1. Report Security Classification: UNCLASSIFIED

2. Security Classification Authority:

3. Declassification/Downgrading Schedule:

4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

5. Name of Performing Organization:
JOINT MILITARY OPERATIONS DEPARTMENT

6. Office Symbol: C	**7. Address**: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207

8. Title (Include Security Classification):

Cyberspace—A New Medium for Operational Warfare

9. Personal Authors:
Kevin L. Achterberg, LCDR, USN

10.Type of Report: FINAL	**11. Date of Report**: February 3, 2003

12.Page Count: 21 **12A Paper Advisor (if any):**

13.Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. Ten key words that relate to your paper:

Cyberspace, Information Operations, Information Warfare, Computer Network Attack / Defense, NCW

15.Abstract:

Transformation to the information age will give rise to a new medium for operational warfare—cyberspace—just as the industrial age ushered in the new mediums of air and sea (in particular, undersea). Cyberspace (and corresponding information warfare and operations) will take its place next to air, land and sea as a fourth medium that the joint operational commander will have to consider in applying Operational Art across all levels of war generally and at the operational level of war specifically.

16.Distribution / Availability of Abstract:	**Unclassified** X	**Same As Rpt**	**DTIC Users**

17.Abstract Security Classification: UNCLASSIFIED

18.Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT

19.Telephone: 841-6461	**20.Office Symbol:** C

NAVAL WAR COLLEGE
Newport, R.I.

CYBERSPACE—A NEW MEDIUM FOR OPERATIONAL WARFARE

by

Kevin L. Achterberg
Lieutenant Commander, USN
February 3, 2003

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Joint Military Operations (JMO) Department.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: ______________________________

TABLE OF CONTENTS

Section Page

Introduction…………………………………………………………………. 1

The Threat is Real………………………………………………….............. 3

Cyberspace vs. Operational Art……………………………………………... 5

Cyberspace and the Operational Level of War……………………………… 7

Cyberspace: The Tie that Binds…………………………………………… 10

Holistic Approach to Developing and Fighting in Cyberspace…………….. 12

Conclusions………………………………………………………………… 14

Recommendations………………………………………………………….. 15

Bibliography……………………………………………………………… 17

Cyberspace: The virtual space created by computer systems and the networks that link them.[1]

"Cyberspace is no longer science fiction. Today, networked information systems transport millions of people there to accomplish routine as well as critical tasks. And the current trajectory is clear: increased dependence on networked information systems. Unless these systems are made trustworthy, such dependence may well lead to disruption and disaster."[2]

Introduction:

Transformation to the information age will give rise to a new medium for operational warfare—cyberspace—just as the industrial age ushered in the new mediums of air and sea (in particular, undersea). Cyberspace (and corresponding information warfare and operations) will take its place next to air, land and sea as a fourth medium that the joint operational commander will have to consider in applying Operational Art across all levels of war generally and at the operational level of war specifically.

In order to meet the increasingly complex and asymmetric challenges that are emerging in an era of increasing globalization, technology proliferation, and regional instability (driven by population growth, resource scarcity, and inequitable wealth distribution), the U.S. military is in the process of transforming from an industrial age force, which is focused heavily on using superior technology, highly centralized command and control, concentrated forces and massive firepower to meet the bipolar threats of the Cold War, to an information age force that leverages information superiority to enable widely distributed forces guided by decentralized command and control to deliver tremendously lethal *and/or* non-lethal combat power across the information age battlefield. "Bombing them into the stone age" is transforming into "striking at precisely the right time and place". Standoff high power sensing is transforming into up close

[1] Kenneth M. Morris, User's Guide to the Information Age, New York, NY: Lightbulb Press, 1999, p. 8.
[2] Fred B. Schneider, Trust in Cyberspace, Washington, D.C.: National Academy Press, 1999, p. 11.

and personal sensing of the target or area of interest. Command and control at the "headquarters" is transforming into command and control provided through the network. Small numbers of expensive, relatively non-maneuverable and highly capable multi-mission platforms are transforming into larger numbers of relatively inexpensive "combat expendable" modular instruments that are tailored to the mission and that gain their combat power through distribution and unprecedented levels of information gathering, fusing and sharing.

