AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

NETWORK-CENTRIC OPERATIONS – PROMISE, CHIMERA, AND ACHILLES' HEEL: CHALLENGES AND PITFALLS FOR NETWORKS AND INFORMATION INFRASTRUCTURE

by

Eric E. Silbaugh, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: James A. Rothenflue, Lt Col, USAF

Maxwell Air Force Base, Alabama

April 2005

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

AU/ACSC/5472-2341/2004-04

Abstract

Network-Centric Operations (NCO) concepts and capabilities are central to DoD transformation efforts and are predicted by advocates to have wide-ranging impacts on the conduct of warfare and military forces. We highlight the centrality of NCO to DoD transformation efforts using examples from Joint Vision 2010/2020, the OSD Office of Force Transformation, and Service transformation documents. Next, we examine NCO concepts to identify core characteristics and then identify the underlying capabilities levied on the supporting network. We then analyze several required capabilities to identify challenges and potential impacts should our networks fail to achieve the required performance or collapse under attack. We illustrate these challenges using examples from OEF and OIF. We see that NCO relies heavily on collaboration and information sharing and creates a radical and challenging set of requirements for the supporting networks and information infrastructure. Current and near-term capabilities leave a significant gap between the network and information infrastructure envisioned and required by NCO. Without this underlying infostructure, the projected benefits of NCO concepts will not be realized and any dependent military capabilities will suffer. We provide recommendations for mitigating some of the identified capability gaps and vulnerabilities.

...we must achieve: fundamentally joint, network-centric, distributed forces capable of rapid decision superiority and massed effects across the battlespace. Realizing these capabilities will require transforming our people, processes, and military forces.

—Donald H. Rumsfeld, Secretary of Defense[1]

Introduction

Network-centric Operations (NCO)[2] concepts and capabilities are central to DoD transformation efforts and are predicted by advocates to have wide-ranging impacts on the conduct of warfare and military forces.[3] NCO concepts cover the entire military response to the Information Age including ways of thinking, human and organizational behavior, and the networks we use across the tactical, operational, and strategic levels of warfare. In a broad sense, NCO is about harnessing networks and networked forces to create military advantages and capabilities. These advantages are expressed in terms such as massed effects, decision superiority, speed of command, and self-synchronization.[4] The ability to adapt our thinking and behavior to Information Age challenges is dependent upon the underlying network's capabilities.

NCO will require our networks to exhibit various characteristics (such as robustness, high bandwidth, and interoperability) to achieve the predicted advantages and capabilities. We must understand the implications of these requirements to determine how best to implement the supporting networks. Conversely, we must understand how NCO capabilities will be impacted should any of these characteristics be denied or never come to fruition. Understanding the requirements levied upon our networks is a fundamental requirement to developing networks that will support and enhance NCO.

We will see that NCO relies heavily on collaboration and information sharing and creates a radical and challenging set of requirements for the supporting networks and information

infrastructure. Current and near-term network capabilities leave a significant gap between the network and information infrastructure envisioned and required by NCO. Without this underlying infostructure, the projected benefits of NCO concepts will not be realized and any dependent military capabilities will suffer.

We will first highlight the centrality of NCO to DoD transformation efforts using examples from Joint Vision 2010/2020, the OSD Office of Force Transformation, and Service transformation documents to demonstrate the importance of NCO to the DoD. Next, we will examine NCO concepts to identify core characteristics and then identify the underlying capabilities levied on the supporting network. These sources of NCO thought come primarily from DoD authors; however, many other countries and alliances are also interested in NCO-like concepts including the United Kingdom, Canada, Australia, New Zealand, and NATO.[5] We will then analyze several capabilities required of our networks to determine some of the attendant requirements and challenges. This analysis will include potential impacts should our networks fail to achieve the required performance or collapse under attack. I will illustrate these challenges using examples from my experience while on the CENTCOM/J6 staff during Operations ENDURING FREEDOM and IRAQI FREEDOM (OEF and OIF). Finally, our analysis will provide some recommendations to mitigate associated vulnerabilities introduced by relying upon our networks and the promises of NCO.

Notes

[1] Donald Rumsfeld, "Transformation Planning Guidance," (Washington D.C.: OSD, 2003). as quoted in Office of Force Transformation, "The Implementation of Network-Centric Warfare," ed. OSD (Washington D.C.: U.S. Government Printing Office, 2005).
[2] Network-centric Operations (NCO) is a newer and more general term for a concept previously known as Network-centric Warfare (NCW). Likewise, Network-enabled Capability (NEC) is the terminology used in the UK and NATO for nearly identical concepts. NCO differs somewhat from the concepts of Information Warfare (IW) and Information Operations (IO) which deal with attack upon and defense of information itself. Similarly the concepts of

2

Notes

Network Warfare (Netwar) and Cyberwar focus on attacks upon and through networks rather that their use to create advantages and capabilities. While IW, IO, Netwar, and Cyberwar are related to and may have impacts upon NCO, these concepts are outside the scope of this paper.

    [3] David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network-Centric Warfare: Developing and Leveraging Information Superiority*, 2nd (revised) ed., *Information Age Transformation Series* (DOD Command and Control Research Program, 2000), David S. Alberts et al., *Understanding Information Age Warfare* (Washington D.C.: DOD Command & Control Research Program, 2001), David S. Alberts and Richard E. Hayes, *Power to the Edge: Command and Control in the Information Age*, *Information Age Transformation Series* (DOD Command and Control Research Program, 2003).

    [4] Alberts, Garstka, and Stein, *Network-Centric Warfare: Developing and Leveraging Information Superiority*.

    [5] Office of Force Transformation, "The Implementation of Network-Centric Warfare." pages 58-61

Network-Centric Transformation

DoD transformation efforts are affecting nearly every facet of our military including people, organizations, processes, and equipment. NCO concepts are central to these transformation efforts at all levels and are referenced either explicitly or implicitly. We will look at *Joint Vision 2010* (JV2010) and *Joint Vision 2020* (JV2020), the OSD Office of Force Transformation document *Military Transformation: A Strategic Approach*, and each of the Service's transformation roadmaps to identify the reliance of these visions upon NCO. Understanding this reliance will motivate and inform our analysis of the infrastructure requirements to support NCO.

Joint Vision 2010 & 2020

The future world envisioned by JV2010 has a more lethal battlespace that will require increased stealth, mobility, dispersion, and higher-ops tempo from our forces. The response proposed by JV2010 includes the operational concepts of Dominant Maneuver, Precision Engagement, Focused Logistics, and Full Dimensional Protection all focused by Information Superiority to create Full Spectrum Dominance. JV2020 retains and elaborates upon the same construct.[1]

These operational concepts all rely on information superiority or NCO-like concepts. Full Spectrum Dominance seeks the ability to "conduct prompt, sustained, synchronized, operations globally across all domains." JV2020 specifically notes that a key enabler of this capability is information superiority.[2] Dominant Maneuver identifies information superiority as enabling adaptive concurrent planning, coordination of dispersed units, and anticipation of events. Precision Engagement depends on linking sensors, delivery systems, and weapons via networks. Information networks will support Focused Logistics with real-time asset visibility, a Common

Relevant Operational Picture (CROP), enhanced decision-support tools, and seamless connection to the commercial sector. Protecting information content and systems is identified as a critical need for Full Dimensional Protection.[3]

Information Superiority is the lens focusing all of these operational concepts that will produce a competitive advantage when translated into superior knowledge and decisions. Better decisions made faster than our opponent can react should allow us to shape the battlefield to our advantage.[4] Underlying information superiority are global, interconnected, end-to-end information capabilities provided by the network-centric environment of the Global Information Grid (GIG).[5] Besides the direct linkages to networks and information superiority, we will see that capabilities identified in each JV2010/20 operational concept have parallels in NCO concepts.

Military Transformation: A Strategic Approach

The OSD Office of Force Transformation (OFT) provides overall DoD transformation guidance. *Military Transformation: A Strategic Approach*[6], produced by the OFT, outlines a high-level vision for DoD transformation efforts. In particular, NCO is identified as the conceptual framework that will shape much of DoD transformation efforts. NCO concepts explicitly underlie two of the six critical operational goals[7] of transformation and are the foundation for two of the four pillars[8] of military transformation. Finally, the emerging way of war this transformation will produce and the corresponding Joint Operations Concepts are explicitly constructed around NCO principles: Information superiority, shared awareness, self-synchronization, dispersed forces producing massed effects, and compressed operations that eliminate boundaries between organizations and increase speed of command.[9] Thus, DoD transformation is directly linked to achieving promised NCO benefits.

