Network-Centric Warfare and the Data-Information-Knowledge-Wisdom Hierarchy

Col. Harry D. Tunnell IV, U.S. Army, Retired

EACH TIME PEOPLE use smartphone apps, they are creating a form of digital information unknown to most soldiers less than a decade ago. Today, people produce so much digital information at such a rapid rate that it is physically impossible to store all of it.[1] In 2010 alone, consumers stored more than six exabytes of new data on personal computers (PCs) and other devices—this is 24,000 times the amount of information stored in the Library of Congress.[2] "Big data" are produced somewhere every day, and volumes of data are characteristic of modern combat operations. Soldiers must become experts with systems that manage, manipulate, transform, and analyze data. In the 21st century, tactically relevant information is produced, monitored, and shared in the digital space; commanders must learn to take advantage of data if they are to exercise mission command effectively.

Col. Harry D. Tunnell IV, U.S. Army, Retired, is principal at InRef, LLC, a new media consultancy, and a Ph.D. student in informatics at the Indiana University School of Informatics & Computing. He is a West Point graduate and holds an M.S. in information systems from the University of Maryland Baltimore County. Col. Tunnell's research interests are network-centric warfare theory, military informatics, and secondary user experiences. He has served in combat in Panama, Iraq, and Afghanistan. Col. Tunnell is the sole inventor on two U.S. patents, has written two books for the Army, and has seven vendor and vendor-neutral information technology certifications.

The Department of Defense (DOD) concept for network-centric warfare theory predates the 9/11 terrorist attacks that immersed our nation in its longest war.[3] Before the war, network-centric warfare theory was an important transformational concept, and Congress was briefed about its implementation within DOD. However, the theory was not adopted as the basis for operational doctrine. Rather than emphasizing U.S. advances in technology, doctrine has used European colonial experiences as the underpinnings for the war's counterinsurgency (COIN) doctrine.[4] This represents a missed opportunity.

Network-centric warfare theory is different from other doctrinal frameworks because of how it takes advantage of technological capabilities available only to U.S. forces. The U.S. government has an advantage because other countries simply cannot afford the high level of information technology (IT) investments needed to support network-centric operations. The U.S. government is the largest single purchaser of IT in the world, and out of an approximately $75 billion expenditure in 2011, DOD consumed about half.[5] Network-centric warfare theory promotes myriad technologies that allow U.S. military forces to gain information superiority over an adversary and apply combat power decisively through improved decision making; the networked capability enables these benefits.[6] The IT for such operations is increasingly available in Army formations.[7] The level of IT investment the U.S. government already makes for DOD enables information superiority; therefore, it is unlikely an adversary could counter the advantage gained through network-centric operations. Because neither adversaries nor allies and coalition partners make comparable IT investments, network-centric warfare theory would allow DOD to take advantage of an exclusively U.S. capability.

The U.S. military must overcome resistance to network-centric warfare theory so it can take advantage of its huge IT investments to win wars. Three factors can explain this resistance. First, while adequate individual IT components have been available for more than a decade, only recently have they been integrated sufficiently to create a useful information system (IS) for Army small-unit planning and tactical command and control. (The IS capabilities of other services are beyond the scope of this paper.) Second, analysis of training with digital systems shows that there has not been an accompanying shift in doctrine and work practice (e.g., standard operating procedures) meaningful enough to take full advantage of advances in IT.[8] Based on such reports, one can conclude that 21st-century Army doctrine and work practice remain rooted in the work practice developed for the manual processes, analog equipment, and older digital technologies that contemporary systems have replaced.[9] Consequently, commanders in the field are often using archaic techniques with a cutting-edge IS. Third, many analysts believe the cultural change needed for acceptance of network-centric warfare theory is overdue.[10]

The level of IT investment the U.S. government already makes for DOD enables information superiority…

This paper describes how to integrate a "data-information-knowledge-wisdom" (DIKW) hierarchy into a network-centric-capable IS framework. The hierarchy can help commanders understand how to interact with data in order to convert it into something useful for decision making in combat.

