No. 3
March 2016

The Mitchell Forum

Leading in the 21st Century: The Network Centric Challenge

Col Herbert C. Kemp, Ph.D., USAF (Ret.)

About the Forum

The Mitchell Forum exists to give an open venue to authors with ideas and thoughts on national defense and aerospace power. The series features topics and issues of broad interest and significant impact to current and emerging policy debates. The views expressed in this series are those of the author, and not necessarily those of the Mitchell Institute.

Abstract

The transition of military organizations from the industrial age to the information age has been a process of fundamental transformation, and one that is occurring at an accelerated pace— faster even than previous technology driven transformations, such as the use of aircraft and wireless communications.

As the US military and other militaries cope with these changes, they are moving toward "network centric" operating constructs that require changes in both organizational and leadership models to maximize the information potential of networks. But industrial militaries operate almost entirely within modernist organizational models, whereas information age militaries exhibit elements of both modernism and postmodern models and ideas. These developments hold great importance for future military and intelligence operations, and the conduct of modern wars.

This paper looks back and examines the evolution of military organizations from the industrial age to the information age, and assesses the implications of this transition for both organization and leadership in military operations of the 21st century.

Introduction

Journalist and author Frances Cairncross first coined the phrase "the death of distance" in a 1995 article in *The Economist*, elaborating on it further in her 1997 book.[1] Her theme focused on the impacts of the revolution in communications in erasing borders, and removing geographical distance as a factor in international business and international affairs. Cairncross wrote on these issues during a period of rapid expansion of the Internet and amidst an awakening of the tremendous potential power of information. With near instantaneous communications made possible virtually anywhere on the globe, it was becoming clear that if two people did not need to exchange some physical artifact, it mattered not whether one of the two was in the next room or on another continent. With this rapid improvement in global communications, the sheer volume of information exploded and the near instantaneous velocity of information often resulted in significant compression of traditional decision cycles.

The convergence of instantaneous global communication, exponential increases in the volume and velocity of information, and the resulting compression of decision cycles have combined to produce the so-called "network centric environment."

The convergence of instantaneous global communication, exponential increases in the volume and velocity of information, and the resulting compression of decision cycles have combined to produce the so-called "network centric environment."[2] Just as these and related phenomena have affected the way nations and societies conduct business, politics, science, and the arts, they have also affected the way our military establishment, and our intelligence enterprise, conduct warfare and operations.

The Network Centric World

The network centric enterprise arises from the combination of extensive computing power and ubiquitous networked communications. This network enables competitive sensing of the environment, the establishment of virtual organizations capable of collaboration in real time, and the creation of highly efficient value chains.[3] In parallel with the rapid expansion of information technology and the network, the level of complexity has also increased at an accelerating rate. "Current developments in communications and information technology have created operations where our technologies and processes are highly integrated," Shah Selbe observed in 2009.[4] As a result the impact of technology on organizations, their processes, and their people has become more pronounced in the network centric world. Selbe goes on to note that the power of network enabled capabilities far exceeds the capability of the original networked infrastructure, and offers the ability for expanded collaboration and distributed decision making. As a result, an environment is created "for resolving established problems that were, at one time, insolvable."[5]

The Evolution from Industrial Age Warfare to Information Age Warfare

For centuries, the ability of a commander to lead military forces in battle was limited by line of sight or by the limited distances cavalry could scout ahead of the main force. Even after the introduction of industrial age warfare (beginning with trains and telegraphs in the US Civil War) and extending to the dawn of flight and the advent of wireless communications in the early 20th century, this paradigm shifted very little. Conducting military operations required physical proximity.