These are but a few of the numerous transformation efforts that will continue to pervade our war fighting philosophy in the months and years that lie ahead. The bottom line is that as technology and regional instability continue to proliferate around the globe, our current comparative technological advantage will continue to diminish in the face of the exponentially increasing aggregate complexity of the future security environment. As a result, U.S. military forces must continue to increasingly focus on information age capabilities to maintain and extend their current comparative advantage. Information age warfare will see air, land and sea superiority joined in importance by information superiority and unfettered access and freedom of maneuver in cyberspace. Hence, Joint operational commanders and the forces under their cognizance will become increasingly reliant on information networks and the cyberspace medium to accomplish their operational and tactical objectives, as shown in Afghanistan where generals and admirals were much more likely to comment on bandwidth than bombs.[3]

Cyberspace is the underpinning foundation upon which these new advantages have been and will continue to be built. However, as Clausewitz teaches us, enemy interaction will undoubtedly focus on exploiting the critical vulnerabilities that may be present in this new and relatively untested battle space. Here in lies the problem. By failing to cull out cyberspace as a

[3] Vernon Loeb and Thomas Ricks, "1's and 0's Replacing Bullets in U.S. Arsenal," Washington Post, February 2, 2002.

separate and distinct medium, the Defense Department and its Joint forces operating forward are ill equipped and not organized, trained or educated to consider the cyberspace medium in the deliberate or crisis action planning process, or to fight and win the war in cyberspace, both of which will be required to maintain the momentum in battle in information age warfare. Furthermore, the far reaching system of networks, operating independently or through the Internet, will increasingly include mobile nodes that communicate wirelessly while in close proximity to the enemy. Our current organizational and operational approaches to securing these networks in the face of the adversary is rooted in an industrial age mindset that creates a potential seam through which a perceived inferior adversary can reduce or eliminate our advantage while simultaneously gaining his own.

The Threat is Real

"Many of the countries whose information warfare efforts we follow realize that in a conventional military confrontation against the U.S., they cannot prevail. These countries recognize that cyber attacks against civilian computer systems in the U.S. represent the kind of asymmetric option they will need to 'level the playing field' during an armed crisis against the United States."[4] This quote succinctly describes the motivation for and potential impact of our adversaries undertaking a cyber warfare campaign against civilian networks. Given the ongoing work in the establishment of the Defense Information Infrastructure (DII), it follows that U.S. military networks will increasingly become prime targets as traditional tightly integrated and closed systems are phased out and replaced by open systems that depend upon the common network infrastructure for their successful employment. Moreover, as these networks, which

[4] George Tenet, U.S. CIA Director, quote from prepared remarks made to Senate Governmental Affairs Committee, <http://www.cia.gov/cia/public_affairs/speeches/archives/1998/ dci_testimony_062498.html>, June 24, 1998.

support such vital operational functions as command and control (including collaboration), command and control warfare, logistics, fires, and intelligence, become more and more essential to Joint operations, the veracity by which potential adversaries seek to exploit this source of advantage will increase precipitously.

In particular, "China appears interested in researching methods to insert computer viruses into foreign networks as part of its overall information operations strategy,"[5] and some reports suggest the Chinese military plans to elevate IW to a separate service on par with its army, navy and air force. This would include detachments of network warriors organized into "shock brigades," which will be used to employ high-powered microwave and other directed energy weapons to take the offensive initiative in cyberspace.[6] Similarly, it must be assumed that other countries such as Iraq, Iran, North Korea and Russia, to name a few, are also aggressively pursuing cyberspace capabilities of their own.

In addition to the clear and present danger presented by these state-sponsored activities, many non-state actors, each with their own agenda, also pose a significant threat to our freedom of action in cyberspace. These actors include terrorist groups, terrorist sympathizers and anti-U.S. hackers, and thrill seekers.[7] Attacks launched by these groups can be equally as devastating, especially to systems that leverage the publicly accessible global connectivity of the Internet.

