Maneuver the Net: Lines of Information and Battle Command

A Monograph
by
MAJ Kenneth E. Viall
United States Army

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

Second Term AY 00-01

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

Major Kenneth E. Viall

Title of Monograph: Maneuver the Net: Lines of Information and Battle Command

Approved by:

_____, Monograph Director
COL James Connelly, M.S.

_____, Director, School of Advanced Military Studies
COL Robin P. Swan, MMAS

_____, Director, Graduate Degree Programs
Philip J. Brookes, Ph.D.

Accepted this 23d day of May 2001 by:

Abstract

Maneuver the Net: Lines of Information and Battle Command, by Major Kenneth E. Viall, 80 pages.

This monograph sought to determine if Army transformation forces could integrate leadership and technology to achieve information superiority during maneuver in the land dimension. Leadership and technology could provide a synergy of application where each dimension supports the other in the friendly force component of information management and protection. Information and knowledge were examined in relation to the concept of Network-Centric Warfare. Analysis examined whether transformation force leadership (battle command) could be expected to integrate technology with operational concepts to achieve information superiority with timely, accurate, and relevant information. Timeliness concerns the rapidity of information transmission and concerns the design of information systems with technology and human components. Accuracy represents the certainty inherent in each element of information based primarily on sources and presentation. Relevance provides a measure of the importance of each element of information based on contributions to knowledge during operations. The monograph determined that neither the technological dimension nor the leadership dimension of information alone provides sufficient timeliness, accuracy, and relevance to ensure information superiority for transformation forces during maneuver. However, the synergy of both have great potential for overcoming the complexity of information support to maneuver.

TABLE OF CONTENTS

List of Illustrations

List of Tables

List of Figures

CHAPTER ONE

Information and Future War

Half a century ago rapidity of transmission of information in campaigns was generally measured by the speed of the couriers; distant movements were left to take care of themselves or neglected, since, if discovered, they could only be reported after the event; immediate operations were limited; the chessboard was small. . . . [now] the nerves extending from the controlling brain to the striking arm—that is, the lines of thought transmission—should be the most perfect, the most rapid, and the most certain that science can give. – Brigadier General George Scriven, 1915.[1]

General George Scriven wrote the passage in the epigraph above to recognize the profound effect that that the telegraph, telephone, and early wireless radios had on the conduct of operational campaigns prior to World War I. Computers, satellites, and advanced digital communications have extended the "lines of thought transmission" to unprecedented distances while also harnessing a complex array of sensors to enhance situational awareness. Science and technology trends herald further advances that the military must consider for the future of warfare.

Information support to recent operations marked a transition from legacy voice and platform-centric systems to network-based information systems and offered unprecedented information transfer capacities. The information demands in Kosovo operations in 1999 required great reliance on commercial satellite bandwidth to meet perceived information requirements. Satellite communications and digital computer networks are expected to provide great capabilities for future transformation forces.

Joint doctrine defines information superiority as "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[2] Information superiority provides the foundation for Joint Vision 2020[3] since "virtually all of the advanced military systems and capabilities . . . draw on new information

---

[1] George Percival Scriven, *The Service of Information, United States Army*, Circular, no. 8 (Washington, DC: Govt. print. off., 1915), 14.

[2] Joint Chiefs of Staff, *Information Operations.*, Joint Publication 3-13 (Washington D.C.: U.S. Government Printing Office, 1996).

[3] Joint Chiefs of Staff, *Joint Vision 2020* [Online] (Joint Staff, 2000, accessed November 3, 2000); available from http://www.dtic.mil/jv2020/jv2020a.pdf.

technologies. . . . [and] every facet of America's military posture is now permeated with digital processors and software."[4] General Eric Shinseki, Chief of Staff of the Army, stressed the importance of information superiority for the conduct of future warfare in the 1999 Army vision statement.[5] Ongoing Army Force XXI digitization experiments investigate "the application of micro-processors to achieve a seamless information flow for coordinating and employing warfighting assets."[6] The Army's draft objective force capstone operational concept, TRADOC Pamphlet 525-5, envisions the existence of "responsive, reliable, mobile, non-line-of-sight, network-centric C4ISR [Command and Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance] capabilities that integrate accurate, real-time intelligence with operational and support systems to enable rapid, accurate targeting, agile maneuver and precision support."[7]

Further challenges to the achievement of information superiority involve the operational framework, including the selection of lines of operations that lead to a decisive mission outcome.[8] Decisive operations are often characterized by transitions involving deployments and complex maneuvers. The concept of a line of information represents a theoretical sum of information, flowing via various means parallel but distinct from the line of operations, connecting different echelons with each other and with bases of information. Lines of information can diverge from traditional, physical lines of communication by way of the electromagnetic spectrum to transit aerial relays including communications satellites. Historical examples abound where military

---

[4] Lauren B. Thompson, "Military Supremacy and How We Keep It," *Policy Review*, no. 97 (Oct/Nov 1999): 28

[5] Eric K. Shinseki, *The Army vision: Soldiers on Point for the Nation . . . Persuasive in Peace, Invincible in War* [Online] (1999, accessed 12 October 1999); available from www.hqda.army.mil/OCSA/vision.htm.

[6] Steven J. Fox, "Unintended Consequences of Joint Digitization," in *Sun Tzu and information warfare: a collection of winning papers from the Sun Tzu Art of War in Information Warfare Competition*, ed. Robert E. Neilson (Washington, DC: National Defense University Press, 1997), 126.

[7] Headquarters Training and Doctrine Command, *Force XXI Operations: A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Early Twenty-First Century (31 July 2000 Draft)*, TRADOC PAM 525-5 (Washington, DC: United States Army Training and Doctrine Command, 2000).

[8] Headquarters Department of the Army, *Operations (DRAG Edition)*, Field Manual 3-0 (Washington, DC: U.S. Government Printing Office, 2000), 5-8.

forces conducting decisive maneuver temporarily overextended their line of information, with effects ranging from a slight degradation of force effectiveness to actual culmination.[9] With expected advances in information technology, can future Army transformation forces integrate leadership and technology to maintain information superiority during similar maneuvers and transitions?

Information, Transformation, and Network-Centric Warfare

Information flow gained a speed advantage using signal flags and field telegraphs to extend lines of information from the strategic telegraph network to field headquarters beginning with the American Civil War. Overseas deployments used undersea telegraph beginning with the Spanish American War and added communications satellites by the Vietnam War. During World War I, the telegraph and telephone proved insufficient to keep pace with operational advances and wireless telegraphy was not widely available. Information flow gained a spatial advantage when units in World War II had access to more radios to achieve electromagnetic connectivity for long-range command and control. However, applications at the tactical level often required the occupation of remote hilltops to provide radio relay over rugged terrain that would also be considerations in Korea and Vietnam.

Vietnam provided the testing ground for the first rudimentary data transfer and long range satellite communications that would be further developed during operations in Grenada and Panama. Information flow gained a processing and storage advantage with the proliferation of computers to lower and lower echelons in Operation Desert Storm and Restore Hope, Somalia. Not until Operation Uphold Democracy, Haiti, did common-user data networks become available for deployed command and control.

---

[9] Kenneth E. Viall, "Big Blue Arrows: Lines of Information and the Transformation Force" (Monograph, Ft. Leavenworth, KS: U.S. Army School of Advanced Military Studies, 2001).This monograph continues to trace the impact of advancing technology levels on information support during operational movement begun the author's previous monograph. Without a robust network as envisioned in Network-Centric Warfare, a marked contrast has existed between the level of information support built up over time at a base of operations and the level of support that could be extended along lines of information in support of forces in motion.

Army transformation plans as of 2001 include a medium-term conversion of a number of conventional brigades to Interim Brigade Combat Teams (IBCT), and the development of an Interim Division (IDIV), to focus science, technology, leadership, and organizational development on solutions for crafting a more strategically relevant Army, an Objective Force, for future conflicts. Information has a dominant role in the success of these organizations, because when "empowered with internetted communications and intelligence packages, an IBCT will be capable of deploying anywhere in the world in ninety-six hours to immediately begin operations across the spectrum of conflict."[10]

Douglas A. Macgregor, in *Breaking the Phalanx: A New Design for Landpower in the 21st Century* proposed similar capabilities and even suggested a C4I battalion at Army Corps level, to provide a theater-wide base of information akin to theater logistics support relationships assigned to the Army by Title X, United States Code.[11] Other writers forecast that

> . . . combat units can be organized into smaller task-organized elements that are more mobile than units today . . . [that] can operate within an enemy's decision cycle since they will leverage information to accelerate the pace of operations. Because these units are networked on an information system, they can fulfill multiple taskings on a nonlinear battlefield and be mutually supporting. Forward staffs can be reduced and commanders can use the information network to reach back to out-of-area staffs and exploit resident expertise in analysis centers . . . Smaller sized units, increased lethality, and reduced forward staffs . . . will result in increased agility and decreased vulnerability, in part due to a shrunken logistics footprint.[12]

The Army leadership believes that the integration of all brigade subcomponents in a network increases the lethality of the brigade. Optimized for small scale contingency operations, brigades can expect a semi-permissive entry to an area using a C-130 capable airfield or will follow a forced-entry unit after airfield seizure to immediately begin operations on complex and urban terrain.[13]

---

[10] James Dubik, "IBCT at Fort Lewis," *Military Review* 80, no. 5 (Sep-Oct 2000): 18

[11] Douglas A. Macgregor, *Breaking the Phalanx: A New Design for Landpower in the 21st Century* (Westport, CT: Praeger Publishers, 1997), 71.

[12] Lawrence E. Casper, Irving L. Halter, and others, "Knowledge Based Warfare: A Security Strategy for the Next Century," *Joint Force Quarterly*, no. 13 (1996): 85

[13] Dubik, 23.

An interim division will likewise be expected to deploy rapidly and be "heavily reliant on reach-back (through organic and joint assets) for theater and national [intelligence] resources."[14] When serving as an Army Forces (ARFOR) headquarters for units including an IBCT, reach-back also helps subordinates "leverage organic and non-organic resources from outside the [area of operations] . . . reduces the [unit] footprint . . . enhances operational agility and further reduces force protection requirements."[15]

Concern about technology in war permeates the literature on future war and thus influences the development of future concepts. For example, the concept of Network-Centric Warfare (NCW) represents an acceptance of the role of increasingly sophisticated information technologies for future warfare. NCW transcends a pure information system focus to provide an operational concept that integrates the effects of sensors, decision-makers, and shooters to create increased combat power with enhanced information superiority. Characteristics of Network-Centric Warfare include common situational understanding, reachback capability for operational planning, intelligence, fires, sustainment, and force protection to minimize in-theater presence, and the requisite organization, doctrine, and training to leverage the power of information.[16]

However, achieving benefits from Network-Centric Warfare may require leaders that can understand the fundamental nature of information and knowledge in warfighting. In *Command and War*, Martin Van Creveld notes the historical shortfalls in information despite technological advances and changes in command and control structures.[17] Information systems have physical constraints including line-of-sight radio propagation, communications channel capacity, and

---

[14] David L. Gosinski, "The Interim Division," *Military Intelligence Professional Bulletin* 26, no. 2 (Jul-Sep 2000): 9

[15] Headquarters Combined Arms Center, *ARFOR Organization and Operational Concept (Draft)* [Online] (Headquarters, Combined Arms Center, 2000, accessed 2 February 2000); available from FTP://160.149.109.31/TF ARFOR/.

[16] David S. Alberts, John J. Gartska, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority* (Washington, DC: C4ISR Cooperative Research Program, 1999), 86.

Richard Lee Armitage, Andrew F. Krepinevich, and Others, "National Security in the 21st Century: The Challenge of Transformation," *Joint Force Quarterly*, no. 16 (1997): 18

[17] Martin L. Van Creveld, *Command in war* (Cambridge, Mass: Harvard University Press, 1985), 258.

computer network congestion. Human cognitive abilities, perceptions, and organizational designs may not neatly match information system capabilities. Achieving information superiority at the decisive time and place will require technologically savvy battle commanders who can adapt information systems to the terrain and force disposition.

Army Field Manual 3-0, *Operations*, describes information as one element of combat power linked to four others: maneuver, firepower, protection, and the most essential one—leadership. Commanders can use information "to shape the operational environment and create the conditions for employing the other elements of combat power."[18] Potential adversaries will also benefit from technology. Predictable air defense and logistics networks may be replaced by "porous, distributed, and autonomous formations able to absorb repeated strikes with little loss of people or effectiveness."[19] Thus, information itself remains neutral, and opposing forces must find ways to gain a position of advantage relative to each other in the conduct of operations.

Technology, Leadership, and Network-Centric Warfare

This monograph sought to determine if Army transformation forces can integrate leadership and technology to achieve information superiority during maneuver in the land dimension. Based on a common framework for information and information technology, leadership and technology could provide a synergy of application where each dimension supports the other. The thesis specifically considered the friendly force component of information management and protection vice degradation of enemy information systems.

First, the monograph examined the nature of the information environment to provide the framework for analysis. Information and knowledge definitions were derived. A working definition of "network" was related to military information and the hierarchy of information.

Second, analysis determined whether the technology supporting the concept of "Network-Centric Warfare" provides timeliness, accuracy, and relevance of information for

[18] Headquarters Department of the Army, 4-9.

[19] Robert H. Scales and others, *Future warfare: Anthology* (Carlisle Barracks, Pa.: U.S. Army War College, 1999), 70.

Army forces conducting maneuver in the land dimension. Digitization, advanced communications satellites, and new network technologies provide the tools that the transformation force must apply. This area is important since "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."[20] Military theory and writings on Network-Centric Warfare and information operations were reviewed to find the best definition or framework for the answer.

Next, analysis examined whether transformation force leadership (battle command) could be expected to integrate technology with operational concepts to achieve information superiority with timely, accurate, and relevant information. A review of current operational concepts of transformation coupled with analysis from the Center for Army Lessons Learned from Bosnia, Kosovo, digital rotations, and experiments highlighted the relationship of human cognitive abilities to network information systems as technology improved.

Finally, based on the analysis of leadership and technology, the contributions of both dimensions to information superiority were summarized. Particular focus was placed on areas where timeliness, accuracy, or relevance could be enhanced. Implications for future operational concepts were presented.

Network-Centric warfare categorizes information according to timeliness, accuracy, and relevance. Timeliness concerns the rapidity of information transmission and concerns the design of information systems with available technology. Accuracy represents the certainty inherent in each element of information based primarily on sources. Relevance provides a measure of the importance of each element of information based on contributions to knowledge at a particular point in an operation. These three criteria are commonly used qualities of military information.[21]

---

[20] Alberts, Gartska, and Stein, 91.

[21] Robert D. Cox, "Information Pathology and the Army Tactical Command and Control System (ATCCS): Is ATCCS a Cure?" (Monograph, School of Advanced Military Studies, US Army Command and General Staff College, 1990), 2. See also appendix one for a comparison of intelligence and information criteria from joint doctrine.

Timeliness represents the rapidity of transmission of information between nodes irrespective of the nature of the information. Technology may provide timeliness from near speed of light to long delays for certain types of messaging systems. Conversely, leadership may allow information to stagnate in computers or could short-circuit long message queues when a high priority, relevant message is found to speed transmission.

Accuracy measures correctness of information, or how close it is to actual truth. Technology inserts its own level of resolution, such as grid locations and elevation data on digital maps. Technology may correlate multiple data sources to provide better accuracy.

> How accurate and precise a piece of information is also bears on its relevancy. The degree of accuracy of a piece of information is how true it is. . . . The precision of a piece of information deals with how specific or defined it is. . . . Commanders require that information be both accurate and precise enough for them to make their decisions.[22]

The perception of accuracy may be as crucial to leaders as the actual accuracy of information. Leadership levels of trust in the technology can range from overconfidence that the digital view of the battlefield is perfect, to a lack of confidence in any digital representation not corroborated with human contact. Bomb damage assessment of targets struck in Kosovo in 1999 seems to suffer from such accuracy concerns.[23] Yet elaborate control measures for targeting still applied from the strategic level down to even the laser-guided bombs that pilots controlled to the desired point of impact.

Relevance measures the value of information, relative to time, space, and purpose. Relevant information can be difficult to discern, and is not dependent on large amounts of information.[24] Relevance is central to battle command. It is derived from commander's intent. Thus relevant information "must indicate some future event or condition that relates to the

---

[22] Philip L. Swinford, "Decision Making Implications of Digital Information Systems for the Battalion in Combat" (Thesis, Ft. Leavenworth, KS: U.S. Army Command and General Staff College, 1997), 36.

[23] Timothy L. Thomas, "Kosovo and the Current Myth of Information Superiority," *Parameters* 30, no. 1 (Spring 2000): 15

[24] Jasper A. Welch, "C3I Systems: The Efficiency Connection," in *Selected Analytical Concepts in Command and Control*, ed. John Hwang, Military operations research v. 2 (New York: Gordon and Breach, 1982), 8.

outcome the commander is trying to influence."[25] Technology may not offer much assistance in determining relevance unless it can codify operational expectations using computer artificial intelligence or other computer data sorting techniques that help systems present information. Conversely, decision makers may be presented with an information overload where the relevant information comes buried in an avalanche of irrelevant data. The overwhelming flood of messages on first day of Desert Storm indicates the possibility of similar floods during any military conflict.[26]

Summary

Although information has a central role in future operational concepts, Joint Vision 2020 recognizes the relationship between technology and human decision-making, since

> Information superiority neither equates to perfect information, nor does it mean the elimination of the fog of war. Information systems, processes, and operations add their own sources of friction and fog to the operational environment . . . . the joint force of 2020 will use superior information and knowledge to achieve decision superiority. . .[27]

Examination of the ability of lines of information to support future maneuver in a complex land environment is relevant to ongoing Army transformation. The technological dimension represents the sum of capabilities that provide mechanisms for the transfer of information via various media, and the storage and processing at various nodes, and the assistance rendered to humans to build knowledge. The leadership dimension represents the human dimension of information and the influence on command and control, complexity in operational planning, emplacement of tactical operations centers, and the interpersonal nature of human communications. The synergy of the two may provide the requisite information superiority at the decisive time and place to achieve success on future battlefields.

---

[25] Swinford, 36.

[26] James F. Dunnigan, *Digital Soldiers: the Evolution of High-tech Weaponry and Tomorrow's Brave New Battlefield*, 1st ed. (New York: St. Martin's Press, 1996), 293.