Service Transformation Plans

NCO concepts are either explicit or implicit throughout the *Air Force Transformation Flight Plan*.[10] More specifically, network-centric concepts underlie five of sixteen desired AF transformational capabilities and are implicit in four of the remaining transformational capabilities.[11] The *Army Transformation Roadmap*[12] envisions creating fully networked battle command capabilities that enable interdependent network-centric warfare.[13] NCO concepts are evident throughout the discussion of battle command which in turn underlies each of the Army's four major operational concepts. Battle command on-the-move (BCOTM) is intended to produce rapid, integrated, simultaneous, and synchronized operations.[14] The envisioned GIG is a highly mobile, self-organizing, self-healing, multilevel secure, resilient network transporting multiple forms of information across all echelons.[15] The *Naval Transformation Roadmap*[16] envisions three operational concepts all connected by FORCEnet. NCO attributes are present throughout the discussion of FORCEnet. Specifically, it will be a single, comprehensive C2 network combining sensors, networks, decision aids, weapons, and supporting systems. FORCEnet will use multiple transmission paths to create a fault-tolerant, adaptable, self-organizing, self-monitoring, self-healing, secure, continuously available network that enables collaboration and adaptive mission planning and rehearsal.[17]

Thus, NCO concepts and its expected benefits are deeply embedded within DoD, Joint Staff, and Services' transformation guidance. As a result, DoD transformation (and our future military capability) is unlikely to be successful unless NCO delivers these expected benefits.

Notes

[1] CJCS, "Joint Vision 2010," (Joint Staff), CJCS, "Joint Vision 2020," (Joint Staff).
[2] CJCS, "Joint Vision 2020." page 3
[3] Ibid. pages 6-9, 20-27
[4] CJCS, "Joint Vision 2010." page 19 and CJCS, "Joint Vision 2020." pages 2, 8-9

Notes

[5] CJCS, "Joint Vision 2020." page 9

[6] Office of Force Transformation, "Military Transformation - A Strategic Approach," ed. OSD (U.S. Government Printing Office, 2003).

[7] Ibid. pages 17-19

[8] Ibid. pages 23-26

[9] Ibid. pages 31-33

[10] XPXC, "The U.S. Air Force Transformational Flight Plan," (HQ USAF, 2003).

[11] Ibid. pages vi and vii and Table 1 on page 19

[12] "United States Army Transformation Roadmap," (US Army, 2003).

[13] Ibid. pages xvii, 1-3 thru 1-12

[14] Ibid. pages 2-1 thru 2-6

[15] Ibid. pages xi, 3-7, 4-4, and others

[16] "Naval Transformation Roadmap 2003," (US Navy, 2003).

[17] Ibid. pages 63-80

Network-Centric Characteristics and Attributes

Network-Centric Warfare (NCW), now known as NCO, was a concept first introduced by then Vice Admiral A. K. Cebrowski and Mr. John Gartska.[1] Many of the concepts cited are not new; they are a synthesis of ongoing discussions on the role of information warfare and information superiority and the transition from and industrial to an information age. Below we will examine three major works on NCO and trace NCO concepts from the expected results, back through the enabling processes, and finally to the characteristics and attributes required of the underlying networks and information infrastructure (also called infostructure). NCO-like discussions are not confined to DoD. We will also examine a recent article from the UK and compare their NEC concepts and expected results with the requirements levied on the infostructure. Before analyzing these works we will highlight some expected characteristics of the network-centric environment common to all of these sources.

The Network-Centric Environment

The predicted future environment has stealthy, mobile forces widely dispersed upon a non-contiguous[2] battlefield operating at very high operational tempos. Forces with these attributes will be more lethal and effective than ever before. Furthermore, NCO predicts a compression of the tactical, operational, and strategic levels of war and the need to operate seamlessly across organizational boundaries.[3]

NCO foresees a proliferation of lower cost, independent sensors and actors that will depend upon distributed rather than embedded intelligence. These sensors are predicted to become nearly ubiquitous and deliver more types of and more detailed information as the costs of technology decline. Traditional platforms (aircraft, tanks, ships) may also disappear as we know

them by evolving from integrated, intelligent networked entities into self-organized "packs" and "swarms" of independent sensors, weapons, and decision-makers with distributed intelligence connected through the infostructure.[4] We can already begin to see the impact this vision will have on, and our dependence upon, the infostructure connecting these "swarms." Now we will examine the expected results of NCO and trace those back to the associated infostructure requirements.
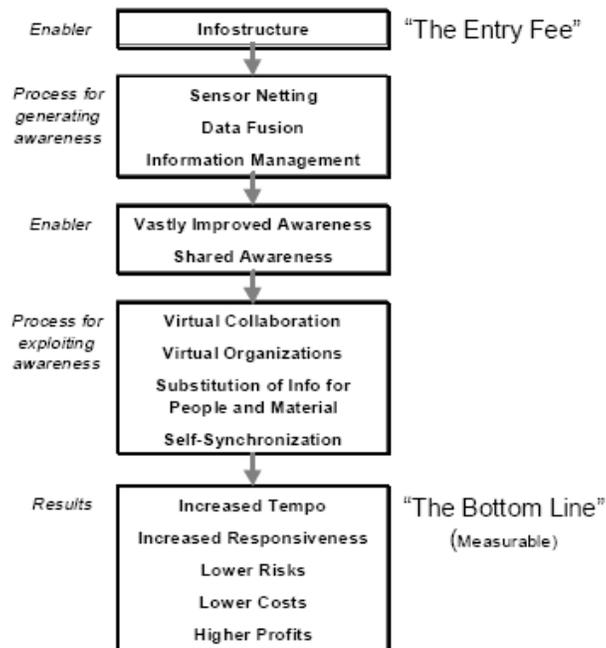
Network-centric Warfare

The book *Network-Centric Warfare: Developing and Leveraging Information Superiority*[5] was one of the first efforts to describe NCO. The authors defined NCW (now NCO) as a combination of forces, information technology, and thinking:

> NCW focuses on the combat power that can be generated from the effective linking or networking of the warfighting enterprise. It is characterized by the ability of *geographically dispersed forces*…to create a high level of *shared battlespace awareness* that can be exploited via self-synchronization and other network-centric operations to achieve commanders' intent. NCW supports *speed of command*—the conversion of *superior information position* to action...In brief, NCW is not narrowly about technology, but broadly about an emerging military response to the Information Age.[6] [emphasis added]

Information Age warfare and NCO, as expressed in *Understanding Information Age Warfare*[7], requires information superiority: Creating a dynamic, relative advantage in the information domain while denying the same to our adversaries. Information advantage is assessed not in terms of the information and communications capabilities of our forces relative to our adversary's. Rather, advantage is assessed by the information capabilities available to our forces relative to their mission needs.[8]

Together, these works describe a network-centric enterprise (see Figure 1) and identify the key capabilities and attributes required for NCO. We will trace these attributes from the expected results, through processes and enablers, to the underlying network requirements. In

both, a network consists of nodes (entities) and the links among them. Nodes do things (sense, decide, act) and information is passed over links from one battlespace entity to another. These networks plus the information they contain constitute the information infrastructure, or infostructure.[9] We will use this term infostructure throughout the rest of this paper. Note that this infostructure is the "entry fee" and key enabler in the chain leading to the expected results (see Figure 1).

Figure 1: The Network-Centric Enterprise.[10]

The expected results of NCO are an increased operational tempo greater speed of command which will increase the lethality, survivability, and responsiveness of our forces. Ideally these forces will be adaptive, agile, and self-synchronizing without delays imposed by static C2 hierarchies. These combined results should enable us to create synchronized, massed effects from widely dispersed and mobile forces and shape the battlefield faster than our opponents. Together, NCO concepts are expected to produce dramatic increases in military effectiveness.[11]

Collaboration by decision-makers distributed throughout echelons and across organizations is used to develop shared knowledge and understanding of the battlespace and the commander's intent. This shared understanding will then reduce the time required for planning and execution and produce higher-quality decisions. Collaboration must be a continuous, inclusive process where all required personnel are interconnected and can participate interactively (two-way communication) and also requires shared awareness.[12]

Shared awareness depends on networked sensors, data fusion, and information sharing. Wide and rapid sharing of media-rich and content-rich information by sensors and other producers increases accessibility to information but also requires controlling access to and protecting information. Thus, tools and software agents are necessary that find and fuse widely shared information from across the network, create common relevant operational pictures (CROPs), and provide views of information tailored to the problem at hand.[13]

Collaboration and shared awareness will levy heavy requirements on the underlying infostructure. This infostructure is assumed by NCO advocates to be ubiquitous, robust, high-performance, easy to use, and facilitate finding and filtering relevant information and fusing this information in a timely manner.[14] Robust networking must ensure connectivity and interoperability and provide the necessary speed and reduced latency. All battlespace entities will connect via the network — not necessarily directly node-to-node. This will require a geographically and hierarchically dispersed network to provide secure, seamless connectivity between dispersed and highly mobile entities.[15]

This infostructure will incorporate large amounts of commercial technology that will also be available to our adversaries. Thus, the advantage we gain from technology will be dynamic and possibly fleeting.[16] High rates of technological change will also force backwards compatibility

11

with both our own and coalition forces to operate across several, co-existing generations of technology.[17]

NCO requires that information on the network be trustworthy and useful which drives requirements in quality, security and assurance, and reach. Quality information requires completeness, accuracy and precision, timeliness, and consistency between sources. Security and assurance of information requires availability, privacy, integrity, authenticity, and non-repudiation. Information reach requires information sharing and access to high-quality services across multiple security levels, echelons, organizations, and functional groups.[18]

Collaboration and information sharing alone will place significant demands on the projected infostructure. NCO advocates note that increased synchronization implies increased dependence on the infostructure and a higher sensitivity to errors, both in information and execution, which could lead to reduced operational robustness.[19] This dependence and sensitivity only increases the required performance of the infostructure.