Background of the Network-Centric Warfare Concept

Network-centric operations were considered so essential to DOD transformation before 9/11 that the U.S. Congress, in Public Law 106-398, required the Department of Defense to report on the implementation of the concept.[11] The object of network-centric operations is to take advantage of advances in IT so leaders can improve their speed of command to act decisively against an enemy.[12] A RAND Corporation case study compared the performance of an Army Stryker brigade combat team (BCT), which is a digitally equipped, networked infantry unit, and a non-digital, non-networked U.S. Army light infantry BCT in a training scenario.[13] The case study showed that speed of command for the networked commander was about 3 hours, versus 24 hours for the non-networked commander. The accurate identification of friendly, neutral, and enemy forces was approximately 60 percent better with networking. The networked formation had a 1:1 (friendly:enemy) casualty ratio, while the non-networked force suffered a 10:1 casualty ratio.[14]

Information system theory and Army mission command doctrine describe how an IS does not operate independently of people.[15] An IS consists of equipment that collects, processes, stores, displays, and disseminates information.[16] People use policies, procedures, and communications as they manage and process data to enhance decision making with automation. Network-centric warfare theory frames decision making in terms of four domains of conflict: physical, information, cognitive, and social.[17]

The DIKW hierarchy is a knowledge management structure that helps people make data become meaningful for decision making. The elements of the DIKW hierarchy are—

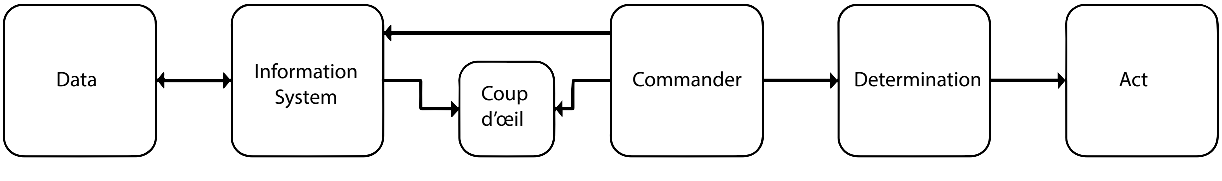
● *Data*: raw, frequently unstructured items apart from context or interpretation.[18] Data are the first link between an IS and the DIKW hierarchy. People use an IS to interact with the data.

● *Information*: data that have been transformed to have meaning for human beings by being organized with specific relationships between the data.[19] Information adds value to a person's understanding about something.[20] People use an IS to perform this transformation.

● *Knowledge*: information that is transformed so it is has patterns and repeatable processes.[21] It is independently useful for decision making. People use an IS to perform this transformation.

● *Wisdom*: the application of intuition to accumulated knowledge applied in a visionary or anticipatory manner.[22] People do not use an IS to create wisdom. Rather, they review knowledge discerned through data-information-knowledge transformations and apply personal intuition to create wisdom.

A 19th-century seminal work on military theory, *On War,* provides the elements that military commanders can use to bind an IS, people, and the DIKW hierarchy together for network-centric operations. The elements are *coup d'œil* and determination. Coup d'œil is the ability of a military commander to quickly make sense of battlefield activity and come to a tactically sound conclusion.[23] Being determined, or resolute, is the courage to accept responsibility and act once a decision is made.[24] Clausewitz's concept for coup d'œil fits well with the framework for creating wisdom; it provides the context for a military-specific type of intuition. In addition, Clausewitz's notion that determination balances coup d'œil by providing the courage to act captures the culminating act of decision making supported by an IS. Coup d'œil and determination together link the DIKW hierarchy to competent, informed tactical decisions in battle and the leader's will to act. The figure illustrates the relationship between a commander, coup d'œil, and an IS in the DIKW hierarchy. The transformations from data to information and from information to knowledge occur with use of the IS. The transformation from knowledge to wisdom only occurs when a commander



Relationship Between a Commander, Coup d'œil, and an Information System

has a well-formed, mature coup d'œil to apply to knowledge during operations.

