

# Fundamentals of Distributed, Networked Military Forces and the Engineering of Distributed Systems

Jeffrey R. Cares  
Alidade Consulting

Raymond J. Christian  
Robert C. Manke  
NUWC Division Newport



**Naval Undersea Warfare Center Division  
Newport, Rhode Island**

Approved for public release; distribution is unlimited.

## **PREFACE**

This report was prepared under NUWC Division Newport Project No. 798D530, "Total Systems Engineering."

The technical reviewer for this report was Joseph A. Gouveia (Code 21).

The authors wish to acknowledge the constructive comments provided by the Chief of Naval Operations Strategic Study Group.

**Reviewed and Approved: 9 May 2002**



**Ronald J. Martin**  
**Head, Submarine Sonar Department**



**REPORT DOCUMENTATION PAGE***Form Approved*  
**OMB No. 0704-0188**

Public reporting for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

|   |                                     |   |
|---|-------------------------------------|---|
| <b>1. AGENCY USE ONLY (Leave blank)</b> | <b>2. REPORT DATE</b><br>9 May 2002 | <b>3. REPORT TYPE AND DATES COVERED</b> |
|---|-------------------------------------|---|

|   |                           |
|---|---------------------------|
| <b>4. TITLE AND SUBTITLE</b><br><br>Fundamentals of Distributed, Networked Military Forces and the Engineering of Distributed Systems | <b>5. FUNDING NUMBERS</b> |
|---|---------------------------|

|  |  |
|--|--|
| <b>6. AUTHOR(S)</b><br><br>Jeffrey R. Cares, Raymond J. Christian, Robert C. Manke |  |
|--|--|

|   |  |
|---|--|
| <b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b><br><br>Naval Undersea Warfare Center Division<br>1176 Howell Street<br>Newport, RI 02841-1708 | <b>8. PERFORMING ORGANIZATION REPORT NUMBER</b><br><br>TR 11,366 |
|---|--|

|  |   |
|--|---|
| <b>9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b> | <b>10. SPONSORING/MONITORING AGENCY REPORT NUMBER</b> |
|--|---|

|                                |
|--------------------------------|
| <b>11. SUPPLEMENTARY NOTES</b> |
|--------------------------------|

|  |                               |
|--|-------------------------------|
| <b>12a. DISTRIBUTION/AVAILABILITY STATEMENT</b><br><br>Approved for public release; distribution is unlimited. | <b>12b. DISTRIBUTION CODE</b> |
|--|-------------------------------|

|   |
|---|
| <b>13. ABSTRACT (Maximum 200 words)</b><br><br>Defense community innovators have proposed concepts for using cutting-edge technologies to solve long-standing military challenges, including destruction of time-critical targets, theater-wide surveillance, power projection, and access to littorals. These concepts assume great benefits from networking that will enable military advantage via the use of distributed systems. However, the advantages of networking, as well as the implications of engineering distributed systems, have not been fully articulated. This report describes how distributed, networked forces provide advantage; translates the advantage to engineering aspects of distributed system characteristics, functionality, and design goals; and introduces a method for developing the engineering competencies required to design effective distributed, networked military forces and related systems. |
|---|

|  |   |
|--|---|
| <b>14. SUBJECT TERMS</b><br>Information-Age Warfare      Network-Centric Warfare<br>Military Networks              Systems Engineering | <b>15. NUMBER OF PAGES</b><br>22<br><b>16. PRICE CODE</b> |
|--|---|

|  |   |  |  |
|--|---|--|--|
| <b>17. SECURITY CLASSIFICATION OF REPORT</b><br>Unclassified | <b>18. SECURITY CLASSIFICATION OF THIS PAGE</b><br>Unclassified | <b>19. SECURITY CLASSIFICATION OF ABSTRACT</b><br>Unclassified | <b>20. LIMITATION OF ABSTRACT</b><br>SAR |
|--|---|--|--|



## TABLE OF CONTENTS

| Section   | Page |
|---|------|
| 1 INTRODUCTION .....  | 1    |
| 2 FUNDAMENTALS OF DISTRIBUTED, NETWORKED MILITARY FORCES ..   | 3    |
| Basic Building Blocks.....                                    | 3    |
| Basic Functions.....  | 3    |
| Defining Characteristics.....                                 | 4    |
| Design Goals of Distributed Forces.....                       | 6    |
| Advantage in Distributed, Networked Systems.....              | 8    |
| Potential Design Principles .....                             | 9    |
| 3 ENGINEERING OF DISTRIBUTED, NETWORKED MILITARY FORCES ..... | 11   |
| Distributed Systems Development .....                         | 11   |
| Distributed Systems Paradigm Shifts.....                      | 14   |
| 4 CONCLUSIONS .....   | 17   |
| 5 REFERENCES.....   | 17   |



# **FUNDAMENTALS OF DISTRIBUTED, NETWORKED MILITARY FORCES AND THE ENGINEERING OF DISTRIBUTED SYSTEMS**

## **1. INTRODUCTION**

The essence of victory in any competition is creating and exploiting advantage. Throughout history, advantage has been achieved in military competition by many means—through superior numbers, overwhelming firepower, clever maneuver, secrecy and deception. Any student of military history can add to this the list. How advantage is measured, valued, planned for, and realized is the focus of the military arts, as well as the basis for design and engineering of military forces and equipment.

