

1 **Net-Centric Environment**

2 **Joint Functional Concept**

3 *Version 0.95*



18 **30 December 2004**

19

20

21	Table of Contents	
22	Executive Summary	iv
23	1.0 Concept Purpose	1
24	1.1 Statement of Purpose	1
25	1.2 Definition of the Net-Centric Environment	1
26	2.0 Illustrative Vignette	3
27	2.1 Background.....	3
28	2.2 The Networked Setting	3
29	2.3 Situation	4
30	2.4 Execution	5
31	3.0 Central and Supporting Ideas.....	9
32	3.1 Statement of the Military Problem.....	9
33	3.2 Emerging Operational Environment.....	9
34	3.2.1 Current Platform Centric Environment.....	9
35	3.3 Central Idea.....	10
36	3.4 Principles Essential to Applying the Concept to a Wide Range of Scenarios ..	12
37	3.4.1 Technical Area Principles.....	13
38	3.4.2 Knowledge Area Principles	15
39	3.5 Application of Concept within a Campaign Framework	19
40	4.0 Capabilities and Attributes.....	21
41	4.1 Areas	21
42	4.1.1 Knowledge Area	21
43	4.1.2 Technical Area	21
44	4.2 Capabilities	22
45	4.2.1 Knowledge Capabilities	22

46	4.2.2	Technical Capabilities.....	24
47	4.3	Attributes.....	26
48	4.3.1	Knowledge Attributes.....	26
49	4.3.2	Technical Attributes.....	27
50	5.0	Implications.....	31
51	5.1	Doctrine.....	31
52	5.2	Organization.....	31
53	5.3	Training.....	31
54	5.4	Materiel.....	32
55	5.5	Leadership and Education.....	32
56	5.6	Personnel.....	33
57	5.7	Facilities.....	33
58	6.0	Scope.....	34
59	6.1	Timeframe and Applicable Military Functions and Activities.....	34
60	6.2	Impact of Strategic Guidance and Deviations in the Concept.....	34
61	6.3	Impact of Future Context Documents and Deviations in the Concept.....	34
62	6.4	Risks and Mitigation.....	35
63	6.5	Assumptions.....	36
64	6.6	Relationship to Other Joint Concepts.....	36
65	Appendix A	Reference Documents.....	A-1
66	Appendix B	Glossary.....	B-1
67	Appendix C	List of Acronyms.....	C-1
68	Appendix D	Table of Capabilities and Attributes.....	D-1
69	Appendix E	Implications for Experimentation.....	E-1
70	E.1	First-Order Information Value Chain For The NCE JFC.....	E-1

71	E.2 The Net-Centric Environment Joint Functional Concept Value Proposition.....	E-3
72	E.3 Other Recommendations for Experimentation.....	E-5
73	E.4 Phases of a Research and Experimentation Campaign.....	E-6
74	E.5 Elements and Tools for NCE JFC Research and Experimentation	E-7
75	E.6 Other Research Topics for an Experimentation Campaign.....	E-7
76	E.7 Areas for Developing Future Hypotheses	E-8
77	Appendix F Mapping Capabilities to Attributes.....	F-1
78	Appendix G Contributors	G-1

79

Executive Summary

80 The purpose of the Net-Centric Environment
81 Joint Functional Concept is to identify the
82 principles, capabilities and attributes required
83 for the Joint Force to function in a fully
84 connected framework. This concept also
85 provides the net-centric functional context for
86 other joint concepts, and it supports joint
87 experimentation¹ and the measurement
88 framework for evaluating joint initiatives.

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

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

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

The Military Problem

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

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

¹ Joint Operations Concepts, 2003

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

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

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

120 **1.0 Concept Purpose**

121 ***1.1 Statement of Purpose***

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

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

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

136 ***1.2 Definition of the Net-Centric Environment***

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

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

149 Net-Centric capabilities focus directly on human interaction through knowledge sharing
 150 enabled by the dramatic advances in information technology. The effectiveness and
 151 efficiency of operating in a mature Net-Centric Environment will be achieved through the
 152 evolutionary development and implementation of Doctrine, Organization, Training,
 153 Materiel, Leadership and Education, Personnel, and Facilities (DOTMLPF) appropriately
 154 suited for the utilization of network-enabled information and interactions. The Joint Force

² Joint Operations Concepts, 2003

³ Joint Operations Concepts, 2003

⁴ CJCSI 3170.01D

⁵ Joint Operations Concepts, 2003

155 can then derive and use knowledge in superior decisionmaking processes and apply
156 capabilities effectively, robustly, and flexibly to achieve desired effects. This allows the
157 Joint Force and its mission partners⁶ to function more efficiently (faster and better) in the
158 execution of traditional missions. More significantly, these new capabilities allow forces
159 to be employed in fundamentally different ways by integrating the Joint Force across
160 progressively lower echelons. The Joint Force will thereby increase its effectiveness and
161 efficiency by having the capabilities to undertake new missions as well as capabilities to
162 better execute its current missions.

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

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

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

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

⁸ FORCenet Functional Concept (draft version 1.1.1) 091404 pg 1.

184 2.0 Illustrative Vignette

185 2.1 Background

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

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

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

206 2.2 The Networked Setting

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

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

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

232 ***2.3 Situation***

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

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

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

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

257 **2.4 Execution**

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

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

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

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

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

296 By operating in a Net-Centric Environment, ERTs and USR teams are able to collaborate
 297 with CJTF units, other response teams, and all pertinent relief organizations, **synchronize**
 298 **their actions**, quickly deploy to areas where people are potentially trapped inside

299 buildings and execute immediate search and rescue actions. All organizations responsible
300 for casualty activities *automatically post casualty updates*, allowing network participants
301 to access near real-time information on current casualty locations, status, severity of
302 injuries, and availability and location of nearest ERT and USR teams and equipment,
303 supplies, current on-site conditions, and status of casualty logistical/medical support
304 infrastructure.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

412

413 **3.0 Central and Supporting Ideas**

414 ***3.1 Statement of the Military Problem***

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

425 ***3.2 Emerging Operational Environment***

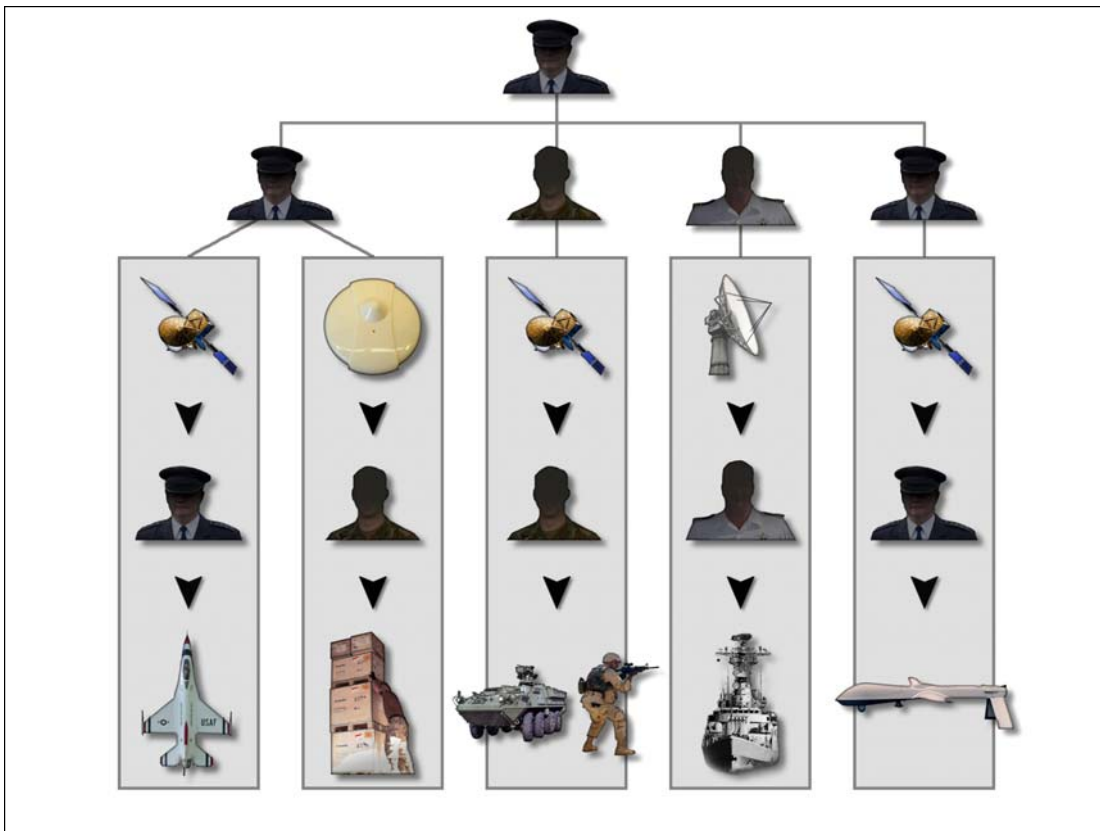
426 The changing character and conduct of warfare and conflict resolution require a
 427 fundamental shift in the way the U.S. military integrates and employs the elements of the
 428 Joint Force. Joint Force elements are increasingly being put into unfamiliar situations
 429 within complex, uncertain, and rapidly changing operating environments. To succeed in
 430 these environments, they need the ability to rapidly integrate varied, dynamic, and often
 431 unanticipated sets of capabilities, potentially drawn from across and beyond the Joint
 432 Force and its mission partners, in order to achieve the effects they require to meet their
 433 mission objectives. They need to reduce the impediments to the flow of information and
 434 reduce the inherent friction¹¹ of adjusting Joint Force and mission partner capabilities to
 435 new tasks and missions. The Joint Force and its mission partners need to greatly increase
 436 the level of integration among their various capabilities and function at increasingly
 437 lower echelons.

438 **3.2.1 Current Platform Centric Environment**

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

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

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



463

464

Figure 3-1—Platform Centric Environment

465 **3.3 Central Idea**

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

468 Advances in information technologies are revolutionizing the ability for all members of
469 the Joint Force and mission partners to share information and collaborate,¹² creating new
470 central principles and paving the way for significant increases in the effectiveness and
471 efficiency of the Joint Force and its mission partners. Collaboration is defined as joint
472 problem solving for the purpose of achieving shared understanding, making a decision, or
473 creating a product¹³ across the Joint Force and mission partners. It allows experts to
474 integrate their perspectives to better interpret situations and problems, identify candidate
475 actions, formulate evaluation criteria, decide what to do, and execute those decisions. In
476 the context of this concept, collaboration is used to share and improve information,
477 awareness, and understanding among the elements of the Joint Force and its mission
478 partners; support decisionmaking; and synchronize activities.

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

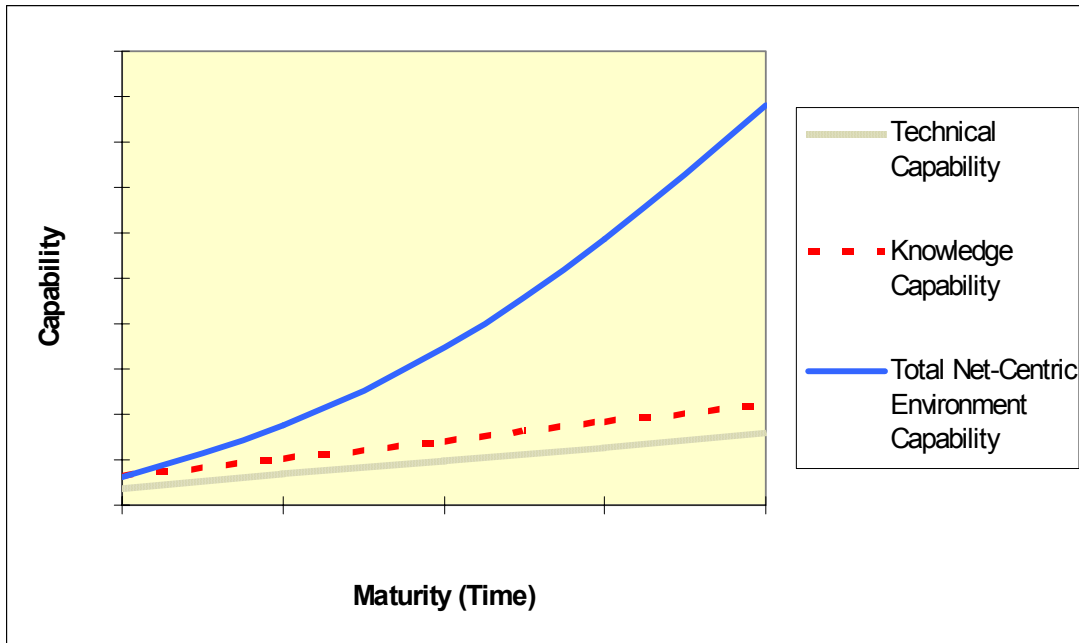
490 However, investments that only address the technical and informational aspects of this
491 environment will only garner limited gains in the overall agility and utility/effectiveness
492 of the Joint Force. Transitioning from a platform-centric environment requires
493 surmounting internal and external organizational and policy barriers to the sharing of
494 awareness, understanding, decisionmaking, and the synergistic application of force
495 capabilities. This cultural change must be supported by training and education, as well as
496 by ensuring that Joint Force elements have incentives to use the technical networks of the
497 Joint Force and its mission partners to draw on appropriate capabilities, regardless of
498 their geographic or organizational location. While this can be done to a limited extent
499 through the formal coordination mechanisms within and among institutions, the agile
500 operation of a force requires the enabling of both formal and informal collaboration
501 across the Joint Force, and the ability to establish and utilize relationships with mission
502 partners.