[27] Joint Chiefs of Staff, *Joint Vision 2020*.

Chapter 2

Knowledge and Information

The flow of men and materiel during battle is ever toward the front. The flow of orders and instructions is toward the front. But the prevailing flow of information, on which the writing of orders and instructions for combat are based, is ever toward the rear, and the volume of it seems to increase according to the square of the distance from the fighting line. -- S.L.A Marshal, in *Men Against Fire.* [28]

The framework for analysis for lines of information in a network environment includes the nature of information and knowledge, the information environment, basic concepts of military information, command and control, operational concepts of maneuver, and information warfare. The nature of information and knowledge with respect to technology falls in the realm of cognitive science. To simplify analysis, definitions of information and knowledge for purposes of this monograph were chosen along the interface of technology and humanity. The information environment includes the state of technology, commercial, and military systems and includes a definition of network. Military information includes concepts such as "system of systems" and Network-Centric Warfare. Maneuver focuses the analysis on one of the biggest challenges for information systems. The framework then provides the backdrop against which technology and leadership interact to provide timely, accurate, and relevant information.

Nature of Information and Knowledge

Joint doctrine outlines a cognitive hierarchy built upon data, with processing changed to information, with cognition transformed to knowledge, and with judgment ultimately yielding understanding. Data inherently meshes well with technology. Information relies on context. The same information can exist in two places at once, and have different value to different people. [29] Information theorists have viewed information using differing metaphors: information as the message (content), information as the medium (conduit), or information as "an embedded

---

[28] S. L. A. Marshall, *Men against Fire: the Problem of Battle Command in Future War* (Gloucester, Mass.: Peter Smith, 1978), 100.

[29] Joint Chiefs of Staff, *Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations*, Joint Publication 6-0 (Washington D.C.: U.S. Government Printing Office, 1995), I-4. See also Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway*, 1st ed. (New York: Thunder's Mouth Press, 1994), 323.

physical property of all objects that exhibit organization and structure."[30] All three metaphors allow information to be derived from data streams

> . . . primarily by technological processing: an electromagnetic pulse is converted to a set of symbols on a radar screen. Humans can also be part of this processing. Transformation of information into knowledge is, however, a cognitive process done by humans, if humans are the decision making entities.[31]

Information can also have chaotic characteristics. Claude Shannon's theory of information leads to the conclusion that while the "value of 'information' is hard to quantify, its converse—the 'reduction of uncertainty'—can easily be measured in bits."[32] Information management with technology reduces uncertainty

> . . . with formal representation of information entities and flow to facilitate the construction of computer models which allow specific functions . . . to be automated. Exactness and objectivity are central to this approach, which is based on the manipulation of symbols, mathematical description and the search for appropriate algorithms.[33]

Context provides external cues to add meaning to data. For example, during conversation, the glance of an eye toward an object provides a point of reference to inform the listener of the intended meaning of the spoken words.[34] As context is to information, experience and memory are to knowledge, and "speculative thinking, imaginative leap, and original insight are needed to invent knowledge that is new to all."[35]

Knowledge remains primarily a human attribute, since despite "the rise of artificial intelligence and other 'knowledge technologies,' knowledge is created by human beings—by knowledge workers …and by knowledge consumers."[36] Knowledge exists in two forms-explicit

---

[30] John Arquilla and David F. Ronfeldt, eds. *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, Calif.: Rand, 1997), 148.

[31] Alexander H. Levis and Michael Athans, "The Quest for a C3 Theory: Dreams and Realities," in *Science of Command and Control: Coping with Uncertainty*, ed. Stuart E. Johnson and Alexander H. Levis, AIP information systems series; v. 1. (Washington, D.C.: AFCEA International Press, 1988), 7.

[32] J.S. Lawson, "The State Variables of a Command Control System," in *Selected Analytical Concepts In Command And Control*, ed. John Hwang, Military operations research v. 2 (New York: Gordon and Breach, 1982), 75.

[33] Blaise Cronin and Elisabeth Davenport, *Elements of Information Management* (Metuchen, N.J.: Scarecrow Press, 1991), 1.

[34] Nicholas Negroponte, *Being Digital*, 1st ed. (New York: Knopf, 1995), 135.

[35] Dale E. Zand, *Information, Organization, and Power: Effective Management in the Knowledge Society* (New York: McGraw-Hill, 1981), 69.

[36] Don Tapscott, *The Digital Economy: Promise and Peril in the Age of Networked Intelligence* (New York: McGraw-Hill, 1996), 44.

and tacit. Explicit knowledge exists in forms available to all—from common sense (people eat food) to published works (how to cook). Tacit knowledge remains internal to each individual, everything from personal thoughts to personal writings. Explicit and tacit knowledge display "symbiotic relationships whereby tacit knowledge contributes to explict knowledge and vice versa."[37]

Modern businesses seeking to remain relevant recognize that the "new economy is also a knowledge economy based on the applications of human know-how to everything we produce and how we produce it."[38] Challenged to harness the tacit knowledge extant in their organizations, they ask:

> What knowledge is worthwhile? Who in the organization should have it? Who should receive it? Why, what are they to do with it? . . . Worthwhile knowledge reduces uncertainty when a decision is make. Knowledge that does not reduce uncertainty is either redundant or irrelevant.[39]

Knowledge theory recognizes the value of individuals for their tacit knowledge (based on experience) and their contribution to explicit knowledge via communication. Literature on knowledge work defines a "Silo" as a "metaphor for the too self-contained unit into which stuff gets dumped into and extracted from, but which has no communication with the other silos . . . that comprise the organization."[40] By design, business leaders seek to use networked communications to stimulate communication, minimize silos, thus generating more knowledge that is relevant.

The seam where technology fades to humanity appears between information taken in context and the explicit form of knowledge. Higher levels of the cognitive hierarchy, including understanding (and wisdom), are assumed to manifest themselves as explicit knowledge to interface with technology. For this analysis, information encapsulates data and explicit

---

[37] Michael E. D. Koenig, T. Kanti Srikantaiah, and American Society for Information Science, *Knowledge Management for the Information Professional*, ASIS monograph series (Medford, NJ: Published for the American Society for Information Science by Information Today, 2000), 11.

[38] Tapscott, 7.

[39] Zand, 9.

[40] Koenig, Srikantaiah, and American Society for Information Science, 32.

knowledge and concerns that which can be represented and transmitted using technology. Knowledge encapsulates tacit knowledge and understanding, and represents that which remains within each individual or is shared via interpersonal communications to another.

Nature of the Future Information Environment

Army transformation planners forecast the potential for conflict globally, in various complex terrains, with conventional and asymmetric threats. Major General James Dubik, commenting on the expectations of the IBCT, noted that

> In reviewing the operational environment, two things remain constant—Korea and Southwest Asia. The Army must be able to fight in these places . . . . But recent operations are examples . . . what is the future Kosovo? What is the future Bosnia? What is the future Somalia? . . .we have to be fast.[41]

As the terrain and adversary will vary, so will the information infrastructure—from the highly networked to the barely connected. The United States and many high-technology countries benefit from extensive fiber optic cable connections, cellular networks, and ubiquitous commercial communications satellite coverage. The synergy of such connectivity allows interesting applications, such as "[rail] cars [that] are bar-coded and can be tracked by using sensors that are in turn connected to fiber-optic cables along the tracks."[42] High technology breeds high expectations, and users might not realize that the infrastructure at home is certainly not global—despite personal examples to which disconnected cell phone users would attest.

Steven Black's brief study of commercial communications infrastructure abroad focused on Asia, Africa, and Europe, and Russia and revealed various degrees of modernization. High capacity undersea fiber-optic cables (offering between 280 Mb/s to over 5 Gb/s carrying capacity) provide most intercontinental connectivity. Commercial communications satellites also allow long range connections but as of 1996,

> . . . satellite trunk transmission capacity worldwide (but excluding the U.S) is about .19 terabits per second . . . However, fiber optic cable currently carries almost twenty times

[41] Dubik, 20.
[42] Tapscott, 84.

> the traffic as satellite systems . . . [and its capacity] is expected to increase roughly six-fold . . .[43]

Internal to each continent and country, Black's analysis showed wide disparities in the telephone density and internet connectivity. For example, Russia, Europe, and selected Asian countries displayed a high level of technology, with satellite telephones filling some gaps. Most Asian countries and almost the entire continent of Africa demonstrated little coverage, with Africa accounting for only one percent of the world's telephones. Advances in technology will undoubtedly continue to provide fiber optic connections and deeper connectivity to developing countries, sometimes at an advantage without a large previous investment in older technologies.[44]

The challenge of extending information from fixed infrastructure to mobile users requires various types of radio systems. Although the signal strength relates to the distance and power of radio emitters, proliferation and proximity of emitters could result in accidental or planned (enemy) interference. For military applications, implementation of new wideband signaling spreads traditional signals over a wider band of frequencies at lower power, which offers improved resistance to jamming and lower probability of intercept or detection. Timothy Garden, in *The Technology Trap,* outlines the strengths and weaknesses of radio relays, airborne relays, and satellites, demonstrating that no single method can ensure information superiority alone without the redundancy provided by the others.[45]

Although space appears to be an infinite, shared resource, certain strategic orbits or points give space the characteristics of traditional key terrain. Single communications satellites in geo-stationary orbit provide coverage for huge "footprints" of airspace and terrain below.

---

[43] Steven K. Black, *A Sobering Look at the Contours of Cyberspace* (Pittsburgh, PA: Ridgway Center for International Security Studies, University of Pittsburgh, 1996), 14.

[44] Ibid., 19. See also Board on Army Science and Technology National Research Council, *Star 21: Strategic Technologies for the Army of the Twenty-First Century* (Washington, DC: National Academy Press, 1992), 54.

[45] Timothy Garden, *The Technology Trap: Science and the Military*, 1st ed. (Washington, DC: Brassey's Defence Publishers, 1989), 96. See also Martin C. Libicki, *What is information warfare?* (Washington, DC: Center for Advanced Concepts and Technology Institute for National Strategic Studies National Defense University: Government Printing Office, 1995), 29. For urban communications, see Sean J.A. Edwards, "Communications in Urban Environments," in *The City's Many Faces: Proceedings of the Rand Arroyo-MCWL-J8 UWH Urban Operations Conference April 13-14, 1999*, ed. Russell W. Glenn (Santa Monica, CA: Rand, 2000), 535.

Networks of satellites in low-earth orbits, such as the global positioning satellite constellation or the Iridium satellite telephone system, allow lower transmission power. Joint doctrine cautions that since satellite resources are so limited, priority must always be given to other means.[46] When available, satellites can provide the most responsive support for mobile requirements. United States Space command recognizes that

> Satellite communications are almost transparent but essential to terrestrial forces. There are many areas of the world, especially oceans and remote locations, where such communications are the lifeline of military operations. They are critical where there is inadequate infrastructure . . . .We are modifying the remaining [military communications] spacecraft and employment doctrine to provide more information to lower command levels . . . [with] a blend of military, civil, commercial, and international systems to meet our future satellite communications needs.[47]

As communication networks evolve more to pure data networks, the meaning of "network" must be redefined for clarity. Road networks allow transportation from place to place without traveling in a straight line across unfavorable terrain. Communications networks provide means to interconnect dispersed members via a series of switching centers with previously unachievable levels of connectivity. Data networks combine computers and robust communications networks into highly interconnected systems composed of hosts, computer processes, and communications protocols.[48] For example, the Internet standard Transmission Control Protocol (TCP) provides virtual connections between hosts, with error checking and allowance for data characteristics including quality of service, urgency, and security. TCP uses the underlying Internet Protocol (IP), which provides an unreliable, connectionless broadcast with

---

[46] Joint Chiefs of Staff, *Joint Doctrine for Employment of Operational/Tactical Command, Control, Communications, and Computer Systems*, Joint Publication 6-02 (Washington D.C.: U.S. Government Printing Office, 1996), 2-8. See also George Friedman and Meredith Friedman, *The Future of War: Power, Technology, and American World Dominance in the 21st Century*, 1st ed. (New York: Crown Publishers, 1996), 349.

[47] Howell M. III Estes, "Space and Joint Space Doctrine," *Joint Force Quarterly*, no. 14 (1996): 62. General Estes served as Commander in Chief of United States Space Command

[48] Department of Defense, *C4ISR Handbook for Integrated Planning* (Arlington, VA: OASD(C3I), C4I Integration Support Activity, 1996), 2-75. See also WIlliam Stallings, *Handbook of Computer Communications Standards, Volume 3: Department of Defense (DOD) Protocol Standards* (Indianapolis, IN: Howard W. Sams & Company, 1987), 5.

allowance for timeliness and precedence of information. Internet protocols have shortcomings for military use based on their design for a permissive environment.[49]

With high connectivity, networked computers interact regardless of physical proximity, and can distribute tasks to be accomplished in parallel on numerous disparate hosts. Expectations are that distributed processing will be

> . . . advanced to the point that a new application process needs to interact only with the operating system or network protocol, one step above interaction at the hardware level. . . . [Technology] will advance by 2020 so that applications will interact at a level of abstraction (meaning) that is far above the hardware level.[50]

Some futurists see the convergence of computing, communications, and content industries into a more information-centric synergy—an Infosphere. Consider the Infosphere as an imaginary space that intersects the physical world in nodes and lines of information technology, human interaction, and stored information (books, electronic media).[51] Cyberspace thus represents the technological dimension of the Infosphere. One author studied technological solutions to couple global positioning data with computer network nodes to "ground cyberspace," mapping virtual locations to geographic locations.[52] Winn Schwartau, in *Information Warfare: Chaos on the Electronic Highway,* describes cyberspace

> . . . as being divided into groups of local or regional cyberspace—hundreds and millions of smaller cyberspaces all over the world. These smaller cyberspaces are capable of functioning independently of one another. . . . Connecting the countless local and personal cyberspaces are the world's communications networks: think of the wires, fibers, and microwave and satellite transmissions . . .[53]

To achieve the high degree of networking required to extend cyberspaces for military applications, the Defense Science Board envisioned a satellite, aircraft, and unmanned aerial

---

[49] Martin C. Libicki and National Defense University. Center for Advanced Concepts and Technology., *Defending cyberspace, and other metaphors* (Washington, DC: National Defense University, 1997), 25.

[50] National Research Council, 118.

[51] Tapscott, 58. See also Libicki and National Defense University. Center for Advanced Concepts and Technology., *Defending cyberspace, and other metaphors*, 5.

[52] Dorothy E. Denning and Peter F. MacDoran, "Grounding Cyberspace in the Physical World," in *Cyberwar: Security, Strategy, and Conflict in the Information Age*, ed. Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden (Fairfax, VA: AFCEA International Press, 1997), 126.

[53] Schwartau, 328.

vehicle (UAV) network that could "adapt to changes in the locations (i.e., the mobility) of its end users; [with] no centralized nodes or base stations that would enforce the use of a vulnerable star topology . . ."[54]

The threshold across which a collection of loosely connected systems emerges into a true network relates to the redundancy and resiliency of the connections. The future information environment will include widely differing levels of technology, including fiber optic cables, spread spectrum radio, and powerful computers. Satellites communications will be marginally available but highly demanded. Robust networks can only exist with stable infrastructure or assured electromagnetic spectrum.

Future operational concepts

Careful design of organizational structure addresses both overall capabilities of the unit (external outputs), and the division of knowledge-work into spheres of influence (internal structure). Tacit and explicit knowledge interact as the sum of group abilities transcends individual limits. Thus, organizational design must encapsulate the interplay of knowledge and information, since

> . . . organizational boundaries—the "seams" in the organization—are important to a military offense because they define what units require explicit coordination from a command point of view. Organizational seams are important . . . in a defensive posture because they represent points where disruption of explicit, inter-unit communications in real time will do more to disrupt overall capabilities that the disruption of intra-unit communications. This is simply because inter-unit coordination more often involves explicit communication and coordination, and intra-unit coordination more often involves tacit forms of coordination in addition to, but often in place of, explicit communication. [55]

Systems thinking provides a way to view complex organizations from a macroscopic vantage point. Similarly, complex communications networks are considered systems, with a goal

---

[54] Defense Science Board, *Report of the Defense Science Board (DSB) Task Force on Tactics and Technology for 21st Century Military Superiority*, Vol. 1 (Washington, DC: Office of the Secretary of Defense, 1996), V-17.

[55] John P. Crecine and Michael D. Salomone, "Organization Theory and C3," in *Science of Command and Control: Coping with Complexity*, ed. Stuart E. Johnson, Alexander H. Levis, and National Defense University, AIP information systems series (Washington, D.C.: AFCEA International Press, 1989), 47.

of an "information processing architecture that will provide the standards and protocols needed to network standard serial . . . computers, signal processors, parallel processors, neural networks, and optical computers into one 'system of systems' . . ."[56] Networked unit characteristics include the accurate detection, identification and tracking of hard to find targets, coordination of attacks from geographically distributed forces, and the ability to rapidly assemble and disperse units. Admiral William Owens popularized the concept of systems thinking for military application at primarily the technical level. [57]

Network-Centric Warfare refined the "system of systems" concept further, envisioning three levels of connectivity: sensor-to-shooter, force direction, and force coordination (C2). Sensor-to-shooter decouples the sensors from weapons platforms via networked communications. Force direction covers the execution of actions, or direct tactical command and control. Force coordination concerns the planning for future operations and supports the visualization of the battlefield.[58] Network-Centric warfare requires the presence of an Infosphere that

> . . . enables the creation of shared battlespace awareness and knowledge. This awareness and knowledge is leveraged by new adaptive command and control approaches . . . The 'bottom line' here is increased tempo of operations, increased responsiveness, lower risks, lower costs, and increased combat effectiveness.[59]

To emphasize the human dimension of technology in warfare, some theorists have proposed terms like Human-Centric Warfare, Dominant Battlespace Knowledge, and Operations-Centric Warfare.[60] The latter concept objects to the focus on technology in Network-Centric Warfare, arguing that it primarily applies at the sensor-to-shooter level by transforming platform specific engagements to network-enabled engagements, without similar impact at the force

---

[56] National Research Council, 44.

[57] Stuart L. Brodskey, "Control Systems Aspects of Command and Control," in *Selected Analytical Concepts In Command And Control*, ed. John Hwang, Military operations research v. 2 (New York: Gordon and Breach, 1982), 41. See also William A. Owens, "The Emerging System of Systems," *Military Review* 75, no. 3 (May–June 1995): 15

[58] Alberts, Gartska, and Stein, 65.