Even well into the late 20th century, military units typically deployed to battle as essentially self-contained units. What was needed was brought with the unit. Long haul communications connected them to the rear and back to the US, but everything needed for combat, both physical assets and information assets, came with the unit. As a result, these organizations required highly centralized planning to organize and decentralized execution to account for ambiguity. However, this methodology also creates seams that can result in information loss and often suffer from a lack of flexibility when the unexpected occurs.[6]

Following the Gulf War in 1991, computing and communications technology had advanced sufficiently in terms of both capacity and reliability that it became militarily feasible to begin to

Following the Gulf War in 1991, computing and communications technology had advanced sufficiently in terms of both capacity and reliability that it became militarily feasible to begin to rely on rear elements for substantial information requirements …

rely on rear elements for substantial information requirements to support forward combat operations. This also enabled a gradual reduction in the size of forward deployed command elements. Thus the concept of "reachback" entered military parlance, becoming a new way of doing business.[7]

The reachback concept quickly evolved to the more advanced concept known as "distributed operations," in which geographically dispersed elements are operationally synchronized through communications networks to achieve a specific effect in the operational area. This was an important distinction when comparing distributed operations to reachback. Whereas in the case of reachback, forward organizations were able to access information held in the data bases of organizations back home, the deployed units did not necessarily control the way in which the databases were populated or the priorities to which the stateside units operated. With the concept of distributed operations, the organizational construct changed and virtual organizations operating at multiple locations could come under the command and control of overseas units, via the network.

In the case of the Air Force the result was a globally distributed network of ground stations, to process sensor data in real time from aircraft flying anywhere in the world. It became possible for a ground commander in Afghanistan to communicate with a remotely piloted aircraft unit in Nevada, whose full motion video (FMV) was being exploited in real time by a Distributed Common Ground System (DCGS) ground station in Virginia, all under the command of a Combined Air and Space Operations Center (CAOC) in the US Central Command area of responsibility.[8] Kinetic effects still needed physical proximity in this paradigm, but the information could be sent anywhere, and the powerful enabler was the network.

The concept of network centric warfare emerged in the mid-1990s as the efficacy of distributed systems was proved in support of ongoing operations around the world. The emerging capability was seen as a true paradigm shift, as seismic as the invention of gunpowder or the airplane.[9] Every aircraft, ship, and tank had the potential to become a node in the network, and the capabilities produced were seen as a revolution in military affairs.[10] This offered the possibility of much greater agility in responding to situations in the theater of operations, the possibility for emergent planning rather than centralized preplanning, and the potential for much greater economy of force through improved precision in the generation of operational effects.[11]

As the power of the network emerged, it was also becoming clear that the cyberspace where the network operated was, itself, becoming an operational domain, albeit manmade.[12] As a measure of just how profound this shift was, the United States Air Force added cyberspace as a third operational domain, in addition to air and space, in which it must achieve superiority in combat.[13] As the US has grown ever more reliant on the network for military operations (and, for that matter, commercial operations), the network has also increasingly come under attack from individuals, non-state actors, and state-sponsored entities. The bar for entry into cyber war is relatively low. Anyone with a computer, Internet access, and reasonable computer skills can enter the fray. It should come as no surprise that the current conflicts involving terrorism are being fought, at least in part, through the network. This is an asymmetric challenge to the technological superiority of industrialized nations, and one that is difficult to counter.[14] Cyber war has become a daily fact of life for the operators of military networks; these cyber attacks can have results ranging from penetration of networks, to theft or corruption of data and even potential denial of service in the networks.[15] Defending the network has become as important a military function as defending the nation's airspace.

Organizational Implications

Command and control (C2) in an industrial age military organization closely follows a modernist theory model, as described by Mary Jo Hatch.[16] It relies on rational decision-making on the basis of observable data, is hierarchical in nature, and op-

erates on the basis of deeply ingrained norms and values. "Industrial Age military organizations use simple, often linear command and control mechanisms," David Alberts and Richard Hayes observed.[17] Centralized planning is a principal artifact of industrial age command and control and, in execution, leads to specialized organizations that do not necessarily share information with each other. Organizational processes, structures, and equipment are designed to optimize the performance of the unique missions of each unit and this may not translate into the ability to collaborate or interoperate with other units having different specialized missions. This works well for industrial age warfare but is less adaptable to information age warfare.[18]

The US military has undergone previous technology-driven transformations, but organizational adaptation has typically lagged the advent of new technology. Cavalry, for instance, remained in use well after the introduction of motorized vehicles and tanks. RAND's Carl Builder argued that the real question to address was not how to adapt new technologies to the existing enterprise but, rather, how to adapt the enterprise to the new technologies.[19] He distinguished the concept of "enterprise" from the usual list of missions, roles, and objectives, defining the use of the term as being "in the business sense of the *primary purposeful activity* of an organization."[20] Writing just before the millennium, Builder accurately foresaw a future in which conflict with non-state actors would move to center stage, and in which the information sphere would be a principal venue for 21st century conflict.