Understanding "Power to the Edge"

Power to the Edge[20] begins with affirming the NCO tenants described above and moves on to illustrate the concepts of smart pull, post-before-processing, and the need for interoperability. Access to information is the domain of smart pull and post-before-processing. Smart pull is premised on a Web-like scenario that allows users to obtain the necessary information on-demand without requiring interaction with producers. Older paradigms required intelligence in producers to know who needed to know their information and where the information should be sent. Smart pull shifts the burden of obtaining information to one of access, description, discovery, filtering for relevance, and interpreting and fusing by the "edge" user. Post-before-processing requires producers to make both raw and processed information immediately

available. This should ensure information timeliness bounded only by availability and performance of the network and information management and dissemination tools and policy.[21]

Interoperability is a key derived requirement. Systems must support a rich array of connectivity and ensure entities are connected to the network with standard protocols. Users must be able to find, retrieve, and understand information (which requires data and metadata standards). The network must advertise and provide high quality information and adaptive computational services with flexible access control. Finally, networks must support the required applications and protocols to create collaborative environments.[22]

The authors of *Power to the Edge* require the underlying network to be ubiquitous, secure and trusted, robust, protected, and high-bandwidth. This requires multi-mode communications media integrated into a multi-hop, beyond-line-of-sight, dynamically routed network. It must also be self-managing and adaptive to node and link failure and provide quality of service guarantees based on bandwidth, latency, reliability, and precedence. This network will take advantage of commercial technology using Internet Protocol (IP) as the common standard and other open-systems standards and protocols as necessary. Commercial security standards will be used to handle mobile code, denial of service, and insider threats. Security and risk management must also be an integral design consideration.[23] This is an incredible list of required infostructure capabilities.

Network-enabled Capabilities

The United Kingdom has developed a concept of Network-Enabled Capabilities (NEC) which shares many similarities with NCO although NEC seems to have an evolutionary, vice revolutionary, outlook.

> NEC shares the tenets of NCW but is more limited in scope in that it is not a
> doctrine or vision. Nor does it seek to place the network at the center of

capability in the doctrinal way that the term NCW implies. Rather, NEC is much more concerned with evolving capability by providing a coherent framework to link sensors, decision makers and weapon systems to enable emerging UK doctrine on effects-based operations to be achieved.[24]

NEC depends on shared awareness between and collaboration with multiple group members. Gathering, maintaining, and presenting relevant information that is consistent across all group members is a key requirement. NEC expects the future battlespace to be teeming with information but this information will not be pushed to the user. Instead, a small part of this information pool will be presented and the user will actively search for additional information across multiple networks. This requires tools capable of proactively searching for, exchanging, and manipulating information while ensuring security.[25]

NEC requires a resilient information infrastructure which must provide a secure, assured environment meeting dynamic requirements. These requirements include the capability to share and access the required information, transparent information flow across domains, and robustness in the face of communications limitations and jamming. Additional requirements are efficient management of information sharing and end-to-end performance guarantees based on the operational situation.[26] Again, this describes a supremely capable infostructure far beyond our current achievements.

Overall, NCO and NEC provide a consistent set of concepts that rely on collaboration and information sharing and create an extremely demanding set of requirements for the supporting networks and information infrastructure. Without this infrastructure, NCO concepts and advantages will not be fully realized. How to implement this infostructure is yet to be determined:

> Networks are merely a means to an end; they convey "stuff" from one place to another and they are the purview of technologists. *NCW does not focus on network-centric computing and communications*, but rather focuses on

14

information flows, the nature and characteristics of battlespace entities, and how they need to interact.[27] [emphasis added]

This leaves a significant gap between the network and information infrastructure envisioned and required by NCO and current or near-term capabilities. Analyzing infostructure requirements and identifying both key areas to close this gap and pitfalls to avoid is the focus of the next section.

Notes

[1] Aurthur K. Cebrowski, "Network Centric Warfare: Its Origin and Future," *Naval Institute Proceedings* (1998). ADM Cebrowski was the Director of OFT, Mr. Gartska is Chief Technology Officer, JCS/J6.

[2] Non-contiguous means a battlefield with no continuous front but with pockets of operations spread across the battlefield. Also known as a non-linear battlefield.

[3] Alberts, Garstka, and Stein, *Network-Centric Warfare: Developing and Leveraging Information Superiority*. page 88

[4] Ibid. pages 65-79

[5] Ibid.

[6] Ibid. page 88

[7] Alberts et al., *Understanding Information Age Warfare*.

[8] Ibid. pages 53-54

[9] Alberts, Garstka, and Stein, *Network-Centric Warfare: Developing and Leveraging Information Superiority*. page 94

[10] Ibid. from figure 6 on page 36

[11] Ibid. pages 2, 6-8, 11-13, 36, 55-62, 88-91 and Alberts et al., *Understanding Information Age Warfare*. page 71

[12] Alberts, Garstka, and Stein, *Network-Centric Warfare: Developing and Leveraging Information Superiority*. pages 38, 108 and Alberts et al., *Understanding Information Age Warfare*. pages 27-28, 62, 71-73, 91, 200-201, 225

[13] Alberts, Garstka, and Stein, *Network-Centric Warfare: Developing and Leveraging Information Superiority*. pages 36, 45, 65 and Alberts et al., *Understanding Information Age Warfare*. pages 4, 24-27, 48, 59, 127, 185-202

[14] Alberts, Garstka, and Stein, *Network-Centric Warfare: Developing and Leveraging Information Superiority*. pages 91, 100-103, 187 and Alberts et al., *Understanding Information Age Warfare*. pages 24-27, 125-127

[15] Alberts, Garstka, and Stein, *Network-Centric Warfare: Developing and Leveraging Information Superiority*. pages 6, 38, 88-90, 116, 191 and Alberts et al., *Understanding Information Age Warfare*. pages 57, 67, 84, 90, 99

[16] Office of Force Transformation, "The Implementation of Network-Centric Warfare." page 68 and Alberts, Garstka, and Stein, *Network-Centric Warfare: Developing and Leveraging Information Superiority*. pages 189-192

Notes

[17] Alberts, Garstka, and Stein, *Network-Centric Warfare: Developing and Leveraging Information Superiority*. page 200

[18] Alberts et al., *Understanding Information Age Warfare*. pages 86-91, 96-97, 101, 107, 159

[19] Ibid. pages 157, 235-236

[20] Alberts and Hayes, *Power to the Edge: Command and Control in the Information Age*.

[21] Ibid. pages xiv-xv, 82-83, 118-120, 171

[22] Ibid. pages xvi-xvii, 92, 107-108, 118-120, 158, 175, 194-199, 225-226

[23] Ibid. pages xv, xx, 6, 82, 90-92, 102, 128, 134-135, 141, 175, 186, 194-197, 226

[24] Anthony Alston, "Network Enabled Capability - the concept," *Journal of Defense Science* 8, no. 3 (2003). page 108

[25] Ibid. pages 111-112, 114-115

[26] Ibid. pages 111-112, 114-115

[27] Alberts, Garstka, and Stein, *Network-Centric Warfare: Developing and Leveraging Information Superiority*. page 93

Required Infostructure Capabilities

We have seen the radical requirements NCO concepts levy on our networks and information infrastructure. Proponents of NCO are not blind to these challenges.