[59] Ibid., 86.

[60] Charles C. Krulak, "Knowledge Based Warfare: A Security Strategy for the Next Century," *Joint Force Quarterly*, no. 14 (1996): 22

direction or coordination level. Rather, Operation-Centric Warfare envisions that network technology will reduce the requirement for detailed planning, to the point that

> . . . during operations, soldiers fight the enemy, not the plan. By going from audio inputs referencing a plan to visual inputs referencing the current situation, soldiers achieve a level of common understanding, mental speed and agility analogous to moving from a slide rule to a calculator.[61]

Specifics aside, the operational concepts all follow a common theme—that the synergy of technology, operational art, and proper organization can enable the vision of a true information age military.[62]

As technology advances, more letters have been added to the command and control digraph (C2) to create the current term C4ISR—Command and Control, Communication, Computers, Intelligence, Surveillance, Reconnaissance. The command and control portion of C4ISR "is the decision-making portion . . . [that] not only performs the battle management function but also manages the combat support and battlefield logistics . . ."[63] Command and control systems include the people, procedures, communications, facilities, and equipment needed to provide force direction and coordination. C2 theorists have developed various models of decision-making.[64] When time is not available, 'satisficing' replaces optimization to find the first acceptable solution. Command and control has a different focus at strategic, operational, and tactical echelons, nesting purpose and actions in overlapping time and space. Division of the battlespace into smaller sets allows a division of labor among echelons.[65] At the tactical level,

> . . . what emerges then is a C2 system with a two-part mission. It continues to help control subordinate elements fighting the front-line battle. But it must also help direct planning and executing the battle against follow-on echelons.[66]

---

[61] Leon J. Laporte and Winn Noyes, "Operation-Centric Warfare: The Bold Shift," *Army Magazine* 50, no. 8 (August 2000): 20

[62] Casper, Halter, and others, 82.

[63] National Research Council, 55.

[64] Alberts, Gartska, and Stein, 74. Models include John Boyd's Observe, Orient, Decide, Act (OODA); Dr Joel Lawson's sense, process, compare, decide, and act; and Dr. Richard Hayes headquarters effectiveness assessment tool , monitor, understand, develop alternative actions, predict, decide, and direct.

[65] Ibid., 69.

[66] Dennis H. Long, "Army Command and Control Requirements for the Eighties," in *Selected analytical concepts in command and control*, ed. John Hwang, Military operations research v. 2 (New York: Gordon and Breach, 1982), 35.

Maneuver entails the "employment of forces on the battlefield through movement in combination with fires or fire potential, to achieve a position of advantage with respect to the enemy in order to accomplish the mission."[67] Command and control provides the linkage between concept and execution since "the commander cannot control the environment himself. His control derives from a real or threatened delivery of ordnance onto a target."[68] Networked forces can redefine the principle of mass to embrace effects vice continual presence, as

> **. . .** the commander and his subordinates can see each other digitally, they no longer need to maintain line-of-sight visual communications . . . [allowing] units to disperse more. . . . Units that base their battlefield movements on the enemy and terrain, rather than on command and control, will give birth to a new kind of maneuver: patternless maneuver . . . .[which] defies anticipation and complicates the enemies understanding.[69]

Future organizations must be agile and capable enough to deploy where needed to achieve decisive results. General Frederick Franks considers rapid deployment essential due to the ". . . need for staying power and ensuring the capacity is perceived by a potential adversary. Staying power means the ability to press the initial advantage gained until the strategic objective is achieved."[70] The transitions occasioned by increased speed, rapid fire, and maneuver of future forces may make it more difficult to provide information to maintain situational awareness.[71] Commanders and their staffs at various command posts during maneuver must recognize the effect movement and enemy action has on information as the friendly information system stretches to support maneuver toward hostile forces. Thus, synchronizing the plans and information developed by the staff with the commander's continual assessment of the battlefield will also be more difficult at the time when it is most needed.

Deployment provides the first transition as widely dispersed units coalesce from various home stations via multiple modes of travel to an operational theater. During Operation Joint

---

[67] Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02 (Washington D.C.: U.S. Government Printing Office, 1999), 272.

[68] Lawson, 61.

[69] Robert R. Leonhard, *The Principles of War for the Information age* (Novato, CA: Presidio, 1998), 113.

[70] Frederick Franks, "Battle Command," *Military Review* 76, no. 3 (May–June 1996): 194

[71] Michael Mehaffy, "Vanguard of the Objective Force," *Military Review* 80, no. 5 (September-October 2000): 10.

Endeavor in Bosnia, 1995, the early air deployment of the Task Force Eagle assault command post to Tuzla air base established immediate satellite connectivity while the bulk of the task force moved overland to cross the Sava river, bringing additional information assets.[72] Coalition nations participating as members of the Implementation Force (IFOR) recognized the high technology role of the United States as

> . . .the only NATO member with such capabilities as large air-craft carriers, long-range strike aircraft, fielded stealth technology, space-based C4I satellites and sensors, advanced aerial surveillance and reconnaissance systems, global lift, strategic logistics assets, and advanced weaponry based on the nascent revolution in military affairs. In Bosnia, 46 of 48 satellites which have been used by IFOR and SFOR [headquarters] for C4I functions belonged to the United States.[73]

Coalition operations may require U.S. forces to reduce their use of C2 technology to the lowest common denominator to ensure interoperability with allied nations.[74]

In addition to allied interoperability, future conflict will include adversaries actively trying to deny friendly force information superiority. Information warfare consists of "actions taken to achieve information superiority by affecting adversary information . . . [and] information systems, … while defending one's own."[75] As early as 1982, C2 theorists thought units could

> . . . improve their own force measure of effectiveness . . . by ensuring the timely, accurate flow of alert, warning, and coordination C2 data for own forces and by applying a counter-C2 campaign against the enemy aimed at reducing his available reaction time and information accuracy through delay, destruction, deception, and saturation of his C2 channels.[76]

As the United States becomes more sophisticated in conducting information operations, adversaries may resort to "…human networks and internal lines of communication using fiber-

---

[72] Operation Joint Endeavor was the 1st Armored Division deployed as an Multinational Division (North) headquarters under a North Atlantic Treaty Organization led headquarters to Bosnia-Herzegovina from late 1995 to 1996. As a long-term peacekeeping mission, it provides examples of multi-national integration, mountainous geography and cold climates, and extensive satellite communications reliance.

[73] John Hillen, "After SFOR: Planning a European Led Force," *Joint Force Quarterly*, no. 15 (1997): 77

[74] Peter Leahy, "ANZUS: A View from the Trenches," *Joint Force Quarterly*, no. 17 (1998): 90

[75] Headquarters Department of the Army, *Information Operations.*, Field Manual 100-6 (Washington, DC: U.S. Government Printing Office, 1996), 2-2.

[76] D.M Schutzer, "C2 Theory and Measures of Effectiveness," in *Selected analytical concepts in command and control*, ed. John Hwang, Military operations research v. 2 (New York: Gordon and Breach, 1982), 144.

optic cable or other fairly secure media . . . to transmit a good deal of information back and forth without using radios."[77] A 1996 study by the Defense Information Systems Agency concluded that commercial infrastructure provided over ninety-five percent of global defense communications requirements.[78]

Future Lines of Information

Information and knowledge converge at the nexus of the Infosphere and battle command. Information networks have emerged with great power for warfighting (table 1).

Element	Industrial Age Paradigms	Information Age Paradigms
Information	Nodal Communications Data with Context Explicit Knowledge Tacit Knowledge	Networked Communications Data with context Explicit knowledge (Shared Faster, networked systems) Tacit Knowledge (Shared Faster, interpersonal communications)
Firepower Maneuver Protection	Platform-Centric Engagements Sensor-shooter same or near observers Maneuver to mass force and fires, gain and maintain contact	Network-Centric Engagements Linked Sensors and shooters Spread information to guide force and fires Maneuver out of contact to strike decisively at time and place of commander's choosing.
Battle Command	Plan-Centric Operations Detailed planning Battle command describes and directs employment	Operations-Centric Warfare Execution in lieu of plan focus Fight the enemy, not the plan Battle command provides vision Information guides force to achieve intent

Table 1 Impact of Information on Elements of Combat Power

Achieving the full potential of information will require full understanding of the benefits and limitations of information systems. New ways of thinking about information can be guided by the concept of the Infosphere. Leveraging information as an element of combat power can be realized by first

[77] Michael Hanlon, *Technological Change and the Future of Warfare* (Washington, DC: Brookings Institution Press, 2000), 115.

[78] Brian E. Fredericks, "Information Operations at the Crossroads," *Joint Force Quarterly*, no. 16 (1997): 98

> . . . replacing physical geography with infography (e.g., lines of communication) [which] may alter the conduct of warfare. Information peaks and ridges may become the centers of gravity for future warfare. Information intersections become as important for targeting as nodes or command bunkers, both from an offensive and defensive point of view.[79]

In this environment, maneuver provides the biggest challenge in time, space, and relation to the enemy for friendly information superiority. Technology and leadership together must be focused on the information gap.

[79] James Hazlett, "Just in Time Warfare," in *Dominant Battlespace Knowledge: the Winning Edge*, ed. Stuart E. Johnson and Martin C. Libicki (Washington, DC: National Defense University Press, 1995), 141.

Chapter 3

Technology and Information

The real value of the modern means of communication eluded [German Chief of Staff Alfred] Schlieffen and his school . . . the telegraph, telephone and radio provided the magic agent which was supposed to make their visionary system of command work. . . . Hence, the communication illusion, which was generated by the devices technology provided, created a deceptive faith in an absolute, centralized but effective mode of command. It encouraged the military leadership to ignore the factor of randomness and the principle of inner-system cognitive tension, and to repress the healthy penchant for tactical initiative. – Shimon Naveh, from *In Pursuit of Military Excellence.*[80]

If Naveh's "communication illusion" implied faith in centralized command and control, an equivalent modern "information illusion" implies the "deceptive faith" that the Infosphere is ubiquitous--even during transitions (movement, maneuver), with a thinking adversary intent on imposing his own will. Future concepts do not negate the fundamental nature of war with revolutionary technology--"friction together with fog, ambiguity, chance, and uncertainty will dominate future battlefields as it has in the past . . . although technology is important, it is only a tool."[81] In these environments, can technology provide timeliness, accuracy, and relevance of information for Army forces conducting maneuver in the land dimension?

Information Technology and Maneuver

Military information systems require greater redundancy, security, and flexibility than commercial equivalents.[82] Echoing conclusions first espoused by Martin Van Creveld, Manual De Landa, in *War in the Age of Intelligent Machines*, noted, "unless a tactical [information] system manages to disperse the fog of war, it eventually self-destructs."[83] Maneuver stresses systems by simultaneously uncovering new information while the force moves away from established infrastructure. Information systems must support maneuver by providing

---

[80] Shimon Naveh, *In Pursuit Of Military Excellence: the Evolution Of Operational Theory*, The Cummings Center series . 7. (London ; Portland, OR: Frank Cass, 1997), 59.

[81] Williamson Murray, "Thinking About Revolutions in Military Affairs," *Joint Force Quarterly*, no. 16 (1997): 76.

[82] Michael Ryan and Michael Frater, *A Tactical Communications System for Future Land Warfare*, Working Paper 109 ed. (Australia: Land Warfare Studies Centre, 2000), 4.

[83] Manuel De Landa, *War in the age of intelligent machines*, Swerve ed. (New York: Zone Books, 1991; Reprint Cambridge, Mass: MIT Press, 1994), 82.

"information to whoever (or whatever needs it, quickly and with reasonable security."[84] In this environment, commercial systems may only have value when they can be protected from adversary disruption.[85] Military networks must rely on

> . . . radio and optical links to connect elements . . . in the face of unknown terrain, adverse weather, and enemy jamming. The network would take advantage of satellites and high-altitude, long endurance UAVs to ensure wide area communications connectivity.[86]

Despite advanced satellites and aerial relays, there remains a ground terrestrial communication requirement where line-of-sight radios require periodic hilltop retransmission sites to provide a robust communications network to support maneuver.[87] Increasing proximity to enemy forces could result in electronic jamming, and "in network-centric warfare, the stakes are so high that this vulnerability should not be downplayed."[88] The complex frequency spectrum environment used by radio systems and collected by intelligence systems presents additional synchronization challenges to prevent interference and protect sources.[89] For mobile users, the most critical commodity for information technology is energy. Batteries provide chemical energy to mobile users, and fuel runs power generators that support mobile command posts. One estimate of conducted by the Defense Science Board determined that it would require 3,400 batteries for a 3,000 Man brigade to operate for thirty days.[90]

Current fielded systems for the majority of the force include the limited data transfer on Single Channel Ground and Airborne Radios (SINCGARS). Future digital radios may provide better service. Combining different technologies in innovative ways could solve the "basic problem of a battlefield network . . .that while some nodes support very large data pipes, a number of nodes will be operating at SINCGARS data rates. . . .[leading to a] notion of one-way

---

[84] National Research Council, 52.
[85] Ibid., 53.
[86] Ibid.
[87] Pat Cooper, "Bosnia Study Highlights U.S. Communications Inadequacies," *Defense News*, (January 13, 1997): 14, as quoted in Hanlon, 53.
[88] Ibid., 58.
[89] David T. Signori and Harold A. Cheilek, "An Overview of Joint Tactical Command and Control," in *Selected analytical concepts in command and control*, ed. John Hwang, Military operations research v. 2 (New York: Gordon and Breach, 1982), 163.
[90] Defense Science Board, V-38.

data broadcasting via [Global Broadcast Satellite] of very large data files … and very low bandwidth querying back to the data sources."[91] For applications in urban terrain, the Defense Advanced Research Projects Agency (DARPA) has even investigated a "drop off [disposable] relay compatible with SINCGARS and the future software radio."[92]

Charles Dunlap, in an article outlining critical vulnerabilities to the future joint force, points out the potential adversaries perspective in a cautionary manner, where an adversary can use information as well as the United States:

> . . . commercial satellites will provide high-resolution images that were previously the exclusive domain of intelligence services in developed nations. The Internet is a simple, cheap, risk-free way of collecting intelligence data. Another innovation, individual telephones linked by satellite for soldiers on the battlefield, will be extremely vulnerable to monitoring by un-friendly forces. Perhaps the greatest source of red team information will be the media. Equipped with the latest technology and free from reliance on or control by any government, the media will be able to report on every aspect of U.S. military operations nearly instantaneously.[93]

The backbone of the dispersed force's Infosphere will remain the constellation of communications satellites. Previous conflicts have demonstrated that the Department of Defense can have marginal impact on the total satellite capacity fielded for the early stages of a crisis due to the long and expensive launch process and the difficulty in performing even the slightest orbital maneuver to better support a geographic area. Future commanders may benefit from the work underway to field "tactical satellites that can be launched on demand for battle-field specific tasks. . . communications, battle management, intelligence, force projection."[94]

Tactical satellite ground terminal systems deployed into Croatia during the Sava river bridge crossing supported command and control and preparation for the movement of 1st BCT into Bosnia. Due to force protection prohibitions on initial occupation of remote sites before

---

[91] Harlan Ullman and National Defense University. Center for Advanced Concepts and Technology., *Shock and Awe: Achieving Rapid Dominance* (Washington, DC: Center for Advanced Concepts and Technology, 1996), 128.

[92] Edwards, 534.

[93] Charles J. Jr. Dunlap, "Joint Vision 2010: A Red Team Assessment," *Joint Force Quarterly*, no. 17 (1998): 49

[94] National Research Council, 45.

mine clearing, satellite communications terminals provided the initial linkages between subordinate brigade combat teams and Task Force Eagle command posts.[95]

Global Broadcast Satellite systems provide the greatest bandwidth under the footprint of a steerable spot beam (up to 24Mb) similar to the commercial equivalent digital satellite television. Spot beam focus could be contentious given competing requirements in a theater of operations.[96] Technology also provides some protection for satellite communications, if ground users remain at specific locations, since

> Communications to and from know locations (e.g., satellites, UAVs) can use digital technologies to focus on frontal signals and discard jamming that comes in from the sides. Digital compression techniques coupled with signal redundancy mean that bit streams can be recovered intact, even if large parts are destroyed.[97]

Space architects realize the crucial role satellites play in future warfare. Expectations call for information enabled organizations than can decentralize decision-making, increase tempo, and forego planning based on dominant knowledge of the enemy. However, technical experts remain cautious until the operational concepts are tested, and then believe that if "these concepts are viable, measures will be needed to protect information systems, control the use of space, and deny an enemy access to vital information."[98] If jamming or satellite disruption impedes the flow of information to units in motion, other networks could overcome the shortfall via aerial retransmission of terrestrial systems. Revolutionary technology may supplement the network, since key intelligence information may be

> . . . obtained by satellites and high-flying aircraft using sensors that report to upper echelons, which are often located at the rear of deployed forces. After some delays and processing, selected data will flow to forward-located small units. Besides this support, the small, forward unit will need, as it always has, highly detailed and timely information about terrain and the disposition of opposing forces. . .[99]

---

[95] Gregory J. Premo, "22nd Signal Brigade Support to Operation Joint Endeavor" (Briefing, 24th Signal Regimental Symposium, 1996).

[96] Stuart A. Carter, "Pull, Push or Shove: Global Broadcast Service and Intelligence Support to Maritime Forces" (Monograph, School of Advanced Military Studies, Command and General Staff College, 1998), 16.

[97] Libicki, *What is information warfare?*, 29.

[98] Thomas G. Behling and Kenneth McGruther, "Satellite Reconnaisance of the Future," *Joint Force Quarterly*, no. 18 (1998): 24

[99] National Research Council, 49.

In addition to computers embedded in the sensor-shooter grid, command posts and mobile users can expect computers to assist with "intelligence extraction, synoptic organization of intelligence, and interpretation of command decision into detailed directives to the field."[100] Challenges to achieving the distributed network needed for Network-Centric Warfare include

> . . . more difficult obstacles than occur in most civilian environments: (1) continually varying prioritization of processes; (2) robustness when large parts of the distributed system disappear without warning; (3) a vast range of data types, inference types, and hardware; (4) accommodation of several levels of security and access.[101]

Command and control procedures can also be challenged by communications outages. Information supporting situational understanding requires "organizing databases so that the desired elements can be retrieved rapidly and reliably by distributed decision makers in the presence of a changing communication environment."[102] The ability to short circuit traditional information hierarchies by direct broadcast **"**dissemination of intelligence, targeting, and other data at all levels. . . . [to] units, key nodes, and leaders [who] will be more widely dispersed, leading to the continuation of the empty battlefield."[103]

Technology users must consider that military technology is to civilian technology (personal communications and computers) as a military weapon is to a personally owned weapon. As computer networks allow direct interference between users competing for finite resources, information assurance and digital discipline will be required to preserve the lethality of the overall system-of-systems.