Finally, the malicious insider poses perhaps the most serious risk of all. The insider possesses access to and an understanding of the critical network infrastructure that is being used

[5] U.S. Defense Department FY2000 Annual Report to Congress on the Military Power of the People's Republic of China, Defense Link < http://www.defenselink.mil/news/Jun2000/china06222000.htm>, June 2000, section C, paragraph 1.(c).

[6] Willliam Arkin and Robert Windrem, "The U.S.-China Information War", MSNBC.com <http://www.msnbc.com/news/607031.asp>, August 19, 2001.

in the battle space. Insiders are extremely difficult to detect in our current lexicon of network defense, and therefore can potentially cause catastrophic consequences across all levels of warfare. For example, by interjecting a simple worm virus on the inside of a networked system, the area of cyberspace being relied on for one or more operational functions could be denied for an extended period of time.

Cyberspace vs. Operational Art

The mud slinging over the impact that all of this 'networking' will have on the employment of operational art (OpArt) is seemingly endless. Daily newspaper articles and monthly professional journals are consistently littered with conjecture on these two subjects. Proponents of OpArt claim that network centric warfare (NCW), which is the Navy's concept for how it will wage information age warfare, is not a decisive form of combat,[8] and warn that putting all of our eggs in the NCW basket is a risky proposition that may cause us to unwittingly culminate.[9] On the other side of the argument are those that purport NCW will render OpArt obsolete.[10] While all of this bantering back and forth makes for interesting reading, it actually does little more than confuse the majority of the audience it is trying to reach. The number of government and defense personnel that understand either OpArt or NCW, let alone both, is staggeringly small. Furthermore, NCW is as of yet an unproven concept; therefore, attempting to comment on its true impact on warfare is of little more than speculative value.

[7] Michael A. Vatis, "Cyber Attacks during the War on Terrorism: A Predictive Analysis," Institute for Security Technology Studies at Dartmouth College, <http://www.ists.dartmouth.edu/ISTS/counterterrorism/ cyber_a1.pdf> September 22, 2001, p. 1.

[8] Dr. Milan Vego, "Net-Centric Is Not Decisive," U.S. Naval Institute Proceedings, January 2003, p. 57.

[9] David M McFarland, Monty Ray Perry, and Steven R Miles, "Joint Operational Art Is Alive," U.S. Naval Institute Proceedings, October 2002.

[10] CDR Erik J. Dahl, "Network Centric Warfare and the Death of Operational Art," NWC JMO Department Publication 1012, Winter Trimester, 2002-3.

Looking at the situation from a more realistic point of view, it is clear that networks and the influence of cyberspace are here to stay, and while this fact may result in a substantial reduction in the fog and friction of war, it will never eliminate them completely. Space and force considerations such as enemy interaction, weather, and terrain will continue to keep these two demons alive and well in future conflict. Therefore, OpArt will continue to provide essential utility at the strategic, operational and tactical levels and across the spectrum of conflict from peace to war. However, the current body of OpArt and its implementation must be expanded to include cyberspace considerations. Current reference and teaching materials on the subject fail to distinguish cyberspace as a medium to be considered in the practice of OpArt. For example, the most widely used OpArt text in today's Joint Professional Military Education (JPME) is Dr. Milan Vego's Operational Warfare, which contains nearly 700 pages of material covering the concept of OpArt in great detail. However, the material presented is almost exclusively focused on an industrial age implementation, with only a handful of pages devoted to discussing potential information age implications.