> The [near term] infostructure we can reasonably expect…will have shortfalls…continued vulnerabilities, a lack of connectivity and bandwidth, particularly for that stubborn last mile, and problems with mobility and survivability.[1]

> …there is every possibility that the unintended consequences of wiring up the battlespace and hoping for the best will, in fact, degrade performance…NCW needs…analyses and experiments…to understand how we can reap the huge potential of NCW, while avoiding the pitfalls of unintended consequences.[2]

Others are also beginning to comment on the various challenges and potential pitfalls of relying on NCO.[3] Our task in this section is to examine several, but not all, characteristics required from our infostructure by NCO and infer some required capabilities and potential vulnerabilities. First, we will examine the nature of networks and identify some inherent characteristics and vulnerabilities. Next, we will examine the capabilities necessary for our networks to exhibit the required resilience, utility, and resistance to failure required to support NCO. Then, we will delve into challenges from NCO for network ubiquity and robustness in terms of bandwidth, latency, and connectivity. Finally, we will discuss the impacts of information sharing, information overload and network topology, and interoperability on our networks and current practices. Throughout I will use examples of SATCOM and other network systems based on my experience on the CENTCOM/J6 staff in OEF and OIF to illustrate how these characteristics manifest in practice.

The Nature of Networks

> A network consists of nodes (entities) and the links among them.…the *nature of the links that will provide the best performance* under a wide range of battlespace

environments and conditions *is one of the key questions that needs to be addressed* as we take NCW from concept to reality.[4] [emphasis added]

Understanding how the nature of nodes and links affect the performance of networks is our current task. Dr. Albert-Laszlo Barabasi and his co-workers have studied many different networks, both natural and artificial, and have presented some of their results in a book entitled *Linked*.[5] Others have also studied the Internet using very different methods yet come to strikingly similar conclusions.[6] We will examine some of these inherent network properties in this section and use these properties to analyze recent examples of military networks in the next sections.

Dr. Barabasi and his colleagues have found that most complex networks in nature exhibit scale-free properties. Scale-free means there is no average number of links connected to a given node. Instead, there are a few hubs (nodes) with many links, many nodes with few links, and a continuous distribution between these limits with an inverse relationship between the number of links to each node and the number of nodes. Airline route maps, the Internet, and the World Wide Web (Web) are all networks that exhibit scale-free properties. In scale-free networks, highly connected hubs will form and fundamentally define the network's connectivity—these hubs hold the network together. These hubs also determine the network's structural stability, dynamic behavior, robustness, and tolerance to error and attack.[7]

In dynamic networks, such as the Internet and the Web, a node's connectivity changes over time. These researchers found via computer simulation that dynamic networks can exist in one of two states. In one state, the network is scale-free with each hub competing for links causing a distribution of hub connectivity. In the other state, the network is "winner-take-all" and a single, highly connected hub emerges, similar to a monopoly or a star network.[8] Star networks are

extremely vulnerable to attacks on the central hub; thus, we should attempt to ensure our infostructure has scale-free properties.

The phase change between these states is determined by preferential attachment of nodes to hubs. Dr. Barabasi gives the growth of the Internet as an example. Here preference of attachment was determined by two factors: Cost of connection (distance to a hub) and the quality of access (bandwidth and number of connections).[9] This preferential attachment caused well-connected hubs to grow larger, but prevented formation of a single hub, and thus determined the scale-free properties shown by the Internet.[10] Now we will examine some military networks that seem to exhibit these dynamic, scale-free properties.

Satellite Communications

Satellite communications (SATCOM) were critical during OEF and OIF as the CENTCOM theater has limited terrestrial (fiber, cable) connectivity and because operations required high mobility over large regions. US military SATCOM networks seemed to exhibit preferential attachment and scale-free properties.

Both the Standardized Tactical Entry Point (STEP) ground stations and the very few joint communications nodes in theater connected to terrestrial fiber were in high demand. These STEP and joint sites provided low latency access to CONUS networks, provided a wide array of communications services, and minimized the number of satellite hops within theater due to their large number of links. Thus, communicators at deployed sites fought tooth-and-nail to get their site connected to one of these hubs—a classic example of preferential attachment in a dynamic network. Unfortunately, even with emergency upgrades, these STEP and joint sites were not able to handle the explosive requirements growth.

Four separate military and five different commercial (aggregating vendors and similar satellites) SATCOM systems were in use simultaneously supporting operations throughout CENTCOM's theater. The only interconnections between these SATCOM systems occurred at the already overloaded STEP and joint sites, and not all of these sites had connections to all systems. Thus, these hubs limited the network's connectivity characteristics. Their limitations greatly restricted flexibility to support operations and highlights the need to diversify the number and locations of these sites and provision them appropriately.

Communications satellites themselves are also a type of hub and can be analyzed as a star network. Star networks are exceedingly vulnerable to attacks on the central hub. Jamming satellites is the most likely method to attack SATCOM and can disable all networks a given satellite supports. Some military SATCOM systems have a level of resistance to jamming. However, commercial SATCOM systems have no jam-resistance and limited resistance to unintentional interference. Thus, satellites are a potentially lucrative target for our adversaries as approximately 75% of all CENTCOM theater communications were carried on commercial satellites during OIF.

Military SATCOM (MILSATCOM) programs such as the Mobile-User Objective System (MUOS), Wideband Gapfiller (WGS), and Transformational-SATCOM (T-SAT) are in work to deliver greatly increased communications capacity and more flexible interconnections between satellite systems. Nevertheless, even these systems will meet only a fraction of the projected requirements; and alternatives to SATCOM such as fiber do not reach everywhere, nor are they mobile.[11] Thus, commercial SATCOM will be used by military forces for the foreseeable future.

The above analysis and examples highlight the need to identify, protect, provision, and diversify the connectivity hubs within all our networks, not just SATCOM. We must correctly

predict demand for, provision capacity at, and ensure flexible interconnections between critical connectivity hubs. We must recognize inherent commercial SATCOM vulnerabilities and implement countermeasures to identify, locate, and mitigate the effects of failures or attacks. Future self-organizing, self-healing networks must not be allowed to degenerate into vulnerable configurations due to failure or attack.

Resilience, Utility, and Cascade Failure

Resilience, utility and resistance to failure are highly desirable qualities for our infostructure. Highly interconnected, complex networks usually provide efficient use of resources and lower costs. These scale-free networks also exhibit high resilience against random failures. Under random failures, a significant fraction (up to 80%) of nodes can be removed and the network will still remain connected. Random failures predominantly affect small nodes with a few links. However, the hubs with many links are the source of a network's robust connectivity. Dr. Barabasi and his co-workers have shown in simulations that preferentially attacking hubs caused complete collapse of network connectivity after a critical threshold of hubs (much less than 80%) was removed.[12] Thus, the hubs which provide desired network characteristics simultaneously create vulnerabilities to attack.

In the world of NCO, nodal connectivity is not the only measure of merit. The utility of a collaborative network is measured by the number of users. A "law" attributed to Dr. Metcalfe, inventor of the Ethernet, maintains that the utility of a network increases proportionally to the square of the number of users—this is a beneficial effect. Double the number of users and utility quadruples. However, an "inverse Metcalf's Law" effect comes into play as users are disconnected from the network by failure or attacks. If 80 percent of a network's *users* have been disconnected, the remaining network (while still fully interconnected) retains only 4 percent

of its *utility* for collaboration! Meanwhile, collaboration utility is *zero* for all the disconnected users. Thus, a network under attack may retain its connectivity but become useless for collaboration. Preventing utility collapse will require protecting both hub and user connectivity to the network from disruption.

Highly connected networks are usually robust to failure; but when something goes wrong effects can cascade throughout the system. Cascading failures are a dynamic property of networks, but they usually do not happen instantaneously. The blackouts of 1996 and 2003 affecting the US and Canadian power grids are an example of this phenomenon.[13] The Internet is also subject to widespread congestion collapse and routing instability at various times. [14]

Given this potential, we must identify the warning signs of impending cascade failure in our networks—and search diligently for the first hint of trouble. Identifying warning signs and how to sense them is outside the scope of this paper. However, several researchers provide some intriguing suggestions and examples.[15] At the least this will require a complex, distributed network of sensors that sense the network to help create a self-healing and self-managing network.

Creating a resilient and useful network will require us to protect our connectivity hubs against preferential attack. Users must stay connected to the network to prevent a utility collapse; this requires protecting their links from disruption and providing users multiple connectivity paths. Finally, preventing cascade failure will require continuous vigilance and a deep understanding of our networks.

Ubiquity and Robustness: Bandwidth, Latency, and Connectivity

Ubiquity and robustness are two concepts that describe a network available everywhere, at high bandwidths, all the time. These properties are tied to bandwidth, latency, and connectivity.

A network's capacity and a link's bandwidth are usually the only parameters discussed by NCO advocates. But parameters such as latency and connectivity also have a huge impact on ubiquity and robustness. We will discuss the implications of all three parameters below.