> . . . infantrymen [and] tankers . . .have to qualify with … their 'weapons system' prior to use. However, computer-system administrators and operators don't qualify on their systems. . . . Misuse or abuse of these systems could seriously degrade or disrupt national assets, yet access to these systems is granted to individuals who haven't met any published DoD or service-wide standards or certification.[104]

---

[100] Ibid., 57.

[101] Ibid., 119.

[102] Brodskey, 45.

[103] Headquarters Training and Doctrine Command, *Force XXI Operations: A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Early Twenty-First Century*, TRADOC PAM 525-5 (Washington, DC: United States Army Training and Doctrine Command, 1994), 2-8.

[104] Harry Rauduege, "Defensive Information Operations: A J-6 Perspective," *Army Communicator* 23, no. 4 (Fall 1998): 56

Vice Admiral Arthur Cebrowski, at the 1999 Command and Control Research and Technology Symposium, noted that "beyond the structure of the network, operation of the network by knowledgeable professionals provides the other ingredient of robustness."[105] Well-designed systems may provide information to protect forces by maintaining cohesion, avoiding mistakes, and ensuring freedom of action. However, systems must increase the effectiveness of the force to achieve victory vice simply avoiding defeat.[106] Self-induced information friction can be just as disruptive as enemy induced information operations. For example, military users spread computer viruses in Bosnia until "half of the client computers used by the U.S Army in Bosnia were infected."[107] Non-doctrinal command and control headquarters deployed to Bosnia also relied heavily on national intelligence systems. One study recommended fewer and more focused intelligence information links to Warfighters and a better integration of user knowledge of capabilities to frame requests.[108]

Future networks can also capitalize on the abilities of individual soldiers to serve as sensors, if equipped with requisite communications.[109] Unlike civilian networks, military environments require both a mobile user and a transportable network infrastructure. Maneuvering the network implies movement of the backbone of the Infosphere, coupled with fires or the threat of fires (protection), to gain a position of advantage to provide information support relative to the enemy.[110]

---

[105] J.R. Wilson, "Network-Centric Warfare Marks the Frontier of the 21st Century Battlefield," *Military & Aerospace Electronics* 11, no. 1 (Jan 2000): 17

[106] Welch, 4.

[107] Libicki and National Defense University. Center for Advanced Concepts and Technology., *Defending cyberspace, and other metaphors*, 21. The author, serving with Task Force Eagle from December 1995 until November, 1996, personally observed the Word Concept Macro virus, which was often found embedded in many Microsoft Word documents commonly used to pass operations orders and plans, and the more disruptive "Cruel" boot sector virus that invariably led to loss of data on the infected machine.

[108] William P. Clappin, "Moving Signals Intelligence From National Systems to Army Warfighters at Corps and Division" (Thesis, Ft. Leavenworth, KS: U.S. Army Command and General Staff College, 1998), 59.

[109] Brian Nichiporuk, Carl H. Builder, and United States. Army, *Information Technologies and the Future of Land Warfare* (Santa Monica, CA: Rand Arroyo Center, 1995), 65.

[110] Ryan and Frater, 18.

Edward Waltz, in *Information Warfare Principles and Operations,* describes the concept for future systems to incorporate four kinds of information: access (status data), messaging (conversation), interpersonal (collaboration), and broadcast (warnings, situation updates). Based on the category of information, the network should automatically adjust user bandwidth "on the basis of mission priorities, timeliness, security, and connectivity"[111] The envisioned Army tactical internet will "probably be the most complex computerized network in the world. . . . [using] more routers than any telephone company in America manages."[112]

Michael Hanlon, in *Technological Change and the Future of Warfare,* describes the increasing optimism ascribed to three concepts for future war: the system of systems, dominant battlespace Knowledge, and Global Reach-Global Power. Hanlon criticizes the pessimism of a "vulnerability school of thought [that] frequently invokes the term asymmetric warfare . . ."[113] Systems-of-systems are not as vulnerable as critics would hold, as "redundancy works against the possibility of breaking the whole system . . .the overall system would not collapse but rather degrade slowly. . . . [suggesting] an opponent would be defeated before he could defend against, or counter, or defeat the capabilities we could bring against him."[114] However, complex environments including urban, forest, and mountainous terrain imply challenges to such systems.[115]

Naval forces operating away from the littorals exemplify the difference between integrating the "relatively small number of 'mega platforms' of the U.S Navy and the smaller but more numerous Army and Air Force platforms."[116] Ground operations present different

---

[111] Edward Waltz, *Information Warfare Principles and Operations* (Norwood, MA: Artech House, Inc., 1998), 129. Waltz refers to the Advanced Battlefield Information System (ABIS).

[112] Mark D. Caivo, "Digitizing the Force XXI Battlefield," *Military Review* 76, no. 3 (May–June 1996): 69. For a detailed description of Army tactical internet, see Rick Makowski, "EPLRS-More than Just data," *Army Communicator* 15, no. 1 (Winter/Spring 1990)

[113] Hanlon, 15-16.

[114] Admiral William A. Owens, "Introduction," in *Dominant Battlespace Knowledge: the Winning Edge,* ed. Stuart E. Johnson and Martin C. Libicki (Washington, DC: National Defense University Press, 1995), 12.

[115] Hanlon, 197.

[116] John Rhea, "'Infocentric' Warfare Networks Being Built on COTS Base," *Military & Aerospace Electronics* 10, no. 1 (Jan 1999): 20

challenges, and since "no military information system can see everything to required detail at once, it has to rely on cuing, filtering, and pinpointing."[117] The power of the concept revolves around the demand that

> . . . network bandwidth requirements will be great in order to handle all of the digital transmissions. In addition to sensors, network transmissions will be required down to the level of the individual land warrior, e.g., for position location, status reporting. The utility of the future systems will be greatly diminished if there are persistent information backlogs and disconnects because of inadequate bandwidth.[118]

Alternatively, careful preparation can reduce information transfer requirements by building context before operations. Thus, knowledge can spring from smaller messages based on previously built context, reducing the need for bandwidth.[119] An analogy exists with the computer's use of a cache of information taken from disk to prevent the faster processor from being forced to wait on slower disk drive access before completing a task. Although not all relevant information can be predetermined, significant strain could be lifted from communications channels with

> . . . physical prepositioning of information at operational and tactical command posts . . .[since] even a non-dramatic delivery method such as U.S Postal Overnight Express would yield an equivalent data channel of 18Mbps (based on a 10 Gb hard drive). . .[120]

Other critics of Network-Centric Warfare believe the "popular notion of information dominance . . .simply goes too far, as does the concept of dominant battlespace knowledge."[121] Robert Metcalfe, founder of 3Com Corporation, remarked that the power of networked computers equaled the square of the number of users. Alberts, Gartska, and Stein warn that for Network-Centric Warfare,

> Metcalf's law is really about potential gains; there is no guarantee that simply hooking things ups will make the results better. In fact, there is every possibility that the

---

[117] Stuart E. Johnson, Martin C. Libicki, and National Defense University Press., *Dominant Battlespace Knowledge: the Winning Edge* (Washington, DC: National Defense University Press, 1995), 35.

[118] Scott E. Graham, Patrick K Valentine, and Lee E. Washington, *Enhancing Performance in Light Infantry Digital Tactical Operations Centers* (U.S. Army Research Institute for the Behavioral and Social Studies, 1997), 9, Report 1709.

[119] Hazlett, 140.

[120] Bernal B. Allen, "The Non-linear Nature of Information and Its Implications for Advanced Technology Forces" (Thesis, Naval War College, 1998), 18.

[121] Hanlon, 67.

> unintended consequences of wiring up the battlespace and hoping for the best will, in fact, degrade performance particularly if doctrine, organization, training, and other key elements of the process are not changed to take advantage of the new configuration.[122]

Robert Leonhard notes one such conflict in the debate over the difference between mission tactics and detailed control. For a subordinate organization to truly employ mission tactics, where they can react to opportunities that may not have been foreseen, the organization must have access to sufficient resources—maneuver units, fire support, logistics, etc—to take advantage of situations without seeking approval from higher echelons. Under Network-Centric Warfare, competition for resources (especially fires) can become more intense as the distance from sensor to shooter increases.[123]

C2 System Level Analysis

Infosphere aside, command functions have remained a focus of much of the technological development of future networks, a phenomenon not unique to any one country. For example, Soviet theory for command and control demonstrated that "combat practice has convincingly confirmed one of the basic control principles: where the fate of the battle is decided—that is where the commander is."[124] Humans add a depth and complexity to the command and control function that technology cannot. Battlespace awareness entails synergy between a detailed view and gross overviews without detail—at different levels of abstraction.[125]

Information nodes can spring from anywhere. In Albania during the Kosovo crisis, a single satellite telephone in a tent provided an initial refugee information point. Additional civilian and military infrastructure provided more support and extended the reach around Tirane

---

[122] Alberts, Gartska, and Stein, 100.

[123] Robert R. Leonhard, *Fighting by MInutes : Time and the Art of War* (Westport, Conn.: Praeger, 1994), 110.

[124] D. A. Ivanov and others, *Fundamentals of Tactical Command And Control : a Soviet view*, Soviet military thought ; no. 18. (Washington, DC: U.S. Air Force, 1977), 100.

[125] Robert E. Conley, "Military Command and Control (C2)," in *Selected Analytical Concepts In Command And Control*, ed. John Hwang, Military operations research v. 2 (New York: Gordon and Breach, 1982), 17. See also Alberts, Gartska, and Stein, 116.

airfield, Albania, in support of JTF Shining Presence, the refugee and humanitarian relief mission.[126] Information resources converged as rapidly as possible to meet the requirements.

Commander influence in allocation of priorities will remain critical because the "commander's force surveillance *system* will consist of borrowed parts that must be *focused* on the tactical problem . . ."[127] A sensor grid, coupled with a communications grid and shooter grid composed of kinetic warfare elements, can only be effective when elements of all three can be linked at the desired point. Shooters and communications without sensors have no targets. Sensors and communications without shooters are impotent. This linkage will be the most important during maneuver, when the challenges to communications are the greatest, because

> . . . if we have surveillance and weapons, but we cannot connect the two, the solution is still zero. This is what we experience in today's non-virtual, circuit specific communications when a targeting network fails.[128]

Besides direct immersion in the information volume, commanders also rely on the organization of functional staff expertise, communications, and equipment into command posts (CPs) or Tactical Operation Centers at lower echelons (TOCs). Command posts provide different degrees of mobility, information-handling capacity, and may include specific functional expertise not generally available (military lawyers, public affairs, or space support liaison).

> Today's command centers are identified by copious, visible communications and computational gear(and the associated electromagnetic emissions), the physical movement of paper and other official supplies, plus enough comings and goings of all sorts to differentiate these centers from other venues of military business.[129]

Command post positioning in the defense can be optimized and balanced between friendly advantage and enemy threat. The positional balance of the command post between a front line and other command echelons depends on the "need to maintain uninterrupted

---

[126] Michael Ignatieff, *Virtual War: Kosovo and Beyond* (New York: Henry Holt, 2000), 43. Details of the military communications support provided in Albania supporting Task Force Hawk in 1999 taken from William Lasher, "HQ EUCOM: A Look Ahead" (Briefing, Fort Gordon, GA: 27th Signal Regimental Symposium, 1999).

[127] Michael Loescher, "The Information Warfare Campaign," in *Cyberwar: Security, Strategy, and Conflict in the Information Age*, ed. Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden (Fairfax, VA: AFCEA International Press, 1997), 199.

[128] Ibid., 202.

[129] Libicki, *What is information warfare?*, 11.

communications with the subordinate staffs, the adjacent units, and the higher staff, and, in the subunits and units, to keep the battlefield under observation as well."[130] Achieving an equivalent effect in an offense requires an echeloned displacement of command posts, sometimes at the very moment when their ability to collect, synthesize, and rebroadcast information is most needed.

Some critics of information technology fear detailed control of all forces by a centralized commander will suppress initiative at lower levels.[131] If information flows both ways, not only will higher commanders gain an appreciation of the lower commander's situation, the lower commander could better understand the higher commander's "big picture," thus fueling initiative based on the higher's intent.[132] Inherently, any solution has value if it provides "timeliness relevant to [the] enemy decision cycle."[133] Common discussion of the role of "the commander" in battle neglects interactions of a great number of commanders in any organization. Each commander organizes command posts, thus

> . . . a real battlefield contains lots of little command and control (C2) nodes, each of which perceives the conflict around him differently, each of which has different priorities. . . . the outcome of the battle is not solely a function of weapon ranges and rates of fire, but rather of countless battlefield decisions and actions.[134]

The reachback demonstrated in Bosnia operations revealed that satellite use competed with other operational requirements for military and commercial satellites. Reachback requires three elements—equipment at the forward area, a communications channel to the rear location, and equipment and processing at the rear area able to add value and make the concepts worthwhile. If rapid deployment or maneuvers strain the abilities of any of the three elements, the system will not provide the needed information. [135]

---

[130] Ivanov and others, 101.
[131] Leonhard, *Fighting by minutes : Time and the Art of War,* 113.
[132] Defense Science Board, V-13.
[133] Welch, 10.
[134] Leonhard, *Fighting by Minutes: Time and the Art of War,* 127.
[135] Benjamin F Fletcher, "22nd Signal Brigade Support to Operation Allied Force" (Briefing, 27th Signal Regimental Symposium, 1999). See also the author's analysis of satellite support in Bosnia and Kosovo, Kenneth E. Viall, "Medium Brigade 2003: Can Space-based Communications Ensure Information Dominance?" (Thesis, Ft. Leavenworth, KS: U.S. Army Command and General Staff College, 2000), 95.

Technology and Information Criteria

Timeliness and Technology

Technology has the greatest effect on the two component parts of timeliness—time of transmission, and time of processing at a node before retransmission or presentation to a decision-maker. Speed of transmission ranges between the speed of light and the speed of a courier. Early commanders had no options to exert long distance control allowing autonomous forces independence of action proportional to their distance from their higher command.[136]

Future commanders must contend with an ". . . increased volume of information that is relevant to commander's coherent view of the operational environment."[137] Timeliness to a commander relates to the balance between the time taken to decide and the time taken to initiate actions to achieve the desired outcome.[138] Latency of information supporting operations also depends on "the time spent by the commander and staff of a given element on one control cycle, that is, on acquiring and studying the situation data, making a sound decision on this basis, and assigning the missions to those who carry them out."[139] For example, commanders expecting imagery to support operations in Bosnia encountered delays and image degradations caused by retransmissions.[140]

The army's current suite of tactical computers, the Army Battle Command System (ABCS), evolved from the Army Tactical Command and Control System (ATCCS). ATCCS design was compartmented into five battlefield functional areas (BFAs): maneuver, fire support, air defense, intelligence, and combat service support. By 1986 functional proponents had neglected

---

[136] C. Kenneth Allard, *Command, Control, And The Common Defense* (New Haven: Yale University Press, 1990), 42.

[137] Macgregor, 50.

[138] Paul E. Girard, "A Function-Based Definition of (C3) Measures of Effectiveness," in *Science of Command and Control: Coping with Complexity*, ed. Stuart E. Johnson, Alexander H. Levis, and National Defense University, AIP information systems series (Washington, D.C.: AFCEA International Press, 1989), 119. See Also Schutzer,,, 140.

[139] Ivanov and others, 46.

[140] James Adams, *The Next World War: Computers are the Weapons and the Front Line is Everywhere* (New York: Simon & Schuster, 1998), 88.

> . . . to develop a C2 system which could communicate with the other[s]…horizontally and vertically. . . . [each] had begun to develop its own system, with its own program office, its own defense contractors, and its own protocols. In effect, the BFAs were only connected by a star on the briefing slides.[141]

System development focused on BFA specific information processing, with less regard for interconnectivity.[142] Battle command experiments continue to show complex networks and large data file transfers. New systems provided some increases in situational awareness, but "the lack of seamless connectivity diminished the potential of the data available to the [unit], primarily with regard to timeliness."[143] These shortcomings have become the focus of attention in ABCS development, with standardized protocols and message formats ensuring basic connectivity.

Major Peter Barnes modeled the information exchange requirements between elements of a composite task force with digitally enabled tanks, field artillery systems, and Longbow Apache helicopters equipped with the Single Channel Ground and Airborne Radios (SINCGARS) and Improved High Frequency Radio Systems (IHFR). His analysis noted that the architecture focused information flow through subordinate system commanders (Longbow, Abrams) and he applied information and queuing theory to mathematically examine information flow in the battalion. Barnes concluded that even when human and environmental factors were excluded, the "typical tactical network became overloaded during critical events."[144]

Infosphere, with all its related complexity, takes time to establish in new areas without infrastructure. However, the predicate to network-centric warfare is the ability to connect any

---

[141] Elizabeth A. Stanley and Army War College. Strategic Studies Institute., *Evolutionary Technology in the Current Revolution in Military Affairs: the Army Tactical Command and Control System* (Carlisle Barracks, PA: Strategic Studies Institute U.S. Army War College, 1998), 28.

[142] Ibid., 31. See also U.S Government Accounting Office, *Tactical Intelligence: Battlefield Automation: Premature Acquisition of the Army's Combat Service Support Control System* (Washington, DC: U.S Government Accounting Office, 1994), Report No. NSIAD-94-51. Despite problems, ASAS and CSSCS "were advanced after failing to minimum requirements for connectivity with other ATCCS systems."

[143] Louis G. Bornham, Michael C. Ingram, and Peter J. Martin, *Information Technology in the Digitized Division* (Fort Leavenworth, KS: TRADOC Analysis Center, 1995), 18, FY 95 Mobile Strike Force Battle Command Experiment.

