOM
Sander, Lt Col Frank	JFCOM/J9
Sarles, Mr. Thomas	
Savage, Mr. Scott	Evidence-Based Research Inc
Schill, Mr. Roger	Northrop Grumman TASC
Schirmer, Mr. Paul	AFC2ISRC/CXOA
Schulz, LTC Richard	JFCOM
Seatherton, LCDR Elliot	JFCOM/J9
Sheehan, Mr. Leo	SAIC
Shephard, Ms. Monica	JFCOM/J9/JPP
Shortt, Mr. Gilbert	Booze Allen Hamilton
Simon, Mr. Anthony	ASD NII
Simpson, CAPT David	EUCOM/J6
Siracuse, Mr. Michael	SAIC
Smith, COL Jeffrey	US Army Signal Center
Smith, Mr. Alden	DISA Def Spectrum Office
Smith, Ms. Becky	ASD/NII/DCIO
Solee, Mr. Christopher	STRATCOM/J88G
Soltis, Ms. Maurita	ASD/NII/DCIO
Spencer, Maj Yessic	CENTCOM/J-6
Stimeare, COL Ronald	Army Net Ops & Security Ctr
Streeter, LCDR Vicky	OPNAV N71
Sullivan, Mr. Shelby	SAF/XCXA

Sunner, CAPT Dave	Navy NNCW
Talkington, LTC Darin	Joint Staff/J6C
Terry, Mr. Jeffrey	CENTCOM
Thomas, Col Howard	HQ USMC/C4
Thornton, Mr. Larry	Dynamics Research Corp.
Titone, Mr. Michael	
Turner, LCDR Charles	STRATCOM/J865
Van Dine, Mr. Wayne	NSA/IAD/CISSP
Walker, Mr. Donald	
Wallace, Ms. Angela	Booze Allen Hamilton
Walters, Mr. Robert	
Waters, LCDR Richard	JFCOM/J694
Watkins, Mr. Jonathan	SAF/XCIES
Wilcox, Lt Col Craig	Joint Staff/J3
Williams, Mr. Gary	HQDA/G-35/DAMO-SSP
Wise, Mr. Wayne	
Yarbourgh, Mr. Norman	ASD/NII
Young, Mr. David, Sr.	JFCOM
Zimmerman, Col Jean Christopher	JFCOM

APPENDIX D. Information Transport Enabling Construct

TABLE OF CONTENTS

1. PURPOSE

In order to support a robust Capabilities-Based Assessment (CBA) and advance the development and application of net-centric capabilities for the future Joint Force, the concept of a Net-Centric Operational Environment (NCOE) is presented in the *Net-Centric Operational Environment Joint Integrating Concept* (NCOE JIC) document. The NCOE is defined as the coherent application of Joint Net-Centric Operations (JNO) capabilities at the Joint Task Force-level and below in order to help achieve decisive outcomes in major combat operations and related scenarios.

Appendix D of the NCOE JIC document is this *Information Transport Enabling Construct*, a supporting document. Its purpose is to amplify how information transport will provide the NCOE's technical foundation. The future Joint Force, particularly "first tactical mile" users, requires a communications infrastructure that provides resilience, survivability and continuity even when the network is under extreme stress. This means an improved infrastructure and also, in response to rapid changes in the tactical and operational situation, the ability to manage that infrastructure dynamically.

This document explores *information transport* as a military function in the NCOE, characteristics of the future infrastructure, and how information transport can be used to solve technical and operational challenges. The timeframe is 8 to 20 years in the future, with an illustrative focus on 2015.

2. MILITARY PROBLEM

The NCOE JIC broadly defines the military problem for this construct: *the Joint Force and mission partners must have rapid access to relevant, accurate, and timely information, and also the ability to create and share the knowledge required to make superior decisions in an assured environment amid unprecedented quantities of operational data.*

A significant part of this problem's technical component relates to information transport. Therefore, *the future Joint Force, particularly first tactical mile users, requires a communications infrastructure that provides resilience, survivability, and continuity, especially while the network is under extreme stress. This not only calls for improved infrastructure, but also the ability to dynamically manage that infrastructure to rapidly support changes to the tactical and operational situation.*

Fully-networked forces require an assured communications infrastructure, providing robust connectivity to the farthest reaches of deployed warfighting nodes, weapons platforms, and assets for intelligence, surveillance and reconnaissance (ISR). The means of connectivity include terrestrial, satellite,

wired, cabled, wireless, optic, and radio frequency. They must facilitate the sharing of information, collaboration, and situational awareness of all forces deployed anywhere around the globe. This is in sharp contrast to today's currently constrained high bandwidth ISR data-links, which cannot always provide the large, time-sensitive data packages from repositories in the continental United States (CONUS) to joint forces either deploying or deployed.

Moreover, joint operations in austere locations—requiring continuous, assured communications for highly mobile users with small lightweight equipment—are currently not as well supported as will be needed in the future. The number, size, and weight of the current user's (i.e., the operator's) equipment and systems, and of general support equipment, prevent a single operator, and likewise a small expeditionary unit, from being able to operate autonomously. Current equipment size and capability do not meet the operational requirement for highly-versatile, highly-maneuverable lethal forces, nor for individuals with little or no combat support infrastructure or logistical tail support. This lack of assured communications for highly mobile forces on the move is a significant impairment to the networked force envisioned in the family of joint concepts.

3. SCOPE

"Information Transport" is broadly defined in terms of the ability to provide the physical communications media over which assured connectivity takes place, supported by switching and routing systems. This construct document describes how the NCOE's data will be electronically moved around a core network backbone to connected nodes (physically or virtually), thereby allowing for the negotiation and transfer of needed information to all echelons at any time.

This construct document also addresses the future assured communications infrastructure (terrestrial, satellite, deployed, wireless—i.e., switches, routers, transponders, terminals) that will provide for network connectivity from the sustaining base to the foxhole, with the primary focus linking the deployed operational and tactical environments. The concepts described in this document enable *applications* and *services* to physically connect and interact across the network, providing warfighters with timely access to mission-essential information. By applying these concepts, joint warfighters at every echelon can realize potentially unprecedented benefits from information (and knowledge) sharing, collaborative decision-making, data discovery, and other secure access to real-time or near real-time information.

The NCOE JIC's timeframe is 8 to 20 years in the future. For continuity, the document's illustrative CONOPS and its three enabling constructs, including this one, all focus on the year 2015. See the NCOE JIC and the *Net-Centric Environment Joint Functional Concept* (NCE JFC) document for information about relevant assumptions and risks.

4. CENTRAL AND SUPPORTING IDEAS

4.1 Central Idea

Information Transport provides the foundation of the Net-Centric Operational Environment by combining assured, timely, resilient, and survivable connectivity with dynamic network management capabilities focused on "first tactical mile" users.

Joint Task Force (JTF) elements are increasingly facing unfamiliar situations within complex, uncertain, rapidly changing operating environments. This necessitates information transport capabilities that:

- Adapt to the changing priorities, policies, and requirements generated by the information moving across it.

- Connect groups as well as individuals in a global network, removing the barriers imposed by geography (natural and man-made) and by physical movement.

- Regulate network connectivity and data visibility of individuals based upon their clearance level and their role in the Joint Force or a mission partner.

- Dynamically adjust to support multi-level security, both as the roles of actors change and as the mission of the Joint Force and its mission partners dictate.

- Support persistent and dynamic shared space.

In the future various commercial and governmental agencies are expected to vie with JTF elements for the same limited radio frequency (RF) spectrum. Therefore, the JTF must have the ability to dynamically manage the electro-magnetic spectrum wherever and whenever deployed. Additionally, beyond dynamic management, we must look at technologies that allow for more utilization of this already limited resource. Effective predictive network management is necessary to assure communications in a highly dynamic joint warfighting environment. The effectiveness of network management will be measured in terms of availability and the reliability of the joint networked operational environment across all domains in adherence to agreed-upon service levels and policies. By combining effective network management with an assured communications infrastructure, the Joint Force can achieve information transport capabilities that meet its needs from the "first tactical mile" to the national level.

4.2 Supporting Ideas

4.2.1 Assured Communications Infrastructure

An assured communications infrastructure can provide the confidence that groups and even individuals can operate effectively in spite of barriers imposed by geography (natural and man-made) and physical movement. For the purposes of this construct, sufficiency is an important element of assured communications, with a sufficient amount of throughput delivered to joint warfighters when and where needed. Near perfect connectivity, coupled with resilient applications and services, is the foundation on which assured communications infrastructure must be set. This calls for an information transport connectivity capable of providing the future Joint Force with the ability to rapidly and effectively connect, transact, discover, and interact across all echelons of command, and with mission partners, in support of major combat operations and other joint operations. The Joint Force must be capable of operating across the strategic, operational, and tactical continuum with a set of integrated, robust, and responsive information networks.

Spectrum access in, use of, and control of space are fundamental to this strategy, including the reliable and affordable transport of payloads and an ability to protect assets in orbit and on the ground. Dynamic management and reallocation of the RF spectrum is part of laying the foundation for assured connectivity. Coupling spectrum management with technologies that more thinly slice the spectrum "pie," while affording spectrum-resilient systems to deployed warfighters to internally mitigate the effects of spectrum congestion, will complete the cycle in providing assured connectivity.

Ultra-wideband technologies will provide additional information transport capabilities. An ultra-wideband transmitter generates signals of very large bandwidths (in excess of gigahertz) by transmitting nanosecond or sub-nanosecond pulses at baseband in a randomized fashion. As a result, an ultra-wideband system is, in reality, a baseband spread spectrum (SS) system (often well below the random noise level) with a very large spreading gain. Many of the characteristics and advantages of conventional SS communications carry over to ultra-wideband. For instance, a typical ultra-wideband system is capable of supporting multiple users, robust against jamming and interference, robust against multi-path fading, and suitable for applications requiring low probabilities of interception and detection (LPI/LPD).

Laser communications is another means of achieving very high capacity communications links with minimal LPI or LPD. This means is particularly useful in environments where precipitation is minimal, and becomes another means of exploiting MILSATCOM assets to support the theater warfighter.