¹² This information sharing and collaboration is done formally and informally, directly and indirectly, and across the force and between the force and appropriate extra-force elements and resources.

¹³ Joint Command and Control Functional Concept

¹⁴ The GIG is defined by the DODD 8101.1, Global Information Grid Overarching Policy, 19 September 2002 as a globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. However, current investments focus on procurement of critical enablers in the information and physical infrastructure domains.

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



517

518 **Figure 3-2—Net-Centric Environment Capability: Greater Than Sum of Its Parts**

519 ***3.4 Principles Essential to Applying the Concept to a Wide Range of***
 520 ***Scenarios***

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

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

526 **3.4.1 Technical Area Principles**

527 ***3.4.1.1 Intelligent Infrastructure***

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

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

558 ***3.4.1.2 Individual Information Management***

559 Advances in information technology will enable the infrastructure to move greater
560 volumes of higher quality information more quickly from producers through processors
561 to consumers.¹⁵ The key advantage is that the generation and fulfillment of information
562 requirements are significantly more efficient because they can be dynamically defined

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

563 and generated by the consumer of the information. *Information management shifts from a*
564 *command function to an individual function.* Interoperability is enhanced through use of
565 common enterprise services supported by a unified data strategy rather than service,
566 command, and function specific information management practices.¹⁶ Since resources
567 will never be infinite and sometimes severely restricted¹⁷, command and organizational
568 responsibilities will focus increasingly on management of available resources. This focus
569 shift implies a significant cultural change supported by education, and increased joint
570 training at lower echelons, including the use of a live virtual constructive joint training
571 environment.¹⁸

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

582 To support individual information management, information will need to be clearly and
583 properly tagged¹⁹ to help individuals and groups more quickly discover and access it.
584 Tagging also allows for the creation of useful ontologies for the information that they
585 produce. A variety of tagging methods, including auto-extraction and auto-generation tied
586 together by an interoperability of the metadata that they produce, will help to make
587 information easily accessible and to help intelligent agents to provide that information to
588 those individuals and groups who have subscribed to it. Information will need to be
589 presented in a proper operational context, so tagging will need to relate contextual
590 information as well.

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

¹⁷ FORCEnet, page 14.

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

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

591 3.4.2 Knowledge Area Principles

592 *3.4.2.1 Information and Decision Rights and Responsibilities*²⁰

593 Each individual actor in the Net-Centric Environment has rights and responsibilities as
 594 they apply to information and decisions. This significant culture shift must be supported
 595 by training and education. Individuals will have the proper incentives to fulfill their roles
 596 as a producer, processor, and consumer²¹ of information. Individuals will also need the
 597 knowledge, experience and confidence to interact effectively. Individuals need to be
 598 prepared to not only exploit the information made available to them, but to also engage in
 599 behaviors that encourage transparency; including ensuring that exploited information is
 600 shared with those who are supposed to have it. The behavior of individuals can be
 601 assessed by feedback they receive from those who interact with them on the network.
 602 Good behavior²² is rewarded with positive feedback—much like a credit score or online
 603 auction rating system. Feedback will be important in building and establishing trust when
 604 operating with new partners because it will limit their ability to discover and access
 605 information. Individuals who do not engage in acceptable behavior will receive negative
 606 feedback, which may be used as a mechanism to specify additional training or limit the
 607 types of tasks deemed appropriate. The quality and quantity of the shared information
 608 across the Joint Force and its mission partners is dependent upon each individual
 609 exercising their rights and fulfilling their responsibilities.

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

617 The rights and responsibilities found at the individual level can also be ascribed to the
 618 group level.²³ The important distinction between individual and group rights and
 619 responsibilities as related to information and decisions is the set of additional factors that
 620 describe the structure and quality of relationships among the individuals within the group.
 621 Groups that do not engage in acceptable behavior will receive negative feedback, which
 622 may be used as a mechanism for additional training or limits on the types of tasks deemed
 623 appropriate for the group. Groups are adaptable, which means they are prepared to

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

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

²² “Good behavior” occurs where the individual or group have not abused their information or decision rights and have fulfilled their information and decision responsibilities to the satisfaction of the group.

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

624 quickly respond to any contingency with the appropriate capabilities mix. This requires
625 versatile and agile forces that are tailorable and scalable for employment and able employ
626 new capabilities in a multi-use manner. Adaptability ensures that groups can rapidly shift
627 from mission to mission.²⁴

628 **3.4.2.2 End-to-End Transparency**

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

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

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

654 **3.4.2.3 Using Communities of Interest**

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

²⁴ JOpsC, p. 16.

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

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

	Formal	Informal
Permanent	Traditional Organizations (Services, Joint Staff)	Standing Communities of Interest (Warfighter Mission Areas, IT Domains, Business Mission Area Domains)
Temporary	Working Groups (Task Forces, “Tiger” Teams)	Dynamic Communities of Interest (JTF Supply Clerk Share Point, Tactical Level Disaster Response)

677

678

Figure 3-3—COI’s within the Net-Centric Environment

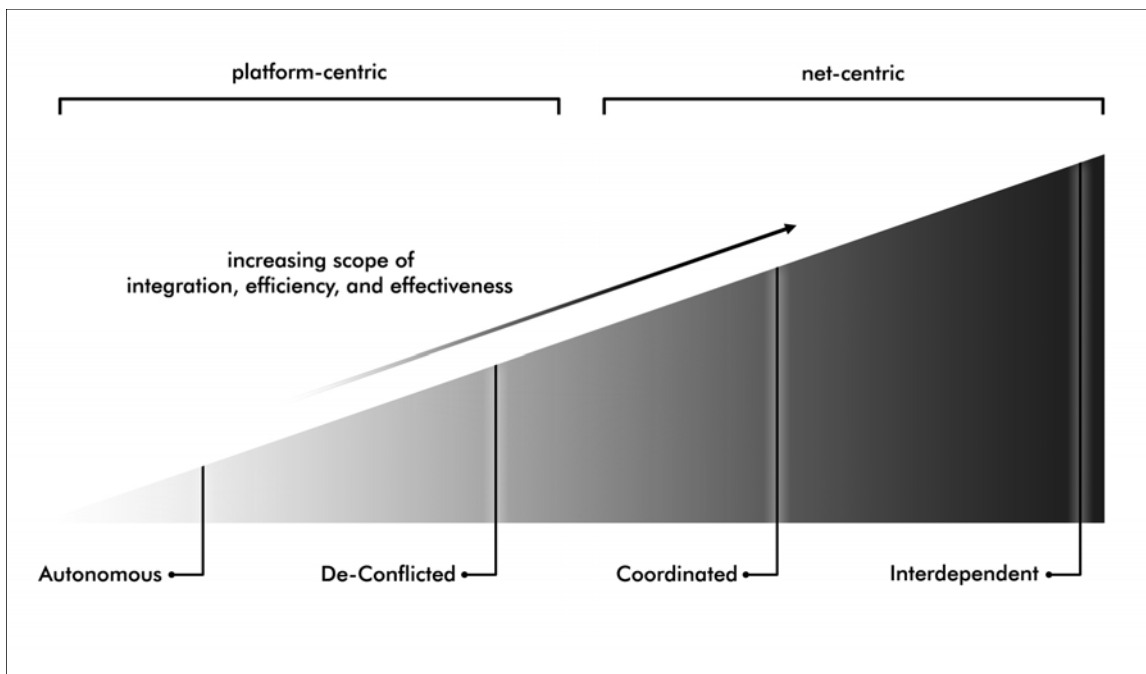
679

3.4.2.4 Interdependence

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

683 Currently, integration of the Joint Force normally occurs at the component or JTF
 684 headquarters level, and is often characterized by autonomy and de-confliction, the lowest
 685 levels of integration. Here the capabilities of each organization or unit stay entirely
 686 separate, even when the parent organizations have some overlap. Because units rarely
 687 employ every capability at their disposal in support of service or component tasking,
 688 significant capability within the JTF remains latent or unused.

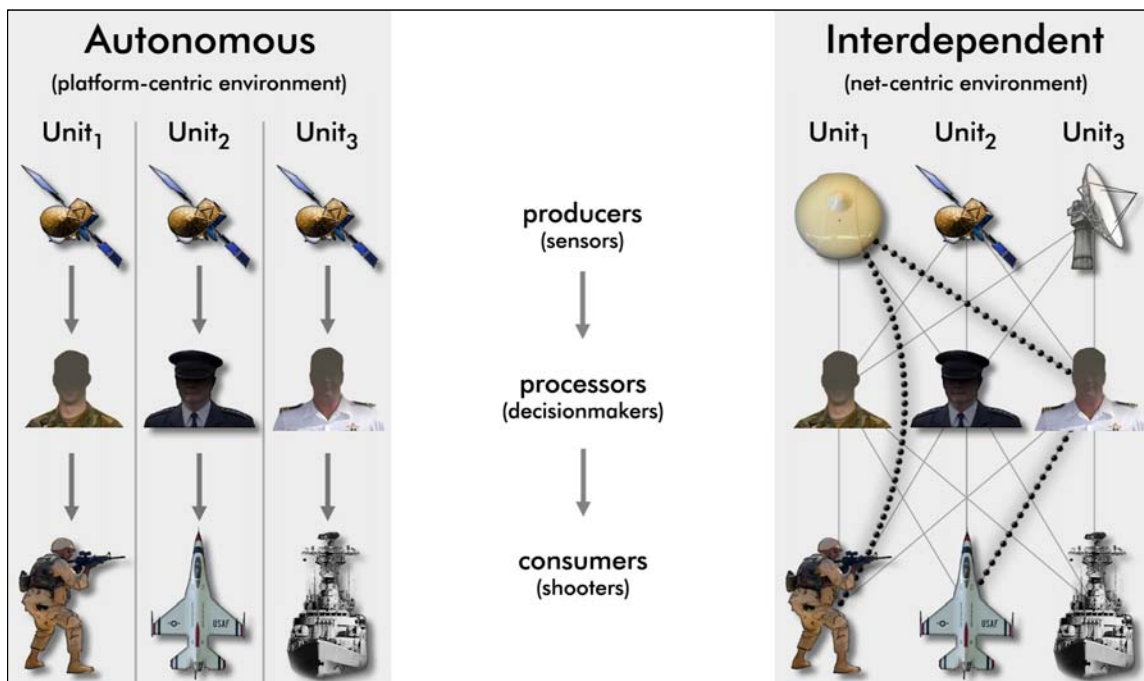
689 By removing the barriers to the flow of information and connecting geographically
 690 dispersed elements, the Net-Centric Environment provides the Joint Force and its mission
 691 partners the ability to exploit the efficiencies of the specialization of labor. Units across
 692 the echelons will no longer need the same degree of organic capabilities to achieve
 693 mission success, because they can confidently rely upon their ability to access the
 694 capabilities they require but which are provided by other units, organizations or
 695 individuals. Capabilities with a relatively low utility or usage in a particular mission can
 696 either remain in garrison or can be more easily employed by other units that have a
 697 greater need. Figure 3.4 illustrates the relative increases in integration, efficiency and
 698 effectiveness of constructive interdependence achieved by moving from a platform
 699 centric to a Net-Centric Environment.



700 **Figure 3-4—Increasing Integration toward Constructive Interdependence**

701 The Net-Centric Environment allows for the creation of capabilities that were heretofore
 702 unavailable or possibly unknown, but which are adapted to the characteristics of the
 703 specific environment in which they are intended to function. This creation of new
 704 capabilities from connection of the latent capabilities within the joint force is referred to
 705 as *constructive interdependence*. Figure 3.5 illustrates the creation of additional
 706 combinations of capabilities (potentially unusable in a platform-centric environment) that
 707 may be derived from the Net-Centric Environment. Note that although figure 3.5 focuses

708 on a sensor-decider-shooter scenario, this idea can easily be extended to other scenarios
 709 such as producer-processor-consumer.