There is an important note of caution. Coup d'œil and determination work together. It is relatively easy using a modern IS to develop situational awareness, but it is much harder to act, particularly when potential consequences of poor decisions include censure from others or injury and death within the command or to the commander. Clausewitz recognized that competence and the ability to be resolute decrease in some leaders based on the duration and frequency of the leader's exposure to danger.[25] This perspective illustrates the need for caution when advocating for "flattening" decision making.[26] Flattening (reducing middle layers of a hierarchy and giving more autonomy to skilled individuals) is not always wise or possible in a networked environment because the authority to decide or act at certain echelons might be restricted (by law, policy, or other constraints). Furthermore, subordinates may wish to defer decisions to a higher headquarters for a variety of reasons. Finally, ease of analysis is not equivalent to experience when it comes to decision making. Just because technology enhances analysis does not mean it improves coup d'œil—a second lieutenant is still an inexperienced leader regardless of the technology used.

The consequence of poorly developed coup d'œil, as applied to the DIKW hierarchy, can be catastrophic if a commander's poor decision (or indecision) affords the enemy an advantage. Even leaders using the DIKW hierarchy could make errors and poor decisions: as Jay H. Bernstein writes, "folly proceeds from error and exacerbates it."[27] Folly and error can come from overreliance on technology. Networks permit flattening an organization; in business, many consider flattening an organization desirable. However, overreliance on technology can increase opportunities for folly to manifest by increasing the number of people making decisions, especially in military organizations. Commanders should avoid *technology-centric* organizational designs based on the capability and performance of hardware and software. They should avoid decentralizing decision making simply because the technology makes it possible. *Network-centric* operations are human-centered. Network-centered warfare theory provides a framework for military leaders to take full advantage of technology. In this human-centered theory, the success or failure of operations is based on the quality of a commander's action rather than the capabilities of technology.

Intuition, a type of domain knowledge that serves as a personal repository of historical information for decision making, is developed through experience and practice.[28] Coup d'œil is a military-specific form of intuition initially formed through training, but it requires close combat experience to reach full maturity. Moreover, intuition has an important place in the design of technological systems. In intelligent systems research, the notion of "sensemaking" includes a goal of designing systems that allows people to access the intuition of other people.[29] Sensemaking is an element of the social domain within network-centric warfare theory.[30]

Computing and Command and Control

A small number of soldiers in ground combat maneuver units have used PCs on a day-to-day basis since the 1980s. Early PCs typically were found in the operations section and were used for office productivity tasks such as writing orders, preparing presentations, or planning troop movements. They were not networked or employed collaboratively. Tactical command and control were exercised according to an established hierarchy with little lateral situational awareness; they were exercised largely through analog voice communication or personal presence.[31] If information was exchanged with another unit, it was often done via analog voice communication or the physical exchange of map overlays and other materials. In addition, specialized items of digital technology, such as artillery computers, were in use before 1990.

As PCs became increasingly common in the military workplace, concepts for digitizing U.S. Army formations were also evolving. By the 1990 Gulf War, Army tactical units communicated using packet-switched mobile networks that provided secure voice, facsimile, and computer communication services.[32] Today, the Army uses the Army Battle Command System (ABCS) to support command and control. ABCS is a digital system intended to integrate other battle management systems into a comprehensive tactical digital architecture.[33] The system normally is associated with battalion and brigade level; however, components are used at other levels. An example is

The 29th Combat Aviation Brigade deployed its Army Battlefield Command System to Bethany Beach, Del., for annual training, 13-27 May 2010. ABCS is a digital system of networked components that gives commanders a better perspective of their operating environment, assets, resources, and strengths. (U.S.National Guard, Sgt. Thaddeus Harrington)

Force XXI Battle Command Brigade and Below (FBCB2), a ruggedized, PC-size computer that displays the common operational picture, provides position location information, is capable of text communication, and operates on the lower tactical Internet (small unit, terrestrial line-of-sight) and upper tactical Internet (battalion and higher, satellite).[34]

Not all components of ABCS technology are recent developments. For example, FBCB2 predates 9/11. Furthermore, not all elements of ABCS were designed to work together. The battle management systems used by different staff sections, for instance, were developed independently.[35] They were integrated into one IS to support command and control over a period of years. Because of this integration, commanders have had many opportunities to employ formations according to network-centric warfare theory. Unfortunately, one of the shortfalls of ABCS implementation is that institutional and unit training are inadequate. Units frequently rely on contractors for training, limiting the manner in which these digital systems are incorporated into training.[36] These practices are indicative of Army-wide technology resistance.[37]