4.2.2 Effective Network Management of Information Transport

Adaptive network management will provide the Joint Force with flexibility by optimizing system and network resources in an ever-changing operational environment. The ability of the future physical network to support rapid, dynamic network access and reconfiguration reinforces adaptive network management to provide a new level of agility to the Joint Force.

Management functionality works in conjunction with information assurance to ensure availability of the enterprise services and applications provided through a hosting environment. Performance of essential tasks must be integrated across the strategic, operational, and tactical levels, and across all Department of Defense (DoD) warfighting, intelligence, and business domains for mission objectives to be achieved. Network management in an NCOE-enabled Joint Task Force must remain dynamic. This dynamic network management is the result of fielded tools and empowered network warfighters having situational awareness of the network and the ability to quickly effect the reallocation of resources to support network events and/or maneuver the network to support changing operational requirements. Network management must provide visibility and control over systems and network resources while anticipating and mitigating the effects of network degradation, outages and attacks. Centralized control and management for an ever-more complex information environment will involve the application of direction to subordinate network management nodes.

Three desired effects are further discussed below:

- **Assured Network Availability**: Provides visibility and control over system and network resources. Resources are effectively managed and problems are anticipated and mitigated. Proactive actions are taken to ensure the uninterrupted availability and protection of system and network resources. This includes providing for graceful degradation, self-healing, fail over, diversity, and elimination of critical failure points.

- **Assured Information Protection**: Protection for the information passing over networks from the time that information is stored and catalogued until it is distributed to users, operators, and decision-makers.

- **Assured Information Delivery**: Provides information to users, operators, and decision-makers in a timely manner. The networks are continuously monitored to ensure that the information is transferred within the correct response time and that the throughput, availability, and performance all meet the user's needs.

The method for service assurance in a collaborative, net-centric environment is to establish operational thresholds, compliance monitoring, and a clear understanding of the capabilities between enterprise service/resource providers and consumers through Service-Level Agreements (SLAs). Proper instrumentation of the NCOE will enable monitoring of SLA adherence, and enable timely decision-making, service prioritization, resource allocation, root cause, and mission impact assessment. To enforce compliance, the SLAs and also Tactics, Techniques, and Procedures (TTPs) will be formalized with appropriate implementation policies.

Adaptive network management will be especially significant for the Joint Force for "first tactical mile" communications, especially if the adversary employs various forms of electronic warfare (EW) to attack the RF spectrum. Once detected by the warfighter or spectrum manager, electronic countermeasures must be employed. These will include modulation techniques for increased robustness, such as combinations of Code Division Multiple Access, Time Division Multiple Access, and Frequency Division Multiple Access. In addition, for forward forces that require more low probability of intercept and low probability of detection, other forms of modulation exist for spread spectrum connectivity, such as pseudo-random phase and frequency hopping.

4.3 Application of the Central and Supporting Ideas

The Joint Force's ability to operationally adapt will depend upon the capability to quickly *establish an information environment,* as articulated in the NCE JFC and the NCOE JIC. This involves the establishment of criteria processes and procedures for the storing and sharing of data/information, including sharing across different environments and supporting *multiple changing communities of interest*. The ever-changing situation and high operational tempo will require a fluid allocation of resources in accordance with shifting priorities and the command intent (i.e., dynamic, priority-based resource allocation).

Adaptive network management of an assured communications infrastructure can be best explained against the backdrop of an operational engagement. Imagine a battle plan involving a two-pronged attack against a defending opponent. During the course of executing this two-pronged attack, planning assumptions regarding the enemy's anticipated force strength and disposition prove to be inaccurate. What was initially the priority attack must now become the supporting effort to the second prong. Prioritization of network resources must therefore shift to meet the changed informational and decision-support demands. The relevant communities of interest (COIs) may not change significantly but the prioritization within those COIs changes markedly. How well can the network adapt to these changes in prioritization? Network managers must stay engaged with those COIs in order to understand the changing operational environment and reshape the information environment to

support. Figure D-1, below, shows such a flow of actions associated with the sustainment of assured connectivity while maneuvering the network to support the emerging operation need.

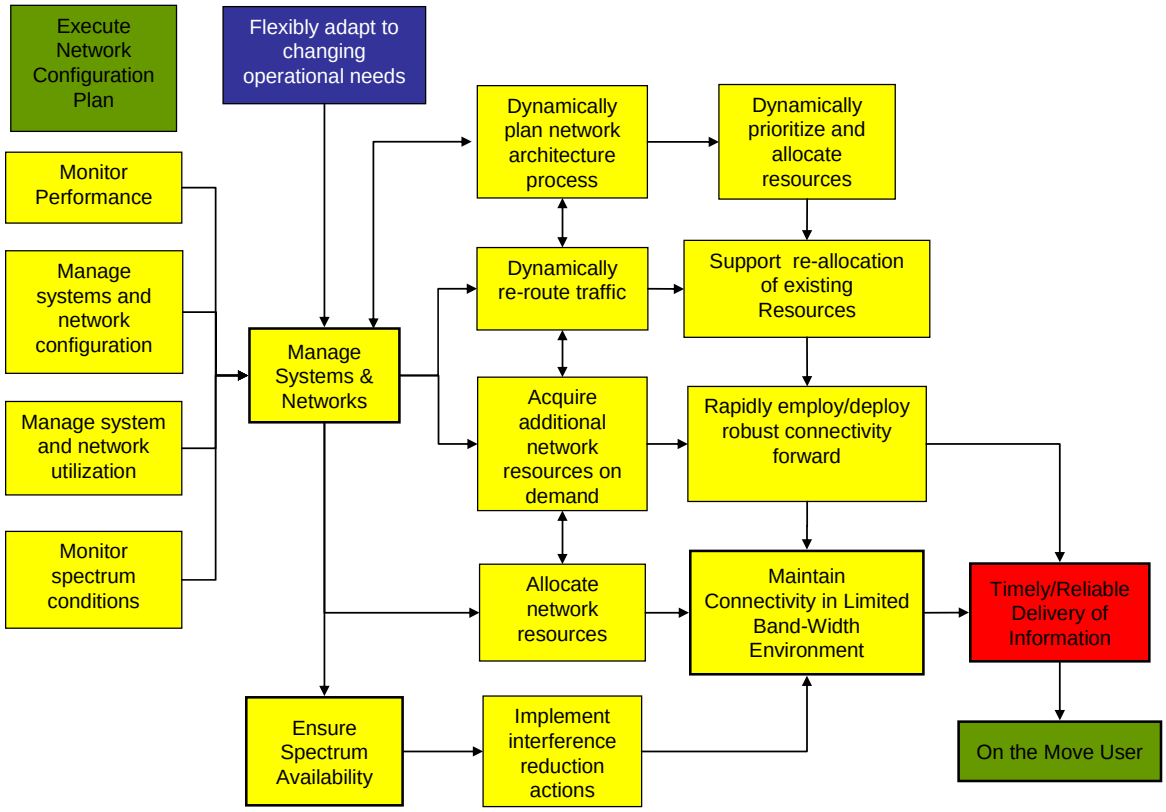


Figure D-1. Dynamic Network Management

As part of establishing the information environment, network managers responded to the needs emanating from within the COIs as determined by prioritization of effort and resources. The robustness of a specific subscriber service interface will be provided, commensurate to the subscriber's relative importance to the COI. With the shift in priorities of effort, so too will shift priorities of resources. Demands for updated imagery, reallocation of unmanned aerial vehicle (UAV) feeds, increased close air support, expanded indirect artillery, etc., will all place a greater demand upon the selected COI member's interface links and points.

Network managers recognize that new priorities were set and quickly analyze the network to determine anticipated data choke-points for decision-makers across the enterprise. A tool-kit of sophisticated network management tools assist the management nodes in support of *dynamic, priority-based resource allocation*. For changes to the network which cannot be done from the theater level, the nature of the changes that need direction and guidance are relayed to the subordinate network management nodes.

5. CAPABILITIES, TASKS AND STANDARDS

This section describes the NCOE's Information Transport enabling capabilities and tasks as derived and modified from those in the NCE JFC. See the NCOE JIC for a discussion of the applicable conditions, along with the processes used to develop and refine the tasks and standards. Collectively, these operational tasks and sub-tasks align with the overarching capabilities of: (1) the *ability to install and deploy scalable and modular critical network elements;* (2) the *ability to optimize network functions and resources;* and (3) the *ability to maintain and survive;* and (4) the *ability to transport information end-to-end.*

5.1 Capability: *Ability to install and deploy scalable and modular critical network elements*

Since the net-centric model depends on having connectivity where and when required, the network must be capable of forward deployment and be tailorable to mission requirements. It must be capable of dynamic reconfiguration as missions/tasks change, and be functional in harsh and/or unimproved infrastructure environments. Relevant to this Information Transport capability are the following tasks:

- *Rapidly deploy/employ robust connectivity forward.*
- *Ability to provide global information transport services.*
- *Acquire additional network resources on demand.*
- *Inform/Update chain of command of network status.*
- *Provide comm links services (non-networked).*
- *Tailor to specific capabilities.*
- *Function under a range of infrastructure and ROE* [Rules of Engagement] *constraints.*
- *Dynamically plan network architecture development processes.*
- *Integrate diverse systems (coalition, interagency and NGOs).*
- *Establish nodes where needed.*
- *Design for rapid insertion and new technology.*
- *Operate without geographic constraints.*
- *Provide ad hoc coalition connectivity.*
- *Connect all assets.*

5.2 Capability: *Ability to optimize network functions and resources*

Relevant to this capability are the following tasks (•) and sub-tasks (o):

• *Ensure spectrum availability.* Once in place, the network must be capable of operating regardless of the radio frequency (RF) spectral environment, as well as dynamically allocate (or reallocate) resources to support all operations and

transitional states along the range of military operations (ROMO). Relevant to this task are these sub-tasks:

- *Monitor spectrum conditions.*
- *Analyze electromagnetic spectrum.*
- *Implement interference reduction actions.*
- *Select radio frequencies.*
- *Report spectrum use status.*

• *Execute network configuration plan.* This task means putting into action a network plan for dynamic allocations of resources, regardless of the geography (distance, obstructions, etc.) and in support all of operations and transitional states along the ROMO. The plan (i.e., the task) must manage access to the network and its associated data, providing ad hoc coalition and inter-agency connectivity while also denying access as necessary. The network must provide continuous, rapid and error-free delivery of information.