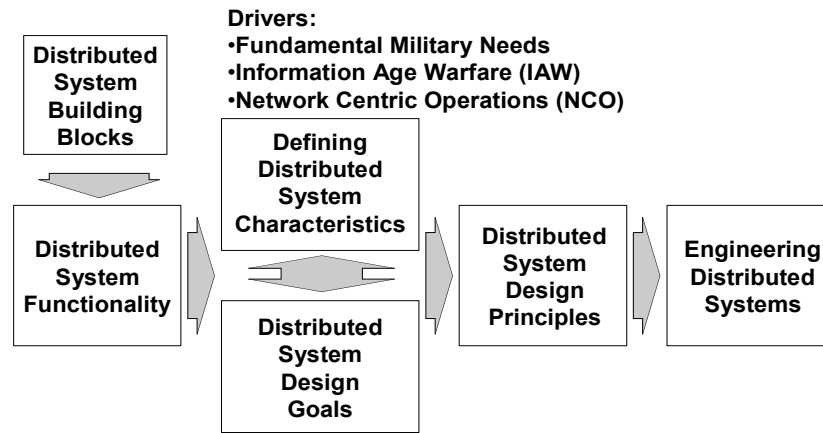
Throughout the last decade, long-range planners in the defense industry have proposed concepts for Information Age Warfare, under the rubric of Network Centric Warfare, that use information technology to solve long-standing military challenges.<sup>1</sup> These challenges include destruction of time-critical targets, theater-wide search and surveillance, long-range power projection, and access to contested littoral areas. Invariably, these concepts rely on the assumed advantages of distributed, networked forces.

While most future defense concepts embrace the idea of networked forces because networking greatly improves current processes, many conceptualizations miss the great power of both networking and distributing. One way that networking improves current processes is the automation of direct connections in a force. Networking and distributing, however, open the door to enormous new potential. Physical and social science researchers have long known from studying networked, distributed systems in other contexts that the true power of networks is realized from the vastly larger number of indirect connections rather than from direct connections. With so many indirect connections, if each only minutely contributes toward achieving value, the whole system can achieve extraordinary levels of performance—typically performing orders of magnitude better than dramatic improvements in the direct connections alone.

Added together, the extraordinary effect of both networking and distributing is itself strong justification for developing distributed, networked forces. Military applications, however, have a unique characteristic that even more profoundly capitalizes on distributed, networked effects: advantage can come not by choosing to exploit superior numbers, overwhelming firepower, clever maneuver, or secrecy and deception, but by simultaneously electing all of these options, developing multiple complementary stratagems, and exploiting the most compelling advantage when the timing is most appropriate. In other words, the primary source of advantage in distributed, networked forces arises from networked effects that are distributed in many dimensions throughout a force and can be summoned for use in the manner of advantage chosen by clever commanders based on evolving conditions.

The central objective of this report is to address a nagging conceptual void in the study of Information Age Warfare: to date; a useful definition of distributed, networked forces has not been established nor have the advantages of distributing and networking been fully and convincingly expressed. This report presents an explicit, basic definition of distributed, networked forces and specifies how advantage accrues from such systems. Moreover, the report also posits a new perspective from which the defense community can develop the engineering competencies required to build effective distributed, networked military systems.

This report comprises two major parts. The first part presents a formulation of the fundamentals of distributed, networked forces. It begins with a formal definition of distributed, networked systems and discusses the basic functions and defining characteristics of the military applications of such systems (see figure 1). These rudiments are used to suggest design goals and design principles for distributed, networked military forces. Building on this translation from the conceptual domain, the second part contains practical advice for engineering the appropriate characteristics into distributed, networked forces, as well as a discussion of the performance advantages and new functionality that would indicate a shift from a centralized/linear, non-networked system paradigm to a decentralized/non-linear, networked system paradigm.



*Figure 1. Formulation of Distributed, Networked Systems*

## 2. FUNDAMENTALS OF DISTRIBUTED, NETWORKED MILITARY FORCES

### BASIC BUILDING BLOCKS

Any system is created from parts. In traditional military systems, most of the parts are physically connected to a relatively small number of larger parts. These parts are in a sense distributed and networked.

The future warfighting concept of a distributed, networked system is different from existing military systems. There are a much larger number of small parts and the greater majority of these parts are not physically connected to the small number of larger parts. Most parts might not be physically connected to another part at all. When this is the case, other types of connections substitute for physical connections. There are, therefore, two basic building blocks of future distributed, networked systems: the parts (generally referred to as “elements”) and the connections between the parts. These are defined as follows:

*Element:* A physical component or part of a distributed, networked system that performs a certain function, such as sensing, information processing, transportation of itself or other elements, etc. Humans, from an abstract perspective, should be considered elements as well, although they are highly capable, unique, and specialized elements. An important conceptual point is that information technology equipment, such as routers, cabling, and computers are physical elements of a system.

*Connection:* Any interaction between elements or between elements and the external world. Examples of connections include communications links, weapon-target pairings, or logical relations like inter-sensor collaboration. Connections may be via physical or non-physical interactions. For example, there can be non-physical interactions between sensors and sensed objects and physical connections between munitions and targets.