The US military has undergone previous technology-driven transformations, but organizational adaptation has typically lagged the advent of new technology.

The need for organizational change to adapt to the information age has been advocated since the 1990s. While network centric warfare was enabled and driven by technology, the fundamental factor in success would be the degree to which humans could organize to operate in the new environment.[21] In 1997, RAND researchers John Arquilla and David Ronfeldt noted the evolution of networked models in the private sector, and advocated a similar evolution for military organizations.[22] Similar to Builder's views, Arquilla and Ronfeldt advocated adaptation as well. They did not, however, recommend an abandonment of hierarchy. Noting that hierarchy had been eroding long before the arrival of the information age, Arguila and Ronfelt argued that the successful path would be one that constructed a hybrid organization that integrated hierarchy with networked organizational models. This might involve a flattened chain of command employing smaller networked maneuver units capable of rapidly concentrating on a specific objective coordinated through the network.[23] In the final analysis, this is essentially the path the US military has followed.

Although no one rules out conventional war between nation-states, the concept of post-modern war and, in the case of Ukraine so-called "hybrid warfare," has taken hold with profound organizational implications. Chris Gray argued that the information age transformation, unlike previous transformations, has greater potential to be continuous as opposed to the more clearly demarcated periods of earlier transformations.[24] He is careful to note, elsewhere, that information effects do not replace kinetic effects—that war is in the end, almost always physical. But Gray emphasizes that information is the underlying foundation of post-modern war and, as such, is also a potential asymmetry in a multi-polar world involving both nation-states and non-state actors. The challenge for the military organization, then, is to adapt in ways that allow for greater flexibility in dealing with emerging situations involving asymmetric capabilities, a radical departure from the modernist force-on-force model of the 20th century.

Alberts and Hayes advocated the concept of "edge organizations," that is organizations that could successfully transfer their decision making to the edges of their network rather than act from the center.[25] In some important aspects, the edge organization resembles the post-modern or post-industrial organization described by Hatch, in that it is flatter, less hierarchical, and boundary-less (at least internally). Alberts and Hayes also observed:

> An edge organization encourages appropriate interactions between and among any and all of its members. Its approach to command and control breaks the traditional C2 mold by decoupling

> command from control. Command is involved in setting the initial conditions and providing overall intent. Control is not a function of command but an emergent property that is a function of the initial conditions, the environment, and the adversaries.[26]

As a result, edge organizations may be less efficient in the performance of familiar, repetitive tasks, but could offer greater agility to perform non-routine tasks and possess a better ability to innovate.

Leadership Implications

For military organizations accustomed to hierarchical leadership models suited to industrial age warfare, the imperative to move to a more networked (post-modern) leadership model is both urgent and culturally difficult. As noted above, moving to a networked organization does not necessarily eliminate hierarchy, but it does decentralize decision-making, empowers units at the edge of the network and potentially decouples command from control. Just as with earlier transformations, the mindset and the organization may lag the technological transformation.

For military organizations accustomed to hierarchical leadership models suited to industrial age warfare, the imperative to move to a more networked (post-modern) leadership model is both urgent and culturally difficult.

Alberts and Hayes cited an experiment in which two groups were asked to solve the same problem. One group was hierarchical and the other group was arranged as a circle. The hierarchy was faster. However, in the circle different individuals assumed the role of leader as they worked through the problem and the circle learned faster – it proved to be more capable of solving complex problems than the hierarchy. This becomes important in understanding concepts of fixed leadership compared to emergent leadership. In the experiment described above, the fixed leader was at the head of the hierarchy and was able to respond faster to a familiar problem. However the circle produced emergent leadership, similar to that required for an effective networked organization, and this, according to Alberts and Hayes, "…explains why it is possible for a network-centric organization to self-synchronize rather than be aimless or incoherent, as some have feared."[27] The ubiquitous presence in the network allows the leader to emerge for the task at hand by virtue of positioning, capability or other factors. If viewed in light of the decoupling of command from control described above, it is the command from the hierarchy that informs all members of the organization of the desired end state (in military terms understanding the commander's intent), but the control devolves to the individual leaders in the network to self-synchronize to lead and execute the tasks as they emerge.