710

711 **Figure 3-5—Increased Combinations of Capabilities in the Net-Centric Environment versus**
 712 **the Platform-Centric Environment**

713 ***3.5 Application of Concept within a Campaign Framework***

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

724 The advantages of operating in a Net-Centric Environment impact all of the functions of
 725 the Joint Force and its mission partners. For example, U.S. forces, could assist local
 726 governments, international relief agencies and NGOs coordinate humanitarian assistance
 727 efforts much more easily in a Net-Centric Environment because the barriers to
 728 information flow would have been removed. COIs, supported by the transparency of the
 729 constituent organizations, will be able to coordinate the distribution of food or medical
 730 assistance more rapidly and effectively than with traditional coordination mechanisms

731 (Focused Logistics Area). Information exchange²⁵ will depend less on information
732 exchange agreements, liaison officers, and formal coordination meetings. There will be
733 formal barriers in place (clearance and role) and informal barriers (behavior as good
734 citizens in the Net-Centric Environment) to establish the visibility of data and address
735 security needs. Joint Force and mission partner planners will be able to share situational
736 awareness, the availability of resources, and readiness of capabilities to be deployed with
737 greater ease, efficiency and effectiveness.

738 The Net-Centric Environment will reduce the friction²⁶ of both large and small mission
739 transitions. The lessening of friction in the course of transitioning from one task or
740 mission to another creates opportunities for the Joint Force to use combinations of
741 capabilities. Over the course of the operation, Joint Forces are less reliant on unwieldy or
742 brittle synchronization mechanisms in a Net-Centric Environment because the
743 information and decision rights and responsibilities are guiding the flow of information
744 and the decision points across a singular effort. As the mission in a complicated,
745 uncertain and dynamic operational environment unfolds, access to the network and the
746 visibility of data will adjust in response to the changing roles and missions of elements of
747 the Joint Force.

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

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

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

768 **4.0 Capabilities and Attributes**

769 This chapter describes the capabilities as well as attributes and related measures required
 770 in the Net-Centric Environment. A capability is the ability to achieve an effect to a
 771 standard under specified conditions through multiple combinations of means and ways to
 772 perform a set of tasks²⁷, and an attribute is a measurable characteristic of a capability.
 773 Appendix D lists the capabilities and supporting tasks as well as attributes and supporting
 774 measures in tabular form.

775 **4.1 Areas**

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

784 **4.1.1 Knowledge Area**

785 The Knowledge Area is where human interactions occur between elements of the Joint
 786 Force and its mission partners, for example, the exchange of information, shared
 787 awareness, shared understanding, and collaborative decisionmaking. Because of the
 788 increasing diversity and scope of organizations and forces involved in Joint Force
 789 operations, the interactions between them become more complicated, requiring new and
 790 more capable collaborative efforts. It is within this area that individuals develop
 791 situational awareness and share this awareness with other entities to produce a shared
 792 awareness. This leads to improved understanding at the individual level and to improved
 793 shared understanding. This process enables the creation of faster, higher quality decisions
 794 both individually and collaboratively as the situation requires. The Joint Force and its
 795 mission partner components will set up ad hoc, and sometimes dispersed mission-based
 796 organizations that will change as the missions and tasks change, which in turn will alter
 797 the information exchange requirements among the entities. Participants in these
 798 networked organizations will be selected based on their knowledge of the problem or task
 799 at hand and the capabilities they provide, and will function with a minimum set of
 800 formalized rules and procedures²⁸.

801 **4.1.2 Technical Area**

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

²⁷ JCDRP (7/2004)

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

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

814 **4.2 Capabilities**

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

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

828 **4.2.1 Knowledge Capabilities**

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

²⁹ Network Centric Operations Conceptual Framework Version 2.0

841 **Ability to collaborate.** Collaboration is extremely important to operating in the Net-
842 Centric Environment. Collaboration must be continuous, include geographically
843 separated participants, and involve all relevant parties. Doctrinal, cultural, and
844 organizational limits to full collaboration will need to be removed, and leaders will need
845 to be trained, and procedures implemented, to develop trust in collaborative
846 decisionmaking processes and organizational structure.

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

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

857 **Ability to share situational understanding.** Where situational awareness is the “who’s
858 where and what are they doing” aspect of battle space knowledge, situational
859 understanding is the “what does it mean and what can I do about it” aspect. Individuals
860 will use reasoning methods and tools to achieve the required level of understanding.³⁰
861 Sharing their understandings with a wide array of participants will provide a synergy that
862 leads to a higher quality collective understanding and contributes to high quality
863 decisionmaking.

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

873 **Ability to achieve constructive interdependence.** Joint Operations establish formal rule
874 sets for combining capabilities from multiple services together to form new capabilities.
875 The idea of constructive interdependence extends this further by employing the network
876 (both human and technical) to allow a virtually limitless combination of latent service
877 and component capabilities in ways that create capabilities not previously achievable. For

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

878 example, an Army unit has pushed quicker than its organic logistics can support
879 ammunition requirements and is in need of quick re-supply. Fortunately, the unit does
880 have an attached truck unit with plenty of fuel. The most direct route to the supply depot
881 requires using a bridge over a swift river which has been weakened by the fighting, and
882 which is now unsafe. A nearby Marine unit has captured its objectives and has an
883 amphibious capability which has already been used and could ferry supplies past the
884 bridge. By looking across the network, the Army unit can ascertain the status of the
885 amphibious equipment, its capabilities and can establish direct contact with the Marine
886 unit to coordinate their activity. The Army unit also discovers via the network that the
887 Marine unit needs fuel immediately. The two units are able to efficiently and effectively
888 combine their respective unused capabilities at the tactical level to better accomplish
889 assigned missions. The Net-Centric Environment will also allow for the identification of
890 opportunities for constructive interdependence can be employed in wargaming and other
891 training exercises.

892 **4.2.2 Technical Capabilities**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

961 **Ability to provide network services.** The network must be capable of providing all
962 services generally associated with network operations such as, connect all assets, share
963 information among interagency/coalition/IO commercial/NGO participants, archive large
964 volumes of data, maintain network status, and keep all nodes informed, support separate
965 constellations of COIs, and support geographically transitioning nodes.

966 **4.3 Attributes**

967 The attributes are the measurable aspects of the capabilities such as those listed in Section
968 4.3.1. The relationships are not one-to-one, but one-to-many, and many-to-many (see
969 Appendix D). In order to assess the effectiveness of capabilities in the Net-Centric
970 Environment, it is necessary to develop a set of performance related metrics. Measures
971 provide the linkage between overarching attributes and metrics by identifying the
972 important qualities of each attribute. The most appropriate metrics and associated units of
973 measurement differ based upon the operational context. Specific metrics are below the
974 scope of this version of the functional concept. However, metrics with scale and unit of
975 measure are required to evaluate specific capabilities. Future versions of this document
976 should include more detailed metrics derived from both the current JIC processes (see
977 section 6.6) and specific net-centric metric development efforts.

978 **4.3.1 Knowledge Attributes**

979 **Agile**

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

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

990 **Quality**

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

- 993 • Appropriate: The extent to which understandings and decisions are suitable and
994 useful for the mission/situation at hand.
- 995 • Relevant: The extent to which an understanding/decision matches command intent
996 and mission objectives.

- 997 • Correct: The extent to which understandings agree with fact.
- 998 • Consistent: Extent to which understandings and decisions are in line with prior
- 999 understandings/decisions.
- 1000 • Accurate: The granularity and precision with respect to fact.
- 1001 • Complete: The extent to which all required elements are present.
- 1002 • Timely: The extent to which the currency of understandings or decisions are
- 1003 appropriate to the mission.

1004 **Trustworthy**

1005 Trustworthy is defined as the extent to which confidence or assurance is held in
1006 information or decisions. Trustworthiness is assessed using the following measures:

- 1007 • Robust: Having or exhibiting strength or vigorous health.
- 1008 • Confident: The extent to which assurance is held in information or decisions.
- 1009 • Willing: The extent to which a force entity possesses the desire to function in a shared
- 1010 information environment.
- 1011 • Competent: The extent to which one is able to perform a task and/or function.

1012 **4.3.2 Technical Attributes**

1013 **Assured**

1014 Assured is defined as having grounds for confidence that an information-technology (IT)
1015 product or system meets its certainty or security objectives. Assurance is assessed using
1016 the following measures:

- 1017 • Authentic: The extent of a security measure designed to establish the validity of a
- 1018 transmission, message, or originator, or a means of verifying an individual's
- 1019 authorization to receive specific categories of information
- 1020 • Confidential: The extent to which confidence or assurance is held in information or
- 1021 decisions.
- 1022 • Non-repudiated: The extent to which the senders/receivers of data are prevented from
- 1023 denying having processed the data. Non-repudiation is measured by the extent to which
- 1024 senders are provided with proof of delivery and the recipients are provided with proof of
- 1025 the sender's identity.
- 1026 • Available: The extent to which authorized users are provided timely, reliable access
- 1027 to data and information services.
- 1028 • Integrity: The extent to which information is protected from unauthorized
- 1029 modification or destruction.

1030 **Robust**

1031 Robust is defined as having or exhibiting strength or vigorous health. It is assessed using
1032 the following measures:

- 1033 • Survivable: The extent of assurance provided a system, subsystem, equipment,
1034 process, or procedure that the named entity will continue to function during and after a
1035 natural or man-made disturbance, for example, a nuclear burst. (*Note:* For a given
1036 application, survivability must be qualified by specifying the range of conditions over
1037 which the entity will survive the minimum acceptable level or post-disturbance
1038 functionality, and the maximum acceptable outage duration.)
- 1039 • Redundant: The extent to which surplus capability is provided to improve the
1040 reliability and quality of service.
- 1041 • Distributed: The extent to which the network resources, such as switching equipment
1042 and processors, are dispersed throughout the geographical area being served. (*Note:*
1043 Network control may be centralized or distributed.)
- 1044 • Resilient: The extent to which recovery from or adjustment to malfunction
1045 (misfortune) or change is easily achieved.

1046 **Agile**

1047 Agile is defined as moving quickly and easily. It is assessed using the following
1048 measures:

- 1049 • Flexible: The extent to which success is achieved in different ways and the extent to
1050 which the network dynamically meets evolving mission requirements.
- 1051 • Responsive: Responsiveness is the extent to which service is provided within required
1052 time.
- 1053 • Diverse: The extent to which the network is not dependent on a single element, media,
1054 or method.
- 1055 • Dynamic: The extent to which the network can adapt when there is a change in status.
- 1056 • Autonomous: The extent to which tasks are undertaken or carried on without outside
1057 control. It is the ability to exist independently; responding, reacting, or developing
1058 independently of the whole.

1059 **Manageable**

1060 Manageable is defined as capable of being controlled, handled, or used with ease.
1061 Manageable is assessed using the following measures:

- 1062 • Scalable: The extent to which the network/system/organization can grow to
1063 accommodate additional users; hardware or software either co-located or globally
1064 distributed from the original system configuration.
- 1065 • Reconfigurable: The extent to which the network/system/organization can
1066 accommodate changes in hardware, software, features or options.
- 1067 • Controllable: The extent to which a network manager has the ability to exercise
1068 restraint, direction over, or perform diagnosis to ensure optimal function and security;
1069 power or authority to guide, monitor, or manage.
- 1070 • Maintainable: The probability that an item will be retained in or restored to a
1071 specified condition within a given period of time, when the maintenance is performed in
1072 accordance with prescribed procedures and resources.
- 1073 • Upgradeable: The extent to which the network or system can accept new versions of
1074 software to meet changing requirements.
- 1075 • Repairable: The probability that the system/network can be to be restored to
1076 satisfactory operation by any action, including parts replacements or changes to
1077 adjustable settings.

1078 **Expeditionary**

1079 Expeditionary is defined as supporting a military operation conducted by an armed force
1080 to accomplish a specific objective in a foreign country. Expeditionary is assessed using
1081 the following measures:

- 1082 • Deployable: The extent of effort required to relocate personnel/systems to a Joint
1083 Operations Area (JOA).

- 1084 • Maneuverable: The extent to which network elements support warfighters on the
1085 move.
- 1086 • Modular: The extent to which the network/system comprises “plug-in” systems/
1087 units/forces that can be added together in different combinations.
- 1088 • Transportable: The extent of mobility within the JOA.
- 1089 • Rugged: The extent to which the system/network can support operations in extreme
1090 environments and/or under conditions of high physical stress.
- 1091 • Reach: The extent to which the network/system can operate over extended distances
1092 to meet mission requirements.
- 1093 • Employable: The time and effort required to commence system operation upon arrival
1094 in the JOA.
- 1095 • Sustainable: The extent to which the network/system is able to maintain the necessary
1096 level and duration of operational activity to achieve military objectives. Sustainability is a
1097 function of providing for and maintaining those levels of ready forces, materiel, and
1098 consumables necessary to support military effort.