Note that in this context the term “distributed, networked force” becomes synonymous with “distributed, networked system.”

### BASIC FUNCTIONS

In military applications, the elements and connections (i.e., the components of a distributed, networked force) conspire to fulfill certain functions; these functions might be executed individually or collectively at many different levels within the force. The basic functions of a networked, distributed force are defined as follows:

*Sensing:* Collecting observations of objects within a sphere of competition as well as observations of the environment. The observations may be obtained passively (by collecting phenomena emanating from objects or the environment) or actively (by causing objects or the environment to emanate phenomena). Direct and indirect forms of sensing objects, phenomena, information, and events are included.

*Transport:* Providing mobility for elements that might not have their own locomotion or for elements that in certain cases are more efficiently transported by other elements. An example of the latter is transportation of a missile to a launch site. While a missile may possess a vehicular function to propel its warhead, this system may not be suitable for autonomous transport to a firing position.

*Netting:* Creating the means of information transfer between elements of the system. Information transferred may include the results of sensing functions, transmission of stored data, messages, movement orders or control signals.

*Information Fusion and Pattern Recognition:* Sharing information among elements for the purpose of collecting observations from sensors, composing informational representations of the battlespace, and determining important patterns within the representations. Information about the non-physical characteristics and behaviors of objects (such as the content of messages) is developed in this function. This includes conversion of raw data into basic information.

*Interpretation, Cognition and Decision:* Consuming information, deliberating and converting deliberations into decisions. This includes not just the individual deliberations and decisions of commanders but also the collective cognitive activity of an entire command structure.

*Influence:* Acting to change physical, informational, or logical states in the battlespace. Influence can include physical destruction with weapons, application of nonlethal force, information warfare, or reconfiguration of friendly elements and connections. Influence includes all kinetic and nonkinetic means of obtaining desired effects for various levels of military response.

## **DEFINING CHARACTERISTICS**

Absent some special considerations, one could argue that the basic functions discussed here apply to any military force. If future distributed, networked forces are to provide unique and revolutionary advantages, there must be particular characteristics that result in the improved performance. The following list, based on research into distributed, networked systems in other contexts, is a set of characteristics—a framework—that defines unique synergies and inter-relationships expected of future distributed, networked military systems:

- Number of elements and collective behavior
- Connection topology
- Connection strength
- Diversity
- Scale.

The realization of these synergies and relationships is the foundation for performance improvements.

### ***Number of Elements and Collective Behavior***

The future distributed, networked system will typically have a large number of elements. Although elements can individually perform the basic functions as defined above, interesting collective behavior begins even when the number of elements is more than two. More complex behaviors develop as the number of elements grows, and networks of tens of elements can exhibit very intricate interactions. Extraordinarily nonlinear “tipping points” can occur when some systems have about 500 elements, but, importantly, the tipping point can disappear with somewhat fewer elements.<sup>2</sup> The same type of system with thousands of elements can cancel out tipping point benefits because of a dramatic increase in command and control overhead. The number of elements and resultant collective behavior will be an important characteristic of future distributed, networked forces.

### ***Connection Topology***

A distributed, networked system will typically be well connected; but a maximally connected system (a system in which all elements are directly connected to all others) is hampered by the same kind of ballooning overhead as a system with too many elements. A minimally connected system (one less connection than there are elements—just enough to link all the elements in one group) can be too brittle and vulnerable. Moreover, lattice-type structures (in which each element is connected, say, to exactly three other elements in a regular matrix) can be too rigid. Most real distributed systems (like the internet) have a mix of connection properties, such as preferential attachment (some elements can be more useful to connect with than others), clustering (elements can be functionally collected in local subsets) or path formation (creation of indirect conduits between elements collaborating on certain tasks through intermediary elements and connections).<sup>3-5</sup> In addition, most real distributed, networked systems assume a specific configuration based on the resources available and the task at hand; they reconfigure as resources or tasks evolve. Note also the dual nature of connections: they are both links between elements that might provide advantage as well as targets for attack. Distributed, networked military systems will likely have a mix of connection properties.

### ***Connection Strength***

Of similar importance to the number of elements and the topology of connections is the strength of connections between elements. This characteristic defines the rate and degree of response and adaptation in distributed, networked systems. For example, some systems with weak connections might require very large control signals to reconfigure elements; if connections in the same system are too strong, then very small control signals can cause uncontrollable changes in the system, perhaps even “freezing” the system if too many strong input signals become operative simultaneously.<sup>2</sup> Most distributed, networked systems have a mix of strong and weak connections, the relative strength of which change over time based on system employment. An example of this characteristic in military forces would be the strength of a phenomenon observed by an element with a sensor function. If the element were close to the source of the phenomenon, the connection would be strong, but if the element were more

distant from the phenomenon, then the connection would be weak. A sensor investigating multiple phenomena is faced with the dilemma of maintaining weak connections with all targets (and therefore reacting poorly to their behaviors) or abandoning all but one phenomenon to maintain a strong and more reliable connection with one target (forgoing a response to all but the remaining target, with which the sensor is now closely coupled).