This has tremendous ramifications for two reasons. First, JPME students are not learning to apply OpArt to the information age; and second, a large portion of our Joint Doctrine is written by these same JPME graduates and therefore does not incorporate information age values and concepts. As a result, we continue to spin our wheels in the mud of the industrial age, and progress toward meeting the transformation goals set forth by the Secretary of Defense[11] is slow and painstaking. In doing so, we lose precious time, which, ironically, as Dr. Vego points out, can never be recovered.[12] Because of this, we risk military obsolescence as both current and

[11] David A. Denny, "Rumsfeld Sees Urgent Need to Transform the U.S. Military," The Information Warfare Site <http://www.iwar.org.uk/news-archive/2002/military/01-31-02.htm>, January 31, 2002.
[12] Dr. Milan N. Vego, Operational Warfare, Naval War College JMO Publication NWC 1004, 2000, p. 47.

potential future adversaries rapidly gain advantage precisely by their *lack* of legacy systems, legacy assets, and a legacy mindset.[13]

A good example of this mindset and how it applies to a cyberspace medium application of OpArt is our current approach to information assurance (IA), which is essentially keeping the bad guys out of our area of cyberspace. The current IA strategy is centered on the notion of defense-in-depth. This concept involves building several layers of protection between the networks access points and the inside of the system, and is very similar to the approach we take in the physical world to protect individual units operating forward. In the world of networks, firewalls and access procedures are layered on one another to keep unauthorized users out of the system. The trouble with this approach, which also mirrors that of the physical world, is that a determined attacker (or malicious insider, who by definition is already 'inside') will eventually find a way to penetrate the layered defense scheme and wreak havoc on the network and/or the information contained within it. The principle difference between the real and virtual worlds has to do with the scope of damage that a single successful attack can inflict. In the real world, a successful attacker may take out a single or small group of units operating in close proximity to on another, while in the virtual world, the entire network and all of the information and functionality it provides is at risk. Therefore, the defense in depth scheme that serves us so well in the physical world is not the ideal approach in the virtual world. This is only one of a large number of important space considerations of the cyberspace medium that must be taken into account by the Joint operational commander.

Cyberspace and the Operational Level of War

[13] Evans & Wurster, Blown to Bits (Boston, MA: Harvard Business School Press, 2000), pg. 6

In addition to the OpArt vs. NCW argument outlined above, there is also a constant consternation over how the operational level of war will be affected with the advent of "everything being networked". The operational level of war focuses on employing military forces to achieve theater-strategic objectives through the planning, preparation and execution of a single campaign consisting of a series of sequenced and synchronized tactical actions.[14] Again, different camps have emerged on what the impact of widely networked forces will be. Some argue that strategic level commanders will no longer need the operational level because they will be able to command and control forces at the tactical level directly through the network. Others claim that the operational level will be compressed but not totally eliminated, while a third group argues that it will not be impacted in the least.[15]

These arguments again highlight the conceptual misunderstanding that pervades the defense community today. In fact, complexity theory suggests that the networking of forces will produce none of the conditions outlined above, and will instead lead to the operational level playing a larger and more vital role in meeting theater strategic objectives. This is difficult to fathom because our current networking lexicon is built around terms such as common operational picture (COP), global information grid (GIG) and Warnet. The following passage taken from a research report prepared by the New England Complex Systems Institute clearly sends an alarming signal that our current path of thinking is taking us in the wrong direction:

> "Generally, the military concept of networks promotes a coherently and globally accessible system that is centrally conceived, centrally engineered, and centrally integrated. Similar attempts at central design in civilian contexts (such as the Microsoft Network) failed to generate the success of the inherently distributed network systems. Accelerating the growth of military

[14] Vego, <u>Operational Warfare</u>, pp. 21-22.
[15] Vego, "Net-Centric Is Not Decisive," pp. 56-67.

> information networks requires a much more systematic and fundamental understanding of the relationship between structure and function."[16]

In other words, a one size fits all network approach is vastly inferior to a distributed network system that is designed specifically to meet the requirements of the task at hand. Joint operational commanders therefore must incorporate network design into the overall process of planning, preparing and executing their mission.