> Bandwidth capacity is significantly limited across the strategic, operational, and tactical levels. Solutions exist for bandwidth problems at the strategic and, possibly, the operational levels…but at the tactical levels, this bandwidth shortage is expected to remain into the foreseeable future.[16]

Bandwidth shortages at the tactical level do not bode well for NCO as this is exactly where the greatest gains can be found. Current difficulties in providing bandwidth to deployed forces in OEF and OIF are well documented[17] and both GEN Franks and GEN Abizaid highlighted bandwidth and C2 shortfalls for mobile, tactical forces in testimony to Congress.[18] Individual tactical units currently require less bandwidth than higher echelon forces, but their requirements will increase as we migrate towards smart pull. And tactical units are much more numerous on the battlefield. Thus, while an individual unit's bandwidth requirements may be reasonable, the aggregate bandwidth requirements from tactical units will impose huge loads on the system, as seen in OIF.[19] MILSATCOM systems such as MUOS and T-SAT must not be delayed and must deliver on their promised capacity as they are critical to delivering NCO capabilities.

Given increased mobility and dispersion of forces on future battlefields, wireless communications will be the primary means of providing "last mile" connectivity. Radio-frequency wireless communications will be the major source of tactical bandwidth (vice optical communications due to weather and other impairments). Unfortunately, the optimal spectrum for line-of-sight and satellite communications is already crowded.[20] Based on my experience, spectrum congestion and interference resolution problems had direct impacts on OIF operations. This will only get worse with more wireless systems.

Mesh networking systems, where each node can relay packets for another, have been proposed to provide tactical wireless connectivity. These systems are under development in the commercial and military sectors.[21] Mesh networks (both terrestrial and airborne) must deal with rapidly changing and intermittent link connectivity, which is much different from the current Internet and will require new protocols and systems.[22] Nodes joining and leaving the network and exchanging routing information will require authentication to prevent attacks and spoofing – authentication is not part of most current protocols. Sparse node distribution across the battlefield due to dispersion and mobility implies fewer options for node-to-node relay which will increase reliance on overburdened SATCOM and drive development of aerial and near-space relay capability.[23] SATCOM and spectrum limitations and mesh networking challenges will ensure that bandwidth in the tactical "last mile" will remain a significant challenge for NCO for some time to come.

Latency-intolerant applications can cause disruptions in operations that call into question the robustness of a network. Latency is the delay introduced by the network when transferring information. The sources of latency are numerous but usually involve propagation delay such as SATCOM hops and queuing delays due to congested links. Delay sets well known upper limits on throughput over SATCOM links; increasing bandwidth will not help, only reducing delay or improving network protocols will help.[24] Latency will only increase with increasing use of wireless networks, dependence on SATCOM, and deployment of distributed sensor networks.[25]

In the CENTCOM theater, the Automated Deep Operations Coordination System (ADOCS) was used simultaneously for time-sensitive targeting (TST) collaboration by multiple, geographically dispersed units. One unit in particular was initially separated from the ADOCS servers by three SATCOM hops which introduced a minimum propagation delay of 0.75

seconds. Link congestion during peak operations often increased one-way latency to well over 1.5 seconds causing ADOCS to crash. Reconfiguring the theater SATCOM network to reduce these latencies took many days and impacted several other units. STE and STU-III telephones also experienced severe difficulty going secure over links with more than two SATCOM hops; this problem was never fully overcome during OIF. Latency tolerance must be designed into applications and protocols for the foreseeable future to ensure robust network services.

Network connectivity can be disrupted by our enemies through direct attack both external and internal to the network, or due to mission profile. Jamming, electro-magnetic pulse, and high-power microwaves are all threats to which wireless systems are vulnerable (especially commercial equipment).[26] Effective anti-jam often requires protection ratios of 100:1; however, there is an inverse relationship between data rates and jamming protection given fixed spectrum and power.[27] Imagine how effective network-centric operations will be when available data rates are reduced by a factor of 100. Integration of the Global Positioning System (GPS) into nearly every platform and weapon also creates an inviting target for our adversaries, as witnessed during OIF.[28] Without countermeasures in place, disruption of GPS could have severe impacts on our mission effectiveness. Even if we cannot protect all systems from these threats, we should at least provide the ability to sense and report interference. The lack of easy access to interference geolocation capability hindered efficient use of ultra-high frequency tactical satellite (UHF TACSAT) communications during OEF and OIF.

The very connectivity we prize also provides the avenue for distributed-denial-of-service (DDoS) attacks through the network, as witnessed by the widely noticed DDoS attack on Yahoo! and the spread of Slammer, Witty, and other recent Internet worms.[29] Researchers are now predicting the rise of "flash worms" which could infect all vulnerable computers on the Internet

in single-digit minutes and cryptographic malware which could hold our data hostage.[30] Launching a DDoS or flash worm attack requires very little infrastructure—a PDA, a cell phone with Internet service, and an attitude will suffice—and defending against these attacks is difficult.[31]

Increasing stealth is a necessary requirement that will limit collaboration of our forces unless applications are designed to operate while disconnected or with intermittent connectivity. Controlling emissions or using infrequent, short, and low data rate transmissions is routinely practiced by the Navy, F-117s and B-2s, and special operations forces to improve stealth. Thus, these forces will not be able to query the network for information during much of their missions. Developing reliable, one-way broadcast reception coupled with smart data caching could improve the situational awareness of these forces.

Overall, providing a ubiquitous and robust network will be difficult and will face inherent tradeoffs between protection and capacity. Bandwidth for mobile, dispersed forces will likely be limited for quite some time; thus, we should carefully experiment with smart pull and ensure our applications are bandwidth efficient. Latency and disconnection-tolerant applications and protocols will be necessary to ensure robust operations. Continued reliance on a network unprotected from external and internal disruption would create significant mission vulnerabilities–whether we can afford the capacity and cost tradeoffs remains to be seen. Finally, the need to continue operations while disconnected from the network may even call into question the NCO premise that platforms will transform into self-organizing "swarms."

Surfing the Information Tsunami: Sharing, Topology, and Interoperability

Information sharing is a foundational NCO tenet. Ensuring data integrity, accuracy, precision, and consistency will be paramount requirements – especially as our adversaries attack

our networks and attempt sophisticated denial, deception, and camouflage to defeat our sensors. Dr. Linton Wells, assistant secretary of defense for network and information integration, notes that "Probably the most stupid idea we could think of is becoming dependent on a network that is not secure."[32] On the other hand, he also notes that the biggest cultural problem is data sharing across both security domains and organizations and that a data strategy should become as important as other transformational efforts.[33]

Difficulties in sharing information across security domains negatively impacted CENTCOM operations during OEF and OIF, particularly information sharing with our coalition partners.[34] Current security policy drove implementation of seven different networks of different security levels as coalition partners could not have access to US networks. Each network required a completely separate infrastructure from the user's desktop to the servers and was limited to slow, human-in-the-loop information exchange guards between networks (except for extremely limited applications). Requirements to collaborate outside the .mil domain and with coalition partners will only increase.[35] Unfortunately, the requirements for immediate posting, smart pull, and collaboration are in direct conflict with current security policies, practices, and access control tools. Solutions may require moving to a risk management security policy vice the current risk aversion policy, and solutions must also simplify the underlying infrastructure to reduce complexity and costs.

Our military operations already suffer from information overload—and the promised proliferation and increasing data rates of sensors and posting of information across the infostructure will only compound the problem. Just finding available information within a sea of data has become a significant challenge. But we also face a challenge to full information access based on topology limitations in directed networks.

Communications and Internet Protocol (IP) networks such as the Internet typically have bi-directional links. Many of the services anticipated for use in collaboration will be Web-based, but the Web is a directed network (links are one-way). Based on Dr. Barabasi's observations, all directed networks break into four regions: IN, OUT, CORE, and ISLANDS (see Figure 2). In these networks each region has different properties—links lead IN to the CORE and OUT from the CORE, the CORE is densely interconnected, and there are multiple ISLANDS not connected to the other three regions. These properties place severe limitations on our ability to search and navigate the Web which are only partially mitigated by search engines.[36] Further, the Global Broadcast System (GBS) is used within the CENTCOM, EUCOM, and PACOM theaters to efficiently deliver video and large files such as imagery products via uni-directional broadcasts in a one-to-many fashion.