1099 **Quality**

1100 Quality is defined as lacking nothing essential or normal. Quality is assessed using the
1101 following measures:

- 1102 • Accurate: The extent to which a transmission/data stream is error-free.
- 1103 • Traceable: The extent to which information is capable of being tracked or traced; the
1104 ability to follow, discover, or ascertain the course of development of something.
- 1105 • Complete: The extent to which all necessary parts, elements, or steps are present.
- 1106 • Consistent: The extent to which information is free from variation or contradiction.
- 1107 • Timely: The extent to which information is received in time to be useful.

1108 **Integrated**

1109 Integrated is defined as including all functions and capabilities focused toward a unified
1110 purpose. Integrated is assessed using the following measures:

- 1111 • Interoperable: The extent to which systems, units or forces can provide services to
1112 and accept services from other systems, units, or forces and to use the services so
1113 exchanged to enable them to operate effectively together.
- 1114 • Accessible: The extent to which all authorized users have the opportunity to make
1115 use of information capabilities.
- 1116 • Visible: The extent to which users and applications can discover the existence of
1117 data assets through catalogs, registries, and other search services. All data assets are
1118 advertised or “made visible” by providing metadata that describes the asset.
- 1119 • Usable: The extent of difficulty regarding the initial effort required to learn and
1120 the extent of recurring effort to use the functionality of the system and/or the extent to
1121 which the context of the information used and/or created by a information capability can
1122 be derived.

1123 **5.0 Implications**

1124 Net-Centric future force structure implications impact all the DOTMLPF areas.

1125 **5.1 Doctrine**

- 1126 • The Information Age may refine the application of the principles of war and the role
1127 of information in warfare will be made more explicit in doctrine.
- 1128 • Doctrine will continue to be a point of departure, guiding principles, and best
1129 practices.
- 1130 • Tactics, Techniques, and Procedures (TTPs) will evolve to reflect the increasing
1131 significance of information in all aspects of military operations.
- 1132 • Development of doctrine will be more dynamic and collaborative and will be driven
1133 increasingly by wargaming and experimentation.
- 1134 • Joint operations will become the norm at successively lower organizational
1135 hierarchical levels.

1136 **5.2 Organization**

- 1137 • The effective application of the elements of national power in the Information Age
1138 will require new organizational relationships between DOD and its mission partners
- 1139 • Within the Joint Force, organizational structures will transform as information and
1140 understanding are shared. New organizations will emerge, existing organizational
1141 structures will change (e.g., flatten) and some organizational structures will disappear.
- 1142 • The Net-Centric Environment will facilitate to a greater extent than is currently
1143 possible the formation of new organizations with diverse structures, resources, degrees of
1144 persistence, charters and missions. For instance, the diverse nature of Communities of
1145 Interest (COI) is best exploited in a Net-Centric Environment.
- 1146 • The extremities of organizations will become increasingly important as these nodes
1147 are fully connected in the environment. Horizontal relationships between organizations
1148 (both formal and informal) will grow more important.

1149 **5.3 Training**

- 1150 • Training curricula will need to change to develop the knowledge, experience, and
1151 desired behaviors for operating in a Net-Centric Environment. The curriculum change
1152 process must also become more responsive to rapidly transforming operational practices.
- 1153 • Exercises will need to focus more on gaining experience and familiarity with a broad
1154 spectrum of players drawn from the Joint Force and its mission partners and utilizing the
1155 Net-Centric Environment as the medium for interaction.
- 1156 • The concept of “train as you fight, fight as you train” will require training and
1157 exercises to take place on portions of operational networks in order to properly simulate
1158 the complex interactions that occur in the Net-Centric Environment. Live Virtual
1159 Constructive training environments will emerge.
- 1160 • Training will need to support the ability of individuals and small groups to plug into
1161 ad hoc teams or COIs without the benefit of the unit cohesion that comes from training
1162 and operating with a standing-unit over a longer period of time.

1163 **5.4 Materiel**

- 1164 • Solutions will be developed to connect traditionally disadvantaged users (those at the
1165 extremities of force or that operates in challenging mediums such as under the sea).
1166 These solutions must support near continuous access to enterprise services regardless of
1167 location or rate of movement. When disconnected from the network, these systems must
1168 continue to operate and allow graceful re-entry to the network to include automatic
1169 synchronization of information between the disconnected systems and enterprise
1170 resources.
- 1171 • Emphasis must shift to developing solutions that support all functional areas as
1172 primary customers as opposed to building better C2 networks.
- 1173 • Materiel solutions must support multiple levels of security in a dynamic COI
1174 architecture.
- 1175 • Identification verification technologies will need to evolve significantly to support
1176 dynamic role based security. Identity management concepts need to mature to support the
1177 dynamic requirements of the Net-Centric Environment.
- 1178 • Information systems must be designed to work with meta-data from a wide range of
1179 communities of interest.
- 1180 • Capabilities must be increasingly interoperable at the information and physical layers.
1181 Increased emphasis on the Net-Ready Key Performance Parameters and additional
1182 interoperability and net-centric processes, in particular systems engineering of end to end
1183 performance to implement real-time requirements, is necessary to ensure Technical Area
1184 Interoperability.
- 1185 • Digitally Assisted Aids/Tools help the commander assemble the information in ways
1186 that improve visualization and help create a rich understanding and assessment of
1187 potential alternatives that enable superior decisionmaking. They provide advanced
1188 planning and cognitive capabilities to aid in courses of action development, modeling,
1189 and simulation capabilities to evaluate COAs and predict results, and supporting
1190 analytical information to aid in dealing with uncertainty.
- 1191 • Intelligent user-modified agents will filter and frame user information requirements
1192 within the network, allowing commanders and staffs to access the information they need
1193 quickly and efficiently. The user-tailored information flow provides feedback to those
1194 teams publishing information so they can continually adjust their collection and fusion
1195 processes in such a way as to provide the most meaningful products, for example,
1196 information pull as well as push.
- 1197 • Fielding of materiel solutions must be better tied to joint training. Fielding of critical
1198 materiel solutions must include resources and planning for recurring training.

1199 **5.5 Leadership and Education**

- 1200 • Leadership will need to deal with the dispersion of authority across the set of
1201 temporary and informal organizational structures that will evolve under collaboration.
- 1202 • Leadership must embrace the cultural change required to effectively function in the
1203 Net-Centric Environment.
- 1204 • Education at all levels must address the new framework provided by the Net-Centric
1205 Environment and reinforce the cultural and cognitive changes required for success in this
1206 environment.

- 1207 • Leadership development will need to address the challenges of decisionmaking in a
1208 Net-Centric Environment.
- 1209 • Educational institutions must continually adapt to provide the best research and
1210 analysis on future warfighting concepts.
- 1211 • Leadership development will need to address the possibilities offered by self-
1212 synchronization and other concepts and their impact on the idea of unity of command or
1213 the command process.

1214 ***5.6 Personnel***

- 1215 • Administrative functions that require simple, repeated decisions will be phased out;
1216 administration will be more efficient, given the enhanced physical, psychological, and
1217 mental demands, and more personnel will be made available for duty in currently
1218 understaffed units.
- 1219 • Operating in a net-centric environment will create new mental and physiological
1220 demands on personnel. These will need to be addressed through a combination of human
1221 engineering (such as ergonomics), process engineering and personnel development.
- 1222 • Expertise not organic to units may be provided by a virtual presence or personnel,
1223 negating the need for a physical presence and/or assignment (e.g., analysts, advisors,
1224 maintainers). Through the use of reachback capability, distributed operations are enabled
1225 allowing for smaller deployed footprints and enhanced mobility, both strategic and
1226 tactical, for joint forces.

1227 ***5.7 Facilities***

- 1228 • Bases and facilities in CONUS and OCONUS will require continued investment and
1229 partnership with commercial information services to support a net-centric infrastructure
1230 and supported data management strategy for forces in garrison.
- 1231 • Training and exercise facilities will require a higher level and more thorough
1232 instrumentation to evaluate unit performance beyond the most basic metrics for success
1233 and to assess the use of information.

1234 **6.0 Scope**

1235 ***6.1 Timeframe and Applicable Military Functions and Activities***

1236 The NCE JFC is written for the Joint Force Commander at the operational level 10-20
1237 years in the future with applicability across all levels of command from strategic to
1238 tactical and across the ROMO.

1239 The NCE JFC provides functional support to the JOCs, other JFCs, and describes the net-
1240 centric capabilities, attributes, and measures in support of the JICs and the Capabilities
1241 Based Assessment (CBA) analysis process. It also provides a conceptual basis and
1242 analytical framework for the operation of the Net-Centric Functional Capabilities Board.

1243 ***6.2 Impact of Strategic Guidance and Deviations in the Concept***

1244 The challenges of the evolving operational environment require that U.S. military force,
1245 all relevant agencies, and coalition partners work together with the Joint Staff and other
1246 DOD agencies to enhance, integrate, and develop new Joint warfighting capabilities. The
1247 mandates set forth in the National Security Strategy, 2004 National Defense Strategy, and
1248 National Military Strategy serve as a basis for the development of strategic and
1249 operational Joint Force capabilities required for operating in the Net-Centric Environment.
1250 The NCE JFC conforms to the strategic guidance by providing the net-centric capabilities
1251 and attributes that enable the U.S. military to conduct the required net-centric tasks and
1252 activities necessary to meet the strategic guidance.

- 1253 • National Security Strategy (NSS): The NSS directs an active strategy to counter
1254 transnational terrorist networks, rogue nations, and aggressive states that possess, or are
1255 working to gain, Weapons of Mass Destruction or Effect (WMD/E). It emphasizes
1256 activities to foster relationships among U.S. allies, partners, and friends. The NSS
1257 highlights the need to retain and improve capabilities to prevent attacks against the
1258 United States, work cooperatively with other nations and multinational organizations, and
1259 transform America's national security institutions.
- 1260 • National Defense Strategy (NDS): The NDS supports the NSS by establishing a set of
1261 overarching defense objectives that guide the DOD's security activities and provide
1262 direction for the National Military Strategy. The NDS objectives serve as links between
1263 military activities and those of other government agencies in pursuit of national goals.
- 1264 • National Military Strategy (NMS): The NMS derives objectives, missions, and
1265 capability requirements from an analysis of the NSS, NDS, and security environment.
1266 The NMS provides focus for military activities by defining a set of interrelated military
1267 objectives and Joint operating concepts from which the service chiefs and combatant
1268 commanders identify desired capabilities and against which the Chairman of the Joint
1269 Chiefs of Staff assesses risk.

1270 ***6.3 Impact of Future Context Documents and Deviations in the*** 1271 ***Concept***

1272 This concept was developed in the context of numerous DOD efforts to transform the
1273 force. The Network Centric Operations Conceptual Framework 2.0, Net-Centric

1274 Operations and Warfare Reference Model 1.1, and DoD Net-Centric Data Strategy
1275 played particularly important roles in the identification of required capabilities and
1276 attributes. This document provides a unifying framework of principles, capabilities and
1277 attributes to integrate the many net-centric efforts underway. Future updates to these and
1278 other net-centric related documents, such as the Net Ops Conops and the future NCOE
1279 CONOPS should reflect the capabilities identified in this concept.

1280 Deviations from this concept (particularly in foundational elements such as definitions) in
1281 future context documents will likely hinder progress toward achieving a net-centric force
1282 by furthering the lexicon issues which have already been identified as problematic.³¹
1283 However, this concept acknowledges that the understanding of the net-centric functional
1284 area is immature and rapidly expanding. As the community's understanding of Network
1285 Centric Operations evolves, new principles, capabilities, and attributes are likely to be
1286 identified and should be incorporated into future revisions of this concept.

1287 ***6.4 Risks and Mitigation***

1288 Military commanders and leaders at all levels will need to manage risks as they operate in
1289 a Net-Centric Environment. Risks remain inherent in the planning and execution of
1290 military operations. Additionally, there are risks associated with identifying, developing,
1291 attaining, and maintaining future net-centric capabilities 10-20 years in the future.
1292 Military leaders must employ prudent risk management strategies, including both the
1293 acceptance of calculated risks and the development of comprehensive risk mitigation
1294 techniques. The risk mitigation discussed below is only a point of departure and the
1295 implications section of this concept provides more details on necessary changes, most of
1296 which address one or more risks. The following list is intended to identify significant
1297 risks associated with implementing a Net-Centric Environment. This list is not intended
1298 to be exhaustive.