Furthermore, the network design must vary the level of detail and complexity that is allowed to flow from the tactical to the operational and strategic levels of war. In general information flows and decisions in complex systems are extremely sensitive to scale, which makes it essential for these flows to match the scale of observation. This concept is clarified in the following example:

> "…observing an army division at the division level means that squad level activities are abstracted in the detail. The commanding general of the division, therefore, is ill suited to focus on squad level contexts, such as small unit tactics, orders or movements. Likewise, a squad leader is ill suited for command of the entire division."[17]

The network design must accurately reflect and control the requisite information flows required to meet the stated objective. In other words, at the operational level, we must learn how to design functionality in and micromanagement out. In a very limited sense, this is precisely what is happening today with 'battle force email'. Watch standers are collaborating at their level in an effort to perform their assigned tasks more efficiently and effectively. Supervisory watch standards are not privy to the collaboration content, and therefore are able to remain focused on the information flows necessary to accomplish the tasks assigned at their level. However, this information flow structure is not embraced by every command, and it is not uncommon to find

[16] Yanam Bar-Yam, "Multiscale Representation Phase I," New England Complex Systems Institute, January 22, 2002, p. 4.
[17] Yanam Bar-Yam, p. 4.

commands that have actually imposed limitations on the use of the collaborative email system below a certain level.

Finally, the purpose of the network being designed will vary widely depending on where in spectrum of conflict a Joint operational commander finds himself. Military operations other than war (MOOTW) will certainly require different network functionality than that of regional or global war. The question of how to "wire up" our forces across this spectrum[18] is non-trivial and will be germane to the operational level commander as he works on building and selecting courses of action to accomplish the assigned objective.

Cyberspace: The Tie that Binds

Joint and coalition interoperability continue to be the Achilles heel for operational commanders operating forward. At the heart of the interoperability problem lies cyberspace, where the vast majority or our tactical systems utilize proprietary networking technology. Here's how a frustrated naval officer assigned to the USS GEORGE WASHINGTON Battlegroup put it:

> "Network centric warfare is a great concept but...the interoperability still isn't there. You have four different systems commands—SPAWAR (Space and Naval Warfare Systems Command), NAVSEA (Naval Sea Systems Command), NAVAIR (Naval Air Systems Command), NAVSUP (Naval Supply Systems Command)—each developing their own systems not in conjunction with one another. So there are big interoperability problems within the Navy itself, and I'm not even getting into the joint world. The Navy really needs to get more on board with the joint world when we develop our systems. Every system we develop needs to be purple, it needs to be joint. How are we going to be able to inter-operate in the joint world? Sometimes that's not always taken into consideration."[19]

[18] Dr. Thomas P. M. Bartlett, "The Seven Deadly Sins of Network-Centric Warfare," U.S. Naval Institute Proceedings, January 1999, p. 37.
[19] Hunter Keeter, "Network Centric Warfare: A Good Idea Whose Time has Come?," C4I News, May 8, 2002.

Moreover, this problem is not endemic to the Navy. A recent planning document prepared by U.S. Joint Forces Command highlights the fact that Combatant Commanders are struggling to share information across defense installations, between government agencies, and with allies. Without exception, solutions to interoperability issues dominated the Combatant Commanders' wish lists that were included with the report.[20]

Unfortunately, the response they will get from the acquisition community will undoubtedly involve a 'technology' solution. The reality is that for the most part, the technology to close the interoperability gaps already exists. The gaps are not created by technology per se, but exist because the government does not own the networking layer, which means no common network standards or services can be defined to facilitate interoperability. Instead, tremendous amounts of blood and treasure are poured into paying the interoperability tax, which consists of writing application level programming interfaces (API's) to enable individual systems to talk to one another. While this approach is manageable for a small number of applications, it quickly becomes untenable as the application matrix grows.