• *Manage systems and networks.* Once deployed, the network must maintain service while under both physical attack and information attack. It should degrade gracefully; that is, it should 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. Relevant to this task are the following sub-tasks:

- *Manage system and network configuration.*
- *Establish system and network configuration.*
- *Create baseline network maps.*
- *Set parameters and thresholds.*
- *Manage IP addresses.*
- *Set network time.*
- *Discover system and network configuration.*
- *Monitor performance—Quality of Service.*
- *Analyze performance trends.*
- *Manage system and network utilization.*
- *Dynamically prioritize and allocate resources.*
- *Dynamically re-route traffic.*
- *Analyze system and network use.*

• *Perform network control.* It is essential to manage the network to ensure that the greatest capability is provided to the warfighter. This means monitoring, tuning, repairing and optimizing the network. Relevant to this task are these sub-tasks:

- o *Detect fault condition.*
- o *Perform fault trend analysis.*
- o *Perform containment response.*

5.3 Capability: *Ability to maintain and survive*

Relevant to this capability are the following tasks (•) and sub-tasks (o):

• *Provide network situational awareness.* Network managers must have the same visibility of the network's status that a ground commander would expect for his assigned forces during an operation. This task therefore refers to monitoring, tuning, repairing and optimizing the network. The following are sub-tasks:

- o *Maintain cyber-situational awareness and network defense.*
- o *Project cyber-situational events.*
- o *ID and maintain awareness of all nodes at all times.*

• *Support all operational and transitional states along the ROMO.* This task involves putting into action dynamic allocations of resources to support capabilities such as "operate regardless of geography (distance, obstructions, etc.)", and "support all operations and transitional states along the ROMO". The network must be capable of dynamically rerouting services as the information environment adapts to the operational environment. A relevant sub-task is:

- o *Negotiate Quality of Service requirements.*

• *Maintain network capabilities and ensure survivability.* Relevant sub-tasks:

- o *Restore/Recover.*
- o *Manage continuity and restoration operations.*
- o *Degrade gracefully and contain cascade failures.*
- o *Continue essential operations in degraded environment.*
- o *Exploit network compromises.*
- o *Provide for self-healing/restoration of network upon degradation.*

5.4 Capability: *Ability to transport information end-to-end*

Information must be assured throughout its life-cycle, particularly during transport. Network managers must be able to monitor the network with smart tools to ensure that information flows match the mission priorities. For this capability the following are relevant tasks:

- *Transmit information.*
- *Perform retransmission/relay/gateway services.*
- *Receive information.*
- *Manage service delivery.*
- *Prioritize service delivery.*
- *Control information flow precedence.*
- *Manage information flow access.*
- *Monitor resource use.*
- *Deliver information.*
- *Select distribution channel.*
- *Invoke transport services.*
- *Manage information access.*

6. IMPLICATIONS

At lower echelons, especially at the "first tactical mile," progressively less distinction will exist between unit-specific platforms and the systems used to connect to broader service in the NCOE. The ability to access the network and to utilize network services will require unit-specific platforms which can also provide network connectivity. The capabilities will provide accelerated decision-making and a significant tactical advantage over the adversary. NCOE capabilities will enable information and decision superiority. New systems and processes alone will not ensure success, however. Joint/Coalition force elements must also develop new doctrine, new organizational relationships, and new training, along with new decision-making and command-and-control tools to achieve decision superiority. Physical transport should, therefore, be viewed as one of a number of enablers that enhance our ability to adapt to new and changing situations.

7. CONSTRUCT DEVELOPMENT AND EXPERIMENTATION

See the NCOE JIC for specific development and experimentation information.

APPENDIX E. Enterprise Services Enabling Construct

TABLE OF CONTENTS

1. PURPOSE

In order to support a robust Capabilities-Based Assessment (CBA) and advance the development and application of net-centric capabilities for the future Joint Force, the concept of a Net-Centric Operational Environment (NCOE) is presented in the *Net-Centric Operational Environment Joint Integrating Concept* (NCOE JIC) document. The NCOE is defined as the coherent application of Joint Net-Centric Operations (JNO) capabilities at the Joint Task Force-level and below in order to help achieve decisive outcomes in major combat operations and related scenarios.

Appendix E of the NCOE JIC document is this *Enterprise Services Enabling Construct*, a supporting document. Its purpose is to refine, conceptually, those identified capabilities specific to providing enterprise services for all warfighters, as required for Joint Net-Centric Operations (JNO) 8 to 20 years in the future. The illustrative focus is the year 2015. This supporting document, along with the NCOE JIC, also refines the conditions, tasks, and standards necessary to conduct a CBA to facilitate the evaluation of joint initiatives.

2. MILITARY PROBLEM

The NCOE will address the following military problem: *The Joint Force and mission partners must have rapid access to relevant, accurate, and timely information, and also the ability to create and share the knowledge required to make superior decisions in an assured environment amid unprecedented quantities of operational data.*

To enable information sharing and achieve information superiority, the NCOE will utilize enterprise services for foundational capabilities. The current information environment can be characterized as platform-centric. Specifically, information and information systems have been designed with producer and organizationally unique terminology and symbology. Previous attempts to solve the Department of Defense (DoD) data interoperability problem have focused on standardized data elements, minimized duplication of data elements across the Department, and reduced need for data element translation. However, this traditional approach, has proven to be too cumbersome to implement across an enterprise of the Department's scope.

Enterprise services provide the common foundation for enabling the future Joint Force by providing consistent, assured, timely, robust, and survivable information services to modular forces in the full spectrum of operational and environmental conditions. The *Net-Centric Environment Joint Functional Concept* (NCE JFC) document identifies Communities of Interest (COIs) as a critical principal for sharing situational awareness and collaborating. The COI approach to data and information interoperability focuses the scope of data

standardization to achievable levels, but necessitates the translation of data between producers and consumers using a COI common vocabulary.

3. SCOPE

In this enabling construct and in the NCOE JIC generally, the terms ”enterprise services” or ”services” for short both refer to enterprise-wide capabilities, accessed primarily by other services or applications. Enterprise services can include both core services, as well as common services for COIs. This document focuses on the foundational, core services. It describes the enterprise, or common, domain-neutral services that provide the foundation for discovering, accessing and using information assets in support of the Joint Force. Those foundational services also support the discovery, access, and use of operational capabilities (i.e., service-based analysis, situational awareness, and decision-support applications).

Users normally do not directly interface with services: users interface with the network via applications. This involves an information-sharing environment consisting of the Joint Force and its mission partners, including interagency, multinational partners, non-governmental organizations, industry, and academia. Additionally, this environment has the characteristics of:

- dynamic organizational relationships and information exchange requirements;

- a fluid network topology, including global span, for a heterogeneous operating environment; and

- multi-faceted information security requirements for a “need to share” information policy.

DoD’s Global Information Grid Enterprise Services (GIG ESS) strategy was introduced in the *Net-Centric Operations and Warfare Reference Model* (NCOW RM), version 1.0. This strategy addresses an environment wherein services are loosely coupled and which are no longer bound to systems. It is characterized by a Service-Oriented Architecture (SOA) comprised of service and/or information producers and consumers. Producers create and make available services and/or information within the network. Consumers can then discover, understand, and use the provided information and/or services. Agreements governing the use of information and services between users and providers are considered Service-Level Agreements (SLAs). SLAs provide an integrated knowledge management (KM), network management (NM), and information assurance (IA) basis to manage and use these enterprise resources at all levels.

For the above environment, this enabling construct identifies the capabilities, and their required tasks, associated with posting, publishing, discovering, and translating information. Additionally, this construct describes the technical capability to enable collaboration among mission partners; support the transition to and integration of service-based applications; and implement role-based information sharing policies.

The NCOE JIC's timeframe is 8 to 20 years in the future. For continuity, the document's illustrative CONOPS and its three enabling constructs, including this one, all focus on the year 2015. See the NCOE JIC and the separate NCE JFC for information regarding relevant assumptions and risks.

4. CENTRAL AND SUPPORTING IDEAS

4.1 Central Idea

The central idea of this construct is that Enterprise Services provide the common foundation for developing pervasive knowledge among Communities of Interest (COIs) by providing consistent, assured, timely, robust, and survivable information services to deployed forces in the full spectrum of operational and environmental conditions.

Enterprise services support decisive *levels of shared knowledge* by enabling the Joint Force to share information and to interact with heterogeneous data, applications, and other services. Enterprise services provide the pervasive network functions which accept a request and return a response through an interface with a user or another service, such as collaboration, messaging, or information discovery and storage. Enterprise services also provide the foundational capabilities to discover information, store information, and exchange information. They establish collaboration sessions, translate information between different vocabularies, and customize information presentation. Enterprise services provide the common mechanisms for diverse Communities of Interest, or COIs, to define member roles and authorizations, manage information access, and manage shared space information content.

COIs will bound the interoperability problem to a set of producers and consumers who focus upon developing agreed-to information terms, definitions and semantic meanings. COIs serve two basic functions in the implementation of information sharing: (1) establish a common vocabulary for shared understanding between information providers and consumers; and (2) establish a shared information space consisting of authoritative information sources, information, and information services. In the terms of the DoD Net-Centric Data Strategy, data must be visible, accessible, understandable, trusted, interoperable, and made available in response to user needs. Although a COI may be formed just to establish a common vocabulary, this document is

oriented to an operational COI comprised of three components: a common vocabulary, authoritative sources, and a shared information space.

A common vocabulary establishes the understandability and interoperability of the data and information either physically stored by the COI or virtually established in distributed physical storage repositories. A COI designates authoritative sources for their data and information to establish trust and to ensure availability of the right information for the enterprise. The shared space establishes COI data and information visibility and accessibility. Data and information in the shared space will have metadata (i.e., labels) called "tags," which are data about the data and the information. The tags enable the discovery of information and provide other important attributes about the data such as source, classification, currency, etc. Access will be controlled through establishment of COI "roles." These roles define the publication, subscription and access authority of COI members.