The difference in capability between legacy command and control tools and a modern tactical IS such as ABCS is enormous. When network-centric warfare theory first was envisioned, the needed command and control systems for Army formations had not been created. Today, the evolution and integration of network-centric capabilities makes it possible to implement network-centric operations. Unfortunately, the intellectual effort necessary to use information-age military tools effectively did not keep up. After 9/11, less offensively oriented military approaches gained ascendency, and a lack of decisive operations was claimed to characterize modern war. The indecisive nature of operations resulted from a *falsely assumed lack* of information superiority that became a common theme of COIN.[38] Because the Army never adopted network-centric warfare theory for conducting operations, it does not have an adequate doctrinal framework to use the superb IT capabilities that reside within every tactical formation.

Network-centric warfare theory is sometimes derided because it is seen as placing too much emphasis on technology, or it is considered unsuitable for COIN and counterterrorism operations.[39] This thinking misses the mark. Network-centric warfare theory is designed to change the perspective about the military use of IT from a platform-centric focus, in which an item of equipment is the centerpiece, to a network-centric focus based on the four domains of conflict.[40] The theory can be applied to any type of military operation—offense, defense, or stability. Furthermore, the idea of network-centric warfare should not be confused with improved speed of command due to better technology, which is a platform-centric notion.

The Army continues to focus on individual equipment as it attempts to digitize operations by introducing more digital technology components rather than unifying how leaders think and fight in the digital space.[41] This leads to capabilities being overlooked. Military technology has advanced to the point that information superiority has been possible for some time.

Some military organizations already have devised means to achieve seamless interservice integration between their combat capabilities. For example, some Army and Air Force units in Afghanistan have integrated their systems (the Army's ABCS, Air Force aircraft systems, and unmanned aerial systems [UASs]) so that pilots and infantrymen can have almost perfect awareness of each other's positions before a fighter aircraft arrives on station.[42] The technology enables leaders to make faster and more informed assessments of the environment before applying coup d'œil and determination. Unfortunately, few leaders recognize the potential that such capability affords soldiers so it remains underutilized.[43]

Applied Network-Centric Warfare Theory

Two vignettes from my experience in Afghanistan during 2009 demonstrate the application of network-centric warfare theory.

Vignette 1. Task Force (TF) Stryker, a Stryker BCT, had recently arrived in Afghanistan and started conducting operations in early August 2009. During the first major offensive mission, TF Stryker elements observed a group of Taliban mining a road at approximately 1900 hours on 1 September 2009 and attacked them with aerial munitions from a UAS.[44] The TF Stryker command group, consisting of the commander and assault command post personnel from the brigade battle staff, were forward at a small combat outpost. The command group observed the attack and commanded follow-on operations from the outpost. The enemy, after the attack, evacuated casualties to an intermediate point, massed additional personnel, and continued to evacuate the most seriously injured to an outpost—a Canadian-advised Afghan police element across the river and outside TF Stryker's area of operations, which provided the highest-quality medical care available. The wounded Taliban were identified by 2100 hours, and the Afghan National Security Forces assumed responsibility for their medical care.[45]

Analysis of vignette 1. The command group relied on a variety of computing devices and multimedia data streams to observe enemy tactics, techniques, and procedures (TTPs) in real time. The command group's equipment included video, Internet chat, radio (digital) voice communication, VoIP (voice over Internet protocol), laptop PCs, position location data, FBCB2, and Land Warrior (a ruggedized wearable computer for infantrymen).[46] Because the command group was located with a Canadian-advised Afghan company, the Canadian advisors provided accurate, timely information from Afghan army and police units. All of these factors contributed to the successful identification and detention of the enemy.

Several enemy TTPs were revealed as a result of the data collected (and transformed into information and knowledge) throughout August 2009 and into September. In fact, by the beginning of September 2009, the IS in TF Stryker had contributed more relevant information about enemy TTPs to BCT-level domain knowledge than combat certification training conducted before the deployment. The data, information, and knowledge discerned during these initial operations would manifest as coup d'œil during subsequent engagements with the enemy. One of the key enemy TTPs the command group now understood was enemy casualty evacuation.