The Internet is a great example of how common standards and services provide for robust networking capabilities across an unlimited range of information technologies and applications. The hardware and software technology is developed to the protocol standards of the Internet. As a result, users can leverage this vast network via a mainframe, desktop, laptop or cell phone, regardless of the operating system or applications running on each. For this reason, forces operating forward have become "highly dependent on IT and networking for accessing information off of the web. When we are down on SIPRNET, we are dead-in-the-

[20] Gail Kaufman and Amy Svitak, "Still Disconnected, U.S. Commanders Detail Communication Shortcomings," DefenseNews, June 3-9, 2002, pp. 1 & 4.

water pretty much. That's how dependent we have become on networking."[21] And yet, this is only the tip of the iceberg with respect to the future potential of leveraging networks in cyberspace. Once the Defense Department takes ownership of the network layer across all of its network systems, interoperability will become mute as legacy systems are removed from service. Until then, however, interoperability will continue to haunt Combatant Commanders and fill their ‘wish lists’.

Holistic Approach to Developing and Fighting in Cyberspace

Doctrinally and organizationally, our current approach to developing network systems and to the two aspects of fighting in cyberspace—computer network defense (CND) and computer network attack (CNA)—for forces operating at the operational or tactical levels of war is fractured across services and across communities within services. For example, the Navy employs civilians, Engineering Duty Officers (EDO’s), Limited Duty Officers (LDO’s) and Information Professionals (IP’s) to design, procure, administrate/manage and provide CND for its information networks. These communities receive no formal training or education in current CNA strategies and tactics, and are not included in the Navy’s CNA effort, which is the responsibility of the Naval Security Group generally and the Cryptology community specifically. There is little if any cooperation or collaboration among the personnel and organizations working the network design, development and CND efforts, and the personnel responsible for CNA. As a result, Navy networks are designed and defended with only cursory knowledge of the potential threats and no knowledge of advanced CNA techniques and strategies. This leads to network systems being fielded with relatively unsophisticated and vulnerable computer and network defense plans and capabilities.

[21] Keeter.

In the Joint world, Joint doctrine buries the CND and CNA functions in independent stovepipes deep in the Information Operations cell.[22] As in the Navy process described above, very little or no cooperation or collaboration takes place between the CND and CNA teams on the Joint operational staff, and the teams themselves are comprised of members from different communities and services. This functional and professional separation creates a seam every bit as big if not bigger than the one described above. This creates an interesting dichotomy; as Joint operational commanders are becoming increasingly dependent on the networking of their forces, the vulnerability of these very systems to attack is growing at an equal or greater pace.

The compartmentalized approach of the Defense organization for computer design and development, CND and CNA flies in the face of what the subject matter experts in the civilian business and academic worlds have concluded.[23] These experts warn against treating security as an internal issue, and repeatedly stress the importance of enterprise wide collaboration in return for better protection. Additionally, the best research shows that a network security strategy based on strictly defensive measures is doomed for failure. Instead, strategies must "accept that the black hats [attackers] will get in, but limit the damage by boxing them into areas where they can't do much harm—and be able to strike back."[24] In other words, separating the network design and development, CND and CNA functions is a recipe for disaster in the face of the myriad sophisticated threats that face the networked Joint force operating forward today and in the future.

[22] U.S. Joint Chiefs of Staff, Joint Doctrine for Information Operations (Joint Pub 3-13), Washington, D.C.: October 9, 1998, p. IV-3.

[23] Karyl Scott, "Zeroing In—Cyberspies may meet their match is security researchers with bright ideas," InformationWeek.com, <http://www.informationweek.com/story/IWK20011102S0012>, November 5, 2001.

[24] Ibid.

Conclusions

Cyberspace is a medium that must be embedded into everything we do in support of Joint and combined operations. We must understand that our potential adversaries are organizing for the information age without legacy force restrictions. Therefore, we must remain keenly aware of how they are implementing their information age strategies. We also must understand that these adversaries clearly recognize the increasing reliance that U.S. forces are placing on network centric warfare. As a result, they will undoubtedly try to exploit this advantage through increasingly determined and sophisticated attacks against our most critical networked information systems. The research is clear, and indicates that our current approach to both network implementation and information security are severely lacking.