COIs, to operate, will rely heavily upon enterprise services, both within the COI and with other COIs. Enterprise messaging services will enable any user in the COI to communicate digitally. As COIs generate and update their data and information, enterprise services will provide the foundational capabilities to discover necessary information in a timely fashion and also to store and exchange information. Further, because the COI will be operating in a dynamic environment, static data translation approaches will not be able to provide the necessary functionality. Enterprise mediation services will dynamically translate information between disparate formats, for display and analysis, using the well-formed vocabularies described above. Collaboration will be possible across echelons via enterprise collaboration services that establish collaboration sessions, translate information between different vocabularies and customize information presentation. Enterprise services will also provide the common mechanisms for COIs to define member roles and authorizations, manage information access, and manage shared space information content. The provisioning of enterprise services is a mixture of centralized, federated, and distributed deployments to maximize information access, assure information protection and achieve machine-to-machine interoperability.

4.2 Supporting Idea: *Service-Level Agreements supported by Service-Oriented Architectures*

For information to be developed, translated into knowledge, and used, COI members must have the foundational capabilities to discover it, store it, exchange it, collaborate using it, manage access to it, translate between different vocabularies and styles of it, and customize its presentation. Each COI member must also be able to collect, process, manipulate and analyze information. In the past, an information consumer within a COI would use an application and associated services to provide automated support in performing

these tasks. This was done through a formal and rigid coupling of operator processes, data structures and information exchanges. This systems-based architecture, with its rigid interfaces, is no longer suitable for the increased demands of fluid information sharing. Industry has already identified this shortfall and now meets its own dynamically changing informational needs by creating a common and consistent information-sharing space using a Service-Level Agreement (SLA), supported by a Service-Oriented Architecture (SOA). SLAs describe the expected performance and behaviors which users can expect from information providers. SLAs are, in large part, determined by the network's capacity and by the criticality of the user's request. Required standards of performance are then identified, along with minimum- and maximum-performance standards. SLAs will be developed across COIs for managing expectations and providing the basis for network management.

A Service-Oriented Architecture is a system for linking information resources on demand: information resources are made available to other participants in the network as independent services, accessed in a standardized way. This provides for a more flexible, loose coupling of resources than exists in traditional systems architectures. A service is a discoverable software entity with well-defined interfaces which are implementation-independent, interacting with applications and other services through a loosely coupled, message-based communication model. In order to support these SOAs, enterprise services will be provisioned using a mixture of centralized, federated, and distributed deployments to maximize information access, assure information protection, and achieve machine-to-machine interoperability.

Services are logical entities, the contracts defined by one or more published interfaces. A *service provider* is the software entity that implements a service specification. A *service consumer* (or *requestor)* is the software entity which calls a service provider (makes a request). A *service consumer* can be an end-user application or another service. A *service locator* is a specific type of service provider that acts as a registry and enables the lookup of service provider interfaces and service locations. A *service broker* is a specific type of service provider that can pass along service requests to one or more additional service providers.

An SOA is a design style for building flexible, adaptable, distributed-computing environments which, fundamentally, are about the sharing and re-use of functionality across diverse applications. Key operational benefits of an SOA include: (1) the ability to separate the rigid data structures in an application from the information exchange between information providers and consumers, and thereby greatly improve interoperability by enabling shared understanding; and (2) greatly improve the flexibility and agility of the information sharing environment by reducing the time and cost to adapt to changes in applications (and their associated data structure), to insert new technology, and to make

dynamic organizational changes. Additionally, an SOA facilitates the re-use of an in-place information infrastructure.

4.3 Application of the Central and Supporting Ideas

Notionally, after an attack by the adversary upon a neighboring state, the Joint Task Force (JTF) Commander decides that combined intelligence assets are required to assess the situation. Intelligence officers receive this order and then immediately rely on the *use of a standard computing environment* to *provide the shared information environment* and *to provide discovery* needed for the operation.

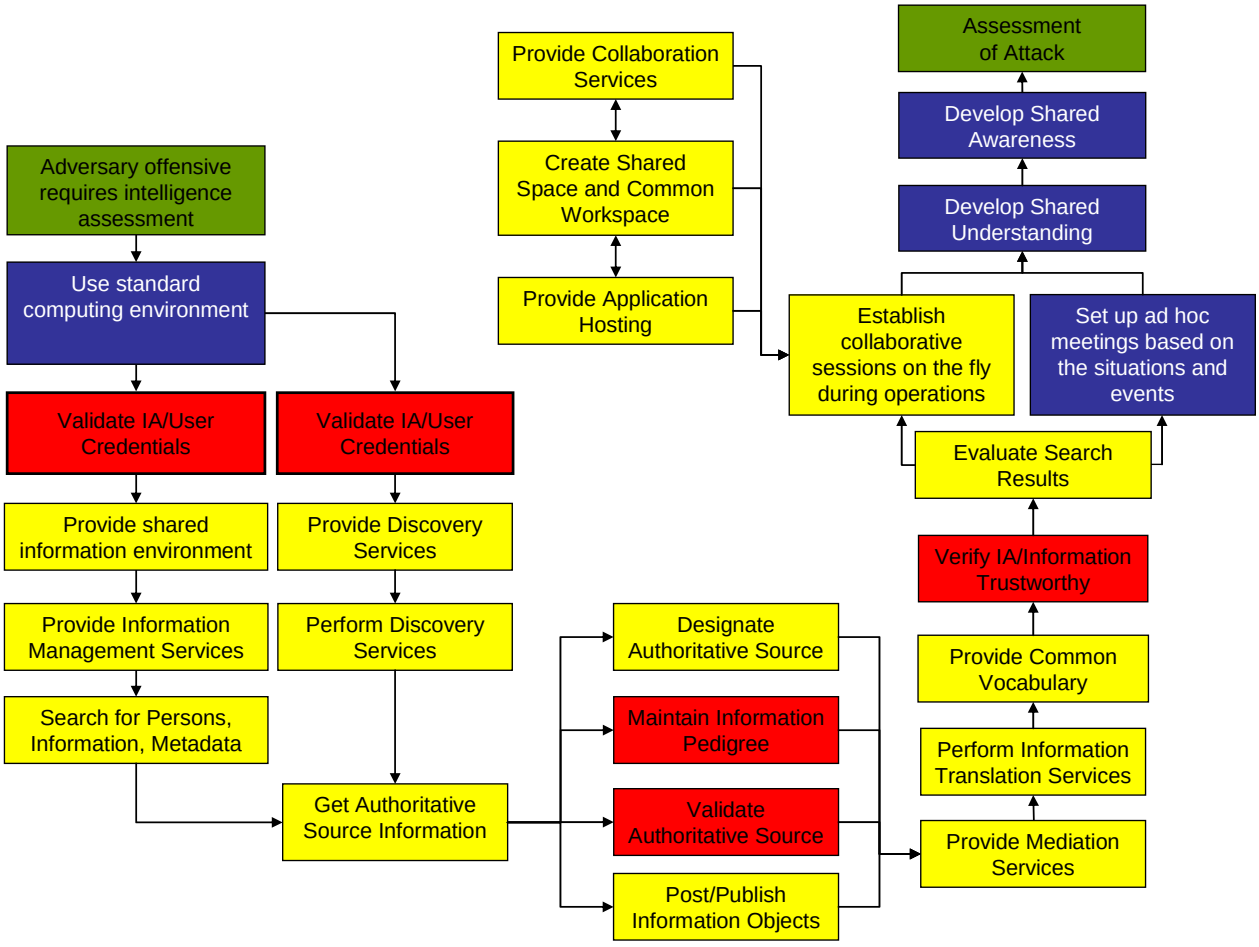


Figure E-1. An Intelligence Reassessment

Information management services are provided to ensure the integration of intelligence, command and control, and combat service support. The shared information environment allows the Intelligence Community to access emerging information derived from *searches for persons, information, and metadata*, as aided through the *performance of discovery services*. *Getting this authoritative*

information and *performing mediation services*, *information translation services* and *providing a common vocabulary* allows the intelligence officers to overcome minor doctrinal differences and to share information between disparate applications, interpreting this timely information within the bounds of the current situation. This interpretation, however, is not done independently but collaboratively, as intelligence personnel *establish collaborative sessions on the fly* and *set up ad hoc meetings based on the situation* when deemed helpful and/or necessary. These collaborative sessions allow for the better *evaluation of search results*, resulting in a more accurate and more actionable attack assessment. Information trustworthiness is validated and assured by overarching Information/security services.

5. CAPABILITIES, TASKS AND STANDARDS

This section lists the NCOE's enterprise services-related capabilities and tasks, derived and modified from capabilities and tasks original to the NCE JFC. See the NCOE JIC for a discussion of the applicable conditions, as well as the processes used to develop and refine the tasks and standards.

5.1 Capability: *Ability to establish an information environment*

This capability involves the establishment of criteria processes and procedures for the storing and sharing of data/information, including to share across different environments, and to support multiple, changing COIs. 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).