Directed networks such as the Web and GBS will require new tools and services to overcome the limitations created by network topology as noted in previous sections. Lack of these tools will hinder information flow and accessibility, smart pull, and shared situational awareness. The twin challenges of information overload and network topology highlight information dissemination and management as an area that must receive intense attention and effort as we become more reliant on NCO.
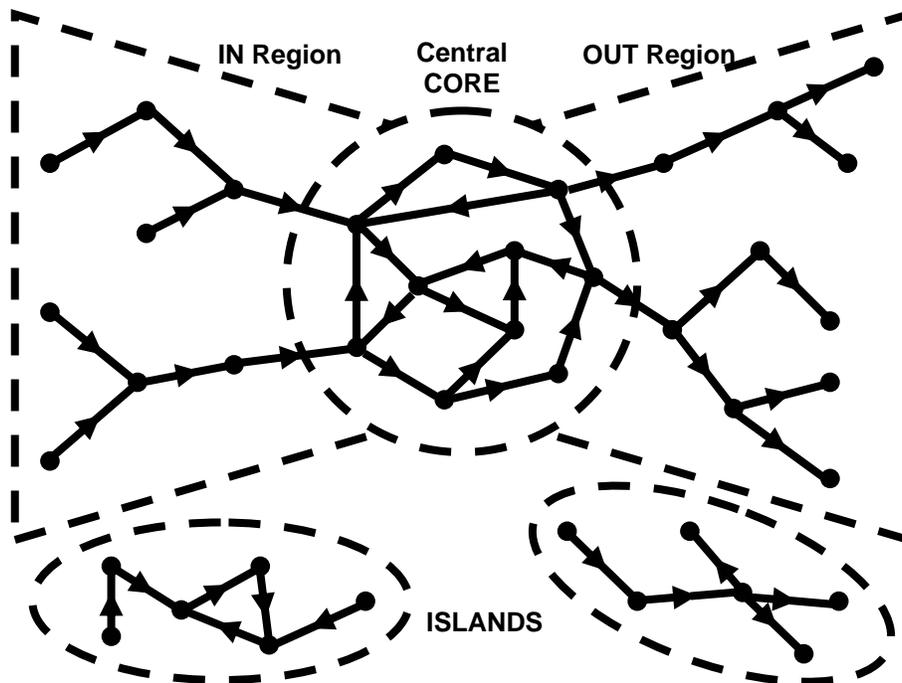
Figure 2: Regions of a Directed Network, after Fig. 12.1 in

Interoperability is subtle—any significant network requires multiple interacting protocols and data and metadata standards to ensure transfer and proper interpretation of data. Merely defining and using standard protocols and data formats is not enough.[37] The users interested in a given capability must choose and implement the same set of protocols and standards. Collaborative tool suites are extremely useful, but are also one of the most complex software tools in use by DoD. Each standardized suite provides a roughly comparable and useful set of functionalities. However, current suites each choose a different set of standard protocols with which to implement its functionality. Thus, the CENTCOM theater was forced to use two standards-compliant collaboration suites that were not interoperable. This led to JTFs using one tool suite to collaborate with lower echelon forces, a second tool suite to collaborate with higher echelons, and the lower echelons (under different JTFs) with no means to collaborate with each other.

Predator UAV video distribution also provides an instructive example. The Predator system was fielded, for programmatic reasons, without a means to disseminate the analog video feed from the ground-control station (GCS) to users scattered across the theater. Deployed communicators devised an *ad hoc* solution using commercial Motion Picture Experts Group (MPEG) video compression equipment. The initial links used an encoder that embedded MPEG data within IP packets. Later, encoders were used that placed MPEG data within IP packets within asynchronous-transfer mode (ATM) cells because the vendor of the original encoder had gone out of business. Due to extreme pressure to increase Predator video distribution, GBS was also pressed into service to carry compressed video. However, GBS had standardized on encoders that embedded MPEG data directly into ATM cells. Each of these three encoders used well-recognized, standardized data formats and protocols. Yet the CENTCOM theater ended up with three mutually non-interoperable UAV video distribution networks. These are only two examples that highlight the need to define sets of standards that provide interoperable end-to-end functional capabilities.[38]

Improved information sharing across domains, across organizations, and with coalition partners will require radical changes to our current security policies and practices. In particular, we need reduce or eliminate the need for separate, complex network infrastructures for each security domain. Overcoming information overload and topology limitations will require new generations of information dissemination and management tools. Finally, true interoperability requires defining and implementing sets of standards that provide end-to-end functional capabilities.

Notes

[1] Ibid. pages 9-10
[2] Ibid. pages 104-104

Notes

[3] Aldo Borgu, "The challenges and limitations of "Network Centric Warfare" - The initial views of an NCW skeptic" (paper presented at the Network Centric Warfare: Improving ADF capabilities through Network Enabled Operations, 2003), Frederick W. Kagan, "War and Aftermath," *Policy Review* (2003), Alfred I. Kaufman, "Be careful what you wish for: The dangers of fighting with a network centric military," *Journal of Battlefield Technology* Vol 5, no. No 2 (2002), Loren Thompson, "The Hidden Dangers of Networked Warfare," in *Issue Brief* (Lexington Institute, 2003).

[4] Alberts, Garstka, and Stein, *Network-Centric Warfare: Developing and Leveraging Information Superiority*. pages 94 and 92

[5] Albert-Laszlo Barabasi, *Linked: How everything is connected to everything else and what it means for business, science, and everyday life* (Plume (Penguin Group), 2002).

[6] John C. Doyle et al., "Robustness and the Internet: Theoretical Foundations," (California Institute of Technology at http://netlab.caltech.edu/internet/, 2002), Walter Willinger and John Doyle, "Robustness and the Internet: Design and Evolution," (California Institute of Technology at http://netlab.caltech.edu/internet/, 2002).

[7] Barabasi, *Linked: How everything is connected to everything else and what it means for business, science, and everyday life*. pages 64-72

[8] Ibid. pages 96-104

[9] Ibid. pages 135-150

[10] Ibid. pages 149-150 and Andre Broido, "Visualizing Internet Topology at a Macroscopic Scale," (CAIDA Topology Mapping Analysis Team at http://www.caida.org/analysis/topology/as_core_network/, 2005).

[11] John W. Smith, "Setting the Conditions for Department of Defense Transformation: On Track to Support Future Joint Operations in Network-Centric Warfare?" (Alexandria, VA: Institute for Defense Analysis, 2003). pages III-22 thru III-32

[12] Barabasi, *Linked: How everything is connected to everything else and what it means for business, science, and everyday life*. pages 112-118, 135

[13] Ibid. pages 110, 119-122

[14] Willinger and Doyle, "Robustness and the Internet: Design and Evolution." and Craig Labovitz, G. Robert Malan, and Farnam Jahanian, "Origins of Internet Routing Instability," (University of Michigan, Department of Electrical Engineering and Computer Science, 1998). and Barabasi, *Linked: How everything is connected to everything else and what it means for business, science, and everyday life*.pages 153-154

[15] Doyle et al., "Robustness and the Internet: Theoretical Foundations.", Labovitz, Malan, and Jahanian, "Origins of Internet Routing Instability.", Willinger and Doyle, "Robustness and the Internet: Design and Evolution."

[16] JFCOM, "Capstone Requirements Document [CRD]: Global Information Grid [GIG]," (Joint Forces Command, Norfolk, VA, 2001).

[17] Robert K. Ackerman, "Data Holds the Key to Network-Centricity," *SIGNAL* (January 2005), Dan Caterinicchia and Matthew French, "Network-centric warfare: Not there yet," in *Federal Computer Week at http://www.fcw.com/article79869-06-09-03-Print* (9 June 2003), Maryann Lawlor, "Iraqi Communications Transition from Tactical to Practical," *SIGNAL* (November 2004), David Talbot, "How Technology Failed in Iraq," *MIT Technology Review* (November 2004).

Notes

[18] "LTG ABIZAID SENATE CONFIRMATION HEARING QUESTIONS AND ANSWERS," (United States Senate at http://www.senate.gov/~armed_services/statemnt/2003/June/Abizaid.pdf, 2003), "THE SENATE ARMED SERVICES COMMITTEE STATEMENT OF GENERAL TOMMY R FRANKS," (United States Senate at http://www.au.af.mil/au/awc/awcgate/congress/franks_09july03.pdf, 2003).

[19] Adam J. Hebert, "Toward Supremacy in Space," *Air Force Magazine Online at http://www.afa.org/magazine/Jan2005/0105space.asp* 88, no. 1 (January 2005), Lawlor, "Iraqi Communications Transition from Tactical to Practical.", Smith, "Setting the Conditions for Department of Defense Transformation: On Track to Support Future Joint Operations in Network-Centric Warfare?" page IV-7

[20] Ackerman, "Data Holds the Key to Network-Centricity." page 41

[21] Paul W. Phister and Igor G. Plonisch, "Military Applications of Information Technologies," *Air and Space Power Journal* Spring 2004 (2004).