The leadership implications for networked military organizations are, in many ways, not unlike the leadership implications for networked commercial organizations. In asking the question, "What factors contribute to effective leadership in virtual team environments?" Timothy Kayworth and Dorothy Leidner sought to fill a void of empirical research in this area of leadership in a 2001 paper.[28] Some of the challenges they listed in their study have less relevance to military organizations than to commercial ones. For example, different time zones were listed as a factor, which tends to be a marginal issue at best in military organizations. However, other challenges are common to the military environment as well, such as the reduction in communications content when compared to face-to-face communication, cultural miscues (such as working in a coalition environment) and greater difficulty in building trust with people whom one has never met.

According to Kayworth and Leidner, early behavioral approaches to leadership "suggest that effective leaders are those who engage in two basic activities: initiating structure and consideration."[29] In their study, those leaders who attended to these two activities were rated as more effective. Translated into a networked military environment, it is likely that commander of a unit in a distributed network will have face-to-face contact with his/her own unit but will be in a networked relationship with headquarters and other surrounding units. Hence, when taking on the task of emergent leader, it would be necessary to provide structure for other networked units that would be needed to support the emergent leader and it would be incumbent upon the emergent leader to be sufficiently attentive to the other members of the network to ensure their understanding and preparedness to support the task.

As militaries grapple with the need to train and educate their leaders to operate in a post-modern world, establishing common terms of reference presents another potential leadership challenge.

As militaries grapple with the need to train and educate their leaders to operate in a post-modern world, establishing common terms of reference presents another potential leadership challenge. Industrial age militaries are almost purely modernist organizations. Information age militaries, on the other hand, are still evolving and reflect attributes of both modernism and post-modernism.

Clearly, modern military organizations in general, and the US military in particular, are in a transformational period spurred on by the post-modern world. This is driven by two major trends: the onslaught of the information age, and the new multi-polar world order. As with most major technology-driven transformations, the changes in the military organization are lagging the technology transformation, but the rate of adaptation at this stage appears to be quicker than with previous periods of transformation. In order to cope with these changes, and to keep pace with potential adversaries who can employ information age technologies as an asymmetric capability, military organizations must transform into more network centric organizational models that more closely reflect the post-modern world in which they will need to operate.

Conclusions

Modernism has, for many centuries, been the organizational paradigm for industrial military forces. While hierarchy remains, hybrid organizations are now in existence that exhibit characteristics of both modernism and post-modernism and feature empowered leaders throughout the network, capable of independently responding and acting on the commander's intent without the need for close centralized control throughout the operation.

While it cannot be said that modern militaries are post-modern organizations (and likely never will be), it is clear that post-modern attributes abound in the paradigm of network centric warfare. The flattening of organizational hierarchies has reduced the level of centralized control while the velocity of information in the network has necessitated the delegation of authority to act to the far-flung edges of the network and away from the center. This has produced an unintended democratizing effect on the military operation as a whole; empowerment of the individual is very much a post-modern idea.

Furthermore, the network centric world is an entirely manmade environment—it is a constructed reality. While much of the data in the network is intended to represent artifacts in the physical world, much of what exists in the network exists only in the network. Warriors in the network centric environment are constantly deconstructing and reconstructing their virtual environments in an effort to stay ahead of the opposition. The information age military has, perhaps unintentionally, backed into another post-modern paradigm. The parallels are likely to continue–this evolution into the information age has not reached its end state.

Footnotes

1 Cairncross, F., (1997). *The Death of Distance: How the Communications Revolution Will Change Our Lives.* Harvard Business School Press, Boston, MA.

2 Alberts, D., Garstka, J., & Stein F., (1999). *Network Centric Warfare: Developing and Leveraging Information Superiority, 2nd Edition (Revised).* DoD C4ISR Cooperative Research Program, Department of Defense, Washington, DC. Available at: http://www.carlisle.army.mil/DIME/documents/Alberts_NCW.pdf

3 Ibid

4 Selbe, S., (2009). Future Systems Engineering and The Role of Complexity. *World Future Review, Vol 1, Issue 2.* Retrieved from Business Source Complete.