[144] Peter R.. Barnes, "Command, Control, Communications and Automation needs for the Combined Arms Team" (Thesis, Ft. Leavenworth, KS: U.S. Army Command and General Staff College, 1994), 65-70.

two points in battlespace seamlessly.[145] Nicolas Negroponte, in *Being Digital,* coined the phrase "the Negroponte switch"—which addresses the challenge of supporting mobile information services:

> . . . bandwidth on the ground is infinite and in the ether it is not. We have one ether and an unlimited number of fibers. While we can be cleverer and cleverer with how we use the ether, in the end we ought to save all the spectrum we have for communication with things that move, which cannot be tethered, like a plane, boat, car, briefcase, or wristwatch.[146]

Sensor to shooter links can achieve timeliness dependent on the expected degree of connectivity. For targeting, mathematical models can show that the

> . . . optimal [solution], from a decision point of view, is a centralized strategy. In this case all of the data are communicated to a central location where they are used to decide between the alternate hypotheses (target presence or absence) according to some suitably chosen decision rule. However, this approach requires extensive communications, Therefore, it is desirable to seek decentralized strategies which may be suboptimal from a decision point of view but more satisfactory in terms of communications levels.[147]

In addition, centralized control of networks could result in critical failure with disruption of the central node.[148] Distributed, redundant design could refocus timeliness on a more local basis. Stressing the network during movement had been difficult to test in the training environment. During the 4th Infantry Division March 1997 Advanced Warfighting Experiment (at brigade level), "the battlefield was relatively static, without cross-attacking units or relocating ('jumping') command posts."[149]

Based on the numbers of computers used to process information in modern command posts, these CPs have grown in size, implying a reduction in their agility.[150] The relatively static positioning of command posts to support operations in Bosnia allowed increased provision of information services, including video teleconferencing to brigade combat team level. The

---

[145] Ryan and Frater, 10.
[146] Negroponte, 24.
[147] Brodskey, 52.
[148] Ibid., 54.
[149] Stanley and Army War College. Strategic Studies Institute., 43.
[150] Richard E. Jr. Volz, "An Objective Information Architecture for the Army of the Twenty-First Century: Courting Athena" (Thesis, Ft. Leavenworth, KS: U.S. Army Command and General Staff College, 1996), 3.

displacement of the Task Force Eagle rear command post and associated logistics infrastructure from Lukavac, Bosnia to Slavonski Brod, Croatia in 1996 required complex synchronization of all available communications systems.[151]

When command posts and units displace during battle, a "communications network should be able to cope with a considerable degree of movement by combat elements without needing to redeploy. . . .when required to move, the components of the communications system must have the ability to change location as rapidly as the elements that they serve."[152] The stark contrast between civilian expectations and military systems exists because

> . . . current information technologies are based on fixed land based infrastructures that provide large communication pipes (bandwidth). This infrastructure does not exist on the modern battlefield. Radio systems are the least favored of all communication means by industry because of inherent errors, bandwidth constraints, and decreased reliability. Army operations, on the other hand, demand a high degree of mobility. . . [which] can only be obtained through the use of radio systems.[153]

Overall, technology provides great potential for timeliness of information. Challenges arise as information flow increases, especially during maneuver, while capability decreases. Procedures must counter the "myth that once collected and stored it is better to ask the system vice recollect the information again"[154] At this point, systems must allow highly accurate, relevant information to become the priority.

Accuracy and Technology

In some respects military systems deliberately provide less accuracy than technology can deliver. For example, four military voice telephone trunks (16kbs each) are favored over one high-grade commercial telephone trunk (64kbs). Military personnel can "accept intelligible voice whereas most commercial telephone systems provide a high quality . . . level of speech reproduction."[155] Human interaction can provide accurate transmission of information.

---

[151] Premo.
[152] Ryan and Frater, 5.
[153] Volz, 16.
[154] Welch, 8.
[155] Ryan and Frater.

As information flow relies increasingly on data networks, commanders need a measure of the accuracy of information. Information fusion relies on "data from sources with various degrees of reliability. . . . both technical and human information sources are fallible and subject to bias."[156] Technology alone is no panacea, and the problem lies in a "subtle trap for the commander: the danger of masking the incompleteness and uncertainty of that information."[157]

The commonly used Global Positioning System (GPS) constellation relies on a number of satellites broadcasting signals, such that the ground receiver can correlate four signals to derive accurate time and location. As the satellite constellation orbits continuously, military GPS receivers indicate a "figure of merit", or estimation of the accuracy of the position based on the geometry of satellites in view. GPS prediction software can also uncover discrete periods at any location where accuracy is poor, as satellites cross the horizon before another rises into view.

Technology also assists accuracy in the correlation of multiple sensors, particularly radars tracking aircraft when multiple data sources may or may not refer to the same item. The location of a computer icon on a display presents its own degree of inaccuracy. For example, during the Interim Brigade Combat Team command post exercise in 2000, staff users noted that the relative positions of two friendly (blue) and enemy (red) icons changed at two different levels of map resolution. Players could not determine if the two units were in contact or bypassing each other.[158]

Another element of accuracy relates to the time value of information. Even the most precise position location of a friendly or enemy element loses values with the passage of time. Early digitization efforts experimented with systems where ". . . the red shape representing enemy

---

[156] Roy M. Gulick and Anne W. Martin, "Managing Uncertainty in Intelligence Data--An Intelligence Imperative," in *Science of Command and Control: Coping with Uncertainty*, ed. Stuart E. Johnson and Alexander H. Levis, AIP information systems series ; v. 1. (Washington, D.C.: AFCEA International Press, 1988), 11.

[157] Stuart E. Johnson, Alexander H. Levis, and National Defense University, *Science of Command and Control: Coping with Uncertainty*, AIP information systems series ; v. 1. (Washington, D.C.: AFCEA International Press, 1988), vii.

[158] Personal observation at Interim Brigade Combat Team, Command Post Exercise, Fort Leavenworth, Kansas, October 2000.

vehicles can be made to change color as the information on which it was based gets older."[159] Computer processing could also model likely ranges of motion and indicate an increasing circle of possible locations based on unit characteristics until new data points can be integrated to relocate the unit. Accuracy presents the greatest challenge to computer processing, where it becomes difficult to design systems to ensure ". . . that decision makers get exactly the information they need at just the right time, neither earlier nor later, and at just the right place."[160]

Technology provides accuracy but must indicate the degree of reliability of the presented information to gain the trust of users. Commanders must deal with the dilemma that "the uncertainty of a C2 System generally reaches an acceptable level after the required action time has past."[161] Increased understanding and trust in the systems may increase the level of uncertainty acceptable to a commander.

Relevance and Technology

Network-Centric Warfare proposes that broadcast information can "provide relevant information to each level of command simultaneously, eliminating the need for field commanders to divert their attention from the immediate concerns of battle to brief their superiors."[162] Presumably, relevant information will be easily separated from the irrelevant. Technology has not demonstrated solutions to transform incomplete intelligence data into relevant information.[163]

Thomas P. Coakley, in *Command and Control for War and Peace*, raises the issue that starting from a given set of unknown information, as the situation develops, additional relevant questions are discovered concerning "information that the commander doesn't even know is

---

[159] Adams, 113. TRW appliqué computers were applied as an initial digitization experiment at Fort Hood, Texas.

[160] Charles B. Wang, *Techno Vision: The Executive's Survival Guide o Understanding and Managing Information Technology* (New York: McGraw-Hill, 1994), 140.

[161] Harry L. Van Trees, "C3 Systems Research: A Decade of Progress," in *Science of Command and Control: Coping with Complexity*, ed. Stuart E. Johnson, Alexander H. Levis, and National Defense University, AIP information systems series (Washington, D.C.: AFCEA International Press, 1989), 38.

[162] Wilson, 15.

[163] Gulick and Martin, 11.

needed."[164] A priori decisions on where to allocate information resources, focus sensors, and place command posts provide the framework for discovery of shortfalls. Commander's critical information requirements (CCIR) must drive C4ISR planning to provide the start point that should provide adequate coverage for discovery of relevant information. Jasper Welch noted the relationship to game theory, where

> . . . no matter how bad things are, there is always a best thing to do. It may be poor, but it is the best thing to do under the circumstances. There is a corollary to that in communications: No matter how narrow the bandwidth, there is always a best message to send.[165]

Technology can only provide limited help in selecting the most relevant message. In the complex environment of multiple command nodes, relevance also becomes a local phenomenon. Information critical to one echelon could be considered irrelevant at another. Smart information filters embedded in computers could "adapt to the existing bandwidth (reduced by jamming) and be capable of selecting and excluding nice-to-know information as the system capability degrades."[166] These filters also presume a method of categorization of information.

Artificial intelligence and expert systems research had not been deemed ideal for threat environments, because military situations

> . . . cannot be sharply envisaged far in advance . . . success stories of AI expert systems have tended to be for relatively well-structured problems, such as medical diagnosis, oil exploration, and engineering design. . . intelligence knowledge refers to a moving target . . and is institutional and dispersed . . .[suggesting] categorizing knowledge into three levels of generality: [doctrine], intelligence preparation of a [theater], and judgments developed in the course of a particular engagement.[167]

Critics of Network-Centric Warfare concur that filters and expert systems will have value, but will be "limited to elementary clerical sorting and some pattern recognition for photo

---

[164] Thomas P. Coakley, *Command and control for war and peace* (Washington, D.C.: National Defense University Press : U.S. G.P.O., 1992), 139.

[165] Welch, 8.

[166] Ibid., 9.

[167] Rex V. Brown, "Normative Models for Capturing Tactical Intelligence Knowledge," in *Science of Command and Control: Coping with Complexity*, ed. Stuart E. Johnson, Alexander H. Levis, and National Defense University, AIP information systems series (Washington, D.C.: AFCEA International Press, 1989), 68.

interpretation . . .[for] there has yet to be a computer program that can differentiate between a feint and a main effort."[168] Ultimately, humans will judge the relevance of information.[169]

Technology and Information Superiority

Technology offers great value but unrealistic expectations. Digitally enhanced organizations in the Army have yet to demonstrate significant improvements relative to the cost of technology.[170] Technology could facilitate increased understanding, but could also provide "diverging concepts of ongoing operations leading to dysfunctional misunderstandings at different levels in the chain of command."[171] Context is critical for understanding, since

> . . . the transmission of data without the associated context further diminishes the clarity of the message, especially when the receiver is in a different contextual environment than the sender. The more impersonal the means of transmission, the greater the lack of context will produce misinterpretation . . .as more powerful technological tools intrude into the process of command, the bring with them the risk that a generation of officers will be more inclined by instinct to turn to a computer screen than to survey the battlefield, and that the use of precise operational terms will be displaced by computer talk.[172]

Technology offers the greatest benefit in timeliness of information. Technology also provides accuracy but insufficient measures of accuracy to inform users. However, technology provides limited assistance with determining the relevance of information. Futurists warn that "capabilities, no matter how impressive to the engineer or technologist, may prove irrelevant in the next war."[173] Military leadership must provide the oversight for the proper application of technology.

---

[168] Alan D. Zimm, "Human-Centric Warfare," *U.S. Naval Institute Proceedings* 125, no. 5 (May 1999): 30

[169] Cox,, 42.

[170] Karen L Sinclair, "Information and the Future of Battle Command" (Thesis, Ft. Leavenworth, KS: U.S. Army Command and General Staff College, 1996), 30. Sinclair's study of results of Desert Hammer VI indicated that a "digitally enhanced brigade did not perform significantly better than a non-digitized brigade . . . systems were not fully integrated . . . [and] battle command was not enhanced."

[171] Adolph Carlson, "A Chapter not yet Written: Information Management and the Challenge of Battle Command," in *Sun Tzu and information warfare: a collection of winning papers from the Sun Tzu art of war in information warfare competition*, ed. Robert E. Neilson (Washington, DC: National Defense University Press, 1997), 114.

[172] Ibid., 116.

[173] Scales and others, vii.

Chapter 4

Leadership and Information

> *"But the world, as we experience it, is a very analog place. From a macroscopic point of view, it is not digital at all but continuous. Nothing goes suddenly on or off, turns from black to white, or changes from one state to another without going through a transition."* –Nicholas Negroponte, 1994.[174]

Technology in the future will only provide value in relation to humanity. Businesses that tried to reengineer themselves with information technology in 1997 reported marginal success rates, where the "number one culprit on everyone's list is resistance to change."[175] Military applications have encountered the same dynamic. Can transformation force leadership (battle command) integrate technology with operational concepts to achieve information superiority with timely, accurate, and relevant information?

Knowledge based warfare

Trust in technology provides the biggest obstacle to leadership. Charles Wang, chief executive officer (CEO) of Computer Associates, notes the challenges faced by corporate Chief Information Officers (CIO), due to a

> . . . fundamental disconnect between the technology executive and the rest of corporate management, a mismatch caused by disparities in training and temperament.. . the two parties lacked a basic vocabulary to have a meaningful dialogue.[176]

Wang's experience was that while CEOs were proud of their investments in technology and convinced that technology had value, they were unable to quantify the results. CEOs remained reliant on CIOs to assess the effectiveness of the investment.[177] Knowledge management scientists recognize the human influence and that ". . . technology is always a *possible* means of doing things and whether or not it serves its purposes depends in part on users' attitudes toward it."[178]

---

[174] Negroponte, 15.
[175] Tapscott, 3.
[176] Wang, x.
[177] Ibid., 26.
[178] Mark Addleson, "Organizing to Know and Learn: Reflections on Organization and Knowledge Management," in *Knowledge Management for the Information Professional*, ed. Michael E. D. Koenig and

Overconfidence in technology provides an equivalent obstacle. Technology itself "does not provide knowledge, although it can play a useful part . . .[to] help people who are willing to use [it] to find information."[179] Ensuring information superiority requires the same level of commander interest that maneuver, fire support, and logistics demand. Wang's disconnect applies in military simulations, including the Corps Battle Simulation used to exercise Army divisions. Unfortunately,

> . . . the training environment's use of 'perfect' communications—the assumption that communications are always available, and in the desired capacities—has contributed to a serious deficiency in warfighting commander and staff training. Commanders and their staffs are being taught to expect perfect and unlimited communications—hence, perfect knowledge—and that there is no need to include the J6 or G6 in planning for the battle.[180]

Students of the Command and General Staff College in 1996 included communications realism in the final exercise, Prairie Warrior '96, by replicating information nodes in the simulation and establishing rules for information flow. For example, a seventy-five percent bandwidth reduction for unit command posts during their movements applied to account for differences in single-channel radio versus mobile subscriber equipment. One of the participants, Lieutenant Colonel Richard Volz, noted importance of the human dimension, stating:

> The American military can achieve superiority of battlefield information, and we must do so in order to exploit fully our technological superiority. But human beings will never gain anything approaching complete information dominance, because information alone does not, and will never equate to knowledge and wisdom about the enemy.[181]

Transcending Network-Centric Warfare in favor of knowledge-based warfare encounters the challenge that tacit information is not easily transferred as data without the underlying logic or context.[182] Tacit information or knowledge feeds on experience, when the "transmitter . . . and the receiver . . . hold a common body of knowledge, and thus communication between [them] can

---

T. Kanti Srikantaiah (Medford, NJ: Published for the American Society for Information Science by Information Today, 2000), 155.

[179] Ibid.

[180] Eric R. Christensen, "Communications: Train as You Fight," *Military Review* 76, no. 3 (May–June 1996): 31

[181] Scales and others, 63.

[182] Alberts, Gartska, and Stein, 127.

be in shorthand."[183] The gap between operational concepts and technology could be narrowed by developing an objective system with a

> . . . battle control language that will give commanders control of computational power . . [with] statements that look like operations, orders, unit TOEs (tables of Organization and Equipment, and map graphics. The language will let commanders control, interrogate, and understand a nearly instantaneous information flow about unit status and logistics. Incoming intelligence will be correlated and displayed in seconds. Continuous simulations, which will run in the background, will be used to test alternatives. Broad mission orders from the commander will automatically generate implementing instructions to units.[184]

Collaborative planning tools and ABCS integration hint at some of these features. New knowledge springs from analysis, since "the essence of preparation, of planning, is the analysis of data which are at best only partially relevant: historical data, exercise and test results, and intelligence."[185]

Information overload can potentially decrease the effectiveness of battle command. Cognitive scientists describe the "*data availability paradox:* more and more data is available in principle, but our ability to interpret what is available has not increased."[186] In addition, although communications capacity and computer processing power have grown exponentially, requirements have also grown exponentially.[187] To handle increased demands on a scarce resource, efforts to increase the supply side include advances in broadcast radio propagation.[188] Besides leveraging what information sources are available, high performance units must also plan for periods of information loss, and

> . . . lower the demand for information by adjusting tactics, especially in very difficult electromagnetic environments . . . In areas you might call 'communication dead zones,' tactics may need to be based on zero situational awareness.[189]

---

[183] Negroponte, 21.
[184] National Research Council, 118.
[185] John Hwang, *Selected analytical concepts in command and control*, Military operations research v. 2 (New York: Gordon and Breach, 1982), ix.
[186] David D. Woods and Emily S. Patterson, *Can We Ever Escape From Data Overload?: A Cognitive Systems Diagnosis*, National Technical Information Service (Cognitive Systems Engineering Laboratory, Ohio State University, 1998), 3.
[187] Van Trees, 38.
[188] Edwards, 532.
[189] Ibid.

Technology has induced additional stress in organizations. Dynamics of information effects on humans include increased clutter (too much data), excess workload (too little time), and uncertain relevance (too complex). Studies of data overload conclude that "the message from users, a message carried in their voices, their performance, their errors, and their adaptations, is one of technology-induced complexity."[190] Donald Pihl, Commander of the 9th Infantry Division (experimental), experienced similar complexity with some of the earliest computerized command post experiments. Pihl believed in the role of the commander, since

> . . . the command and control (C2) process is personal. The commander is the center . . . and is in charge of using the information from its five points – maneuver, fire support, intelligence, logistics, and air defense. C2 is not a place; there is no inherent magic in a command post. . . . C2 is a process that moves with the commander.[191]

Computerized command posts still collected data, analyzed it, and presented information via a shared database. Pihl noted that the "commander and the subordinate commanders, with supporting staffs, do not need the same information in real time. There is a hierarchy of information needs and a range of timeliness."[192] Two concerns about the application of technology were the mobility afforded the commander and an overload of information. Suggested solutions included more mobile equipment, preformatted messages to reduce bandwidth requirements, and database replication to allow the commander to enter any command post and gain equivalent situational awareness.