[22] Kiran Challapali, Dagnachew Birru, and Stefan Mangold, "Spectrum Agile Radio for Broadband Applications," *CommsDesign at http://www.commsdesign.com/printableArticle/?articleID=29100659* (23 Aug 2004), Bruce Fette, "Three Obstacles to Cognitive Radio," *CommsDesign at http://www.commsdesign.com/printableArticle/?articleID=29100657* (23 August 2004), Bill Krenik, "Clearing Interference for Cognitive Radio," *CommsDesign at http://www.commsdesign.com/showArticle.jhtml?articleID=29100649* (23 Aug 2004), Bill MacFarland, "WLANs are jump-starting cognitive radio," *CommsDesign at http://www.commsdesign.com/printableArticle/?articleID=29100648* (23 Aug 2004), Patrick Mannion, "Smart Radios," *Electronic Engineering Times - Special Supplement* (November 2004), Efstratios Skafidas, "Multichannel basebands meet challenge of Cognitive Radio," *CommsDesign at http://www.commsdesign.com/printableArticle/?articleID=29100655* (23 Aug 2004), Willinger and Doyle, "Robustness and the Internet: Design and Evolution."

[23] XPXC, "The U.S. Air Force Transformational Flight Plan." appendices B and D

[24] M. Luglio, C. Roseti, and M. Gerla, "TCP Performance over Satellite in cas of Multiple Sessions per Links using Efficient Flow Control and Real OS" (paper presented at the Proceedings of 10th Ka and Broadband Communications Conference, Vicenza, IT, 2004), D. C. Palter, *Satellites and the Internet: Challenges and Solutions*, 1 ed. (Sonoma, CA: SATNEWS Publishers, 2003).

[25] "Net Centric Operations and Warfare Reference Model for the Joint War Fighter: " A Concept for the Enterprise View"," in *GIGv2.0 Selected Briefings CD-ROM* (Washington D.C.: OSD, CIO/Architecture and Interoperability Directorate, 2002), Scott Burleigh et al., "Delay-Tolerant Networking: An Approach to Interplanetary Internet," *IEEE Communications Magazine* (June 2003), Forrest Warthman, "Delay-Tolerant Networks (DTNs): A Tutorial," (Interplanetary Internet Special Interest Group at http://www.ipnsig.org/reports/DTN_Tutorial1.pdf, May 2003).

[26] John P Geis, *Directed Energy Weapons on the Battlefield: A new vision for 2025, Occasional Paper No. 32, Center for Strategy and Technology* (Maxwell AFB, AL: Air University Press, 2003), Carlo Kopp, "The Electromagnetic Bomb - a Weapon of Electrical Mass Destruction," *Air and Space Power Chronicals* (1996).

Notes

[27] John G. Proakis, *Digital Communications*, 4 ed. (McGraw-Hill Science/Engineering/Math, 2001), Bernard Sklar, *Digital Communications: Fundamentals and Applications*, 2 ed. (Prentice Hall PTR, 2001), Roger E. Ziemer, Roger L. Peterson, and David E. Borth, *Introduction to Spread Spectrum Communications*, 1 ed. (Prentice Hall, 1995).

[28] Jim Garamone, "CENTCOM Charts Operation Iraqi Freedom Progress," in *American Forces Information Service* (DefenseLINK at http://www.defenselink.mil/News/Mar2003/n03252003_200303254.html, 25 Mar 2003), Hebert, "Toward Supremacy in Space."

[29] David Moore et al., "The Spread of the Sapphire/Slammer Worm," (CAIDA at http://www.caida.org/outreach/papers/2003/sapphire/sapphire.html, 2003), Colleen Shannon, "The Spread of the Witty Worm," (CAIDA at http://www.caida.org/analysis/security/witty/, 2004).

[30] Ivan Balepin, "Superworms and Cryptovirology: A Deadly Combination," (University of California-Davis, Department of Computer Science at http://vx.netlux.org/lib/aib01.html, 2003), Tim Freeman, "Extortion Worms: Internet Worms tha Discourage Disinfection," (at http:/www.fungible.com/nodisinfect.html, 2002), Stuart Staniford et al., "The Top Speed of Flash Worms," *Proceedings of the ACM* (2004), Adam Young and Moti Young, "Cryptovirology: Extortion-Based Security Threats and Countermeasures" (paper presented at the Proceedings of the 1996 IEEE Symposium on Security and Privacy, 1996).

[31] David Moore et al., "Internet Quarantine: Requirements for Containing Self-Propagating Code," (University of California - San Diego, 2002).

[32] Ackerman, "Data Holds the Key to Network-Centricity." page 39

[33] Ibid. pages 37-41

[34] Office of Force Transformation, "The Implementation of Network-Centric Warfare." page 30

[35] Ackerman, "Data Holds the Key to Network-Centricity." pages 37-41

[36] Barabasi, *Linked: How everything is connected to everything else and what it means for business, science, and everyday life*. pages 167-169

[37] Smith, "Setting the Conditions for Department of Defense Transformation: On Track to Support Future Joint Operations in Network-Centric Warfare?" pages III-43 thru III-47 and IV-10 thru IV-16

[38] Ibid. pages III-43 thru III-47 and IV-10 thru IV-16

Summary and Recommendations

Topology, robustness, and vulnerability cannot be fully separated. All complex systems have their Achilles' heel.[1]

Network-centric Operations (NCO) concepts and capabilities are central to DoD, Service, and allied transformation efforts and are predicted to have wide-ranging impacts on the conduct of warfare and military forces. The predicted future environment has stealthy, mobile forces widely dispersed upon a non-contiguous battlefield operating at very high operational tempos. The tenants of NCO are that a robustly networked force improves information sharing and collaboration. Ultimately this should provide improved decision quality and increased mission effectiveness by massing effects from widely dispersed and mobile forces and allows us to shape the battlespace faster than our adversary using synchronized effects.

NCO involves a consistent set of concepts that rely on collaboration and information sharing and create a radical and challenging set of requirements for the supporting networks and information infrastructure. Current and near-term network capabilities leave a significant gap between the network and information infrastructure envisioned and required by NCO. Without this underlying infostructure, the projected benefits of NCO concepts will not be realized and any dependent military capabilities will suffer.

Our analysis of infostructure requirements has identified some key capability gaps to address and highlighted some potential pitfalls to avoid:

- Bandwidth for mobile, dispersed forces will be limited for quite some time; thus, we must carefully experiment with smart pull and ensure our applications are bandwidth efficient.

- We must identify, protect, provision, and diversify the connectivity hubs within our networks, and recognize inherent commercial SATCOM vulnerabilities and implement countermeasures to limit the effects of failures or attacks.

- Effective collaboration requires protecting user and hub connectivity to prevent the "inverse Metcalfe effect" from creating a network utility collapse. Continued reliance on networks unprotected from external and internal disruption will create significant mission vulnerabilities.

- Preventing cascade failure will require a deep understanding of our networks and continuous vigilance using a distributed network of sensors that sense the network

- Tools for information dissemination and management must receive intense attention and effort to prevent information overload. We must create tools and services to overcome the limitations on discovery, access, and transfer imposed by network topology.

- Latency and disconnection tolerance must be designed into applications and protocols for the foreseeable future to ensure robust network services.

- Improved information sharing across security domains will require radical changes to our current security policies and practices.

- True interoperability requires defining and implementing sets of standards that provide end-to-end functional capabilities.

NCO' dependence on the infostructure creates a set of challenges and potential vulnerabilities that can only be overcome through critical analysis, superlative systems engineering and implementation, and continued investment in people, organizations, and equipment. Whether the sweeping vista of NCO's ultimate goals can ever be achieved remains

to be seen. However, even attempting to create the networks and information infrastructure demanded by NCO will produce vastly more capable and robust networks and information capabilities and enhance our military forces.

Notes

[1] Barabasi, *Linked: How everything is connected to everything else and what it means for business, science, and everyday life*. pages 121-122

Bibliography

"LTG ABIZAID SENATE CONFIRMATION HEARING QUESTIONS AND ANSWERS." United States Senate at http://www.senate.gov/~armed_services/statemnt/2003/June/Abizaid.pdf, 2003.

"Naval Transformation Roadmap 2003." US Navy, 2003.

"Net Centric Operations and Warfare Reference Model for the Joint War Fighter: " A Concept for the Enterprise View"." In *GIGv2.0 Selected Briefings CD-ROM*. Washington D.C.: OSD, CIO/Architecture and Interoperability Directorate, 2002.

"THE SENATE ARMED SERVICES COMMITTEE STATEMENT OF GENERAL TOMMY R FRANKS." United States Senate at http://www.au.af.mil/au/awc/awcgate/congress/franks_09july03.pdf, 2003.

"United States Army Transformation Roadmap." US Army, 2003.