Additionally, OpArt and the operational level of war will both be critical to preparing and fielding forces in the information age. Unfortunately, cyberspace is a medium that receives little attention either in Joint education or practice. Instead, we continue to expend our precious intellectual capital on speculating why it will or won't work, when in reality few of us really have a thorough enough understanding of either of the two concepts, let alone how they will impact one another. Networking forces is much, much more than simply developing new technology. The technology we have today is sufficient to network the majority of our forces, but the organizational considerations have not been flushed out sufficiently to permit the application of the technology that exists. OpArt and the operational level of war have never been in danger of being supplanted by NCW, but they must change to incorporate the cyberspace medium. After all, the primary source of advantage in distributed, networked forces arises from networked effects that are distributed in many dimensions throughout a force and can be summoned for use in the manner of advantage chosen by clever commanders based on evolving conditions.[25] Sounds like a good start to an information age definition for OpArt.

Recommendations

Information age warfare like the industrial age before it will require warriors who are trained, educated and experienced in applying the forces and mediums at their disposal in accomplishing their assigned mission. The difference is, in the information age, a fourth medium of cyberspace will join the fray, which will require a whole new body of material to be generated. Additionally, organizational structures and tactics, techniques and procedures that served us well in the industrial age will need to be revisited in the context of the new medium of cyberspace. Specifically, the following recommendations are provided as first steps toward transforming to an information age force:

1. Cyberspace must be added to the OpArt body of literature. This new medium has important space, time and force considerations that have yet to be formally documented. Furthermore, cyberspace not only directly supports the operational functions of land, air and sea forces, it also requires operational functions to support itself. For example, operational logistics in cyberspace might be equated to bandwidth.
2. JPME must embrace this new medium and teach it to the future Joint leaders of our services. It must be given equal emphasis as the mediums of air, land and sea.
3. We must develop new procedures and organizational structures to ensure information security in the information age. Our current Defense-in-depth strategy must be supplanted by a strategy of intrusion tolerance. Doctrinally and organizationally, the

[25] Jeffrey R. Cares, Raymond J. Christian and Robert C.Manke, "Fundamentals of Distributed, Networked Military Forces and the Engineering of Distributed Systems," Naval Undersea Warfare Center Division, Newport, RI, May 9,

current compartmentalization of the CND and CNA functions must be eliminated. An intrusion tolerance strategy demands cyber warriors who are prepared to defend and strike back. In short, we must develop a holistic approach to fighting in the new medium of cyberspace.

4. Proper implementation of cyberspace as a fourth medium of operational warfare is the key to solving the Combatant Commanders' interoperability woes. Therefore, the focus on technology solutions must be shifted to include much more germane matters such as network layer control, organizational alignment and inter-service collaboration on network development.

2002, p. 1.

Bibliography

Alberts, Garstka, & Stein, Network Centric Warfare, 2nd Edition (Revised), Washington, D.C.: CCRP, February, 2000.

Arkin, William and Windrem, Robert, "The U.S.-China Information War", MSNBC.com <http://www.msnbc.com/news/607031.asp>, August 19, 2001.

Bar-Yam, Yanam, "Multiscale Representation Phase I," Boston, MA: New England Complex Systems Institute, January 22, 2002.

Bartlett, Dr. Thomas P. M., "The Seven Deadly Sins of Network-Centric Warfare," U.S. Naval Institute Proceedings, January 1999.

Bateman, Robert L., Digital War, Novato, CA: Presidio Press, 1999.

Cares, Jeffrey R., Christian, Raymond J. and Manke, Robert C., "Fundamentals of Distributed, Networked Military Forces and the Engineering of Distributed Systems," Naval Undersea Warfare Center Division, Newport, RI, May 9, 2002, p. 1.

Chandler, Robert W., The New Face of War, Mclean, VA: Amcoda Press, 1998.

Committee on Network Centric Naval Forces, Network-Centric Naval Forces, Washington, D.C.: National Academy Press, 2000

Dahl, CDR Erik J., "Network Centric Warfare and the Death of Operational Art", Naval War College JMO Department Publication NWC 1012, Newport, RI, Winter Trimester, 2002-2003.