During the first digital force logistics rotation at the National Training Center (NTC), communication planners experimented with new digital radios embedded in most tactical vehicles. Maneuvering the net entailed ensuring

> . . . that node-center jumps, [data radios], enhanced position-location reporting system and radio-access unit coverage were synchronized with the brigade maneuver and force-protection plans. Force protection of the node centers was critical to ensuring the

---

[190] Woods and Patterson, 7.

[191] Donald Pihl, "Facing up to Real World Communications Problems," in *Control of Joint Forces: A New Perspective*, ed. Clarence E. McKnight (Fairfax, VA: AFCEA International Press, 1989), 43.

[192] Ibid.

> brigade's success. [the] BCT commander . . . understood the need to protect node centers and ensured engineer assets were allocated to dig them in.[193]

Leaders who value information take steps to ensure its availability. Commanders experienced with technology have discerned that "it is no longer sufficient to simply establish communications and automation links . . . they must recognize and act to minimize inherent vulnerabilities in systems."[194] Leadership can focus technology and degrade or augment the effects of technology on timeliness, accuracy, and relevance of information.

Leadership and Information Criteria

Timeliness and Leadership

Information timeliness and leadership relate in an interesting way. In an environment where staff officers misunderstand the value of certain elements of information, technological means could deliver critical items to a command post only to have poor procedures allow the information to age past the point of relevance. Collecting information for twice daily battle update briefs provides a potential example of this phenomenon. Conversely, commanders and staff officers recognizing information that is not routinely processed as a priority or transmitted to specific echelons could short-circuit routine channels and ensure the information benefits the organization.

In tactical operations centers at most echelons, the "battle captain, with the aid of the battle NCOs, is the center of TOC information management."[195] A study of digital technology's impact on light infantry unit tactical operation centers outlined several key characteristics of the digital battle captain: a grounding in technology, operational experience, and understanding of the commander's visualization of the battlefield.[196]

---

[193] Welton Chase, "Team Signal Excels in Army's First Digital Logistic-Focused National Training Center Rotation," *Signal* 24, no. 4 (Winter 1999) Accessed May 9, 2000. Available from www.gordon.army.mil/regmktg/AC/Vol24No4/124sig.htm. BCT commander Rich Lynch also served as Interim Brigade Combat Team commander during the May 1999 student simulation, and echoed his sentiments on protection information assets to support maneuver plans.

[194] Fredericks, 100.

[195] Graham, Valentine, and Washington, 17.

[196] Ibid. 20.

Nicholas Negroponte visited an admiral in the 1970s who would walk around the command center and direct a junior seaman at a computer console to execute commands. Negroponte noted that despite the competence of the seaman,

> . . . the admiral was unprepared to plan an attack through such an indirect interface. He knew the seaman was looking at the situation through the keyhole of the computer system's small display. The admiral preferred interacting directly with a large wall map of the 'theater' on which he would thumbtack little blue and red ships of appropriate shape. . . .it was not an either/or interface; it was both/and. . . . simply stated, said that redundancy was good. In fact, the best interface would have many different and concurrent channels of communication, through which a user could express and cull meaning from a number of different sensory devices (the user's and the machines). Or, equally important, one channel of communication might provide the information missing in the other.[197]

Such redundancy in systems could speed the decision cycle. Schutzer described information based on three discrete elements. An initial event "signals emergence of a situation requiring action," to which exists a desired first response which would "restore or continue the desired equilibrium." Delayed decisions could lead to a "point in time at which unopposed evolution of the situation will preempt the commander's ability to implement his desired first response."[198] General Frederick Franks also cites the challenge of deciding when to make a decision, requiring commanders adept at being "capable of rapid synthesis of information and then having the organizational feel for that command echelon and what is and is not possible over time, also helps you know when you need to decide."[199] Rapid synthesis becomes easier with experience and with proper human-computer interfaces that have the "complexity of the network placed at the information node, not the user terminal."[200]

Innovative presentation techniques could allow the user to glean as much information from a particular area as required. Welch makes an analogy to a newspaper article, where the title provides a topic area, the lead paragraph provides the bottom line, and the rest of story unfolds so that the reader can "get as much of the story as you could get in that length of time.

---

[197] Negroponte, 98.
[198] Schutzer, 139.
[199] Franks, 18.
[200] Volz, 49.

So, the story reveals itself in a big spiral."[201] Once decisions have been made based on enough information, the "commander should be able to issue orders in a familiar form, have them translated rapidly into detailed orders needed by field units, and have them transmitted securely to those units."[202]

Leadership can have a wide range of effects on timeliness of information. Commander and staff experience may improve efficiency and prevent information latency. Information management procedures and friction could have negative implications if staff officers favor procedures over action. Overall, leadership has a neutral effect on timeliness.

Accuracy and Leadership

Leadership provides the ultimate judge of accuracy. Studies of Army battle command computers determined ". . . that commanders did not always trust their computer displays, but instead went with their intuition."[203] Intuition is inherently beneficial, when formed based on years of operational experience. Intuition would be amplified if commanders had an equivalent degree of experience with technology. The use of expert systems to augment intuition may have value "but requires more time and increases the workload of the decision maker using it."[204] Even in a networked environment, informal communications remain relevant since "commanders need an informal way to balance the demands of the system of systems through their own intuition and that of their subordinates."[205]

Commanders throughout history have employed the concept of "the directed telescope" to fill perceived knowledge gaps. For example, Napoleon used trusted aides to gather information from subordinate echelons and assess friendly conditions, glean intelligence, and

---

[201] Welch, 8.
[202] National Research Council, 56.
[203] Stanley and Army War College. Strategic Studies Institute., 45.
[204] Didier Perdu and Alexander H. Levis, "Evaluation of Expert Systems in Decision Making Organizations," in *Science of Command and Control: Coping with Complexity*, ed. Stuart E. Johnson, Alexander H. Levis, and National Defense University, AIP information systems series (Washington, D.C.: AFCEA International Press, 1989), 89.
[205] John H. Jr. Tilelli, "Putting JV 2010 into Practice," *Joint Force Quarterly*, no. 17 (1998): 80

articulate his intent to subordinate commanders.[206] General George Patton, while commanding Third Army in World War II, valued information and organized staffs to gain the most benefit. Patton's directed telescope included the

> . . . use of the 6th Mechanized Cavalry Group as the Third Army Information Service. He had studied the problem of military information management via his readings of military history. He understood he could be overwhelmed with information. But the wise use of his staff coupled with his innovative techniques in obtaining information allowed him to assimilate only the most critical information he needed to make operational decisions.[207]

Today, a commander's direct influence on information collectors may be limited to certain assets, especially in a networked environment.[208] Modern day directed telescopes in the form of VTC, and other direct links provide direct information but must be balanced against the reduction of bandwidth providing connectivity between lower echelons. Such connectivity in the early stages of operations in Kosovo suffered since

> . . . satellite resources day to day [are] a scare commodity for [most systems] . . . no one else would have been serviced without taking someone off. . . . [the] loss of channels hindered numerous missions to include special ops, humanitarian ops, training, and testing.[209]

Perception of accuracy may be as important as the reality. For example, military digital terrain elevation data (DTED) is available with varying degrees of elevation resolution, including 100-meter separation. Mapping programs that predict a particular point to be a specific elevation may be no more accurate than the standard paper map. If these attributes are known, digital and paper maps can provide the same level of abstraction for the purpose desired.

Regardless of accuracy, the sequence of information received can also affect the outcome. Daniel Serfatey's study determined that "decision makers usually place undue confidence in the correctness of prior decisions and assessments . . .[but conversely] people tend

---

[206] Gary B. Griffin, *The Directed Telescope: A Traditional Element of Effective Command* (Fort Leavenworth, KS: Command and General Staff College, 1991), 8.

[207] Jeffrey R. Sanderson, "General George S. Patton, Jr.: Master of Operational Battle Command, What Lasting Battle Command Lessons can we Learn from him?" (Monograph, Ft. Leavenworth, KS: U.S. Army Command and General Staff College, 1997), 29.

[208] Swinford, 54.

[209] Lasher, Slide 16.

to place greater emphasis on newer information than on prior information."[210] Serfatey's research implied that the order of receipt of information mattered, and consistent recent reports from the same source increased the commander's confidence in that information. Commanders may also have strong beliefs irrespective of their confidence of contrary incoming information.[211] As a result, real planning only occurs in the early stages of problem solving. Once the commander becomes wedded to a concept, despite new contradictory evidence, "their elaborate mental model of the battlefield probably includes the high cost of moving troops as opposed to the relatively low cost of changing a belief in a hypothesis."[212]

Trust drives the perception of accuracy. Trust in subordinates, technology, and the environment increases the perceived value of information; mistrust in the same increases uncertainty.[213] Trust in subordinates can be justified or misplaced. The underlying challenge for the commander is to discern "if what is being reported is a random act, a deception, a reaction to his observation, or the actual planned location for a given enemy subunit. . . .[or] friendly subordinate units. . . . the overall effect . . . is to potentially increase the amount of uncertainty a commander perceives."[214]

Video teleconferencing provides a means of increasing accuracy in the interpersonal dimension. Admiral James Ellis, Commander of Joint Task Force Noble Anvil, used VTC to clearly express commander's intent, but noted the negative side effects of increased staff work, possibility of detailed control, and poor execution of discussed tasks, as there would often be no documentation to the details of the VTC discussion.[215] VTC for higher-level commands has filled the niche that voice communications still holds for lower echelons. Voice can also convey stress

---

[210] Daniel Serfaty, Elliot E. Entin, and Robert R. Tenney, "Planning with Uncertain and Conflicting Information," in *Science of Command and Control: Coping with Complexity*, ed. Stuart E. Johnson, Alexander H. Levis, and National Defense University, AIP information systems series (Washington, D.C.: AFCEA International Press, 1989), 92.

[211] Ibid., 95.

[212] Ibid.

[213] Zand, 41.

[214] Swinford, 66.

[215] Admiral James O. Ellis, "A View from the Top" (Briefing, Joint Task Force Noble Anvil, Operation Allied Force, 1999).

and other human emotions.[216] Video can convey facial expressions and body language. Joseph Brendler's study of information for military applications asked, "is the affective communications gain achieved with one VTC worth the loss of a dozen relatively non-affective telephone channels? Or is the VTC important enough to allocate lift assets to move the required equipment ahead of other important weapons systems?"[217] LTC Robert Leonhard also cautions that VTC wastes tactical bandwidth that could be better used for collaborative white-boards to clearly coordinate plans at lower echelons.[218]

Ultimately, leadership judges accuracy through perception. Directed telescopes and intuition fill perceived gaps as commanders quest for certainty. However, leadership must also focus information on relevance, for there are

> . . . few things as dangerous as a comprehensive, accurate answer to the wrong question. This is psuedoknowledge. It easily misleads management into erroneous actions. Psuedoknowledge has mushroomed with the advent of computers, which have made available masses of data that answer questions managers have found too costly to ask before. In too many instances, however, the data are collected but not used because they answer irrelevant questions.[219]

Overall, leadership improves accuracy by applying intuition, trust, and perception to determine truth. Leadership has a positive impact on accuracy, employing directed telescopes, voice and video, and direct observation to build context and generate knowledge.

Relevance and Leadership

Leadership provides the context by which relevance is measured. Although a future organization will "use modern communications and even computers, and it will require leadership of the highest order; but at the heart of the process lies the mind of the commander . . .[from which] a dominating concept of operations must emerge."[220] The concept of battle command

---

[216] Edwards, 541.

[217] Joseph Brendler, "The Stuff that Binds: On the Nature and Role of Information in Military Operations" (Monograph, School of Advanced Military Studies, Command and General Staff College, 1995), 1-27.

[218] Leonhard, *The Principles of War for the Information age*, 197.

[219] Zand, 10.

[220] William E. Depuy, "Concepts of Operation: The Heart of Command, the Tool of Doctrine," in *Control of Joint Forces: A New Perspective*, ed. Clarence E. McKnight (Fairfax, VA: AFCEA International Press, 1989), 9.

gained prevalence over the more technically oriented term "command and control" in an effort to focus discussion more on "the art of command and battle leadership…"[221] Battle command builds in part on the knowledge of the state of environment and visualization of an end state, particularly the spatial relationship between battlefield elements.[222] In natural perception, humans use all senses to gain awareness. For example, in a cluttered visual scene, human eyes naturally pick out relevant information.[223] Artificial perception using computer screens limits human abilities to discern relevant information.

Information management consists of interrelated activities of information filtering and information production. For example, filtering categories for electronic mail messages can include: ignore based on external marking, open and ignore, open and use, open and identify as critical. Technology can provide the indicators for humans to judge relevance. Based on filtering, information production could consist of raw message forwarding, limited judgments, or detailed problem solving.[224] Relevance revolves around two questions: "how much would current conditions have to change for me to change my decision, and what information or conditions, not presently known, would cause me to change my decision?"[225] Context becomes critical since

> Whether or not something is information and whether or not the information is appropriate or relevant is always established when people give meaning to things in the context of the narratives and their interest pertaining to the particular projects with which they are involved.[226]

In one example during a command post exercise, an "officer described waking up from two hours of sleep to find 218 new e-mail messages in his in-box, of which four were relevant to his

---

[221] Franks, 5.
[222] Lawson, 62.
[223] Woods and Patterson, 13.
[224] Jared T. Freeman and others, *Training in Information Management for Army Brigade and Battalion Staff: Methods and Preliminary Findings* (U.S. Army Research Institute for the Behavioral and Social Studies, 1997), 22, Technical Report 1073.
[225] Zand, 10.
[226] Addleson, 156.

concerns."[227] Technology of most use to commanders helps filter information and translates simple concepts into precise instructions for subordinate commanders.[228]

Sensors have limitations, and commanders must prioritize information needs to reduce uncertainty.[229] Task Force Hawk's deployment to Albania in support of operations in Kosovo utilized "target acquisition radars positioned on the Albanian border . . . [that] peered into Kosovo and identified Serb Artillery which was then pounded from the air."[230] Tactical satellite systems enabled connectivity despite the rugged terrain, but achieving this level of support required most of an entire Army division's satellite allocation.[231] For this mission application, the cost of achieving information superiority exceeded the risk of not having the communications assets for another conflict.

Commanders can make an a priori decision based on intuition to weight the information effort by assigning additional assets or priorities. Command post location and functional mission also influence the provision of information. Technology offers limited solutions, because "in order to mass information, [commanders] must have agilely assignable bandwidth and individual units must have transmission technology capable of accepting [it]."[232] Franks experience with information management leading VIII Corps during Operation Desert Storm is that

> As our Army experiments with more precise, electronically displayed situational awareness made possible by technology, we must watch what types of input influence our mind's eye picture of reality and where that picture requires the commander to be. For instance, in making decisions during *Desert Storm*, I got maybe 20 percent of my information during battle from CP input, 50 percent from being up front on the battlefield and getting assessments from my commanders and 30 percent from embedded memory of education and training.[233]

---

[227] Freeman and others, 1.

[228] Richard G. Kaiura, "Light Infantry Battalion-and-below Battle Command in the Early Twenty-First Century: What Advanced C4I Capabilities are Required and Which Enabling Technologies are Not Being Developed?" (Monograph, School of Advanced Military Studies, Command and General Staff College, 1999), 54.

[229] Charles J. Green and James D. Edwards, "III Corps Expands the Knowledge Base for Employing Sensors," *Army Magazine* 50, no. 8 (August 2000): 26

[230] Ignatieff, 99.

[231] Fletcher.

[232] Allen, 19.

[233] Franks, 16.

Frank's experience is consistent with other commanders. General Tilelli, Commander of United States Forces Korea, noted that one of his command post exercises,

> . . . demonstrated that ample information can be generated. As in other commands, the concern is differentiating between the relevant and irrelevant. Using the critical requirements of the commander as a filter, C4I architecture can be manipulated to deselect information irrelevant to effective and timely decision making.[234]

Leadership provides the focus for relevant information that technology does not. Commander's critical information requirements provide a window into the mind and expertise of the commander. Networked environments should not only use CCIR as filters to mine databases for relevant data, but also provide a mechanism for CCIR to rapidly change and be disseminated as the commander applies expertise. Achieving a level of expertise remains important since

> . . . experts appear to have an overall sense of what is happening in a situation—an ability to judge it prototypically. Whereas novices may be confused by all the data elements, experts see the big picture, and they appear to be less likely to fall victim to information overload.[235]

Leadership provides information relevance. Leadership judges and determines relevance based on expertise developed with experience.

Leadership and Information Superiority

Leadership provides the operational concept which information technology must support. Technology can provide a deceptive faith that posting information to a web page or clicking send on an electronic mail ensures that information will be received where needed.[236] Admiral Ellis warns future commanders that information potentially "will control you and your staffs . . . and lengthen your decision cycle."[237]

Shimon Naveh recognizes the fundamental difference between front line commanders fighting the current battle and higher echelon commanders planning the next operation, which causes a cognitive tension between operational and tactical problem solvers.[238] Information

---

[234] Tilelli, 80.
[235] Gary Klein, *Sources of Power: How People Make Decisions* (Cambridge, Mass.: MIT Press, 1998), 152.
[236] Ellis.
[237] Ibid.
[238] Naveh, 132.

systems can provide relevance with leadership when priority involves the "idea of gaining knowledge or . . . enabling commanders to apply professional judgment while exercising command and control in combat."[239] Timely and accurate information can be relevant only with respect to human understanding of the battlefield, since

> . . . knowledge—battlefield information—is a two-edged sword. Mating superior knowledge with speed of movement can provide the means to frustrate the defenders' ability to acquire and mass fires and thus allow an attacker to cross the deadly zone intact to accomplish an operationally decisive maneuver.[240]

Leadership has a neutral effect on timeliness of information. It can impede timeliness if procedures or awareness conflict. Leadership could enhance timeliness when relevant information is salvaged from an overloaded system. Leadership improves accuracy by evaluating systems and personnel based on trust. Leadership has great impact on relevance by definition, since relevance relates to the context of the operation set by the leader.

[239] F.G. Hoffman, "Joint Vision 2010: A Marine Perspective," *Joint Force Quarterly*, no. 17 (1998): 36

[240] Scales and others, 142.