Vignette 2. At approximately 1930 hours on 23 September 2009, intelligence reporting to the TF Stryker command group (located in the tactical operations center) indicated that a Taliban formation was in the TF Stryker area; a retasked UAS found the enemy group, and their location was disseminated to the battalion operating in the area.[47] The enemy was attacked using Army aviation. Because the command group already understood enemy casualty evacuation TTPs, the battle staff was ordered to perform an immediate analysis of how and where the enemy would evacuate their casualties.

The understanding that developed during earlier operations was used to turn the ongoing data-information-knowledge transformations of this engagement into wisdom. Through coup d'œil, the command group understood the enemy would seek out high-quality medical facilities and evacuate casualties quickly over good routes. Enemy casualties were subsequently identified because IS use was guided by this refined coup d'œil.

Analysis of vignette 2. Several months before deploying to Afghanistan, the geospatial engineer section of the battle staff collected data about the terrain and infrastructure of the anticipated area of operations. The data were refined and updated during the first 50 days of combat. After the aerial attack on the enemy, a geographic IS was used to evaluate the data and perform an assessment of where the enemy might evacuate their casualties. Four options were selected; however, they were all outside the TF Stryker area of operations. After approval by the TF Stryker commander, the staff communicated the options via email to TF Stryker liaisons with other coalition units. By midnight, Afghan police, dispatched based on the predictive analysis, identified six wounded enemy fighters at the first predicted location and agreed to take responsibility for them.[48]

Summary of vignettes. Forces seldom find enemy personnel after evacuation from the battlefield because they seldom get feedback about the enemy evacuation channel in time to act. Typically, reports about enemy casualties come through intelligence reporting days, weeks, or months after the event—if ever. A network-centric warfare framework integrated with the DIKW hierarchy and coup d'œil improved decision making during combat based on the BCT's IS output. The integration enabled TF Stryker data and information transformations across the operational area, leading to knowledge that resulted in enemy detention (vignette 1). The framework also enabled accurate prediction because of transformations from knowledge to wisdom, guided by a honed coup d'œil, that the force acted upon in minutes (vignette 2). These experiences demonstrate that the predictive planning and preemption, integrated force management, and execution of time-critical missions envisioned by network-centric warfare theorists are possible.[49]

Conclusion

The framework provided for network-centric warfare theory integrates people, the IS, and traditional military theory. Army forces already have applied such a framework innovatively during real-world infantry combat operations in Afghanistan. Technically competent, courageous, and well-trained soldiers remain important for the successful implementation of network-centric warfare theory. Technology cannot replace the essential and historically significant aspects of traditional military leadership. The integration of network-centric warfare theory with the DIKW hierarchy, coup d'œil, and determination provides soldiers with unparalleled opportunities for knowledge discovery and action in an information-rich environment. This enhances human decision making in the intense, uncertain environment of close combat. ***MR***

NOTES

1. James Manyika, Michael Chui, Brad Brown, Jacques Bughin, Richard Dobbs, Charles Roxburgh, and Angela Hung Byers, "Big Data: The Next Frontier for Innovation, Competition, and Productivity" (McKinsey Global Institute, May 2011), 3-4, <http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation>.

2. Ibid., 3.

3. Arthur K. Cebrowski and John J. Garstka, "Network-Centric Warfare: Its Origin and Future," *Proceedings* 124, no. 1139 (1998), <http://www.usni.org/magazines/proceedings/1998-01/network-centric-warfare-its-origin-and-future>; Department of Defense (DOD), *Report on Network Centric Warfare Sense of the Report*, Arthur L. Money (March 2001), 8, <http://www.dodccrp.org/files/ncw_report/report/ncw_sense.pdf>.

4. Raymond J. Curts and Joseph P. Frizzell, "Implementing Network-Centric Command and Control," report for the *10th International Command and Control Research and Technology Symposium: The Future of C2* (17 March 2005): 4, 16-18, 20-21; John Nagl, "Learning and Adapting to Win," *Joint Force Quarterly* 3rd Quarter, no. 58 (2010): 123-24.

5. CIO [U.S. Chief Information Officer] Council, "A year in Review: Outcomes and Lessons Learned from Implementing Agency-Led TechStat Reviews Across the Federal Government" (Washington, DC: U.S. Government Printing Office [GPO], 8 December 2011), 10; Report of U.S. Chief Information Officer on federal information technology budgets, Steven VanRoekel, "Federal Information Technology FY 2013 Budget Priorities: 'Doing More With Less'" (Washington, DC: GPO, 2012), 4-6.