Relevant to this capability are the following tasks (•) and sub-tasks (o):

- *Provide application-hosting environment*. Relevant sub-tasks:
    - o *Manage application hosting services.*
    - o *Provide standard computing environment.*
    - o *Provide server administration services.*
    - o *Run application.*
    - o *Exploit network compromises.*
    - o *Provide for self-healing/restoration of network upon degradation.*
    - o *Operate the application hosting environment.*
- *Provide subscriber service provider interface*. Relevant sub-tasks:
    - o *Manage subscriber's environment.*
    - o *Provide subscriber hardware platform.*
    - o *Provide subscriber operating systems.*

o *Run client environment applications.*

• *Customize subscriber presentation.*

• *Maintaining information and knowledge connectivity in limited bandwidth environment.*

5.2 Capability: *Ability to establish appropriate organizational relationships*

These tasks focus on establishing the mechanisms that will enable the "operationalization" of COIs. Relevant to this enterprise services capability is the following task (•), its sub-tasks (o), and their sub-sub-tasks (--):

• *Provide COI environment.*

o *Get authoritative source information.*
-- *Validate authoritative source.*
-- *Designate authoritative sources.*
-- *Create subscription.*
-- *Maintain pedigree of information.*
-- *Post information objects.*
-- *Publish information objects.*
-- *Advertise information, products, services.*

o *Provide shared information environment.*
-- *Create shared space.*
-- *Create common workspace.*
-- *Provide COI management resources.*

• *Discover organizational structure.*

5.3 Capability: *Ability to collaborate*

These tasks establish the mechanisms for pervasive collaboration in the networked environment across echelons as necessary. They are listed as tasks (•), sub-tasks (o), and sub-sub-tasks (--):

• *Establish a collaborative session.*

o *Provide collaboration services.*
-- *Manage collaborative services.*
-- *Determine resource availability.*
-- *Provide collaboration communication capability.*
-- *Provide shared interactive capability.*

-- *Conclude collaboration.*

o *Provide collaboration management.*
-- *Provide named group association.*

o *Maintain a consistent collaborative session (i.e., always on).*

- *Establish schedule of recurring meetings.*
- *Establish a role-based, adaptable, tailorable individual knowledge framework.*
- *Know availability of knowledge assets.*
- *Set up ad hoc meetings based on the situation and events.*
- *Establish collaborative sessions "on the fly" during operations.*
- *Maintain traceability of collaborative process.*
- *Establish ownership rights on collaborative products.*

5.4 Capability: *Ability to identify/store/share/exchange data/information*

These tasks refer to the ability to share and exchange information. They are listed as tasks (•), sub-tasks (o), and sub-sub-tasks (--):

- *Provide discovery services.*

  o *Manage discovery services.*
  o *Formulate discovery search.*
  o *Perform discovery search.*
  o *Search for services.*
  o *Search for information.*
  o *Search for persons.*
  o *Search for metadata.*
  o *Evaluate search results.*

- *Provide messaging services.*

  o *Manage messaging services.*
  -- *Manage message boards.*
  -- *Manage data links.*
  -- *Manage email.*
  -- *Manage record traffic.*

- o *Provide asynchronous message capability.*
  - -- *Provide store and forward message service.*
  - -- *Provide organizational messaging services.*
  - -- *Provide message posting services.*
  - -- *Provide inter-application messaging services.*

- o *Provide synchronous* [real-time] *message capability.*
  - -- *Provide instant messaging services.*
  - -- *Provide data link message capability.*
  - -- *Provide organizational messaging services.*

- o *Provide streaming video capability.*

- o *Provide information storage services.*

- o *Establish criteria for storing and sharing.*
  - -- *Manage storage services.*
  - -- *Store information.*
  - -- *Retrieve stored information.*
  - -- *Replicate data.*

5.5 Capability: *Ability to process data and information*

This capability, as it applies to enterprise services, refers to mediation. Below is a task (•), its sub-tasks (o), and its sub-sub-tasks (--):

- • *Provide information mediation services.*

  - o *Manage mediation services.*

  - o Correlate information.
    - -- *Identify product types to correlate.*
    - -- *Create correlated product.*

  - o *Provide information transformation.*
    - -- *Format/Re-format information.*
    - -- *Filter information.*
    - -- *Aggregate-Fuse information.*
    - -- *Identify information voids/deficiencies.*

  - o *Perform translation services.*

5.6 Capability: *Ability to find useful information*

This capability, as it applies to enterprise services, refers to search and retrieval. It involves the following task (•):

- *Provide context-relevant search and retrieval services.*

5.7 Capability: *Ability to optimize network functions and resources*

This capability, as it applies to enterprise services, monitors information flow. It involves the following task (•) and sub-task (o):

- *Provide IM services.*
  - o *Monitor information flow.*

5.8 Capability: *Ability to maintain and survive*

This capability refers to the management of enterprise services. Below is a task (•), its sub-tasks (o), and its sub-sub-tasks (--):

- *Manage enterprise services.*
  - o *Manage information access.*
    - -- *Manage product descriptions.*
    - -- *Manage subscriber IDM profile.*
    - -- *Manage IDM access controls.*
    - -- *Provide subscriber notification.*
  - o *Manage information delivery.*
    - -- *Check subscriber profile.*
    - -- *Prioritize service delivery.*
    - -- *Optimize resource use.*
    - -- *Provide negotiation services.*
    - -- *Provide information management support services.*
  - o *Provide smart push.*
  - o *Provide enterprise information catalogue.*

6. IMPLICATIONS

It is important that enterprise service capabilities support the exchange of information between producers and consumers while leveraging information assurance/security capabilities to protect that information from unauthorized

use or access. These capabilities will allow both the user and information systems to find (discover) and access relevant information, expose the information they produce (post or publish) for others to discover, and collaborate in a much more effective manner. The services capabilities will provide a vision of a fully integrated computing network that includes the use of laptops, servers, handheld devices, programs, applications, and network equipment, all working together.

7. CONSTRUCT DEVELOPMENT AND EXPERIMENTATION

Experimentation for enterprise services should focus on the implementation of two services-related goals: (1) increasing the data that is available to communities or the enterprise, and (2) ensuring that data is usable by both anticipated and unanticipated users and applications. These goals, and the approaches discussed in Section 4, pertain to all legacy and new data assets, such as system files, databases, documents, official electronic records, images, audio files, web-sites, and data-access services, in the Department of Defense, including DoD intelligence agencies and functions.

See the NCOE JIC for a general discussion of further concept development and experimentation.

APPENDIX F. Applications Enabling Construct

TABLE OF CONTENTS

1. PURPOSE

In order to support a robust Capabilities-Based Assessment (CBA) and advance the development and application of net-centric capabilities for the future Joint Force, the concept of a Net-Centric Operational Environment (NCOE) is presented in the *Net-Centric Operational Environment Joint Integrating Concept* (NCOE JIC) document. The NCOE is defined as the coherent application of Joint Net-Centric Operations (JNO) capabilities at the Joint Task Force-level and below in order to help achieve decisive outcomes in major combat operations and related scenarios.

Appendix F of the NCOE JIC document is this *Applications Enabling Construct*, a supporting document. Its purpose is to explore applications as a military function in the NCOE, their characteristics, and how they can be used to solve technical and operational challenges. Several representative examples of applications are presented. This document's primary goals include: identifying applications as a key component of the NCOE, explaining how applications will employed in a Service-Level Agreement (SLA) arrangement, and identifying application-related conditions, tasks, and standards required to conduct a follow-on CBA.

2. MILITARY PROBLEM

The NCOE will address the following military problem: *The Joint Force and mission partners must have rapid access to relevant, accurate, and timely information, and also the ability to create and share the knowledge required to make superior decisions in an assured environment amid unprecedented quantities of operational data.*

Currently, applications are closely tied to individual legacy systems, aligned and dependent upon specific computer architectures unique to each system and largely platform-dependent. These systems have a marginal capacity to share data and functionality, having been designed with the doctrine of the specific military Service embedded in the system architecture, making it difficult to evolve with changes in joint doctrine, different technologies, and new operational capabilities. Future applications must support both customization of individual user information access and display, and the full interoperability of data across the Joint Force.

3. SCOPE

Although focused at the level of the Joint Task Force (JTF) Headquarters and below, the scope of this enabling construct document extends vertically from the strategic level through the tactical layers and also horizontally across communities. The applications addressed apply to both dimensions, enabling organizations and individuals to share mission-specific services and data

across the entire Department of Defense (DoD) enterprise information environment.

Applications provide two distinct military functions: (1) the user's network interface, and (2) access to enterprise resources, including enterprise services, within a configuration specific to a Community of Interest (COI). Applications can be available locally (within the local network) or take the form of a software package that is based upon a Wide Area Network (WAN) and which interfaces directly with JTF decision-makers and COIs for mission-specific tasks or processes. These functional tasks can vary from intelligence, to logistics and personnel administrative-support functions, to more traditional command-and-control (C2) functions. For each COI in the NCOE, application functionality will be provided to the operational user in a manner independent of platform or location—via NCOE networks and services, with provisions for low-bandwidth and disconnected operations.

Employed within an integrated framework of knowledge management (KM), network management (NM), and information assurance (IA), applications in the NCOE provide an important degree of resilience and survivability for the local user. Enterprise services will perform critical common functions in the NCOE, including providing service capabilities that support requirements from "first tactical mile" users, who are the least likely to have continuous access to these resources. Applications are distinguished from core enterprises services, and from other lower-level services used by multiple COIs, by their ability to provide functionality to the local user even with intermittent network connectivity.

As explained in this document, certain applications may be provided as COI Services (that is, services for Communities of Interest). These services provide the capability to share information within the enterprise so that users (machine and human) can use the services to help expedite or automate mission-specific activities, such as the computational analysis, decision-support, and data visualization required by the warfighting user to perform a mission-critical task. Neither term includes the tools, nor the capabilities used, to manage and defend the network. For a discussion of information assurance, see the NCOE JIC.

The NCOE JIC's timeframe is 8 to 20 years in the future. For continuity, the document's illustrative CONOPS and its three enabling constructs, including this one, all focus on the year 2015. See the NCOE JIC and the separate *Net-Centric Environment Joint Functional Concept* (NCE JFC) document for information about relevant assumptions and risks.

4. CENTRAL AND SUPPORTING IDEAS

4.1 Central Idea

NCOE applications enable pervasive knowledge generation and sharing throughout the Joint Force by providing users with a doctrinally and architecturally unconstrained interface and individually configurable access to enterprise resources.

The NCOE will provide the appropriate decision authority with real-time or near real-time data, information, and knowledge, supported by applications and underlying services. This will be accomplished by employing a variety of options, including forward deployment of small footprint applications capable of delivering instantaneous information, and a "reach-back" capability to centralized and well-resourced centers of excellence for a more detailed and thorough analysis.