Chapter 5

Leadership and Technology

> *. . . if a commander's service of information is better than that of his adversary he possesses a wider knowledge and superior control; he selects with certainty his objective and arrives at it first; he perceives weakness before his own is discovered or strength before his weakness is known; he anticipates movements, alters dispositions, executes plans unknown to the enemy; in short, the successful soldier commands the situation by force of superior knowledge, and never is it more true than in war that knowledge is power.* -- Brigadier General George Scriven, Chief Signal Officer of the Army, 1915.[241]

Transforming the military with integrated technology and leadership has been a continual evolution. This monograph examined information and knowledge and how military organizations apply leadership and technology to provide timely, accurate, and relevant information. The specific challenge appears to be achieving information superiority during maneuver and remaining adaptive to situations where information support is degraded.

Towards Information Superiority

Army transformation forces must integrate leadership and technology to achieve information superiority during maneuver. Table 2 outlines key elements of the relationship between technology, leadership, and the three criteria.

	Technology	Leadership
Timeliness	Excellent potential. Predetermined linkages, ranges from speed of light to speed of courier, must also consider latency and processing time.	Neutral impact. Can help or hinder based on procedures or briefing plans. Battle captains can help commanders manage information.
Accuracy	Great accuracy may be masked by poor presentation. Must build trust in systems, use figures of merit (like GPS), automatic track correlation. Must understand digital representation of analog world.	Positive influence with experience. Trust and experience with systems, use of directed telescopes, judgment, use of voice and video to regain personal communications.
Relevance	Limited assistance. Database mining with smart filters, use of artificial intelligence for narrow applications.	Greatest impact. CCIR drives information planning, uses battle command, cdr's intent based on concepts, relative to purpose.

Table 2 Leadership, Technology, and Information

[241] George Percival Scriven, *The service of information, United States Army*, Circular, no. 8 (Washington, DC: Govt. print. off., 1915).

Figure one shows the qualities of information related to technology and leadership where leadership occupies the central position of the diagram. The outer ring represents technology. Various attributes that relate to timeliness, accuracy, and relevance show the interrelationships between technology and leadership. As technology improves, the breadth of the outer ring increases, requiring more elements in the inner ring to deal with the changes. Overall, each information quality retains sufficient support by either leadership or technology to provide the

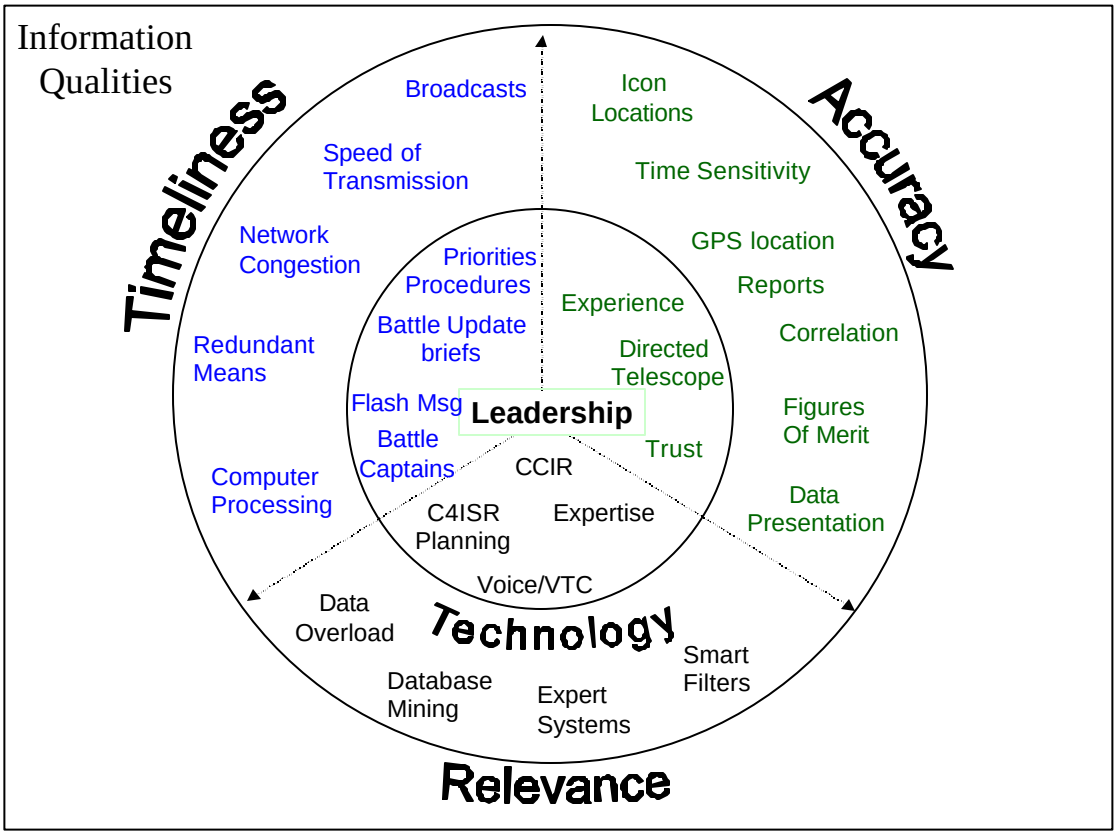

Figure 1 Information Qualities Related to Technology and Leadership

conclusion that future forces can provide timely, accurate, and relevant information during maneuver. However, conclusions on how the two dimensions could be better integrated to achieve information superiority may generate some implications for the organization and training of transformation force units.

Timeliness

Technology provides incredible tools that nonetheless have inherent limitations. Innovative leaders can recognize limitations and still organize information systems to best provide timely information. Experienced leaders use CCIR to organize command posts and focus battle captains to provide the mechanisms for rapid prioritization and transfer of the most accurate and relevant information.

Pre-positioning information assets can also assist in reducing the burden on the network. In logistics planning, the ideal is a perfect logistics system that delivers just in time, but reality allows units to maintain "basic loads" of supplies meant to make a unit self-sufficient for a given period, usually three days. An interesting corollary for information planning could indicate that future units must define a "basic load" of information, probably measured in much shorter time frames, but with the same purpose of allowing a unit to operate for a short period of time without a continual information feed.

Even the highly mobile force requires the periodic transfer of fuel to support operations. Information could easily be transferred as well; future fuel vehicles could become the high bandwidth information conduit that collects routine data from every vehicle they service and downloads updated information to sets the new context for information. Cheap, encrypted compact disks could be dropped like leaflets to encircled units to fuel their information systems.

As networks become critical vulnerabilities, leaders must provide for their defense. For example, a GAO Report noted that jamming of two communications links from a tactical operations center could overcome the redundancy of the system during the Division XXI AWE, but "jamming two frequencies at high power for a sustained time would make the perpetrator vulnerable to detection and counterattack by friendly air or artillery."[242] The interesting question becomes—what priority of fires supports the network's self defense? Can the force detect the jamming and react fast enough?

---

[242] General Accounting Office, *Battlefield Automation: Opportunities to Improve the Army's Information Protection Effort* (United States General Accounting Office, 1999), 8.

Accuracy

Technology provides great accuracy, but it must be understood and believed to be effective. As future soldiers build confidence and provide feedback to systems developers, the development loop will naturally improve the perception of accuracy by users. Provision of alternate means to confirm information also helps the leader judge accuracy. Certain aspects of information that are not easily digitized for transmission will require continued provision of telephone and VTC links to allow evaluation of stress based on voice and body language.

Force XXI vision recognizes the importance of technology training for leaders and soldiers with focus on information management. The goal for all remains

> . . . proficiency in management of the vast quantity of information these new systems will make available. The ability to analyze the commander's intent, translate it into specific information requirements, and quickly select those systems which can best collect, process, display, and disseminate required information will be essential. Training must produce soldiers, leaders and units enabled, not encumbered, by technology.[243]

Principles of communications set standards such a higher to lower, left to right, and supporting to supported to delineate responsibilities. Future principles may include provisions that account for bandwidth (bigger to smaller), modernization (newer to older), and software versions (higher to lower). Such principles could assist in maintaining the free flow of information upon which a network depends. Thus, tactic knowledge could be more readily converted to explicit knowledge with each message sent. Context could be shared by building a picture of the local conditions without worry about conservation of bandwidth. Therefore, accuracy of information will improve over time.

Relevance

Technology provides little help to determining relevance, as the basis of an expert computer system is an expert human being that must be modeled into computer programs. Development of such an expert in the military requires operational experience. Technology

---

[243] Headquarters Training and Doctrine Command, *Force XXI Operations: A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Early Twenty-First Century (31 July 2000 Draft)*, B-1.

provides much of the raw information via brute force dissemination that commanders and staffs sift for relevant information. Leaders need systems that can send the best possible message in times of information degradation such as maneuver.

Maneuvering the network provides a metaphor for the emplacement of information networks to support the various sensors, shooter, and command nodes envisioned for the future battlespace. To achieve information superiority, future leaders must recognize the limitations of technology and the human dimension of information. Battle command abilities can be strengthened in the digital age, where "personal use of the technology creates leaders."[244] The future information environment will be a complex composite of civilian infrastructure and military extensions.

Future operational concepts could employ information to achieve effects that traditional maneuver previously supported. For example, detailed information about Croatian Air Defense radars operating during the NATO bombing campaign in Bosnia was used by diplomats to convince the Croatian Ministry of Defense to cease radar operations.[245] Thus, one element of relevant information had a measurable effect on force employment—a information based turning movement.

Conclusion

Transformation forces can integrate leadership with technology to achieve information superiority with timely, accurate, and relevant information. Human cognitive abilities provide the focus for network information systems. Adaptive leaders solve problems through innovative solutions, facilitated by enough communications to implement solutions.[246] Network systems can shape the commander's battlespace using the power of sensor to shooter technology, especially

[244] Tapscott, 254.
[245] Adams, 89.
[246] C. Kenneth Allard and National Defense University Press., *Somalia operations lessons learned* (Washington, DC: National Defense University Press, 1995), 77.

targeting, that "enables the digitized force to destroy or weaken enemy forces long before they are in direct fire contact. . . . [thus setting] conditions for dominant maneuver at brigade level."[247]

Neither the technological dimension nor the leadership dimension of information alone provides sufficient timeliness, accuracy, and relevance to fully ensure information superiority for transformation forces. The synergy of the two has great potential for overcoming the complexity of information support to maneuver. Careful integration of command and control, operational planning, emplacement of tactical operations centers, and interpersonal human communications with technological enhancements can provide the environment for success in future conflicts.

[247] Benjamin S. Griffin and Archie Davis, "Operation-Centric Warfare: Setting the Conditions for Success at Brigade and Battalion," *Army Magazine* 50, no. 8 (August 2000): 24

Appendices

Appendix 1 Criteria

	Joint Pub 6-0 Communications Information Quality Criteria[248]	Joint Pub 2-0 Intelligence Qualities[249]
Accuracy**	Information that conveys the true situation	Intelligence must be factually correct and convey the situation as it actually exists.
Relevance**	Information that applies to the mission, task, or situation at hand	Intelligence must contribute to an understanding of the situation, to determining objectives that will accomplish the commander's purposes and intents, and to planning, conducting, and evaluating operations.
Timeliness**	Information that is available in time to make decisions	Intelligence must be available and accessible in time to effectively use it.
Usability (Relevance)	Information that is in common, easily understood format and displays	The form in which intelligence is provided to the commander must be suitable for application upon receipt without additional analysis.
Completeness (Accuracy)	All necessary information required by the decision maker	Commanders, staffs and forces must receive all the intelligence available to meet their responsibilities and accomplish their mission.
Brevity	Information that has only the level of detail required	
Security	Information that has been afforded adequate protection where required	
Objectivity		Intelligence must be unbiased, undistorted, and free from political influence or constraint.
Readiness		Intelligence organizations must anticipate and be ready to respond to the existing and contingent intelligence requirements of the commanders, staff, and forces at all levels of command

Table 3 Criteria Selection Matrix

[248] Joint Chiefs of Staff, *Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations*, I-5.

[249] Joint Chiefs of Staff, *Joint Doctrine for Intelligence Support to Operations*, Joint Publication 2-0 (Washington D.C.: U.S. Government Printing Office, 1995), IV-15.

Bibliography

BOOKS

Adams, James. *The Next World War: Computers are the Weapons and the Front Line is Everywhere*. New York: Simon & Schuster, 1998.

Addleson, Mark. "Organizing to Know and Learn: Reflections on Organization and Knowledge Management." In *Knowledge Management for the Information Professional,* ed. Michael E. D. Koenig and T. Kanti Srikantaiah, 137-160. Medford, NJ: Published for the American Society for Information Science by Information Today, 2000.

Alberts, David S., John J. Gartska, and Frederick P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority*. Washington, DC: C4ISR Cooperative Research Program, 1999.

Allard, C. Kenneth. *Command, control, and the common defense*. New Haven: Yale University Press, 1990.

Allard, C. Kenneth, and National Defense University Press. *Somalia operations lessons learned.* Washington, DC: National Defense University Press, 1995.

Arquilla, John, and David F. Ronfeldt, eds. *In Athena's Camp: Preparing for Conflict in the Information Age.* Santa Monica, Calif.: Rand, 1997.

Black, Steven K. *A Sobering Look at the Contours of Cyberspace.* Pittsburgh, PA: Ridgway Center for International Security Studies, University of Pittsburgh, 1996.

Brodskey, Stuart L. "Control Systems Aspects of Command and Control." In *Selected analytical concepts in command and control,* ed. John Hwang, 41-60. New York: Gordon and Breach, 1982.

Brown, Rex V. "Normative Models for Capturing Tactical Intelligence Knowledge." In *Science of Command and Control: Coping with Complexity*, ed. Stuart E. Johnson, Alexander H. Levis and National Defense University, 2, 68-75. Washington, D.C.: AFCEA International Press, 1989.

Carlson, Adolph. "A Chapter not yet Written: Information Management and the Challenge of Battle Command." In *Sun Tzu and information warfare: a collection of winning papers from the Sun Tzu art of war in information warfare competition*, ed. Robert E. Neilson, 103-124. Washington, DC: National Defense University Press, 1997.

Coakley, Thomas P. *Command and control for war and peace.* Washington, D.C.: National Defense University Press : U.S. G.P.O., 1992.

Conley, Robert E. "Military Command and Control (C2)." In *Selected analytical concepts in command and control,* ed. John Hwang, 15-21. New York: Gordon and Breach, 1982.

Crecine, John P., and Michael D. Salomone. "Organization Theory and C3." In *Science of Command and Control: Coping with Complexity*, ed. Stuart E. Johnson, Alexander H. Levis and National Defense University, 2, 45-57. Washington, D.C.: AFCEA International Press, 1989.

Cronin, Blaise, and Elisabeth Davenport. *Elements of Information Management.* Metuchen, N.J.: Scarecrow Press, 1991.

De Landa, Manuel. *War in theAge of Intelligent Machines*. Swerve ed. New York: Zone Books, 1991; Reprint Cambridge, Mass: MIT Press, 1994.

Denning, Dorothy E., and Peter F. MacDoran. "Grounding Cyberspace in the Physical World." In *Cyberwar: Security, Strategy, and Conflict in the Information Age*, ed. Alan D. Campen, Douglas H. Dearth and R. Thomas Goodden, 119-126. Fairfax, VA: AFCEA International Press, 1997.

Depuy, William E. "Concepts of Operation: The Heart of Command, the Tool of Doctrine." In *Control of Joint Forces: A New Perspective*, ed. Clarence E. McKnight. Fairfax, VA: AFCEA International Press, 1989.

Dunnigan, James F. *Digital Soldiers: the Evolution of High-tech Weaponry and Tomorrow's Brave New Battlefield*. 1st ed. New York: St. Martin's Press, 1996.

Edwards, Sean J.A. "Communications in Urban Environments." In *The City's Many Faces: Proceedings of the Rand Arroyo-MCWL-J8 UWH Urban Operations Conference April 13-14, 1999*, ed. Russell W. Glenn, 520-541. Santa Monica, CA: Rand, 2000.

Fox, Steven J. "Unintended Consequences of Joint Digitization." In *Sun Tzu and Information Warfare: a Collection of Winning Papers from the Sun Tzu art of War in Information Warfare Competition*, ed. Robert E. Neilson, 125-144. Washington, DC: National Defense University Press, 1997.

Friedman, George, and Meredith Friedman. *The Future of War: Power, Technology, and American World Dominance in the 21st Century*. 1st ed. New York: Crown Publishers, 1996.

Garden, Timothy. *The Technology Trap: Science and the Military*. 1st ed. Washington, DC: Brassey's Defence Publishers, 1989.

Girard, Paul E. "A Function-Based Definition of (C3) Measures of Effectiveness." In *Science of Command and Control: Coping with Complexity*, ed. Stuart E. Johnson, Alexander H. Levis and National Defense University, 2, 76-90. Washington, D.C.: AFCEA International Press, 1989.

Griffin, Gary B. *The Directed Telescope: A Traditional Element of Effective Command*. Fort Leavenworth, KS: Command and General Staff College, 1991.

Gulick, Roy M., and Anne W. Martin. "Managing Uncertainty in Intelligence Data--An Intelligence Imperative." In *Science of Command and Control: Coping with Uncertainty*, ed. Stuart E. Johnson and Alexander H. Levis, 10-18. Washington, D.C.: AFCEA International Press, 1988.

Hanlon, Michael. *Technological Change and the Future of Warfare.* Washington, DC: Brookings Institution Press, 2000.

Hazlett, James. "Just in Time Warfare." In *Dominant Battlespace Knowledge: the Winning Edge,* ed. Stuart E. Johnson and Martin C. Libicki, 133-148. Washington, DC: National Defense University Press, 1995.

Hwang, John. *Selected Analytical Concepts in Command and Control* Military operations research v. 2. New York: Gordon and Breach, 1982.

Ignatieff, Michael. *Virtual War: Kosovo and Beyond.* New York: Henry Holt, 2000.

Ivanov, D. A., V. P. Savel*ev, P. V. Shemanski*i, and United States. Air Force. *Fundamentals of tactical command and control : a Soviet view = Osnovy upravleniia voiskami v boiu* Soviet military thought ; no. 18. Washington, DC: U.S. Air Force, 1977.

Johnson, Stuart E., Alexander H. Levis, and National Defense University. *Science of Command and Control: Coping with Uncertainty* AIP information systems series; v. 1. Washington, D.C.: AFCEA International Press, 1988.

Johnson, Stuart E., Martin C. Libicki, and National Defense University Press. *Dominant Battlespace Knowledge: the Winning Edge*. Washington, DC: National Defense University Press, 1995.