### *Diversity*

Another important defining characteristic is the diversity of the elements and connections. Many concepts for distributed, networked military forces depend on mass-production of identical elements, but this Industrial Age approach could backfire in complex applications. Research into distributed, networked systems in other contexts shows that the systems best able learn and adapt to their competitors and the environment have diverse elements and connections. When elements and connections are highly specialized and standardized (i.e., when there are a decreasing number of types of elements and connections—a decrease in diversity) adaptation is devalued and systems become much more vulnerable to catastrophic failure in rapidly changing, competitive environments.<sup>6</sup> At the other extreme, however, are concepts for systems where almost every element and connection is unique—these systems would require extraordinary overhead to mensurate interactions between elements and connections. Most real distributed, networked systems have a healthy balance between diversity, standardization and specialization.

### *Scale*

Scale is the extent to which the same system looks different when observed at different levels of resolution. Very few dynamic, competing systems are “scale invariant,” meaning that every important behavior can be observed, understood and influenced from any scale of observation. Most dynamic, competing systems are sensitive to scale, meaning that different behaviors occur at different scales. A distributed, networked system will be inefficient (or even completely ineffective) if it cannot observe, understand or influence behaviors at the scales in which they occur. Scale, in this sense, is an important defining characteristic of distributed, networked forces.

## **DESIGN GOALS OF DISTRIBUTED FORCES**

The building blocks, functions, and defining characteristics begin to describe how distributed, networked forces might operate. The next step is to state the basis on which performance in distributed, networked forces should be judged. A clear idea of why advantage matters will help inform how advantage is accrued. These “design goals,” each considered universally good for distributed, networked forces, include persistent operational advantage, collective competitive behavior, stable system performance, and dynamic adaptability.

### ***Persistent Operational Advantage***

Operational advantage is dependent upon the ability of military forces to adaptively maintain advantageous positions against a clever foe, even when the foe takes surprising initiatives, innovates dramatically, or changes the rules of the game. A distributed, networked force must, therefore, be capable of drawing upon extremely diverse and varied sources of advantage from a finite set of elements and connections. To do this, actions might not always be “optimal,” in the strictest sense; they might temporarily admit disadvantage in order to regain a more persistent operational advantage later.

### ***Collective Competitive Behavior***

The defining characteristics suggest that centralized control of distributed, networked forces requires far too much overhead to be effective. The ability to act as purposeful collectives without the prescribed, centralized control or synchronization of all elements is a design goal of distributed, networked forces. Moreover, an enemy’s ability to discern friendly intent will be dramatically reduced if the macroscopic system actions are not mapped directly or obviously to the actions of the discrete elements. Examples of such behaviors from other contexts include wolf packing, immune system reactions, insect swarm defense, and human crowd dynamics.

### ***Stable System Performance***

The competitive environments in which distributed, networked forces operate can be extraordinarily complex and unpredictable. A distributed, networked force must, therefore, have a fundamental precept of stability in the midst of turmoil. This does not mean that the force should be ossified, simple or uninventive, but that it should have the type of dynamic, controllable stability akin to “physical agility,” including aspects of “balance.” Stable performance implies that the limited loss of elements or connections should not significantly impact the force’s macroscopic behavior.

### ***Dynamic Adaptability***

The linear branch-and-sequel method of operational planning is inappropriate for the dynamic operational environments in which distributed, networked forces compete. Operators, however, will still be required to perform traditional long-term planning functions such as resource allocation, performance assessment, and operational planning. Since these functions entail the ability to simultaneously allocate, assess, and plan at different time scales and in multiple dimensions, distributed, networked forces must be capable of being simultaneously controlled at a great many scales and in a great many dimensions. The ability for forces and the system to self-synchronize is imperative.

Future work is necessary to identify the appropriate measures and levels of effectiveness associated with these design goals.

## ADVANTAGE IN DISTRIBUTED, NETWORKED SYSTEMS

From a traditional perspective, the ideals behind the design goals of persistent operational advantage, collective competitive behavior, stable system performance, and dynamic adaptability might appear to be too good to be true. To be fair to many critics of Information Age Warfare concepts, the concept development community has not provided adequate details regarding the nature and origin of the extraordinary advantages they claim. To remedy this shortfall, this section articulates the primary source of advantage in distributed, networked forces.

Although rudimentary military networks (such as tactical data links) have existed for many decades, preliminary concepts for advanced networked forces began to emerge in the early 1990s (soon after a wider awareness of the internet began to reach the general public). These concepts mirrored a similar phase of technological innovation in other industries: the initial thrust was in developing systems to help people perform current tasks better. In the military, for example, early descriptions of a new “sensor-to-shooter” architecture were met with great interest, mainly because the existing systems for delivering targeting data to users was very time consuming and manpower-intensive. Concepts for providing target imagery directly to the pilots in the cockpit soon became one of the most popular expressions of networked military force<sup>7</sup> and using information technology to improve existing processes continues to be sound. For example, the reaction time of air-to-ground kill chain can be dramatically improved if all the steps in the chain are linked and automated with information technologies. This has been convincingly demonstrated with the improvements in the networked use of unmanned air vehicles (UAVs) from Bosnia to Afghanistan. One drawback, however, is that there is an upper limit on improving processes with networks—the upper limit of the process itself.