- 1299 • The increasing dependence on information processes, systems, and technologies adds
1300 potential vulnerabilities that, if not adequately defended, could be exploited by
1301 adversaries, or result in serious mission consequences. Mitigation: Increased network
1302 security training and emphasis at all levels. Development of new Information Assurance
1303 strategies and technologies.
- 1304 • Elimination of intermediate echelons and the ability to monitor force activity at an
1305 arbitrary level of detail may lead to information-enabled micromanagement, inhibiting
1306 the decentralization of decisionmaking to lower echelons. Mitigation: Wargaming and
1307 experimentation to inculcate value of decentralization. Education.
- 1308 • Overwhelming levels of information may lead to increased decision times or the
1309 inability of leaders to locate and identify decision-relevant information. Mitigation:
1310 Investment in smart agent technology; Training; Wargaming in a Live Virtual Training
1311 Environment.

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

- 1312 • Capability and interoperability gaps in training, equipment, physical interfaces, and
1313 doctrine may pose challenges for operations with less digitally-capable forces.
1314 Mitigation: Retain key legacy interfaces. Increase training with allies in scenarios such as
1315 described in the vignette.
- 1316 • Over-reliance on information and communications technologies may result in forces
1317 incapable of operating effectively in the absence of those technologies due to failure or
1318 attack. Mitigation: Increased reliability of new equipment and appropriate levels of
1319 integrated redundancy in system architectures. Training and exercises that realistically
1320 simulate conditions of failure and attack.
- 1321 • Failure to co-evolve technological, organizational, and doctrinal innovation may lead
1322 to inefficiencies in the deployment and utilization of net-centric systems and concepts.
1323 Such failure may arise from, for example, unresponsive acquisition processes,
1324 organizational and cultural inertia, insufficient scientific advancement, or overly
1325 optimistic assumptions about technical or organizational capabilities. Mitigation:
1326 Increased joint wargaming and exercises, particularly at the small unit level. Increased
1327 investment in commercial technology. Integrated Joint Concept Development and
1328 experimentation.
- 1329 • Insufficient scientific understanding of the psychological and sociological
1330 foundations of cognitive and social behavior results in fielding systems, designing
1331 organizational structures, and developing doctrine that is not effective in real-world
1332 Knowledge systems. Mitigation: Increased research in this area.

1333 ***6.5 Assumptions***

1334 There are several assumptions common to all Joint Functional Concepts that provide the
1335 overarching environment in which U.S. military operations will take place:

- 1336 • Future U.S. joint military operations will take place in a Net-Centric Environment;
- 1337 • Affordable technology will allow coalition partners and other agencies to acquire net-
1338 centric materiel;
- 1339 • The U.S. will be operating in a complicated, uncertain and dynamic global security
1340 environment 10-20 years in the future; and
- 1341 • There will be greater emphasis on asymmetric threats and the possession and
1342 potential use of weapons of ever increasing power.

1343 There are also critical assumptions that are relevant to the NCE JFC:

- 1344 • Substantial continued investment in research and development will overcome
1345 unanticipated barriers to technical advancement that would preclude sustained change in
1346 military operations; and
- 1347 • DOD and Service cultures will evolve at an increasing rate to accept and employ
1348 knowledge area capabilities

1349 ***6.6 Relationship to Other Joint Concepts***

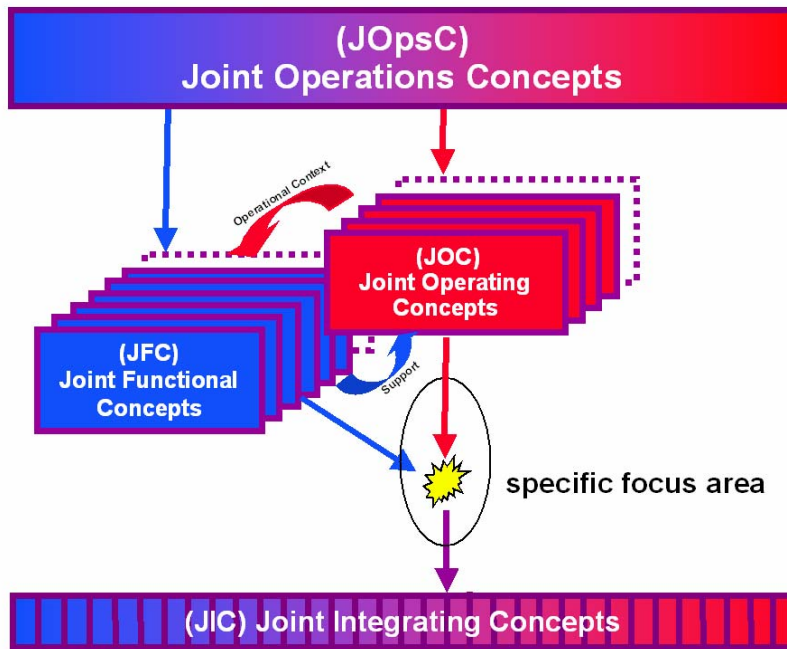
1350 An assumption common to all joint concepts is that future U.S. military operations will
1351 occur in a Net-Centric Environment. The relationship among the various families of
1352 concepts is depicted in figure 6-1. The Net-Centric Environment Joint Functional

1353 Concept must provide net-centric support to each of the joint concepts thereby assisting
1354 the Joint Force Commander in shaping the battlespace. The Net-Centric Environment
1355 Joint Functional Concept:

- 1356 • Identifies essential Net-Centric Environment capabilities that enable the conduct of
1357 net-centric technical tasks and activities across the ROMO in support of joint operations
1358 using a network that is ubiquitous, autonomous, interoperable, and reliably supports
1359 tactical, operational, and strategic needs;
- 1360 • Identifies essential Net-Centric Environment capabilities that enable humans to
1361 leverage the technology and conduct comprehensive collaboration in support of
1362 decisionmaking, staff planning, and battlefield management in a distributed and
1363 decentralized manner;
- 1364 • Supports the Net-Centric Environment capabilities identified in the joint operating
1365 concepts, joint functional concepts, and joint integrating concepts;
- 1366 • Provides a single point of reference to inform and influence the joint concepts
1367 regarding the net-centric military function (net-centric capabilities and attributes); and
1368 • Provides a single point of reference to synchronize net-centric terms and activities.

1369 Capabilities identified in Version 1.0 of the C2 Joint Functional Concept that (1) are
1370 network-related and (2) appear to have application across multiple functional areas, have
1371 been expanded upon in this concept in order to show an integrated, net-centric concept
1372 that, if implemented, will optimize information-dependent capabilities across all
1373 functional areas. These capabilities do not replace the need for specific C2 capabilities,
1374 but rather complement the C2 capabilities by providing a framework to integrate the Joint
1375 Force at a lower, more informal and more efficient level. Figure 6-2 depicts the
1376 relationship of the Net-Centric Environment to the other functional areas.

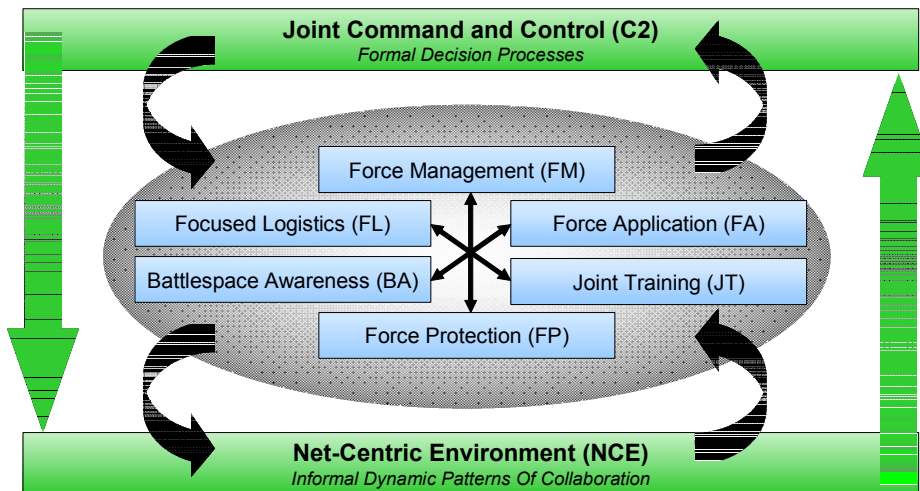
1377



1378

1379

Figure 6-1—Relationships of Joint Concepts



1380

1381

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

1382 **Appendix A Reference Documents**

- 1383 1. “Net Ready Key Performance Parameter, (v1.0)” briefing, n.d.
- 1384 2. 2004 National Defense Strategy, 2004
- 1385 3. ADM GIG BE, 3 January 2003
- 1386 4. ASD NII Memo Subj: Joint Net-Centric Capabilities, 15 July 2003
- 1387 5. ASD NII Net-Centric Checklist v. 2.1, 13 February 2004
- 1388 6. Battlespace Awareness Functional Concept, 4 February 2004
- 1389 7. C4ISR Architecture Framework, 18 December 1997
- 1390 8. CJCSM Instruction 3170.01, “Joint Capabilities Integration Development System”,
1391 12 March 2004
- 1392 9. Concept of Operations for Global Information Grid Net Ops (Net Ops CONOPS)
1393 Final Version, n.d.
- 1394 10. Data Visibility Component Guidance, 24 October 2003
- 1395 11. DOD Architecture Framework (DODAF), v. 1.0, Desktop, 11 February 2004
- 1396 12. DOD Architecture Framework (DODAF), v. 1.0, Volume 1, 9 February 2004
- 1397 13. DOD Architecture Framework (DODAF), v. 1.0, Volume 2, 10 February 2004
- 1398 14. DODD 8101.1, Global Information Grid (GIG) Overarching Policy, 19 September
1399 2002
- 1400 15. DOD Discovery Metadata Standard Review, 2 June 2003
- 1401 16. DOD Net-Centric Data Strategy, 9 May 2003
- 1402 17. Focused Logistics Functional Concept, 4 February 2004
- 1403 18. Force Application Functional Concept, 4 February 2004
- 1404 19. Force Protection Functional Concept, 4 February 2004
- 1405 20. Global Information Grid Enterprise Services (GIG ES): Core Enterprise Services
1406 (CES) Implementation, 10 November 2003
- 1407 21. Homeland Security Joint Operating Concept, 2 February 2004
- 1408 22. Joint Capabilities Integration and Development System (CJCSI 3170.01D), 12 March
1409 2004
- 1410 23. Joint Command and Control Functional Concept, 4 February 2004
- 1411 24. Joint Concept Development and Revision Plan, July 2004
- 1412 25. Joint Operations Concepts (JOpsC), 3 November 2003
- 1413 26. Joint Publication 1-02, “Department of Defense Dictionary of Military and
1414 Associated Terms,” 12 April 2001, (as amended through 23 March 2004)
- 1415 27. Joint Transformation Roadmap, July 2004

- 1416 28. Joint Vision 2020, n.d.
- 1417 29. Major Combat Operations Joint Operating Concept, 5 March 2004
- 1418 30. Military Acronyms, Initials and Abbreviations:
1419 <http://www.fas.org/news/reference/lexicon/acronym.htm>
- 1420 31. National Military Strategy, n.d.
- 1421 32. Naval Operating Concept for Joint Operations, n.d.
- 1422 33. Naval Transformation Roadmap 2003: Assured Access and Power Projection ...From
1423 the Sea, n.d.
- 1424 34. Net-Centric Operations and Warfare Reference Model Version 1.0, 9 December 2003.
- 1425 35. Net-Centric Operations and Warfare Reference Model Version 1.0, 9 December 2003.
- 1426 36. Net-Centric Operations and Warfare Reference Model Version 1.0, 9 December 2003.
- 1427 37. Network Centric Operations DOD Report to Congress, 27 July 2001
- 1428 38. *Network Centric Warfare: Developing and Leveraging Information Superiority*,
1429 August 1999
- 1430 39. Quadrennial Defense Review Report, 30 September 2001
- 1431 40. Stability Operations Joint Operating Concept, March 2004 (Draft)
- 1432 41. Strategic Deterrence Joint Operating Concept, 11 February 2004
- 1433 42. The National Security Strategy of the United States of America, September 2002
- 1434 43. The U.S. Air Force Transformation Flight Plan, November 2003
- 1435 44. Transformation Planning Guidance, 30 April 2003
- 1436 45. *Understanding Information Age Warfare*, 1 August 2001
- 1437 46. United States Army Transformation Roadmap 2003, 1 November 2003
- 1438