Applications in the NCOE will enable pervasive knowledge by:

- Customizing the discovery, access, fusion, processing, and display of tailored information based on mission objectives and the role of the individual;

- Providing collaborative tools for dynamic planning and execution that leverage enhanced situational awareness of the battlespace, smart decision tools, machine-to-machine interfaces, and shared knowledge;

- Optimizing the ability of warfighters to share situational understanding including quickly assessing the situation and alternative courses of action;

- Supporting adaptive, distributed, cooperative, and collaborative decision-making with tools and system integration;

- Supporting appropriate organizational relationships across and beyond the Joint Force;

- Continuing to operate even while disconnected from network resources; and

- Allowing application to application interchange/exchange when time sensitivity precludes access of centralized network resources.

This will be accomplished by removing doctrinal and architectural constraints from the information, network, and computing domains, enabling "point of use" of NCOE applications where needed, not prescribed.

4.2 Supporting Idea: *Using Service-Level Agreements (SLAs)*

Service-Level Agreements, or SLAs, between users and network managers will facilitate the flexible application of network resources to meet mission objectives. Established processes and guidance, which will be implemented as part of the integrated KM-NM-IA framework, can leverage SLAs to ensure that the users will receive additional network resources quickly in order to accomplish their specific mission(s). This inherent flexibility of the NCOE will support asymmetrical warfare and a rich interaction with coalition and civilian entities. It also will allow for changing concepts and doctrine, as well as provide for role-based access to the NCOE regardless of the user's geographical location.

SLAs can also be used to efficiently exchange data and/or information between COIs and their respective applications. In this case, SLAs would be negotiated by the service provider with the COI(s) and the sponsoring domain(s). The service provider will publish the SLA in accordance with Service Definition Framework (SDF) guidance, to be defined in the GIG Enterprise Services Strategy (GIG ESS). The SLA will work in conjunction with existing processes and service capabilities to enable the efficient and properly attributed exchange of data and functionality between COIs and users. For example, a SLA between users and network managers will allow for the dynamic allocation of network resources to meet mission objectives. These agreements could support such warfighting essentials as automated direct exchange of data between applications, necessary to accomplish time sensitive tasks in a low bandwidth environment.

Applications in the NCOE must provide data to a user in an intuitive and tailored (i.e., geospatial, timeline, query-based) format and also insulate the user from the details of the underlying services. These applications must be scalable, platform-independent, distributable, and able to use non-deployed databases and computing resources. They must be able to provide complex analyses and multiple courses of action, and simulate complex processes that directly support operations (i.e., logistics movement and support both into and in-theater). Using SLAs supported by a robust and scalable communications backbone, with data provided and indexed by core services, these applications can provide the cross-functional warfighting capabilities identified in the family of joint concepts.

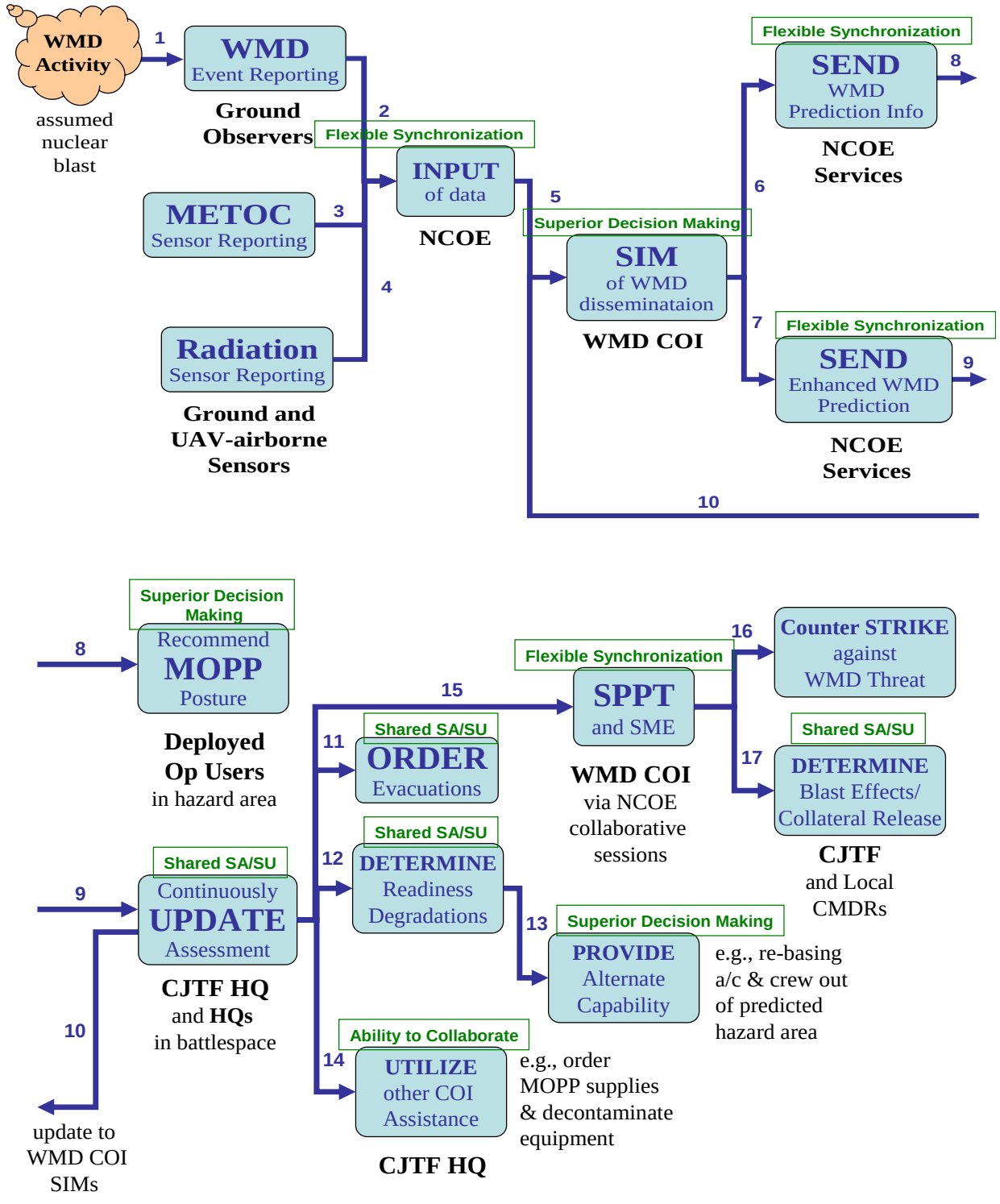
4.3 Application of the Central and Supporting Ideas

The following three examples illustrate the use of applications in the context of the larger NCOE capabilities. Although presented in mission-specific contexts, these use cases can be applied to other scenarios with minimal modification.

4.3.1 Weapons of Mass Destruction (WMD) COI support

The current problem: Operational users need to access subject-matter experts (SME) and highly sophisticated modeling and simulation (M&S) estimates of, the hazards, effects, and lethality of various weapons of mass destruction (WMD). This WMD COI capability is needed by operational users in-theater, with minimal platform footprint and complexity, and with full access to CONUS or OCONUS SMEs, databases, reference material, prediction and monitoring tools, and complex simulations. Currently these services do exist; however, as CONUS assets which must be deployed in-theater, they require specially dedicated logistics and stand-alone computer systems, and are not integrated into current command-and-control (C2) and operational information systems. The prediction and warning decision-support function of the WMD COI is severely limited, due to time delays measured in hours for local Metrological (METOC) and observed WMD activity data—transmitted manually, loaded into these tools, and with the results disseminated as paper messages. There is no automated "reach-back" to CONUS-based analytical tools and SMEs, nor the means to integrate this essential WMD COI force protection information into the local C2 operational picture. As a result, most force protection WMD hazard prediction is done locally, utilizing stale data and tedious manual-plotting techniques and paper tables that date from the 1950s. It is too simplistic, non-specific, or deterministic, and drastically affects operational readiness with overly conservative assumptions that mandate an unnecessarily high Mission-Oriented Protective Posture (MOPP) that degrades operational readiness and/or otherwise underestimates WMD effects, exposing personnel unnecessarily.

The NCOE solution:



Figures F-1 (top) and F-2 (bottom). Weapons of Mass Destruction (WMD) COI Support

By providing a ubiquitous networked connectivity with each operational user and heavily resourced and geographically remote COIs, their enhanced capability can be utilized in a timely manner. The key element in WMD defense is time. Observations of WMD activity (detonations, sensor reports, etc.) and local METOC data must be provided to WMD analysis and prediction simulation-based tools, with the synthesized results then disseminated electronically into the local tactical picture to gain operational relevance. NCOE applications will enhance shared situational awareness and superior decision-making by providing actionable information on WMD effects within the local battlespace.

Use Case:

- WMD activity is reported by on-the-ground observers reporting an explosion in a WMD threat area. The assumed WMD threat is nuclear and the blast observations support that assumption.

- Local METOC conditions are captured and stored. Blast locations and characteristics are inputed, and radiation sensors (ground and UAV airborne) are deployed for continuous reporting.

- CONUS WMD COI on watch pulls data via NCOE services from the threat area and executes a prediction and monitoring simulation of WMD dissemination. This predictive "cloud" of information is sent immediately via NCOE services to the deployed operational users in the hazard area, with recommendations for setting MOPP levels on personnel and an assessment of the time(s) required for the MOPP posture.

- The JTFHQ and other HQs in the effected battlespace receive an enhanced WMD prediction from the WMD COI that includes geospatial, time-phased maps of predicted contamination, lethality on unprotected civilian and military personnel, and suggested evacuation/maneuver routes that avoid the majority of the hazard. This assessment is continuously updated by the COI simulations, and by sensors deployed in the hazard area by local commanders. Since local sensor data is generally not actionable until processed by the WMD COI, the continuous connectivity of data in both directions via the NCOE is crucial to operational readiness.

- The JTF uses the WMD COI predictions of hazards and their longevity in the effected operational zone to:

    - Order evacuations by safe routes, plotting routes that will avoid/minimize the hazard over the next 24 hours to clear civilian and unnecessary troops and equipment from the effected area.