Soon after concepts for networked forces began to circulate in the defense community, concepts for smaller distributed forces began to emerge. The basic assumption is that distributing military force creates more options for a commander, increases the surveillance burden of an adversary, and allows fires to be massed while forces remain dispersed.<sup>7</sup> Studies have shown the increased offensive effectiveness and reduced risk to platform and life with a distributed capability.<sup>8</sup> Without proper networking, however, distributed forces are at risk. Similarly, without more options (i.e., without distributed forces), networking alone is vulnerable to decreasing returns as the performance improvement asymptote is achieved.

There is, therefore, great advantage to both networking and distributing. A simple numerical example explains how the two can complement each other to extraordinary effect. Consider a network of 16 nodes. Under early network-centric warfare assumptions, it was thought that the “power” of this network would be equal to the square of the number of nodes, or 256, which represents the pairs of direct connections that might be made in the network.<sup>7</sup> Alternatively, however, if one is able to summon the contribution of all nodes in all the ways they can possibly be arranged, then this same network would have a “power” of almost 21 trillion. Early network centric concepts missed this important source of advantage. This example underscores what scientists have long known from studying networked, distributed systems in other contexts—the true power of networks stems from the fact that they contain vastly more indirect connections than direct connections.<sup>2,9,10</sup> There can be so many indirect connections that even if each

contributed only minutely toward achieving value, then the whole system can achieve extraordinary levels of performance—typically performing orders of magnitude better than dramatic improvements in the direct connections alone. An example of a program under development to harness the power of indirect connections is the Aegis Combat System Cooperative Engagement Capability (CEC). CEC uses the collective radar returns of distributed, networked radar platforms to compose extremely high-quality tracks on very small, sea-skimming anti-ship missiles, even though each of the radars may themselves hold only a very, very weak return.

Military applications, however, have a unique characteristic that profoundly capitalizes on distributed, networked effects: advantage can emerge from a broad pool of inputs and manifest itself in a multitude of ways, each of which will not likely be evident to an opponent until advantage is ready to be applied. An additional facet that illustrates the combination of direct and indirect connection is where a system might divine a weak target from a sea of noise and then a commander may pass that targeting information directly to an attack platform that has remained hidden until just such a propitious time for employment. A primary source of advantage in distributed, networked forces, then, arises from networked effects distributed in many dimensions throughout a force that can be summoned for use in the manner dictated by evolving conditions. A primary source of advantage in distributed, networked forces is the benefit derived by exploiting indirect effects in multidimensional competition.

## **POTENTIAL DESIGN PRINCIPLES**

The previous sections have laid out components, functions, dynamics, and value propositions for distributed, networked forces. The sources of advantage in such military systems have been discussed. Confident extrapolations can be made about useful design principles of distributed, networked forces. An initial list of these includes the following.

*Recombination:* The ability to aggregate, distribute or interchange physical, informational or logical elements and connections. This design principle provides a distributed, networked force that adaptively evolves to the right number of elements, effective connection topology, requisite diversity and appropriate scales of observation and competitive behavior.

*Dispersion:* Avoiding spatial, informational, or logical centers of gravity while confounding adversary command, control, and scouting resources. This design principle provides one of the most significant contributions to advantage in distributed, networked military systems: advantage can be obscured and protected by dispersal and then marshaled for application.

*Mobility:* Sufficient speed for rapid relocation of elements and reconfiguration of element collectives through physical or logical means. Mobility provides a repertoire of agile maneuvers for a range of operational situations, nimble dispersal, and quick aggregation.

*Stealth:* Greater numbers of elements provide physically smaller elements and stealthier signatures. Distributed, networked effects can suggest ways in which smaller elements can improve collective performance yet reduce observability.

*Proximity:* Most objects in contemporary military systems have such intrinsic value in their physical components that direct proximity to a threat incurs great risk to the platform and, thus, to mission success. Distributed, networked forces can provide a level of proximity dictated by appropriate connection strengths, collective behaviors, and scale considerations. Greater numbers of smaller, stealthier objects, which manifest more of their value in informational and logical contributions than physical combat power, complement the design principle of proximity.

*Flexibility:* Reliable, fluid system substructures with a wide range of interoperability options. A key aspect of this design principle is robustness of information technology architectures and information management schemes. Adherence to this principle would provide a sustained force stability in a distributed, networked force during vigorous adaptation to radical competitive behaviors or extreme environmental conditions.

*Persistence:* Ability of forces to operate without disruption by cyclic logistics. A design principle for distributed, networked forces provides a logistics infrastructure that also capitalizes on distributed, networked logistical effects. One manner to achieve this is to *reduce* constraints on logistics and create a more adaptive flow of goods and service (a notion counter to the Joint Vision Concept of Focused Logistics).

### **3. ENGINEERING OF DISTRIBUTED, NETWORKED MILITARY FORCES**

The previous sections highlighted the fact that there are some fundamental differences to be made in the future distributed military system if a truly disruptive innovation capability is to be realized. It is important to reflect on how disruptive innovation has occurred in order to examine how to move forward and implement such a system and resultant military force. One must examine how the design principles impact traditional system development.