1439

Appendix B Glossary

Term	Definition
Action	A structured behavior of limited duration. (JCDRP 7/2004)
Activity	A structured behavior of continuous duration. (JCDRP 7/2004)
Agility	The ability to move quickly and easily. (<i>Power to the Edge</i>)
Assured	Having grounds for confidence that an information-technology (IT) product or system meets its certainty or security objectives. (NCE JFC)
Assumption	A supposition on the current situation or a presupposition on the future course of events, either or both assumed to be true in the absence of positive proof, necessary to enable the commander in the process of planning to complete an estimate of the situation and make a decision on the course of action. (JP 1-02)
Attribute	A testable or measurable characteristic that describes an aspect of a system or capability (CJCSI 3170.01D)
Capability	The ability to achieve an effect to a standard under specified conditions through multiple combinations of means and ways to perform a set of tasks (JCDRP 7/2004)
Collaboration	Joint problem solving for the purpose of achieving shared understanding, making a decision, or creating a product across the Joint Force and mission partners. (NCE JFC)
Communities of Interest	Collaborative groups of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes and who therefore must have a shared vocabulary for the information they exchange. (DOD Net-Centric Data Strategy)
Condition	A variable of the environment that affects performance of a task. (JCDRP 7/2004)
CONOPS (Concept of Operations or Commander's Concept)	The overall picture and broad flow of tasks within a plan by which a commander maps capabilities to effects, and effects to end state for a specific scenario. (JCDRP 7/2004)
Criterion	A critical, threshold, or specified value of a measure. (JCDRP 7/2004)
Data	Information without context. (JC2FC v1.0)
Doctrine	Fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application. (JP 1-02)
De-confliction	Preventing elements of the Joint Force from operating at cross-purposes. (NCE JFC)
Effect	An outcome (condition, behavior, or degree of freedom) resulting from tasked actions. (JCDRP 7/2004)

Term	Definition
End state	The set of conditions, behaviors, and freedoms of action that defines achievement of the commander's objectives. (JCDRP 7/2004)
Expeditionary	Supporting a military operation conducted by an armed force to accomplish a specific objective in a foreign country. (JP1-02)
Friction	The amount of organizational effort required to bring a certain set of capabilities to bear in a specified amount of time. (NCE JFC)
Geo-spatial Information	The concept for collection, information extraction, storage, dissemination, and exploitation of geodetic, geomagnetic, imagery (both commercial and national source), gravimetric, aeronautical, topographic, hydrographic, littoral, cultural, and toponymic data accurately referenced to a precise location on the earth's surface. (JP 1-02)
Information	Facts, data, or instructions in any medium or form with context that is comprehensible to the user. (JC2FC v1.0)
Information Resource	Information and related resources, such as personnel, equipment, funds, and information technology (USC Title 44)
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (USC Title 44 (Paperwork Reduction Act))
Infrastructure	All building and permanent installations necessary for the support, redeployment, and military forces operations (e.g., barracks, headquarters, airfields, communications, facilities, stores, port installations, and maintenance stations). (JP 1-02)
Integrated	All functions and capabilities focused toward a unified purpose. (NCE JFC)
Interdependence	A mode of operations based upon a high degree of mutual trust, where diverse members make unique contributions toward common objectives and may rely on each other for certain essential capabilities rather than duplicating them organically. (JS J7 JTD)
Interoperability	The extent to which systems, units or forces provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together. (DoDD 4630.5)
Joint	Connotes activities, operations, organizations, etc., in which elements of two or more Military Departments participate with interagency and multinational partners. (JS J7 JTD)

Term	Definition
Joint Force	The term “Joint Force” in its broadest sense refers to the Armed Forces of the United States. The term “joint force” (lower case) refers to an element of the Armed Forces that is organized for a particular mission or task. Because this could refer to a joint task force or a unified command, or some yet unnamed future joint organization, the more generic term “a joint force” will be used, similar in manner to the term “joint force commander” in reference to the commander of any joint force. (NCE JFC)
Joint Functional Concept (JFC)	An articulation of how a future joint force commander will integrate a set of related military tasks to attain capabilities required across the range of military operations. Although broadly described within the Joint Operations Concepts, they derive specific context from the joint operating concepts and promote common attributes in sufficient detail to conduct experimentation and measure effectiveness. (JCDRP 7/2004)
Joint Integrating Concept (JIC)	A JIC describes how a joint force commander integrates functional means to achieve operational ends. It includes a list of essential battlespace effects (including essential supporting tasks, measures of effectiveness, and measures of performance) and a CONOPS for integrating these effects together to achieve the desired end state. (JCDRP 7/2004)
Joint Operating Concept (JOC)	A description of how a future Joint Force Commander will plan, prepare, deploy, employ, and sustain a joint force against potential adversaries’ capabilities or crisis situations specified within the range of military operations. Joint Operating Concepts serve as “engines of transformation” to guide the development and integration of joint functional and Service concepts to describe joint capabilities. They describe the measurable detail needed to conduct experimentation, permit the development of measures of effectiveness, and allow decisionmakers to compare alternatives and make programmatic decisions. (JCDRP 7/2004)
Joint Operations Concepts (JOpsC)	An overarching description of how the future Joint Force will operate across the entire range of military operations. It is the unifying framework for developing subordinate joint operating concepts, joint functional concepts, enabling concepts, and integrated capabilities. It assists in structuring joint experimentation and assessment activities to validate subordinate concepts and capabilities-based requirements. (JCDRP 7/2004)
Knowledge	Data and information that have been analyzed to provide meaning and value. Knowledge is the collection of various pieces of processed data and information that have been integrated through the lens of understanding to begin building a picture of the situation. (NCE JFC)
Lethality	The capability to destroy or neutralize a target. (NCE JFC)

Term	Definition
Material	All items (including ships, tanks, self-propelled weapons, aircraft, etc., and related spares, repair parts, and support equipment, but excluding real property, installations, and utilities) necessary to equip, operate, maintain, and support military activities without distinction as to its application for administrative or combat purposes. (JP1-02)
Manageable	Capable of being controlled, handled, or used with ease. (NCE JFC)
Measure	Quantitative or qualitative basis for describing the quality of task performance. (JCDRP 7/2004)
Measures of Performance	Measures designed to quantify the degree of perfection in accomplishing functions or tasks. (JCDRP 7/2004)
Measures of Effectiveness	Measures designed to correspond to accomplishment of mission objectives and achievement of desired effects. (JCDRP 7/2004)
Metadata	Information about information; more specifically, information about the meaning of other data. (JP 1-02)
Metric	A quantitative measure associated with an attribute. (JCDRP 7/2004)
Mission	The end state, purpose, and associated tasks assigned to a single commander. (JCDRP 7/2004)
Mission Partners	Includes allies, coalition partners, international organizations, civilian government agencies, non-government agencies, and other non-adversaries who are involved with the activities or operations of the Joint Force. (NCE JFC)
Multinational Organizations	A collective heading for intergovernmental and international organizations. (JP 3-16)
Net-Centric Environment	The Net-Centric Environment is a framework for full human and technical connectivity and interoperability that allows all DOD users and mission partners to share the information they need, when they need it, in a form they can understand and act on with confidence; and protects information from those who should not have it. (NCE JFC)
Net-Centric (network centric) Operations	The exploitation of the human and technical networking of all elements of an appropriately trained joint force by fully integrating collective capabilities, awareness, knowledge, experience, and superior decisionmaking to achieve a high level of agility and effectiveness in dispersed, decentralized, dynamic and uncertain operational environments. (NCE JFC)

Term	Definition
Network Centric Warfare	An information superiority oriented concept of operations that generates increased combat power by networking sensors, decisionmakers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. (<i>Network Centric Warfare</i>) A sub-set of Net-Centric Operations, see above.
Objective	A desired end derived from guidance. (JCDRP 7/2004)
Quality	Lacking nothing essential or normal. (Roget's II)
Risk	Probability and severity of loss linked to hazards. (JP 1-02)
Robust	Having or exhibiting strength or vigorous health (Webster's)
Shared Understanding	A shared appreciation of the situation supported by common information to enable rapid collaborative joint engagement, maneuver, and support. (NCE JFC)
Standard	The minimum proficiency required in the performance of a task. For mission-essential tasks of Joint Forces, each task standard is defined by the Joint Force commander and consists of a measure and criterion. (JCDRP 7/2004)
Survivability	The capability of a system and its crew to avoid or withstand a man-made hostile environment without suffering an abortive impairment of its ability to accomplish its designated mission. (NCE JFC)
Synchronization	(1) The arrangement of military actions in time, space, and purpose to produce maximum relative combat power at a decisive place and time and (2) in the intelligence context, application of intelligence sources and methods in concert with the operation plan. (JP 2-0) (JP 1-02)
System	A regularly interacting group of items forming a unified whole. (Merriam-Webster Online)
Task	An action or activity defined within doctrine, standard procedures, or concepts that may be assigned to an individual or organization. (JCDRP 7/2004)
Transparency	Encourages open access to information, participation, and decision making, which ultimately creates a high level of trust and collaboration among stakeholders. (NCE JFC)
Trustworthy	The extent to which confidence or assurance is held in information or decisions (NCE JFC)
Understanding	Knowledge that has been synthesized and had judgments applied to it in the context of a specific situation. Understanding reveals the relationships among the critical factors in any situation. (NCE JFC)

Term	Definition
User	Any individual, organization or automated system that interfaces with the information environment as a consumer or producer. (NCOW Reference Model)
Vignette	A concise narrative description that illustrates and summarizes pertinent circumstances and events from a scenario. (JCDRP 7/2004)

1440

1441 **Appendix C List of Acronyms**

1442	BCT	Brigade Combat Team
1443	C2	Command and Control
1444	CBA	Capabilities Based Assessment
1445	CBRNE	Chemical, Biological, Radiological, Nuclear, and High Yield Explosives
1446	CJTF	Combined Joint Task Force
1447	COA	Course of Action
1448	COIs	Communities of Interest
1449	CONUS	Continental United States
1450	DOD	Department of Defense
1451	DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership and Education,
1452		Personnel, Facilities
1453	ERT	Emergency Response Team
1454	EUCOM	European Command
1455	HA/DR	Humanitarian Assistance/Disaster Relief
1456	HUMINT	Human Intelligence
1457	ICRC	International Community of the Red Cross
1458	IHRN	International Human Relief Network
1459	IRS	Internal Revenue Service
1460	IS	Information System
1461	IT	Information Technology
1462	JCDRP	Joint Concept Development and Revision Plan
1463	JCIDS	Joint Capabilities Integration and Development System
1464	JFC	Joint Functional Concept
1465	JIC	Joint Integrating Concept
1466	JOA	Joint Operations Area

1467	JOC	Joint Operating Concept
1468	JOpsC	Joint Operations Concepts
1469	JP	Joint Publication
1470	JROC	Joint Requirements Oversight Council
1471	JTF	Joint Task Force
1472	MDPs	Military Decisionmaking Processes
1473	NATO	North Atlantic Treaty Organization
1474	NCE JFC	Net-Centric Environment Joint Functional Concept
1475	NC FCB	Net-Centric Functional Capabilities Board
1476	NCO CF	Network Centric Operations Conceptual Framework
1477	NCO	Network Centric Operations
1478	NCOW	Network Centric Operations and Warfare
1479	NCW	Network Centric Warfare
1480	NDS	National Defense Strategy
1481	NGO	Non-Governmental Organization
1482	NMS	National Military Strategy
1483	NORTHCOM	Northern Command
1484	NSS	National Security Strategy
1485	OASD/NII	Office of the Assistant Secretary of Defense for Networks and Information
1486		Integration
1487	OCONUS	Outside the Continental United States
1488	OIRS	Organization for International Relief and Support
1489	OPSEC	Operations Security
1490	QDR	Quadrennial Defense Review
1491	ROMO	Range of Military Operations
1492	RRF	Rapid Reaction Force

1493	SOCOM	Special Operations Command
1494	SOP	Standards Operating Procedure
1495	SOUTHCOM	Southern Command
1496	TPG	Transformation Planning Guidance
1497	TRANSCOM	Transportation Command
1498	TTP	Tactics, Techniques, and Procedures
1499	UAV	Unmanned Aerial Vehicle
1500	UN	United Nations
1501	USR	Urban Search and Rescue
1502	WMD/E	Weapons of Mass Destruction/Effect

1503 **Appendix D Table of Capabilities and Attributes**

1504

1505

Table D-1—Knowledge Area Capabilities

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

1506

Table D-2—Technical Area Capabilities

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

1507

1508

1509

Table D-2—Technical Area Capabilities (continued)