Dahl, CDR Erik J., "We Don't Need an IW Commander," U.S. Naval Institute Proceedings, January, 1999.

Denny, David A., "Rumsfeld Sees Urgent Need to Transform the U.S. Military," The Information Warfare Site, <http://www.iwar.org.uk/news-archive/2002/military/01-31-02.htm>, January 31, 2002.

Evans, Philip and Wurster, Thomas, Blown to Bits, Boston, MA: Harvard Business School Press, 2000.

Forno, Richard and Baklarz, Robert, The Art of Information Warfare, Parkland, FL: Universal Publishers, 1999.

Honeynet Project, Know Your Enemy, Boston, MA: Addison-Wesley, October, 2001.

Kaufman, Gail and Svitak, Amy, "Still Disconnected, U.S. Commanders Detail Communication Shortcomings," DefenseNews, June 3-9, 2002.

Keeter, Hunter, "Network Centric Warfare: A Good Idea Whose Time has Come?," C4I News, May 8, 2002.

Loeb, Vernon and Ricks, Thomas, "1's and 0's Replacing Bullets in U.S. Arsenal—Success in Afghanistan Propels Shift to Equipping Forces with Digital Arms", Washington Post, February 2, 2002.

McFarland, David M., Perry, Monty Ray, and Miles, Steven R., "Joint Operational Art Is Alive," U.S. Naval Institute Proceedings, October 2002.

Morris, Kenneth M., User's Guide to the Information Age, New York, NY: Lightbulb Press, 1999.

Rosen, Stephen P., Winning the Next War, Ithaca, NY: Cornell University Press, 1991.

Sawhney, Mahanbir and Parikh, Deval, "Where the Value Lies in a Networked World," Boston, MA: Harvard Business Review, January, 2001.

Schneider, Fred B., Trust in Cyberspace, Washington, D.C.: National Academy Press, 1999.

Scott, Karyl, "Zeroing In—Cyberspies may meet their match is security researchers with bright ideas," InformationWeek.com, <http://www.informationweek.com/story/IWK20011102S0012>, November 5, 2001.

Spitzner, Lance, Honeypots—Tracking Hackers, Boston, MA: Addison-Wesley, December, 2002.

Tenet, George, U.S. CIA Director, Prepared Remarks made to the Senate Governmental Affairs Committee, <http://www.cia.gov/cia/public_affairs/speeches/archives/1998/dci_testimony_062498.html>, June 24, 1998.

U.S. Defense Department, "FY2000 Annual Report to Congress on the Military Power of the People's Republic of China", Defense Link <http://www.defenselink.mil/news/Jun2000/china06222000.htm>, June 2000.

U.S. Defense Department, "Quadrennial Defense Review Report (QDR)," Washington, D.C.: September 30, 2001.

U.S. Joint Chiefs of Staff, Doctrine for Joint Operations (Joint Pub 3.0), Washington, D.C.: September 10, 2001.

U.S. Joint Chiefs of Staff, Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations (Joint Pub 6.0), Washington, D.C.: May 30, 1995.

U.S. Joint Chiefs of Staff, Joint Doctrine for Command and Control Warfare (Joint Pub 3-13.1), Washington, D.C.: February 6, 1996.

U.S. Joint Chiefs of Staff, Joint Doctrine for Information Operations (Joint Pub 3-13), Washington, D.C.: October 9, 1998.

Vatis, Michael A., “Cyber Attacks during the War on Terrorism: A Predictive Analysis,” Hanover, NH: Institute for Security Technology Studies at Dartmouth College, <http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_a1.pdf>, September 22, 2001.

Vego, Dr. Milan “Net-Centric Is Not Decisive,” U.S. Naval Institute Proceedings, January 2003.

Vego, Dr. Milan, Operational Warfare, Newport, RI: U.S. Naval War College JMO Department Text NWC 1004, 2000.