Studies have shown that internally instigated, disruptive innovations in industry have occurred though the use of an alternate path to their traditional product lines. This alternate path provides a haven where the innovative concept can grow separate from entrenched bureaucracy. The status quo is usually willing to give up a certain market share as nonthreatening. As the new product gains a following, customers ask for additional capability, and eventually the new product overcomes the status quo.<sup>11</sup> This era of technological growth is rife with examples of jumps to new technology paths that at first yield lesser capability but in the long run provide greater growth. The originators of the new path are not sure where the path will eventually lead but they are visionary and innovative enough to recognize the potential. Thus, to realize the disruptive innovation required for network-centric warfare, innovation is required to create a new path, and evolution along the new path will be required to fully exploit its potential.

#### **DISTRIBUTED SYSTEMS DEVELOPMENT**

A distributed, networked system, in the context provided in this report, is the new idea, i.e., the new path that needs to be followed. It has been many years since the military has pursued a disruptive innovation path. How should the development proceed? The development and the implementation of a system necessitate a number of standard programmatic elements, such as engineering and design, test and experimentation, training, manufacture, management, and doctrine. How are these elements affected by the evolutionary nature of the new path? A complete discussion of all these elements is the subject of another report; but, in the context of this report, it is important to highlight a few.

A review of the design principles for distributed, networked forces reveals that the physical parts of the system are over-represented—the informational and logical aspects, although hinted at, do not enjoy the same level of specificity in the design principles as physical elements and tangible connections. Also, it was noted that many of these design principles on the surface appear to concentrate on individual rather than collective attributes. This is largely because the engineering sensibilities required to design intangible behaviors into distributed, networked forces are immature. In other words, the practice of engineering distributed, networked forces has not preceded the need to engineer such forces. There is an intellectual gap that precludes the engineering and design of the ultimate distributed network system. This places the defense community in an awkward position on the wrong side of the learning curve: they must develop the engineering and system engineering competencies for distributed forces, at the same time that they learn how to engineer the actual forces. As a practical point, the two pursuits—the develop-

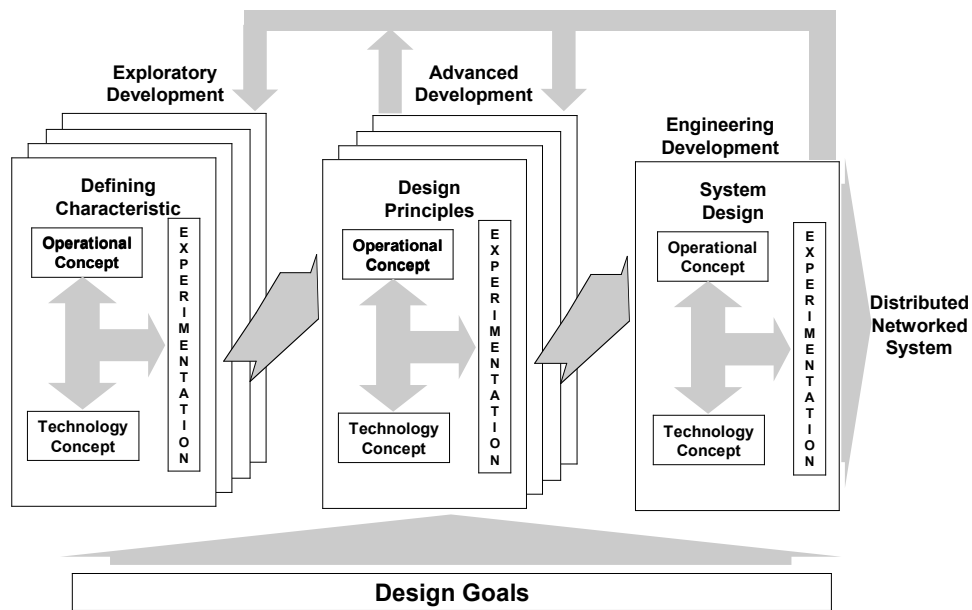
ment of the practice and the development of the products—must co-evolve. A word of caution to managers and decision makers: if this does not occur, the community can do no better than link existing systems together and realize only limited gains.

So, how should the engineering and system engineering capabilities evolve to advance our progress on the learning curve? A traditional defense industry engineer is typically focused on the physical product. As a result, vehicles that might be excellent candidates for a distributed, networked force do not get too far from the design table before additional capabilities are added to the vehicle (largely because the vehicle must compete for developmental resources against other highly capable vehicles). For very practical institutional reasons, therefore, vehicles are designed and engineered as individuals, not collectives. For the concept of a distributed, networked force to mature into reality, a progressive or evolutionary engineering approach is necessary to build simple physical objects and evolve collective characteristics by learning from how the collective performs in simulated, experimental or actual distributed, networked competition. Engineers can then evolve the characteristics of the system, discerning between improvements that should be made to individual components and those that should be made to collective behaviors or structures. This artful evolution of “physical abstracts,” constitutes a new perspective for the engineering of distributed, networked forces.