5 Selbe, p.45

6 Alberts, D., & Hayes, R., (2003). *Power to the Edge: Command and Control in the Information Age.* DoD Command and Control Research Program, Center for Advanced Concepts, Department of Defense, Washington, DC Available at: http://www.dodccrp.org/files/Alberts_Power.pdf

7 Britten, S., (1997). Reachback Operations for Air Campaign Planning and Execution. Center for Strategy and Technology, Air War College, Maxwell AFB, AL. Retrieved from: http://www.au.af.mil/au/awc/awcgate/cst/csat1.pdf

8 Deptula, D., & Marrs, J., (2009). Globally Distributed ISR Operations. *Joint Force Quarterly,* 3rd Quarter, Issue 54. Retrieved from Business Source Complete.

9 Ferris, J., (2004). Netcentric Warfare, C4ISR and Information Operations: Towards a revolution in military intelligence? *Understanding Intelligence in the Twenty-First Century: Journeys in the Shadows.* Retrieved from Business Source Complete.

10 Robinson, T., (2010). It's the Network, Stupid! *Military Technology, Vol 34 Issue 2*, Retrieved from Business Source Complete Database.

11 Ibid, Ferris.

12 Ibid. Alberts, Garska and Stein.

13 USAF, 2010.

14 Featherstone, M., (2008). The State of the Network: Radical Anxiety, Real Paranoia and Quantum Culture. *Journal for Cultural Research*, Vol 12 Issue 2. Retrieved from Business Source Complete.

15 Ibid, Ferris.

16 Hatch, M. (with Cunliffe, A.), (2006). Organization Theory. Oxford University Press, Great Clarendon Street, Oxford, UK.

17 Ibid, Alberts and Hayes, p.49.

18 Ibid.

19 Builder, C., (1999). The American Military Enterprise in the Information Age. In Khalilzad, Z. & White, J., (Eds). *The Changing Role of Information Warfare*. RAND, Santa Monica, CA.

20 Ibid, p.28

21 Ibid. Alberts, Garska and Stein.

22 Arquilla, J. & Ronfeldt, D. (1997). *In Athena's Camp: Preparing for Conflict in the Information Age.* RAND Corporation, Santa Monica, CA. Available at: http://www.rand.org/pubs/monograph_reports/MR880/

23 Ibid

24 Gray, C., (2007). Postmodern War at Peak Empire. *Science as Culture, Vol 16, Issue 2.*

25 Alberts, D., & Hayes, R., (2003). *Power to the Edge: Command and Control in the Information Age.* DoD Command and Control Research Program, Center for Advanced Concepts, Department of Defense, Washington, D.C., http://www.dodccrp.org/files/Alberts_Power.pdf.

26 Ibid. pg. 216-217.

27 Ibid. pg. 184.

28 Kayworth, T., & Leidner, T., (2001). Leadership Effectiveness in Global Virtual Teams. Journal Management Information Systems, 18(3), 7-40.

29 Ibid. pg. 26.

About The Mitchell Institute

The Mitchell Institute educates the general public about aerospace power's contribution to America's global interests, informs policy and budget deliberations, and cultivates the next generation of thought leaders to exploit the advantages of operating in air, space, and cyberspace.

About the Forum

The Mitchell Forum series is produced and edited by Marc V. Schanz, Mitchell Institute's director of publications. Copies may be reproduced for personal use. Single copies may be downloaded from the Mitchell Institute's website. For more information, author guidelines, and submission inquiries, contact Mr. Schanz at mschanz@afa.org or at (703) 247-5837.

About the Author

Col Herbert C. Kemp, Ph.D., USAF (Ret.), served for 28 years as an Air Force intelligence officer. His assignments included command, staff, and diplomatic tours with service in Asia, the Middle East, Europe, and Latin America. In his last assignment, prior to retirement in 2001, Kemp served as deputy director for surveillance and reconnaissance, Headquarters Air Force, Pentagon, Washington, DC. He is currently the president and CEO of OneALPHA Corporation in Herndon, VA.