- Determine MOPP-level mission readiness degradations and provide alternate capability. For example, re-basing aircraft and ground crews out of the predicted hazard areas to facilitate fully operational flight.

- Utilize other COI assistance via the NCOE. For example, order enough MOPP supplies and decontamination equipment into the effected battlespace to provide a continuous operational ability in the effected area.

- The WMD COI provides a continuous SME presence via NCOE-enabled collaborative sessions, supporting the JTF and local commanders in planning counter strikes against the WMD threat and determining possible blast effects and WMD collateral release.

- The WMD/Medical COIs provide an NCOE collaborative presence to local and JTF-level medical assets on treatment and evacuation priorities on WMD casualties. The WMD/Medical COI advises on MOPP measures, decontamination procedures, and helps to solve problems as they arise in collaboration with local users.

4.3.2 Operational Picture Information Fusion

The current problem: Operational users produce a C2 geospatial "picture," often called the Common Relevant Operational Picture (CROP), to represent the time-based geographic movement of platforms of interest as "tracks." Other information (intelligence, logistics, imagery, etc.) with a time-based geospatial character is layered-in to make the CROP relevant to more than the C2 COI, and also to accommodate the multiple sensor platforms and their associated data deployed in routine operations. As more of this un-processed information is provided (in accordance with the DoD Data Strategy) and as more sensors for reporting track positions are added, multiple representations of the same platform or item of interest are represented with differing fidelity and time-bases, causing confusion, information overload, and ambiguity in situational awareness. No ability exists to project the CROP in enough time to analyze future operations, nor to reach back in time to analyze past events.

The NCOE solution:

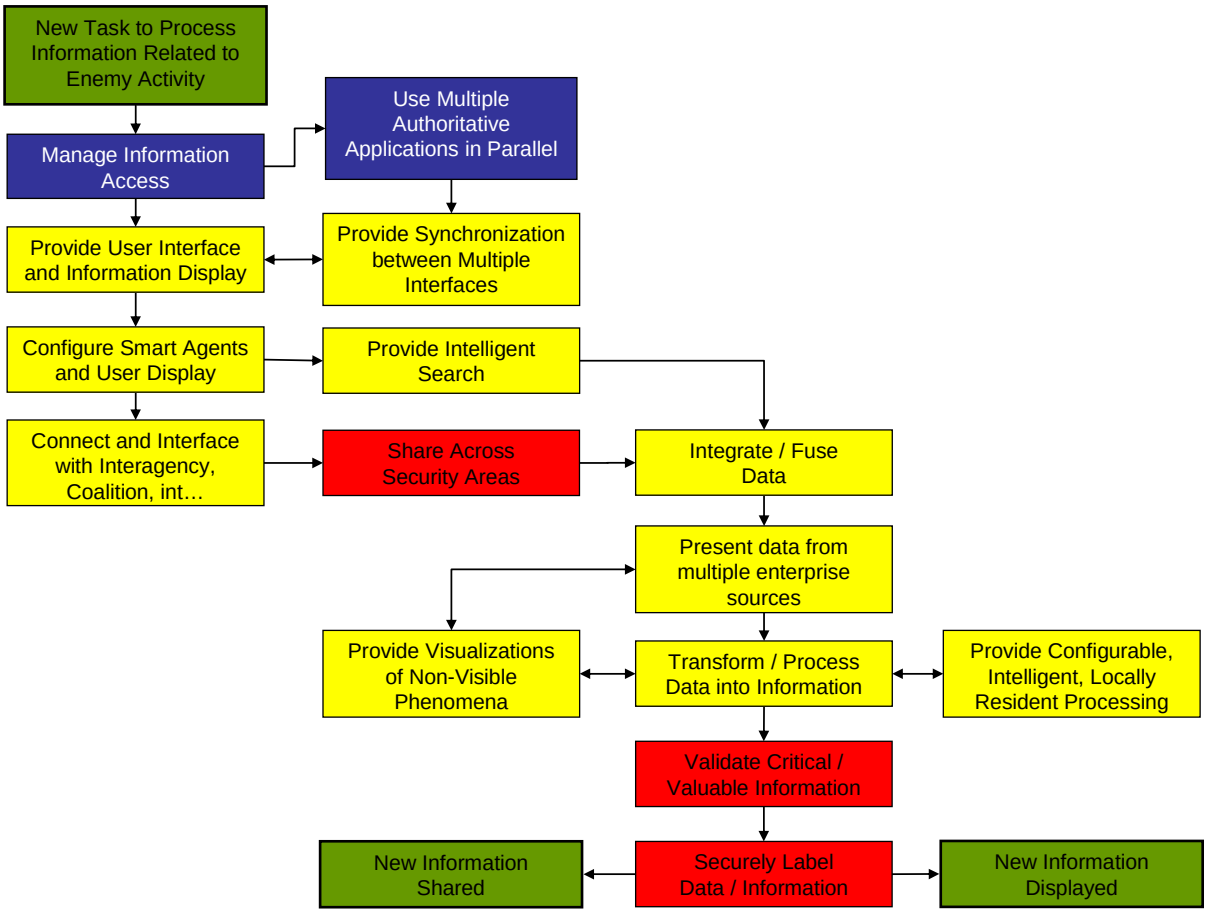


Figure F-3. Operational Picture Information Fusion

By providing application functionality in the CROP, which:

- processes raw sensor and other COI data "as delivered";
- synchronizes that activity among all collaborative users; and
- transforms it into actionable situational awareness,

the NCOE is able to provide some level of shared understanding among all the CROP users involved in the operation. This CROP application functionality will be able to:

- Receive multiple observations of platform activity and fuse them into one track, having a coherent geospatial time-base, and display the results as either a fused synthetic entity or as "raw" sensor reports, if desired.

- Change the time-base to predict the track movement into the future, and also into the past to analyze changes in the operational picture over time.

- Inject COI information of operational and geospatial significance into the CROP, and allow "detail on demand" to avoid confusion, instead tailoring to a particular user's interest.

- Provide alternate, non-geospatial views of the CROP for various purposes, and allow meaningful display of non-cognitive, operationally significant geospatial entities, such as defensive radar coverage in three dimensions around a JTF position.

Use Case:

- Ballistic missile activity is reported by ground observers, and by national and tactical sensor platforms, simultaneously. The assumed threat is conventional and the blast observations support that assumption.

- Sensor data is made available immediately via the NCOE, and routed to various subscribed participants in the affected theater in key situational awareness roles. CROP application functionality fuses those various sensor reports, as they are received, into actionable track entities that use sophisticated software to adjust the time- and geospatial-bases of the disparate information into a common reference frame for JTF situational awareness. Raw data is available on demand for analysis as required.

- NCOE reach-back capability allows the use of specialized COI resources (such as intelligence COI imagery processing) to provide more actionable, processed data in a short, tactically-relevant timeframe. Other COI resources "mine" data from all the sources in the affected area, providing the JTF with operationally-relevant supporting data in a cognitive format, and assisting in making "sense" of the myriad of raw data available to the JTF.

- JTF Air Defense personnel configure a CROP view that "looks" at JTF air defense radar coverage as currently deployed and operating, and constructs a three-dimensional view of the defensive radar search and targeting coverage in a 360-degree view around all threatened JTF assets. Based on this information, mobile AAW assets and aircraft are re-positioned to fill radar coverage gaps that expose the force to missile vulnerability.

- NCOE collaboration among CROP users assists in rapid counter targeting of launch sites. C2 targeting applications are "tipped" by NCOE COI assets in order to rapidly counterstrike and neutralize the threat.

4.3.3 Convoy Movement Planning and Execution

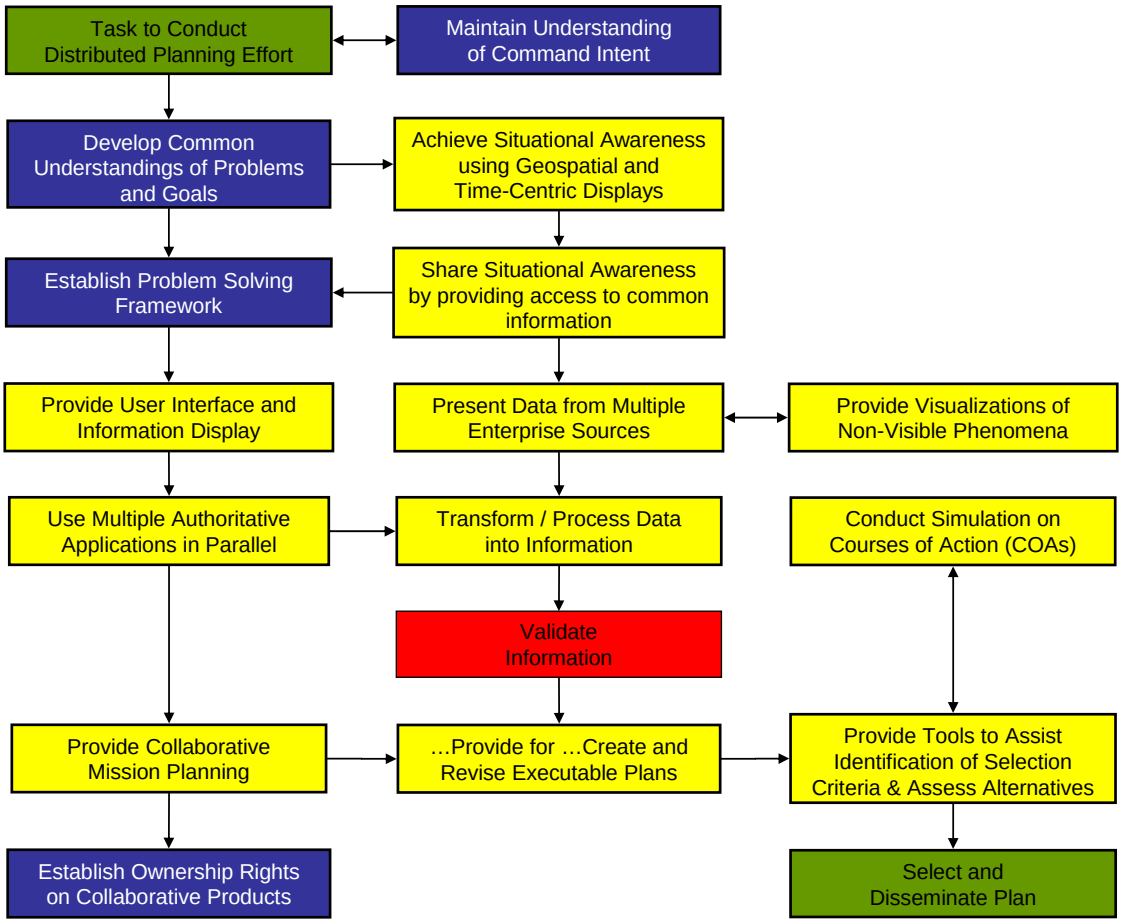


Figure F-4. Distributed Planning

The current problem: Land-based unit movement in the battlespace is largely governed by paper-based operational orders, voice radio reports, and some Blue-Force Tracking (BFT) capability. Units have detailed plans for movement, but revisions to those plans are made ad-hoc by radio and paper message. Plans for those unit movements are made iteratively and collaboratively in a manual, serial planning process that is time-consuming and operationally non-responsive. There is no automated execution monitoring nor "on the fly" revision and collaborative status reporting capability. The JTF then has poor situational awareness of its own force movements, status, and current plans for movement, as well as an inability to quickly and decisively change routes and destinations in response to a macro-tactical view.