Since the engineering competencies for engineering distributed systems are not yet mature enough to be called an engineering discipline, engineering (as a discipline and as practice) will evolve with the development of distributed, networked systems themselves. As the definition and design process mature, engineers will begin to more formally codify the processes, practices, principles, and standards for the development of engineering distributed systems. They will become capable of refining and/or replacing the potential design principles suggested above. Many disciplines not traditionally relevant to the defense industry, such as social network research (the study of the structure of purposeful collectives), mathematical biology (the study of mathematical models of adaptation and response), or evolutionary computation (the study of decentralized problem-solving), may be of great use in developing distributed, networked forces. For this reason, early efforts should be strongly interdisciplinary; engineering efforts will be most successful if they grow not from the recombination of traditional defense industry disciplines but from a practical application of a wider “genetic code” of scientific thought. It may be determined that the engineering aspects are so profoundly different that they give birth to a new field of engineering. This is similar to the evolution of standard engineering disciplines and sciences that resulted in the specialized field of aeronautical engineering.

This is a process whereby a much closer interaction occurs between operational and technology conceptualization, experimentation, basic science and technology, basic research and development, systems engineering, operational doctrine and most importantly resource sponsors. Traditionally stove-piped, these disciplines must work much more synergistically from concept to system fielding. Experimentation and testing at many different levels take on a more critical role than in previous military system developments. This experimentation becomes a crucial cog in the actual engineering of the system. Because the warfighter is an actual entity in the system, the co-evolution of the technical and operational aspects is essential. Both the experimentation and co-evolution must be taken to levels not reached today.

Figure 2 illustrates a process to develop an effective distributed system. There is a need to explore the dimensionality of the defining characteristics both singly and synergistically. Exploratory concept development and small-scale experimentation would provide a rough order of magnitude requirements and parameters to a multidisciplinary distributed systems concept design team. As this understanding evolves, there is a need to explore the dimensionality of the design principles. This advanced development effort would begin to grow subsystems of the distributed, networked system to meet the design goals. These subsystems merge in the engineering development phase where the system is constructed. If the distributed system concept emerges from the experimentation process sufficiently explored, the design team will be able to articulate programmatic requirements based on valid design and verified design principles. The concept would then be ready for acquisition—use of the system in the fielded forces would in turn inform the development of still more advanced distributed, networked forces. A high degree of communication, coordination, and collaboration between all contributors to this process should, of course, be encouraged and enabled. In addition, the extent of iteration between growth steps in the process will depend on the complexity of the distributed, networked force being procured. Finally, and most importantly, the typical systems engineering functions must be employed at each step in the process, not only toward the end of the process.



*Figure 2. Developing Distributed, Networked Systems*

## **DISTRIBUTED SYSTEMS PARADIGM SHIFTS**

If engineering efforts successfully produce both distributed, networked forces and new disciplines in engineering, it will be because a dramatic shift has occurred in the way the defense community thinks about these systems. Such a shift might manifest itself in many ways; the sections below suggest new paradigms that might emerge as engineers investigate the basic functions of distributed, networked forces:

### ***Sensing***

A paradigm shift is required from “sensor-poor” to “sensor-rich” surveillance, i.e., from a condition of organic sensors associated with a relatively small number of platforms to a condition of large numbers of distributed sensors not associated with any particular platform. Sensor-rich surveillance allows:

- Replacement of surveillance plans dominated by uncertainty with surveillance plans concentrated on information conditions.
- A transition from platform-, sensor- or target-focused search to a focus on sensor-target interactions (direct and indirect).
- A transition from intermittent observations to more continuous observations.

### ***Transport***

The use of a great many distributed, networked elements necessitates a rethinking of transport mechanisms. The use of distributed sensors and influence mechanisms will necessitate the following paradigm shifts:

- A transition from a single transport perspective that balances speed, endurance, and payload capability to a distributed transport perspective that can decouple speed, endurance, and payload tradeoffs.
- A transition from a cargo mindset to an auto-locomotive mindset.
- A transition from organic- to parasitic-transport mechanisms.

### ***Netting***

Distributed, networked forces will precipitate a paradigm shift from a limited number of direct connections between platforms to a large number of indirect connections. The changes required for such netting include:

- A transition from few major node servers to more distributed server and agent nodes.

- A transition from discrete path communications and direct connections to multiple router alternatives and indirect connections.
- A transition from a technical preoccupation with bandwidth to a closer coupling of bandwidth requirements to distributed information needs.
- A transition from only active-element communicator to include passive-element responder.

### ***Information Fusion and Pattern Recognition***

Development of a distributed, networked force will change the manner in which information is handled. These changes may include:

- A transition from episodic and inferred information to continuous “actual” information.
- A transition from reliance on information composed from discrete sources to contextually derived information.
- A transition from the display of data to the display of information.

### ***Interpretation, Cognition, and Decision***

Information that contains less uncertainty and is contextually based enables the following paradigm shifts:

- A transition from isolated decision making to collaborative, multi-level decision making.
- A transition from a few centralized decision teams to larger numbers of distributed decision makers.
- A transition from limited decision aids to cognitive facility-machine assistance systems, “intelligence amplification” devices.
- A transition from detailed command-directed decisions and actions to self-synchronization.

### ***Influence***

Distributed, networked forces achieve networked effects that are dispersed in many dimensions throughout a force and that can be summoned for advantage in competition. Distributed, networked forces allow the following changes:

- A transition from attrition-/destruction-based warfare to effects-/disruption-based warfare and asymmetric means.