Klein, Gary. *Sources of Power: How People Make Decisions.* Cambridge, Mass: MIT Press, 1998.

Koenig, Michael E. D., T. Kanti Srikantaiah, and American Society for Information Science. *Knowledge Management for the Information Professional* ASIS monograph series. Medford, NJ: Published for the American Society for Information Science by Information Today, 2000.

Lawson, J.S. "The State Variables of a Command Control System." In *Selected Analytical Concepts in Command and Control,* ed. John Hwang, 61-83. New York: Gordon and Breach, 1982.

Leonhard, Robert R. *Fighting byMminutes : Time and the Art of War.* Westport, Conn.: Praeger, 1994.

_____. *The Principles of War for the Information age*. Novato, CA: Presidio, 1998.

Levis, Alexander H., and Michael Athans. "The Quest for a C3 Theory: Dreams and Realities." In *Science of Command and Control: Coping with Uncertainty*, ed. Stuart E. Johnson and Alexander H. Levis, 4-9. Washington, D.C.: AFCEA International Press, 1988.

Libicki, Martin C. *What is Information Warfare?* Washington, DC: Center for Advanced Concepts and Technology Institute for National Strategic Studies National Defense University, 1995.

Libicki, Martin C., and National Defense University. Center for Advanced Concepts and Technology. *Defending cyberspace, and other metaphors.* Washington, DC: National Defense University, 1997.

Loescher, Michael. "The Information Warfare Campaign." In *Cyberwar: Security, Strategy, and Conflict in the Information Age*, ed. Alan D. Campen, Douglas H. Dearth and R. Thomas Goodden, 197-202. Fairfax, VA: AFCEA International Press, 1997.

Long, Dennis H. "Army Command and Control Requirements for the Eighties." In *Selected analytical concepts in command and control*, ed. John Hwang, 33-37. New York: Gordon and Breach, 1982.

Macgregor, Douglas A. *Breaking the Phalanx: A New Design for Landpower in the 21st Century.* Westport, CT: Praeger Publishers, 1997.

Marshall, S. L. A. *Men against Fire: the Problem of Battle Command in Future War*. Gloucester, Mass.: Peter Smith, 1978.

National Research Council, Board on Army Science and Technology. *Star 21: Strategic Technologies for the Army of the Twenty-First Century*. Washington, DC: National Academy Press, 1992.

Naveh, Shimon. *In Pursuit of Military Excellence: the Evolution of Operational Theory* The Cummings Center series. 7. Portland, OR: Frank Cass, 1997.

Negroponte, Nicholas. *BeingDigital.* 1st ed. New York: Knopf, 1995.

Nichiporuk, Brian, Carl H. Builder, and United States Army. *Information Technologies and the Future of Land Warfare*. Santa Monica, CA: Rand Arroyo Center, 1995.

Owens, Admiral William A. "Introduction" In *Dominant Battlespace Knowledge: the Winning Edge*, ed. Stuart E. Johnson and Martin C. Libicki, 3-17. Washington, DC: National Defense University Press, 1995.

Perdu, Didier, and Alexander H. Levis. "Evaluation of Expert Systems in Decision Making Organizations." In *Science of Command and Control: Coping with Complexity*, ed. Stuart E. Johnson, Alexander H. Levis and National Defense University, 2, 76-90. Washington, D.C.: AFCEA International Press, 1989.

Pihl, Donald. "Facing up to Real World Communications Problems." In *Control of Joint Forces: A New Perspective*, ed. Clarence E. McKnight. Fairfax, VA: AFCEA International Press, 1989.

Ryan, Michael, and Michael Frater. *A Tactical Communications System for Future Land Warfare.* Working Paper 109 ed. Australia: Land Warfare Studies Centre, 2000.

Scales, Robert H., Williamson Murray, Paul K. Van Riper, John A. Parmentola, and Army War College (U.S.). *Future warfare: Anthology*. Carlisle Barracks, Pa.: U.S. Army War College, 1999.

Schutzer, D.M. "C2 Theory and Measures of Effectiveness." In *Selected Analytical Concepts in Command and Control*, ed. John Hwang, 119-144. New York: Gordon and Breach, 1982.

Schwartau, Winn. *Information Warfare: Chaos on the Electronic Superhighway*. 1st ed. New York: Thunder's Mouth Press, 1994.

Scriven, George Percival. *The Service of Information, United States Army* Circular, no. 8. Washington, DC: Govt. print. off., 1915.

Serfaty, Daniel, Elliot E. Entin, and Robert R. Tenney. "Planning with Uncertain and Conflicting Information." In *Science of Command and Control: Coping with Complexity*, ed. Stuart E. Johnson, Alexander H. Levis and National Defense University, 2, 76-90. Washington, D.C.: AFCEA International Press, 1989.

Signori, David T., and Harold A. Cheilek. "An Overview of Joint Tactical Command and Control." In *Selected Analytical Concepts in Command and Control*, ed. John Hwang, 145-164. New York: Gordon and Breach, 1982.

Stallings, WIlliam. *Handbook of Computer Communications Standards, Volume 3: Department of Defense (DOD) Protocol Standards.* Indianapolis, IN: Howard W. Sams & Company, 1987.

Stanley, Elizabeth A., and Army War College (U.S.). Strategic Studies Institute. *Evolutionary Technology in the Current Revolution in Military Affairs: the Army Tactical Command and Control System.* Carlisle Barracks, PA: Strategic Studies Institute U.S. Army War College, 1998.

Tapscott, Don. *The Digital Economy: Promise and Peril in the Age of Networked Intelligence.* New York: McGraw-Hill, 1996.

Ullman, Harlan, and National Defense University. Center for Advanced Concepts and Technology. *Shock and Awe: Achieving Rapid Dominance*. Washington, DC: Center for Advanced Concepts and Technology, 1996.

Van Creveld, Martin L. *Command in war.* Cambridge, Mass: Harvard University Press, 1985.

Van Trees, Harry L. "C3 Systems Research: A Decade of Progress." In *Science of Command and Control: Coping with Complexity*, ed. Stuart E. Johnson, Alexander H. Levis and National Defense University, 2, 24-43. Washington, D.C.: AFCEA International Press, 1989.

Waltz, Edward. *Information Warfare Principles and Operations*. Norwood, MA: Artech House, Inc., 1998.

Wang, Charles B. *Techno vision: the Executive's Survival Guide to Understanding and Managing Information Technology*. New York: McGraw-Hill, 1994.

Welch, Jasper A. "C3I Systems: The Efficiency Connection." In *Selected Analytical Concepts in Command and Control*, ed. John Hwang, 3-13. New York: Gordon and Breach, 1982.

Zand, Dale E. *Information, Organization, and Power :Effective Management in the Knowledge Society*. New York: McGraw-Hill, 1981.

Electronic Sources

Joint Chiefs of Staff. *Joint Vision 2020*. Joint Staff, 2000. Accessed November 3, 2000. Online. Available from http://www.dtic.mil/jv2020/jv2020a.pdf.

Shinseki, Eric K. *The Army vision: Soldiers on Point for the Nation . . . Persuasive in Peace, Invincible in War.* 1999. Accessed 12 October 1999. Online. Available from www.hqda.army.mil/OCSA/vision.htm.

Government Documents

Defense Science Board. *Report of the Defense Science Board (DSB) Task Force on Tactics and Technology for 21st Century Military Superiority* Vol. 1. Washington, DC: Office of the Secretary of Defense, 1996.

Department of Defense. *C4ISR Handbook for Integrated Planning*. Arlington, VA: OASD(C3I), C4I Integration Support Activity, 1996.

General Accounting Office. *Battlefield Automation: Opportunities to Improve the Army's Information Protection Effort*: United States General Accounting Office, 1999.

Headquarters Combined Arms Center. *ARFOR Organization and Operational Concept (Draft).* Headquarters, Combined Arms Center, 2000. Accessed 2 February 2000. Online. Available from FTP://160.149.109.31/TF ARFOR/.

Headquarters Department of the Army. *Information Operations.* Field Manual 100-6. Washington, DC: U.S. Government Printing Office, 1996.

_____. *Operations (DRAG Edition)* Field Manual 3-0. Washington, DC: U.S. Government Printing Office, 2000.

Headquarters Training and Doctrine Command. *Force XXI Operations: A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Early Twenty-First Century* TRADOC PAM 525-5. Washington, DC: United States Army Training and Doctrine Command, 1994.

_____. *Force XXI Operations: A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Early Twenty-First Century (31 July 2000 Draft)* TRADOC PAM 525-5. Washington, DC: United States Army Training and Doctrine Command, 2000.

Joint Chiefs of Staff. *Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations* Joint Publication 6-0. Washington D.C.: U.S. Government Printing Office, 1995.

_____. *Joint Doctrine for Intelligence Support to Operations* Joint Publication 2-0. Washington D.C.: U.S. Government Printing Office, 1995.

_____. *Information Operations*. Joint Publication 3-13. Washington D.C.: U.S. Government Printing Office, 1996.

_____. *Joint Doctrine for Employment of Operational/Tactical Command, Control, Communications, and Computer Systems* Joint Publication 6-02. Washington D.C.: U.S. Government Printing Office, 1996.

_____. *Department of Defense Dictionary of Military and Associated Terms* Joint Publication 1-02. Washington D.C.: U.S. Government Printing Office, 1999.

Articles

Armitage, Richard Lee, Andrew F. Krepinevich, and Others. "National Security in the 21st Century: The Challenge of Transformation." *Joint Force Quarterly*, no. 16 (1997): 15-19.

Behling, Thomas G., and Kenneth McGruther. "Satellite Reconnaisance of the Future." *Joint Force Quarterly*, no. 18 (1998): 23-30.

Caivo, Mark D. "Digitizing the Force XXI Battlefield." *Military Review* 76, no. 3 (May–June 1996): 68-73.

Casper, Lawrence E., Irving L. Halter, and others. "Knowledge Based Warfare: A Security Strategy for the Next Century." *Joint Force Quarterly*, no. 13 (1996): 81-89.

Chase, Welton. "Team Signal Excels in Army's First Digital Logistic-Focused National Training Center Rotation." *Signal* 24, no. 4 (Winter 1999): Online. Accessed May 9, 2000. Available from www.gordon.army.mil/regmktg/AC/Vol24No4/124sig.htm.

Christensen, Eric R. "Communications: Train as You Fight." *Military Review* 76, no. 3 (May–June 1996): 31-32.

Cooper, Pat. "Bosnia Study Highlights U.S. Communications Inadequacies." *Defense News*, (January 13, 1997): 13-15?

Dubik, James. "IBCT at Fort Lewis." *Military Review* 80, no. 5 (Sep-Oct 2000): 17-24.

Dunlap, Charles J. Jr. "Joint Vision 2010: A Red Team Assessment." *Joint Force Quarterly*, no. 17 (1998): 47-49.

Estes, Howell M. III. "Space and Joint Space Doctrine." *Joint Force Quarterly*, no. 14 (1996): 60-63.

Franks, Frederick. "Battle Command." *Military Review* 76, no. 3 (May–June 1996): 4-25.

Fredericks, Brian E. "Information Operations at the Crossroads." *Joint Force Quarterly*, no. 16 (1997): 97-103.

Gosinski, David L. "The Interim Division." *Military Intelligence Professional Bulletin* 26, no. 2 (Jul-Sep 2000): 8-12.

Green, Charles J., and James D. Edwards. "III Corps Expands the Knowledge Base for Employing Sensors." *Army Magazine* 50, no. 8 (August 2000): 25-28.

Griffin, Benjamin S., and Archie Davis. "Operation-Centric Warfare: Setting the Conditions for Success at Brigade and Battalion." *Army Magazine* 50, no. 8 (August 2000): 21-24.

Hillen, John. "After SFOR: Planning a European Led Force." *Joint Force Quarterly*, no. 15 (1997): 75-79.

Hoffman, F.G. "Joint Vision 2010: A Marine Perspective." *Joint Force Quarterly*, no. 17 (1998): 32-38.

Krulak, Charles C. "Knowledge Based Warfare: A Security Strategy for the Next Century." *Joint Force Quarterly*, no. 14 (1996): 20-23.

Laporte, Leon J., and Winn Noyes. "Operation-Centric Warfare: The Bold Shift." *Army Magazine* 50, no. 8 (August 2000): 16-20.

Leahy, Peter. "ANZUS: A View from the Trenches." *Joint Force Quarterly*, no. 17 (1998): 86-90.

Makowski, Rick. "EPLRS-More than Just data." *Army Communicator* 15, no. 1 (Winter/Spring 1990): 12-16.

Mehaffy, Michael. "Vanguard of the Objective Force." *Military Review* 80, no. 5 (September-October 2000): 6-16.

Murray, Williamson. "Thinking About Revolutions in Military Affairs." *Joint Force Quarterly*, no. 16 (1997): 69-76.

Owens, William A. "The Emerging System of Systems." *Military Review* 75, no. 3 (May–June 1995): 15–19.

Rauduege, Harry. "Defensive Information Operations: A J-6 Perspective." *Army Communicator* 23, no. 4 (Fall 1998): 55-58.

Rhea, John. "'Infocentric' Warfare Networks Being Built on COTS Base." *Military & Aerospace Electronics* 10, no. 1 (Jan 1999): 19-22.

Thomas, Timothy L. "Kosovo and the Current Myth of Information Superiority." *Parameters* 30, no. 1 (Spring 2000): 13-30.

Thompson, Lauren B. "Military Supremacy and How We Keep It." *Policy Review*, no. 97 (Oct/Nov 1999): 19-38.

Tilelli, John H. Jr. "Putting JV 2010 into Practice." *Joint Force Quarterly*, no. 17 (1998): 76-80.

Wilson, J.R. "Network-Centric Warfare Marks the Frontier of the 21st Century Battlefield." *Military & Aerospace Electronics* 11, no. 1 (Jan 2000): 13-17.

Zimm, Alan D. "Human-Centric Warfare." *U.S. Naval Institute Proceedings* 125, no. 5 (May 1999): 28-31.

Unpublished Works

Allen, Bernal B. "The Non-linear Nature of Information and Its Implications for Advanced Technology Forces." Thesis, Naval War College, 1998.

Barnes, Peter R.. "Command, Control, Communications and Automation needs for the Combined Arms Team." Thesis, Ft. Leavenworth, KS: U.S. Army Command and General Staff College, 1994.

Bornham, Louis G., Michael C. Ingram, and Peter J. Martin. *Information Technology in the Digitized Division*. Fort Leavenworth, KS: TRADOC Analysis Center, 1995, FY 95 Mobile Strike Force Battle Command Experiment.

Brendler, Joseph. "The Stuff that Binds: On the Nature and Role of Information in Military Operations." Monograph, School of Advanced Military Studies, Command and General Staff College, 1995.

Carter, Stuart A. "Pull, Push or Shove: Global Broadcast Service and Intelligence Support to Maritime Forces." Monograph, School of Advanced Military Studies, Command and General Staff College, 1998.

Clappin, William P. "Moving Signals Intelligence From National Systems to Army Warfighters at Corps and Division." Thesis, Ft. Leavenworth, KS: U.S. Army Command and General Staff College, 1998.

Cox, Robert D. "Information Pathology and the Army Tactical Command and Control System (ATCCS): Is ATCCS a Cure?" Monograph, School of Advanced Military Studies, US Army Command and General Staff College, 1990.

Ellis, Admiral James O. "A View from the Top." Briefing, Joint Task Force Noble Anvil, Operation Allied Force, 1999.

Fletcher, Benjamin F. "22nd Signal Brigade Support to Operation Allied Force." Briefing, 27th Signal Regimental Symposium, 1999.

Freeman, Jared T., Marvin S. Cohen, Daniel Serfaty, Bryan Thompson, and Terry A. Bresnick. *Training in Information Management for Army Brigade and Battalion Staff: Methods and Preliminary Findings.*: U.S. Army Research Institute for the Behavioral and Social Studies, 1997, Technical Report 1073.

Graham, Scott E., Patrick K Valentine, and Lee E. Washington. *Enhancing Performance in Light Infantry Digital Tactical Operations Centers*.: U.S. Army Research Institute for the Behavioral and Social Studies, 1997, Report 1709.

Kaiura, Richard G. "Light Infantry Battalion-and-below Battle Command in the Early Twenty-First Century: What Advanced C4I Capabilities are Required and Which Enabling Technologies are Not Being Developed?" Monograph, School of Advanced Military Studies, Command and General Staff College, 1999.

Lasher, William. "HQ EUCOM: A Look Ahead." Briefing, Fort Gordon, GA: 27th Signal Regimental Symposium, 1999.

Premo, Gregory J. "22nd Signal Brigade Support to Operation Joint Endeavor." Briefing, 24th Signal Regimental Symposium, 1996.

Sanderson, Jeffrey R. "General George S. Patton, Jr.: Master of Operational Battle Command, What Lasting Battle Command Lessons can we Learn from him?" Monograph, Ft. Leavenworth, KS: U.S. Army Command and General Staff College, 1997.

Sinclair, Karen L. "Information and the Future of Battle Command." Thesis, Ft. Leavenworth, KS: U.S. Army Command and General Staff College, 1996.

Swinford, Philip L. "Decision Making Implications of Digital Information Systems for the Battalion in Combat." Thesis, Ft. Leavenworth, KS: U.S. Army Command and General Staff College, 1997.

U.S Government Accounting Office. *Tactical Intelligence: Battlefield Automation: Premature Acquisition of the Army's Combat Service Support Control System.* Washington, DC: U.S Government Accounting Office, 1994, Report No. NSIAD-94-51.

Viall, Kenneth E. "Medium Brigade 2003: Can Space-based Communications Ensure Information Dominance?" Thesis, Ft. Leavenworth, KS: U.S. Army Command and General Staff College, 2000.

_____. "Big Blue Arrows: Lines of Information and the Transformation Force." Monograph, Ft. Leavenworth, KS: U.S. Army School of Advanced Military Studies, 2001.

Volz, Richard E. Jr. "An Objective Information Architecture for the Army of the Twenty-First Century: Courting Athena." Thesis, Ft. Leavenworth, KS: U.S. Army Command and General Staff College, 1996.

Woods, David D., and Emily S. Patterson. *Can We Ever Escape From Data Overload?: A Cognitive Systems Diagnosis* National Technical Information Service: Cognitive Systems Engineering Laboratory, Ohio State University, 1998.