Ackerman, Robert K. "Data Holds the Key to Network-Centricity." *SIGNAL* (January 2005).

Alberts, David S., John J. Garstka, and Frederick P. Stein. *Network-Centric Warfare: Developing and Leveraging Information Superiority*. 2nd (revised) ed, *Information Age Transformation Series*: DOD Command and Control Research Program, 2000.

Alberts, David S., John J. Gartska, Richard E. Hayes, and David A. Signori. *Understanding Information Age Warfare*. Washington D.C.: DOD Command & Control Research Program, 2001.

Alberts, David S., and Richard E. Hayes. *Power to the Edge: Command and Control in the Information Age*, *Information Age Transformation Series*: DOD Command and Control Research Program, 2003.

Alston, Anthony. "Network Enabled Capability - the concept." *Journal of Defense Science* 8, no. 3 (2003): 106-16.

Balepin, Ivan. "Superworms and Cryptovirology: A Deadly Combination." University of California-Davis, Department of Computer Science at http://vx.netlux.org/lib/aib01.html, 2003.

Barabasi, Albert-Laszlo. *Linked: How everything is connected to everything else and what it means for business, science, and everyday life*: Plume (Penguin Group), 2002.

Borgu, Aldo. "The challenges and limitations of "Network Centric Warfare" - The initial views of an NCW skeptic." Paper presented at the Network Centric Warfare: Improving ADF capabilities through Network Enabled Operations 2003.

Broido, Andre. "Visualizing Internet Topology at a Macroscopic Scale." CAIDA Topology Mapping Analysis Team at http://www.caida.org/analysis/topology/as_core_network/, 2005.

Burleigh, Scott, Adrian Hooke, Leigh Torgerson, Kevin Fall, Vint Cerf, Bob Durst, Kieth Scott, and Howard Weiss. "Delay-Tolerant Networking: An Approach to Interplanetary Internet." *IEEE Communications Magazine* (June 2003): 128-36.

Caterinicchia, Dan, and Matthew French. "Network-centric warfare: Not there yet." In *Federal Computer Week at http://www.fcw.com/article79869-06-09-03-Print*, 9 June 2003.

Cebrowski, Aurthur K. "Network Centric Warfare: Its Origin and Future." *Naval Institute Proceedings* (1998): 28-35.

Challapali, Kiran, Dagnachew Birru, and Stefan Mangold. "Spectrum Agile Radio for Broadband Applications." *CommsDesign* at *http://www.commsdesign.com/printableArticle/?articleID=29100659* (23 Aug 2004).

CJCS. "Joint Vision 2010." Joint Staff.

———. "Joint Vision 2020." Joint Staff.

Doyle, John C., Jean Carlson, Steven H. Low, Fernando Paganini, Glenn Vinnicombe, Walter Willinger, Jason Hickey, Pablo Parrilo, and Lieven Vandenberghe. "Robustness and the Internet: Theoretical Foundations." California Institute of Technology at http://netlab.caltech.edu/internet/, 2002.

Fette, Bruce. "Three Obstacles to Cognitive Radio." *CommsDesign* at *http://www.commsdesign.com/printableArticle/?articleID=29100657* (23 August 2004).

Freeman, Tim. "Extortion Worms: Internet Worms tha Discourage Disinfection." at http:/www.fungible.com/nodisinfect.html, 2002.

Garamone, Jim. "CENTCOM Charts Operation Iraqi Freedom Progress." In *American Forces Information Service*: DefenseLINK at http://www.defenselink.mil/News/Mar2003/n03252003_200303254.html, 25 Mar 2003.

Geis, John P. *Directed Energy Weapons on the Battlefield: A new vision for 2025*, *Occasional Paper No. 32, Center for Strategy and Technology*. Maxwell AFB, AL: Air University Press, 2003.

Hebert, Adam J. "Toward Supremacy in Space." *Air Force Magazine Online at http://www.afa.org/magazine/Jan2005/0105space.asp* 88, no. 1 (January 2005).

JFCOM. "Capstone Requirements Document [CRD]: Global Information Grid [GIG]." 1: Joint Forces Command, Norfolk, VA, 2001.

Kagan, Frederick W. "War and Aftermath." *Policy Review* (2003).

Kaufman, Alfred I. "Be careful what you wish for: The dangers of fighting with a network centric military." *Journal of Battlefield Technology* Vol 5, no. No 2 (2002).

Kopp, Carlo. "The Electromagnetic Bomb - a Weapon of Electrical Mass Destruction." *Air and Space Power Chronicals* (1996).

Krenik, Bill. "Clearing Interference for Cognitive Radio." *CommsDesign* at *http://www.commsdesign.com/showArticle.jhtml?articleID=29100649* (23 Aug 2004).

Labovitz, Craig, G. Robert Malan, and Farnam Jahanian. "Origins of Internet Routing Instability." University of Michigan, Department of Electrical Engineering and Computer Science, 1998.

Lawlor, Maryann. "Iraqi Communications Transition from Tactical to Practical." *SIGNAL* (November 2004).

Luglio, M., C. Roseti, and M. Gerla. "TCP Performance over Satellite in cas of Multiple Sessions per Links using Efficient Flow Control and Real OS." Paper presented at the Proceedings of 10th Ka and Broadband Communications Conference, Vicenza, IT 2004.

MacFarland, Bill. "WLANs are jump-starting cognitive radio." *CommsDesign* at *http://www.commsdesign.com/printableArticle/?articleID=29100648* (23 Aug 2004).

Mannion, Patrick. "Smart Radios." *Electronic Engineering Times - Special Supplement* (November 2004): 61-65.

Moore, David, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford, and Nicholas Weaver. "The Spread of the Sapphire/Slammer Worm." CAIDA at http://www.caida.org/outreach/papers/2003/sapphire/sapphire.html, 2003.

Moore, David, Colleen Shannon, Geoffrey M. Voelker, and Stefan Savage. "Internet Quarantine: Requirements for Containing Self-Propagating Code." University of California - San Diego, 2002.

Office of Force Transformation. "The Implementation of Network-Centric Warfare." edited by OSD, 75. Washington D.C.: U.S. Government Printing Office, 2005.

———. "Military Transformation - A Strategic Approach." edited by OSD, 36: U.S. Government Printing Office, 2003.

Palter, D. C. *Satellites and the Internet: Challenges and Solutions*. 1 ed. Sonoma, CA: SATNEWS Publishers, 2003.

Phister, Paul W., and Igor G. Plonisch. "Military Applications of Information Technologies." *Air and Space Power Journal* Spring 2004 (2004): 77-90.

Proakis, John G. *Digital Communications*. 4 ed: McGraw-Hill Science/Engineering/Math, 2001.

Rumsfeld, Donald. "Transformation Planning Guidance." Washington D.C.: OSD, 2003.

Shannon, Colleen. "The Spread of the Witty Worm." CAIDA at http://www.caida.org/analysis/security/witty/, 2004.

Skafidas, Efstratios. "Multichannel basebands meet challenge of Cognitive Radio." *CommsDesign at http://www.commsdesign.com/printableArticle/?articleID=29100655* (23 Aug 2004).

Sklar, Bernard. *Digital Communications: Fundamentals and Applications*. 2 ed: Prentice Hall PTR, 2001.

Smith, John W. "Setting the Conditions for Department of Defense Transformation: On Track to Support Future Joint Operations in Network-Centric Warfare?" 122. Alexandria, VA: Institute for Defense Analysis, 2003.

Staniford, Stuart, David Moore, Vern Paxson, and Nicholas Weaver. "The Top Speed of Flash Worms." *Proceedings of the ACM* (2004).

Talbot, David. "How Technology Failed in Iraq." *MIT Technology Review* (November 2004).

Thompson, Loren. "The Hidden Dangers of Networked Warfare." In *Issue Brief*: Lexington Institute, 2003.

Warthman, Forrest. "Delay-Tolerant Networks (DTNs): A Tutorial." Interplanetary Internet Special Interest Group at http://www.ipnsig.org/reports/DTN_Tutorial1.pdf, May 2003.

Willinger, Walter, and John Doyle. "Robustness and the Internet: Design and Evolution." California Institute of Technology at http://netlab.caltech.edu/internet/, 2002.

XPXC. "The U.S. Air Force Transformational Flight Plan." HQ USAF, 2003.

Young, Adam, and Moti Young. "Cryptovirology: Extortion-Based Security Threats and Countermeasures." Paper presented at the Proceedings of the 1996 IEEE Symposium on Security and Privacy 1996.

Ziemer, Roger E., Roger L. Peterson, and David E. Borth. *Introduction to Spread Spectrum Communications*. 1 ed: Prentice Hall, 1995.