- A transition from a small number of major offensive options to a greater number of distributed offensive options.
- A greater synergy between offense and defense.

## 4. CONCLUSIONS

This report has discussed the need for, the mechanisms of, and the payoff from distributed, networked military forces. A comprehensive rationale is used to express the primary potential sources of advantage in Information Age Warfare. The translation of this advantage to engineering aspects of distributed systems reveals new fundamental characteristics, functionalities, and design goals that will need to be considered in future military systems research, development, and acquisition. A new approach to engineering distributed systems is proposed that focuses on the need to repeatedly test and refine engineering solutions during the course of development. Using such a process, the engineering competencies required to build distributed systems will be created, fostered, and matured. An evolutionary approach must begin in earnest if the defense engineering community is ever to implement future distributed system concepts—both to design advanced concepts that are advantageous and to abandon those that are not. The great power of distributed, networked forces will fail to be realized unless new interdisciplinary engineering efforts are undertaken with the same vigor that new concepts for distributed, networked forces are championed by military planners.

## 5. REFERENCES

1. “Future Warfare: America’s Military Preparing for Tomorrow,” <http://www.dtic.mil/jv2020/>.
2. Stuart Kauffman, *At Home in the Universe*, Oxford University Press, New York, 1995, pp. 16-18 and 170-180.
3. “SFI Working Papers,” <http://www.santafe.edu/sfi/publications/working-papers.html>.
4. “Albert-László Barabási,” <http://www.nd.edu/~alb/>.
5. “Bernardo A. Huberman,” <http://www.hpl.hp.com/shl/people/huberman/Bernardo-Published-Papers.pdf>.
6. Douglas H. Erwin, “Lessons from the Past: Biotic Recoveries from Mass Extinctions,” Santa Fe Institute Working Paper 00-12-067, Santa Fe Institute, Santa Fe, NM, 2000.
7. David S. Alberts, John J. Garstka, and Frederick P. Stein, “Network Centric Warfare (2<sup>nd</sup> Edition),” CCRP Publication, Command and Control Research Program, Office of the Assistant Secretary of the Navy, Washington, DC, August 1999. (Available online at [http://www.dodccrp.org/Publications/zip/new\\_2nd.exe](http://www.dodccrp.org/Publications/zip/new_2nd.exe).)
8. Keith Jude Ho, “An Analysis of Distributed Combat Systems,” Masters of Science in Systems Integration Thesis, Naval Postgraduate School, Monterey, CA, December 2001.

9. Everett Rogers, *Diffusion of Innovations* (4<sup>th</sup> Edition), Free Press, New York, 1995.
10. Duncan J. Watt, *Small Worlds: The Dynamics of Networks Between Order and Randomness*, Princeton University Press, New York, 1999.
11. Clayton M. Christensen, *The Innovator's Dilemma*, Harvard Business School Press, Boston, MA, 1997.

## INITIAL DISTRIBUTION LIST

| Addressee   | No. of Copies |
|---|---------------|
| Defense Advanced Research Projects Agency (DARPA)<br>ATO (T. Meyer); DSO (M. Goldblatt); IPTO (Zachary Lemnios);<br>IXO (D. Wishner); TTO (Allen Adler) | 5             |
| Office of Naval Research<br>ONR-00, ONR-01, ONR-31, ONR-32, ONR-33  | 5             |
| Chief of Naval Operations<br>NOOK (Nancy Harped); N60X (M. Mohler (2)); N74; N74T; N70X (2)   | 7             |
| Naval Research Laboratory (M. Bell)   | 1             |
| Naval Postgraduate School (J. Eagle, W. Hughes)   | 2             |
| Naval War College<br>N00, NWC Library, CNWS   | 3             |
| Naval Air Systems Command<br>NAVAIR 04X (J. Robusto)  | 1             |
| Space and Naval Warfare Systems Center<br>01; 10 (E. Hendricks, M. Gmitruk, S. Stewart, G. Geldorisi)   | 5             |
| Naval Sea Systems Command<br>SEA 05, SEA 05R, SEA 53, SEA 91, SEA 93, SEA 93R, ASTO,<br>PEO-MUW, PMS 403, PMS 407, PMS 411, PEO-SUB, PMS 435            | 13            |
| Naval Surface Warfare Center, Dahlgren Division, Dahlgren (A. Tate)   | 1             |
| Naval Surface Warfare Center, Coastal Systems Station (D. Everhart)   | 1             |
| CNO Strategic Studies Group, Newport<br>N00, NO1 (50)   | 51            |
| Navy Warfare Development Command, Newport<br>N00, NOIT, N3, N3T, N86  | 5             |
| Naval Air Warfare Center, China Lake (D. Janiec, P. Yates)  | 2             |
| OSD, Office of Force Transformation (VADM (Ret.) A. Cebrowski,<br>J. Hanley, L. Feldman, J. Garstka)  | 4             |
| OSD, Office of Net Assessment (A. Marshall)   | 1             |
| Alidade Consulting Inc. (N66604-02-M-1403)  | 10            |
| Defense Technical Information Center (DTIC) (B2A)   | 2             |