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

1510

1511

Table D-3—Knowledge Area Attributes

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

1512

Table D-4—Technical Area Attributes

Attribute	Measure	Definition
Assured Grounds for confidence that an information-technology (IT) product or system meets its certainty or security objectives	Authentic	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual’s authorization to receive specific categories of information
	Confidential	Assurance that information is not disclosed to unauthorized persons, processes, or devices
	Non-repudiated	Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender’s identity, so neither can later deny having processed the data
	Available	Timely, reliable access to data and information services for authorized users
	Integrity	Protection against unauthorized modification or destruction of information
Robust Having or exhibiting strength or vigorous health	Survivable	A property of a system, subsystem, equipment, process, or procedure that provides a defined degree of assurance that the named entity will continue to function during and after a natural or man-made disturbance; <i>e.g.</i> , nuclear burst. <i>Note:</i> For a given application, survivability must be qualified by specifying the range of conditions over which the entity will survive, the minimum acceptable level or post-disturbance functionality, and the maximum acceptable outage duration
	Redundant	Surplus capability provided to improve the reliability and quality of service
	Distributed	A structure in which the network resources, such as switching equipment and processors, are dispersed throughout the geographical area being served. <i>Note:</i> Network control may be centralized or distributed
	Resilient	The extent to which recovery from or adjustment to malfunction (misfortune) or change is easily achieved
Agile Moving quickly and easily	Flexible	Dynamically meets evolving mission requirements.
	Responsive	Provides service within required time
	Diverse	Not dependent on a single element, media, or method
	Dynamic	System adapts when there is a change in status
	Autonomous	Undertaken or carried on without outside control; existing or capable of existing independently; responding, reacting, or developing independently of the whole

1513
 1514
 1515

1516

Table D-4—Technical Area Attributes (continued)

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

1517

1518

1519

Table D-4—Technical Area Attributes (continued)

Attribute	Measure	Definition
Quality Lacking nothing essential or normal	Accurate	The extent to which a transmission/data stream is error-free
	Traceable	Capable of being tracked or traced; Follow, discover, or ascertain the course of development of something
	Complete	Having all necessary parts, elements, or steps
	Consistent	Free from variation or contradiction
	Timely	The extent to which information is received in time to be useful
Integrated All functions and capabilities focused toward a unified purpose	Interoperable	The extent to which systems, units or forces provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together
	Accessible	Opportunity to make use of an information-system (IS) resource
	Visible	Users and applications can discover the existence of data assets through catalogs, registries and other search services. All data assets are advertised or “made visible” by providing metadata that describes the asset
	Usable	Regarding the initial effort required to learn and the recurring effort to use the functionality of the system

1520 **Appendix E Implications for Experimentation**

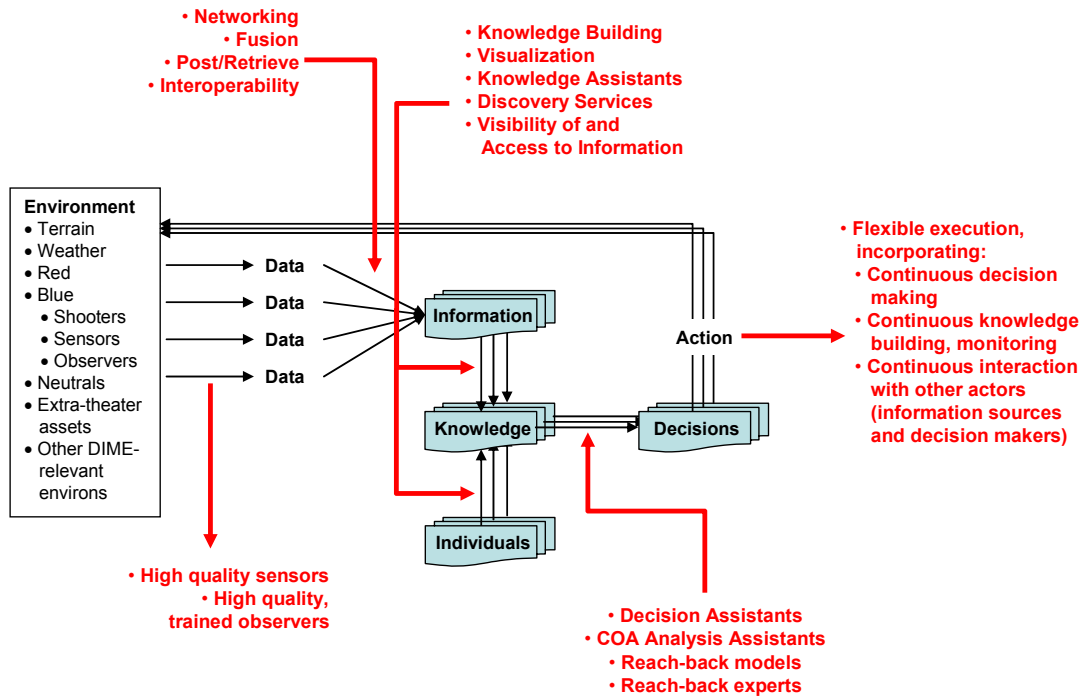
1521 The Net-Centric Environment Joint Functional Concept incorporates advanced and
 1522 emerging concepts and technologies, and deals extensively with areas of endeavor that
 1523 are not yet fully understood, particularly with regard to Knowledge Area issues. As a
 1524 result, a robust campaign of experimentation will be necessary in order to develop, refine,
 1525 test, and demonstrate net-centric concepts and methods.

1526 As a starting point for thinking about this experimentation campaign, this Appendix
 1527 captures a set of first-order hypotheses and issues for experimentation and research that
 1528 surfaced during concept development.

1529 ***E.1 First-Order Information Value Chain For The NCE JFC***

1530 A number of key ideas and postulated cause-effect relationships can be extracted from
 1531 the main document³² to allow one to construct a hypothesized “information value chain”
 1532 for the NCE JFC. This value chain describes a process by which data is gathered from the
 1533 operating environment, transformed into in-context information and actionable
 1534 knowledge, and used in decision processes that lead to force action, which in turn affects
 1535 the operating environment. At each stage in this process, force elements conduct
 1536 activities to gather, process, fuse, and share information. How, whether, and under what
 1537 conditions these processes add value to the force’s mission effectiveness are appropriate
 1538 subjects for a net-centric research and experimentation campaign. Figure E-1 shows one
 1539 portrayal of an information value chain with a set of enablers that must be well-
 1540 understood to contribute effectively to net-centric function of the force.

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



1541
1542
1543

Figure E-1—Illustrative Information Value Chain for the NCE JFC, with enabling assets, technologies, and organizational capabilities³³

1544 Following Figure E-1, sensors (human *and* machine) gather data to characterize the
1545 environment along dimensions relevant to the activity and mission of the force. The
1546 quality of this data extraction process, determined by the technical capability of sensing
1547 equipment, and the capability and training of human sensors/observers, is the foundation
1548 for building high-quality situational awareness. Extracted data is transported to various
1549 points in the force via the force’s human and technical networks, where it can be
1550 processed, fused, correlated, and placed into context. This allows individuals in the force
1551 to have access to information gathered by other force elements; further, it contributes to
1552 consistency in the information representations of individuals across the force (as those
1553 representations are drawn from a common, global set of information sources); and
1554 importantly, it provides for the representation and visualization of information in ways
1555 that are comprehensible and relevant for how it will subsequently be used by force
1556 elements.

1557 High quality information sets allow individuals to transform information resident in
1558 systems and transported across networks to be incorporated into individuals’ knowledge
1559 sets. The NCE JFC characterizes these processes as gaining *awareness* and
1560 *understanding* of the situation. Just as networking allowed information sets to be

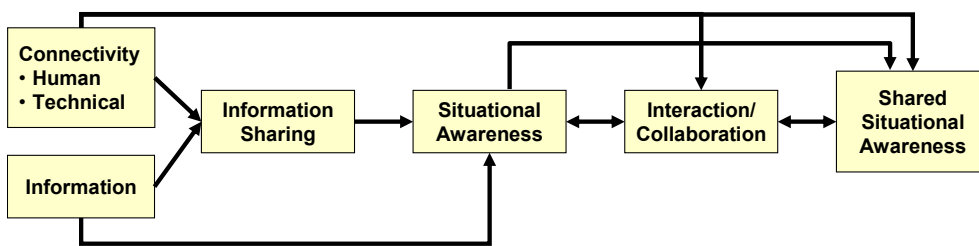
1561 correlated and consistent, networking does the same for knowledge sets. While consistent
 1562 information bases facilitate common perceptions of the situation, it is well known that
 1563 different individuals have different sets of experiences and different ways of thinking,
 1564 and can draw different conclusions when presented with common information.
 1565 Networking allows individuals to synchronize their perceptions, or at least to become
 1566 aware of the different perceptions that exist in different parts of the force.

1567 With knowledge and information sets correlated (and when not correlated, with well-
 1568 understood differences), activities and decision processes undertaken by individuals can
 1569 be correlated in ways that contribute to the agility and mission effectiveness of the force.
 1570 This activity and decision coordination can be direct (taking place through explicit
 1571 collaboration) or indirect (occurring through common ties to the environment, and
 1572 because individuals are commonly trained and have access to relevant and consistent
 1573 pictures of the mission space).

1574 Importantly, decisions in this context refer to both formal planning and decision
 1575 processes involved in command and control and instantiated in doctrine via military
 1576 decisionmaking processes (MDPs) as well as informal decisions made at all levels of
 1577 warfighting and at all echelons of the force. Indeed, the decision by a force member to
 1578 stop his vehicle or to switch display modes on a screen can be considered decisions in
 1579 this framework. The central point is that the kinds of decisions broadly impacted by this
 1580 information- and network-enabled capability go beyond those of formal command and
 1581 control of forces.

1582 ***E.2 The Net-Centric Environment Joint Functional Concept Value***
 1583 ***Proposition***

1584 Figure E-2 illustrates the hypothesized NCE JFC “value proposition,” extracting from the
 1585 NCE JFC text several important elements of the functional concept and how they
 1586 interrelate and follow from one another.



1587

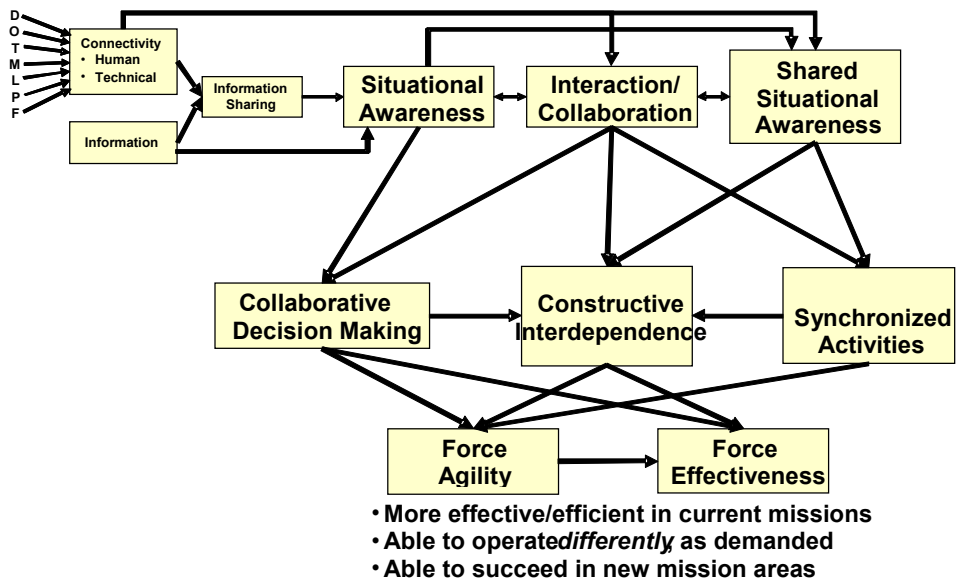
1588 **Figure E-2—Network- and Information-enabled Situational Awareness,**
 1589 **Interaction/Collaboration, and Shared Situational Awareness**

1590 As a network and information enabled concept, the NCE JFC uses its Knowledge and
 1591 Technical networking to create the conditions for information sharing in the force. This
 1592 sharing of information, along with the collection of high-quality and relevant information
 1593 from the force’s Knowledge and machine sensors, improves the level of situational
 1594 awareness possessed by each element in the force. With better situational awareness and
 1595 appropriate DOTMLPF, force elements can interact and collaborate more effectively

1596 (they know more about what they need to know, where that information is likely to be
 1597 found, and with what other force elements their capabilities need to combine, and they
 1598 are interacting and collaborating in a policy, cultural, and technical environment suitable
 1599 for that interaction). This in turn permits force elements to further refine their situational
 1600 awareness, as well as achieve consistency at appropriate levels among their individual
 1601 pictures of the mission space. Thus, not only is situational awareness improved, but high-
 1602 quality shared situational awareness is achieved as well. High quality shared situational
 1603 awareness allows for the development of situational understanding because the parties are
 1604 working from the same or comparable sets of facts. They can then work at sharing their
 1605 deeper cognitive understanding of the unfolding situation. Enhanced shared situational
 1606 awareness and shared understanding allow the Joint Force and its mission partners to
 1607 engage in value added activities such as effects based planning, rapid course of action
 1608 analysis and wargaming of potential options.