6. DOD, Office of Force Transformation, *The Implementation of Network-Centric Warfare* (Washington, DC: GPO, 2005): 8; Ang Yang, "Understanding Network Centric Warfare," *Bulletin of the American Schools of Oriental Research [BASOR]* 23(4)(2004): 2-3.

7. Clay Wilson, *Network Centric Operations: Background and Oversight Issues for Congress* (Washington, DC: Congressional Research Service, 2007): 5, 23-26, and 37.

8. Darrell Collins, "Enabling Army Digital Organizations" (Kandahar, Afghanistan: 5/2/ID (SBCT), forthcoming research paper), 5-7; Gregory A. Goodwin and David R. James, *Decision Making With Digital Systems* (Arlington, VA: U.S. Army Research Institute for the Behavioral and Social Sciences, 2009).

9. Ibid.

10. Curts and Frizzell; Thomas P.M. Barnett, "The Seven Deadly Sins of Network-Centric Warfare," *Proceedings* 125, no. 1151 (1999), <http://www.usni.org/magazines/proceedings/1999-01/seven-deadly-sins-network-centric-warfare>; David S. Alberts and Richard E. Hayes, *Power to the Edge: Command … Control … in the Information Age* (Washington, DC: Command and Control Research Program, 2003), 58; Collins, 6-7.

11. Money, 1; DOD, *Network Centric Warfare: Department of Defense Report to Congres*s (27 July 2001), 1-1. <http://www.dodccrp.org/files/ncw_report/report/ncw_main.pdf>.

12. Cebrowski and Garstka.

13. Daniel Gonzales, Michael Johnson, Jimmie McEver, Dennis Leedom, Gina Kingston, Michael S. Tseng, report prepared for the Office of Force Transformation in the Office of the Secretary of Defense, *Network-Centric Operations Case Study: The Stryker Brigade Combat Team* (Santa Monica, CA: RAND Corporation, 2005), 61-99.

14. Ibid., 105.

15. N. Au, Eric W.T. Ngai, T.C.E. Cheng, "Extending the Understanding of End User Information Systems Satisfaction Formation: An Equitable Needs Fulfillment Model Approach," *MIS [Management Information Systems] Quarterly* 32, no. 1 (2008): 44; Army Doctrine Reference Publication (ADRP) 6-0 (Washington, DC: GPO, 17 May 2012), 2-7 to 2-9.

16. ADRP 6-0, 3-10.

17. Office of Force Transformation, 19-20.

18. Jennifer Rowley, "The Wisdom Hierarchy: Representations of the DIKW Hierarchy," *Journal of Information Science* 33, no. 2 (2007): 170-71; Jay F. Nunamaker Jr., Nicholas C. Romano, and Robert Owen Briggs, "A Framework for Collaboration and Knowledge Management," paper presented at the 34th Hawaii International Conference on Systems Sciences (2001), 3; V. Chiew, "A Software Engineering Cognitive Knowledge Discovery Framework," paper published in *Proceedings*: *First IEEE [Institute of Electrical and Electronics Engineers] International Conference on Cognitive Informatics*, *ICCI 2002* (2002): 1.

19. Nunamaker, Romano, and Briggs: 3; Chiew, 1; JP 1-02, 160.

20. Rowley, 171-72.

21. Nunamaker, Romano, and Briggs, 3.

22. Rowley, 174; Nunamaker, Romano, and Briggs, 3.

23. Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1989), 102-103.

24. Ibid., 141-42.

25. Ibid., 103.

26. Alberts and Hayes, 153, 76; Nathan Minami and Donna Rhodes, "Network Centric Operations and the Brigade Unit of Action," paper presented at the 2007 International Conference of the System Dynamic Society and 50th Anniversary Celebration, Boston, MA (2007), 11, 13.

27. Jay H. Bernstein, "The Data-Information-Knowledge-Wisdom Hierarchy and its Antithesis," paper presented at the 2nd North American Symposium on Knowledge Organization, Syracuse University, NY (18–19 June, 2009), 73.