The NCOE solution:

- By providing application functionality in the NCOE to enable a dynamic, adaptable planning process and an ability to visualize the plan and monitor its execution on the CROP and other situational awareness displays, the JTF will use and deploy assets more effectively. Also, the JTF's ability to respond more rapidly to emergent conditions, and to redeploy forces and supporting units rapidly, is significantly enhanced.

Use Case:

- A logistics convoy is required as part of a major force maneuver to supply fuel and ammunition to a rapidly moving armor unit. As part of the planning process for this operation, the entire 24 hours of the operation was constructed using a geospatial CROP view and collaboratively distributed via the NCOE to all planners and operators. Each planning COI (logistics, operations, air, etc) has had the opportunity to modify the plan based upon their requirements to support it. Reach-back capability is used to run each version of the plan through powerful planning simulations to thereby identify shortfalls based on current conditions, provided in real-time.

- As the plan is executed, a JTF plan simulation application is initialized and updated by BFT reports for the CROP, as well as with inputs from operators based on emergent voice and other communications. This plan is made available simultaneously in the NCOE, with progress monitored by all echelons in the CROP, real-time, and in CROP Plan (future) view.

- Planning applications tip off JTF personnel to problems with planning and execution, suggesting plan changes to support continued execution on time and on the objective.

- In this case, the logistics convoy has made a major navigation error that jeopardizes the armor unit's rate of advance. Adaptive planning and execution applications recognize the deviation from plan of the logistics convoy based on the BFT position, and the plan routes. An alert is passed to the JTF and also to the affected units.

- The logistics convoy receives re-direction orders suggested by the plan execution application, via another route to save time and avoid enemy contact. The armor unit is directed to slow its advance to affect a changed rendezvous with the logistics convoy. The overall effect of this change in operational play is evaluated by NCOE planning applications; an alternate course of action for the operation is proposed, accepted

collaboratively by the JTFHQ and subordinate units, and disseminated via the NCOE.

5. CAPABILITIES, TASKS AND STANDARDS

A capability is the ability to achieve an effect to a standard under specified conditions using multiple combinations of ways and means to perform a set of tasks. The capabilities presented below are derived from the NCE JFC. The NCOE JIC further articulates the relationship and derivation of capabilities, conditions, tasks, and standards. The tasks below are the specific applications-related activities that support each capability. Some of the tasks listed below may support or be dependent upon tasks in the NCOE JIC or other enabling constructs.

5.1 Capability: *Ability to collaborate*

Collaboration requires simultaneous use of applications and processes in close coordination between two or more users that perform a warfighting process. Applications must be available to all users, distributed in the NCOE to enable collaborative processes, such as: planning, logistics movement, targeting, strike, and other time-sensitive or inherently collaborative processes. Users will need a high quality, continuous collaborative capability, scalable to type of function performed, but ubiquitous and always ready for use. Application-based tasks associated with this capability are:

- *Utilize the collaborative information environment through custom user interface.*

- *Provide synchronization between multiple applications with simultaneous user interaction.*

5.2 Capability: *Ability to provide adaptive, distributed, cooperative, and collaborative decision-making and planning*

Superior decision making requires applications that offer alternative Course of Action (COA) support, enhanced insight, or presentation of information entities that are beyond unaided human cognition. These applications optimize the ability of the warfighter to quickly assess the situation and alternative COAs. Applications must be available to all users, distributed in the NCOE, enabling time-sensitive COA analysis with authoritative data (both raw and processed by applications), and available to the user to support such decisions. Examples of application tasks include:

- *Present data from multiple enterprise sources in human intelligible, timely, and fused format.* These fusion applications will need to address the following functional requirements:

- War-gaming
- Environmental effects/prediction
- Visualization of data (geospatial, analogs, multiple dimensional, etc.)
- Analysis of behaviors (Red, Blue, White, Grey, etc)
- Perception modeling
- Sensor/Weapons coverage maps
- WMD lethality and propagation predictions
- Acoustic and electromagnetic environment information
- Information Warfare modeling
- Rehearsal en route

• *Provide the capability for distributed, collaborative, systematic, on-demand, creation and revision of executable plans, with up-to-date options, as circumstances require.*

• *Provide the capability for distributed, collaborative, systematic, on-demand, creation and revision of executable plans, with up-to-date options, as circumstances require.*

• *Identify selection criteria and assess alternatives to decisively control operational situations, through automation in exchange, fusion & understanding of information.*

• *Configure smart agents and user display to execute predictive analysis within a functional area.*

• *Provide data access across multiple COI and between disparate databases.*

5.3 Capability: *Ability to share situational understanding*

This capability includes the ability to keep informed of the tactical, operational, and strategic situation using information presented to all participating users simultaneously, and in a geospatial or other appropriate format for easy cognition. These "views" of information are tailored and based upon the user's role, mission objectives, and security constraints. Applications must be available all users, distributed in the NCOE to enable a shared geospatial operational picture with supporting data in a cognitive format tailored to the user's mission. Data should be shared in real-time, while the applications that process that data should work in near real-time. Applications should fuse, present, and make sense of the data to help users understand the perceptions of the battlespace from Blue, Red, and other perspectives. When all users have the same fused "view" of the battlespace and have the applications to interpret the data, they have attained shared understanding. Some application-based tasks associated with this capability are:

• *Achieve situational awareness using geospatial and time-centric displays of enterprise wide data to relate information with similar characteristics:*

- o *Location/Status/Intentions of friendly forces (current & planned).*
- o *Location/Identity/Status/Intentions of hostile forces (current & projected).*
- o *Location/Intentions of other forces/actors (neutral forces, NGOs, etc.) (current & projected).*
- o *Weather (current & forecast).*
- o *Geospatial information of any other type (terrain, facilities, intelligence etc).*
- o *Political/diplomatic information (current & projected).*
- o *Media reports.*

• *Provide tailored "pictures" to users based on their mission, level of fidelity needed, and their security requirements.*

• *Provide the same capabilities with coalition partners and political/civilian authorities with appropriate security considerations.*

• *Provide fused entities from multiple data (sensor, reporting sources) originators.*

• *Provide a synchronized and low time latency "Operational Picture" to all participants.*

• *Provide access, collation, and display of CROP information at source-level accuracy for first tactical mile users.*

• *Share situational awareness by providing access to common information with specific indication of contextual relevance.*

5.4 Capability: *Ability to identify/store/share/exchange data/information*

Applications must support pulling information from other COIs and help users to visualize, interpret, or render it into the operational picture/display. Data with varying levels of fidelity, time, and accuracy will require discovery, fusion and processing applications to make sense of the information from these disparate sources. Applications must be available to all users, distributed in the NCOE, with multiple-COI authoritative data (both raw and processed by applications) that is available to the user on demand, with proper security classification/routing via secure data labeling. Specific tasks include:

• *Transform/Process data into information.*

o *Information shared with attributed sources, and entity attributes suitable for fusion in multiple disparate applications.*

o *Information shared from multiple COIs and among coalition partners with security considerations accommodated.*

• *Capture, create and display information with local tools while disconnected from the enterprise.*

5.5 Capability: ***Ability to process information***

To the extent practicable, the Joint Force will employ enterprise resources to process information. For the "first tactical mile" user, continuous access to enterprise resources is not feasible. Also, local processing of information can reduce transmission requirements in resources-constrained environments. The following are examples of local processing tasks supported by applications:

• *Integrate Blue and Red data — high level fusion gray/white/interagency/ coalition, etc…)*

• *Provide configurable, intelligent locally resident processing resources.*

• *Enable sharing of enterprise information resources and enterprise process and applications.*

• *Enable rapid configuration and modification of new and existing applications.*

6. IMPLICATIONS

JTF elements are being placed increasingly into unfamiliar situations involving complex, uncertain, and rapidly changing operational environments. An increasing need also exists to directly post data, empower users to pull data effectively from multiple sources, and have access to time-sensitive intelligence. The conduct of warfare and conflict resolution requires net-centric operations with ubiquitous access to relevant applications anywhere in the infrastructure. The application services must be highly adaptive, scalable, available, reliable, easily accessible, and responsive. These capabilities will provide accelerated decision-making and a significant tactical advantage over the adversary.

7. CONSTRUCT DEVELOPMENT AND EXPERIMENTATION

The NCOE's applications environment incorporates advanced and emerging concepts and technologies that must be developed and deployed in a spiral process to allow users to fully comprehend their utility in an operational

environment and to provide feedback for future spirals. A robust combination of experimentation and COI pilots are required to develop, refine, demonstrate, and test the applications portions of the NCOE.

See the NCOE JIC for further development and experimentation information.

APPENDIX G. Scenario, Intelligence Estimate, Illustrative CONOPS (CLASSIFIED)