1609 The value chain just described, while logical, requires research and experimentation in
 1610 order to be verified and operationalized. Topics for an experimental campaign to
 1611 investigate and instantiate this value chain include:

- 1612 • Knowledge networking
- 1613 • Technical networking
- 1614 • Co-evolution of knowledge and technical networking
- 1615 • Information sharing
- 1616 • Situational awareness
- 1617 • Collaboration/interaction
- 1618 • Shared situational awareness



1619

1620 **Figure E-3—Value Proposition Hypothesis: Force Agility and Effectiveness Enabled by**
 1621 **Situational Awareness, Interaction/ Collaboration, and Shared Situational Awareness**

1622 Figure E-3 suggests how the situational awareness, interaction/collaboration, and shared
 1623 situational awareness created by the above-described processes lead to the ultimate
 1624 objective of the Net-Centric Environment Joint Functional Concept: a joint force that is
 1625 unparalleled in its effectiveness, and is effective across a broad spectrum of missions and
 1626 mission conditions (i.e., is *agile*). Components of this value chain include:

- 1627 • Superior Decisionmaking
- 1628 • Constructive Interdependence
- 1629 • Synchronized Activities (including self-synchronization)

1630 Experimental testing of this set of hypotheses is critical, not only to establishing the value
 1631 and validity of net-centric concepts, but also to understanding the factors that bear on
 1632 how such value is created, and what capabilities and actions are necessary in order to
 1633 attain its creation. Better understanding of how information and networking is and can be
 1634 used by commanders and other force elements, how complex military organizations
 1635 operate and adapt in complex environments, how evolving military and information
 1636 technology is affecting the conduct of operations, how that technology can best be
 1637 brought to bear in the joint force, and how the mind turns information into knowledge
 1638 and, ultimately, action, is needed to ensure the successful implementation of the NCE
 1639 JFC.

1640 Specific implications for a research and experimentation campaign involve research in
 1641 the following areas:

- 1642 • Cognitive processes involved in Knowledge collaboration
- 1643 • Knowledge creation from information
- 1644 • Knowledge decisionmaking processes
- 1645 • Effects of distance and networking on collaboration
- 1646 • Developing adaptive learning organizations
- 1647 • Impact of human factors on net-centric operations
- 1648 • Others

1649 ***E.3 Other Recommendations for Experimentation***

1650 In addition to these overarching experimentation issues that relate to how cognitive and
 1651 operational capabilities are created from information and networking capabilities, there
 1652 are research issues associated with how to best field a particular capability in the force.
 1653 For example, suppose it is established that less rigid organizational structures (one
 1654 interpretation of an agile Knowledge network) and a robust Technical network that
 1655 allows for rich communications and information exchange lead to enhanced situational
 1656 awareness, force element interaction, and ultimately to unparalleled force effectiveness.
 1657 The question remains as to which is the best *instantiation* of that organizational structure,
 1658 and which is the best technical *implementation* of communications and information
 1659 networks to achieve the needed awareness and interaction.

1660 In the ultimate end state, where there are ubiquitous sensor networks, perfect fusion tools,
 1661 no restrictions on bandwidth availability and high-resolution, real-time, 3-dimensional

1662 visualization, any collectable information in any force would be available to any force
 1663 element, and virtual collaboration environments would be indistinguishable in terms of
 1664 quality from physical “same room” collaborations. But how close to this end state does
 1665 one have to come in order to achieve effective distance collaboration, make effective
 1666 decisions, or be dominantly effective as a force across the range of military operations?
 1667 Answering such questions requires research in fields of organizational behavior, complex
 1668 organizational analysis, Knowledge-computer interaction, and others. What follows is a
 1669 suggested list of topics relevant to creating effective Net-Centric Environments,
 1670 processes, individuals, and organizations. These topics are an important part of the NCE
 1671 JFC research and experimentation campaign; referencing Figures E-2 and E-3, they deal
 1672 with making each concept and each arrow in the Figures as value-adding as they can be.

- 1673 • Effects of alternative organizational/command structures and doctrine/policy/TTP
- 1674 sets on information sharing, collaboration, and synergistic and synchronized activity.
- 1675 • Determination of effective education and training activities to ensure force elements
- 1676 have knowledge required to successfully operate in a Net-Centric Environment (i.e., what
- 1677 does a net-centric warrior need to know in order to exploit this environment?).
- 1678 • Effects of various technical networking architectures on ability to share information
- 1679 and collaborate.
- 1680 • Correlated effects of knowledge and technical networking capabilities on operations.
- 1681 Effects of alignment/misalignment of knowledge and technical networks.
- 1682 • Research in Knowledge-machine systems to explore concepts of trust (Knowledge-
- 1683 Knowledge trust, Knowledge-machine trust, machine-Knowledge trust, and machine-
- 1684 machine trust).
- 1685 • Technical research into creating high-capacity, survivable, flexible, manageable,
- 1686 deployable, etc. networks.
- 1687 • Technical research into creating effective applications to facilitate information
- 1688 sharing, fusion, discovery and visualization.
- 1689 • Technical research into creating effective distributed collaborative environments.

1690 ***E.4 Phases of a Research and Experimentation Campaign***

1691 A suitable framework for planning and executing such an experimental campaign is
 1692 described in the *Code of Best Practice for Experimentation*,³⁴ which describes the
 1693 execution of methodologically-sound experimentation in complex issue spaces, such as
 1694 that of the Net-Centric Environment Joint Functional Concept. A complete and well-
 1695 designed experimental campaign will involve experiments and research projects
 1696 variously geared towards discovery of underlying and important phenomena, testing of
 1697 hypotheses, and concept demonstration, all of which are critical to getting the theory right,
 1698 understanding its application, and demonstrating its value and limitations to users and
 1699 decisionmakers.

³⁴ Alberts, David S. *Code of Best Practice for Experimentation*. Washington, D.C.: CCRP Publication Series, 2002.

1700 ***E.5 Elements and Tools for NCE JFC Research and Experimentation***

1701 A diverse set of analytic, research, and experimentation tools and methods is required for
 1702 thorough investigation and validation of net-centric concepts. These tools and methods
 1703 include large-scale live military experiments, tabletop or sand table exercises, analytic
 1704 studies, modeling and simulation at many levels of resolution, and combinations of the
 1705 above, and others. Each of these elements has advantages and disadvantages. For
 1706 example, large-scale live experiments often have the highest level of credibility and
 1707 realistic representation of military decisionmaking processes and their impact on
 1708 operational effectiveness, but are expensive, difficult to conduct scientifically, and are not
 1709 repeatable. Modeling and simulation studies are generally repeatable, and may or may not
 1710 be inexpensive, but it is difficult to capture faithfully, even in the most sophisticated
 1711 software agents, the knowledge and decision processes whose enhancement is a focus of
 1712 net-centric systems and processes. As is usually the case when studying complex
 1713 problems, a family of approaches is required.

1714 In designing and implementing a research and experimentation campaign, the full
 1715 complement of analytic and research capabilities available should be brought to bear.
 1716 Some of these elements (inclusive of those discussed above) are:

- 1717 • Large-scale live experimentation
- 1718 • Mixed live-virtual force experimentation
- 1719 • Modeling and simulation studies at various levels of resolution
- 1720 • Modeling and simulation-facilitated Knowledge experimentation, including man-in-
 1721 the-loop and hardware-in-the-loop capabilities to examine effects of real systems on real
 1722 decisionmakers.
- 1723 • Analytical studies of the value of information and collaboration, including the
 1724 development of mathematical representations of information and collaboration effects.
- 1725 • Reviews and integration into experimentation of related research from business and
 1726 academia, especially where cognitive and social issues are explored in venues such as
 1727 distance learning, knowledge management, and distributed work environments.
- 1728 • Multiple levels of security technical, policy, procedures and organizational issues.
- 1729 • Data fusion, both automated and human directed, including algorithms and value
 1730 added for each level of fusion.

1731 ***E.6 Other Research Topics for an Experimentation Campaign***

- 1732 • Testing interdependency
- 1733 • Testing the concept and implementation of Communities of Interest
- 1734 • Testing Communities of Action
- 1735 • Testing external to DOD (e.g., IRS, NATO, IOs, NGOs,)
- 1736 • Man-in-the-loop scenarios to test trust
- 1737 • Testing of machine to machine interface
- 1738 • Leverage off non-DOD experimentation (testing, e.g., Touring)
- 1739 • Testing Knowledge dynamics to recruit towards
- 1740 • Realistic aptitude testing
- 1741 • Dealing with self organizing entities

- 1742 • Cross-portal access
- 1743 • Measuring for cultural and social change
- 1744 • Get inside the asymmetric threat process
- 1745 • Compartmented Activity Data Sharing Process
- 1746 • Rapid database generation
- 1747 • Rapid data mining and analysis tools and techniques
- 1748 • Correlation of multiple resolution M&S and geospatial information
- 1749 • Web-enabled network services for M&S and analysis
- 1750 • Social and cultural impacts on decisionmaking and shared understanding
- 1751 • Artificial intelligence aids for fusion and decisionmaking

1752 ***E.7 Areas for Developing Future Hypotheses***

- 1753 • Ability to establish effective force arrangements
- 1754 • Ability to support enterprise wide and COI specific applications
- 1755 • Ability to perform Network Operations
- 1756 • Ability to dynamically plan network architecture development process
- 1757 • Ability to dynamically allocate network resources
- 1758 • Ability to support separate constellations of COIs
- 1759 • Ability to tailor to specific capabilities
- 1760 • Ability to acquire additional resources on demand
- 1761 • Ability to support geographically transitioning nodes
- 1762 • Ability to support dynamic, priority-based resource allocation
- 1763 • Ability to dynamically re-route services
- 1764 • Ability to implement information assurance
- 1765 • Ability to achieve shared situational understanding
- 1766 • Ability to achieve shared situational awareness
- 1767 • Ability to connect and share information among
- 1768 interagency/coalition/IO/commercial/ NGO players
- 1769 • Ability to share across areas
- 1770 • Ability to collaborate
- 1771 • Ability to perform intelligent search/ smart pull
- 1772 • Ability to develop trust in the information
- 1773 • Ability to share stored information
- 1774 • Ability to archive large volumes of data
- 1775 • Ability to establish rules for machine-to-machine processes
- 1776 • Ability to effectively trust and employ intelligent agents, processes, hardware,
- 1777 weapons, systems, and decision-aids

1778

1779 **Appendix F Mapping Capabilities to Attributes**

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

1780

1781

Figure F-1—Mapping Capabilities to Attributes: Technical Area

1782

1783

ATTRIBUTES	Ability to establish appropriate organizational relationships	Ability to collaborate	Ability to synchronize actions	Ability to share situational awareness	Ability to share situational understanding	Ability to conduct collaborative decision making/ planning	Ability to Achieve Constructive Interdependence
Agile	X	X	X		X		X
Quality	X	X	X	X	X	X	X
Trustworthy	X	X		X	X	X	X

1784

1785

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

1786 **Appendix G Contributors**

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

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

Last Name	First Name	Rank/Pos	Organization
Quinton	Keith	Lt Col	JS J-7
Robinson	Louray	Ms.	AF/XICS - Sumaria
Rohatgi	Mukesh	Mr.	Old Dominions University Research Foundation
Sadauskas	Leonard	Mr.	DASD (DCIO) CP/O
Schuller	Jeffrey	Mr.	Joint Staff/J8 WCAID
Seitz	Gregory	Mr.	Binary Consulting/Army CIO/G6 FCS
Shanley	William	Mr.	USJFCOM J-61
Signori	David	Dr.	Evidence Based Research, Inc.
Siomacco	Edward	COL, O-6	Army C10/G-6
Smith	Brian	Mr.	Evidence Based Research, Inc.
Sobers	Arthur	Mr.	CSC/J-8 Protection Assessment Division
Spencer	Jay	CDR	Joint Staff/J8/Force Application
Stephens	Vincent	Lt	USSTRATCOM/CL132
Stockland	Orville	Mr.	NSA/123
Tabacchi	Len	Mr.	ASD NII
Taylor	Bridgette	Ms.	CSC J8-PAD/DDFP
Valent	Oscar	Mr.	Executive Assistant to Defense S&T Reliance Executive Staff Chair
Van Dine	Wayne	Mr.	DOD/IAA SPO
Veneeri	Janice	Ms.	DISA
Watson	Ian	Mr.	NORTHCOM J5
Whaley	Steven	MAJ	U.S. Marine Corps
Williams	Gary	Mr.	SYColeman/Army G-35
Wilson	Anhtuan	LCDR	PACOM/J622
Young	David	Mr.	USJFCOM/Old Dominion University
Zavin	Jack	Mr.	ASD(NII)/DOD CIO

1787