28. Gu Jiajun and Xie Fenghua, "The Empirical Research on the Domain Knowledge Factors Influencing the Effectiveness of Intuition in Decision Making," paper presented at the Second International Symposium on Knowledge Acquisition and Modeling (30 November-1 December 2009), 299; Robert L. Glass, "Intuition's Role in Decision Making," *Software*, IEEE 25, no. 1 (2008): 95.

29. Gary Klein, Brian Moon, and Robert R. Hoffman, "Making Sense of Sensemaking 1: Alternative Perspectives," *IEEE Intelligent Systems* (2006): 70.

30. Office of Force Transformation, *The Implementation of Network-Centric Warfare*, 20.

31. P.F. Sass and L. Gorr, "Communications for the Digitized Battlefield of the 21st Century," *Communications Magazine*, IEEE 33, no. 10 (1995): 87.

32. Ibid., 91; Paul Sass, "Communications Networks for the Force XXI Digitized Battlefield," *Mobile Networks and Applications* 4 (1999): 140, 42.

33. Minami and Rhodes, 3-4; Gonzales et al., 30-36.

34. This is a generalization of the different tactical Internets for command and control. Small units on an increasingly frequent basis have satellite access, and a higher headquarters can use terrestrial line-of-sight systems; Wilson, 33; Gonzales et al., 65.

35. Gregory A. Goodwin and David R. James, *Decision Making With Digital Systems* (Arlington, VA: U.S. Army Research Institute for the Behavioral and Social Sciences, 2009), 1.

36. Ibid., 18, 23; Brooke B. Schaab, J. Douglas Dressel, and Peter B. Hayes, *Training Requirements of Digital System Operators in a Stryker Brigade Combat Team* (Arlington, VA: U.S. Army Research Institute for the Behavioral and Social Sciences, 2005), vii, 8, 13; Collins, 2, 5-9; *Army Digital Education Survey* (Kandahar, Afghanistan: 5/2 ID [SBCT], forthcoming), 7, 10, 21-22.

37. DongBack Seo, Albert Boonstra, and Marjolein Offenbeek, "Managing IS Adoption in Ambivalent Groups," *Communications of the ACM* 54, no. 11 (2011): 72-73; Rhoda C. Joseph, "Individual Resistance to IT Innovations," *Communications of the ACM* 53, no. 4 (2010): 145.

38. Joint Chiefs of Staff, Joint Staff, *Net-Centric Operational Environment Joint Integrating Concept, Version 1.0* (Washington, DC: GPO, 31 October 2005), D-3; Field Manual 3-24, *Counterinsurgency* (Washington, DC: GPO, 2006), 1-3, 1-4, 5-1 through 5-28; Sean Lawson, "Is Network-Centric Warfare (Finally) Dead? Only Partly" in Sean Lawson ICTs and International Affairs Blog, blog entry posted 14 August 2010, <http://www.seanlawson.net/?p=772>.

39. Barnett.

40. Cebrowski and Garstka.

41. A. Borgman, P. Smith, and D. Johnson, "Tools for Enhancing Distributed, Asynchronous Collaboration in Army Operations," paper presented at the IEEE International Conference on Systems, Man, and Cybernetics (October 11-14, 2009), 3530-31.

42. Jared Cox, "Digital Air-Ground Integration, the Future is Here," *Fires* (2010): 16-17; Joseph Turnham et al., "Digital Air/Ground Integration in Afghanistan: The Future of Combat is Here!" *Fires* (2012): 58.

43. Christopher J. Toomey, "Army Digitization: Making it Ready for Prime Time," *Parameters 33*, no. 4 (2004): 43-45.

44. Harry D. Tunnell IV, "Task Force Stryker Network-Centric Operations in Afghanistan," *Defense and Technology Papers* (Washington, DC: Center for Technology and National Security Policy, National Defense University, 2011), 6.

45. Ibid., 7.

46. Ibid., 2-5; Sam Linn, "An assault CP in a Stryker BCT," *Infantry Magazine* (May-August 2010): 24-25.

47. Ibid., 8.

48. Ibid., 9.

49. F. Stein, J. Garska, and P.L. McIndoo, "Network-Centric Warfare: Impact on Army Operations," paper presented at EUROCOMM 2000, Information Systems for Enhanced Public Safety and Security Conference (2000), 291-92.