NAVAL WAR COLLEGE
Newport, R.I.

The Future Role of Information Operations in Operational Art

by

John R. Moorman

Commander, U.S. Navy

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

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: _____

13 May 2002

Faculty Advisor: Not Applicable

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED

2. Security Classification Authority:NA

3. Declassification/Downgrading Schedule:NA

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

8. Title (Include Security Classification):
The Future Role of Information Operations in Operational Art (UNCLAS)

9. Personal Authors:
CDR John R. Moorman/USN

10.Type of Report: FINAL	**11. Date of Report**: 13 May 2002

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

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: information age, information systems, operational art, network centric warfare, factors, functions, center of gravity, culminating point, joint vision

15.Abstract:
This paper looks at the relationship between the rate of technology development and the role of information operations in the operational art. Computer processing power has doubled every two years since 1959 in accordance with Moore's Law, bringing with it a corresponding decrease in cost. Networking computers has exponentially increased the power of individual computers in accordance with Moore's Law. These technological phenomenon have produced the information age, where the ability to gather, process and exchange information is the source of power and wealth. The military is adapting to the information age, incorporating information systems in its infrastructure and exploring new warfighting concepts such as network centric warfare, that leverage the power of networks. The increasing integration of technology into weapons systems and operational concepts will increase the operational commanders capabilities and vulnerabilities. Without a corresponding increase in information operations capabilities and strategies, the best strategy can be defeated by successful destruction of information systems. Future operational commanders must understand the effects of increasing technological development and integration, and the increasing role and significance of information operations that corresponds with it.

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: 841-3556	**20.Office Symbol:** **C**

Security Classification of This Page Unclassified

"…the ongoing "information revolution" is creating not only a quantitative, but a qualitative change in the information environment that by 2020 will result in profound changes in the conduct of military operations."[1]

Joint Vision 2020

Throughout the history of warfare, commanders have sought to gain information to facilitate their decision making processes and to degrade their enemy's decision making ability. In essence, this was the nature of Information Operations (IO) up to, and throughout much of, the twentieth century.

Today, IO plays a much larger role in warfare, due in large part to the exponential increase in communications and computing capability. According to science and technology experts, the exponential increase in computing technology will continue well into the Twenty-first Century. This begs the question, "What is the future role of IO in warfare?", specifically in the area of operational art, defined as the "component of military art principally concerned with theoretical and practical aspects of planning, preparing, conducting, and sustaining major operations and campaigns to accomplish operational or strategic objectives in a theater."[2]

I contend that the role and significance of IO, as it applies to operational art, will continue to increase as technology continues to develop exponentially and is integrated into warfighting systems.

Specifically, IO will become "as important as those conducted in the domains of sea, land, air, and space."[3] Therefore, the operational commander will increasingly need to

---

[1] Joint Chiefs of Staff, Joint Vision 2020 (Washington, DC: June 2000), 8.
[2] Dr. Milan Vego, Operational Warfare (n.p., copyright 2000), 640.

[3] Joint Vision 2020, 29.

consider the employment of IO in the context of operational art just as he does for operations in the traditional physical domains. The role of IO as a subset of the traditional supporting functions of operational movement and maneuver, fires, protection, logistics, and intelligence will also increase. As the role of IO expands, it will increasingly be used as the ways and means to attain operational, and sometimes strategic and tactical objectives by attacking enemy centers of gravity, applying force either directly, or indirectly through critical vulnerabilities.

Since it is said that good doctrine comes from good operational art, it is worthwhile to look at what currently constitutes IO in today's joint doctrine. Joint doctrine defines IO as "Actions taken to affect adversary information and information systems while defending ones own information and information systems."[4] Further, IO "apply across all phases of an operation, throughout the range of military operations, and at every level of war. Information warfare (IW) is conducted during time of crisis or conflict (including war) to achieve or promote specific objectives over a specific adversary."[5] Joint doctrine explains that there is both offensive and defensive IO. Offensive IO use operations security (OPSEC), military deception, psychological operations (PSYOPS), electronic warfare (EW), physical attack/destruction, special information operations (SIO), and computer network attack supported by public affairs (PA) and civil affairs (CA) to achieve specific objectives. Offensive IO that is used to specifically attack and defend the command and control (C2) target set is referred to as command and control warfare (C2W). Defensive IO use information assurance, OPSEC,

[4] Joint Chiefs of Staff, Department of Defense Dictionary of Military and Associated Terms, Joint Pub 1-02 (Washington, DC: 12 April 2001), 211.
[5] Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Pub 3-13 (Washington, DC: 9 October 1998), I-1.

physical security, counter-deception, counter-propaganda, counter-intelligence, EW, and SIO to protect and defend information and information systems upon which joint forces depend to conduct operations and achieve objectives.[6]

Although current doctrine depicts a robust role for IO in warfare today, there are many who believe the future will require a greater role. Joint Vision 2020 states that "While activities and capabilities employed to conduct information operations are traditional functions of military forces, the pace of change in the information environment dictates that we expand this view and explore broader information operations strategies and concepts."[7] Another prominent proponent of the future role of IO is Andrew W. Marshall, the director of the Office of Net Assessment, part of the Office of the Secretary of Defense, who wrote "protecting the effective and continuous operation of one's own information systems and being able to degrade, destroy, or disrupt the functioning of the opponent's information systems will become a major focus of the operational art. Obtaining early superiority in the information realm will become central to success in future warfare. It has always been important; it will soon be central."[8]

The growing role of IO is directly related to the global transition from the industrial age to the information age. The information age is characterized by a knowledge based global economy, facilitated by advances in information technology such as digital communications, the internet (networking), and computer processing. The result is an exponential increase in the ability to process and share information, and communicate instantly worldwide, resulting in the growth of transnational businesses and

---

[6] Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Pub 3-13 (Washington, DC: 9 October 1998), vi-III-15.
[7] Joint Chiefs of Staff, Joint Vision 2020 (Washington, DC: June 2000), 28.
[8] Andrew W. Marshall, foreword to Zalmay Khalilzad and John P. White, The Changing Role of Information in Warfare (Santa Monica, CA:RAND, 1999), 5-6.

organizations (both legal and illegal) and international trade and interaction that is collectively referred to as "globalization". Therefore, information is increasingly becoming the source of power.

The increasing importance of information has led to the formation of network infrastructures generically categorized in three levels, defense information infrastructure (DII), national information infrastructure (NII), and global information infrastructure (GII). The role of information age technology in warfare was acknowledged by former Secretary of State William Perry when he stated that "We live in an age that is driven by information. Technological breakthroughs are changing the face of war and how we prepare for war."[9]

This driving force behind the power and significance of present and future information technology is found in two modern day principles or "laws". In 1965, Gordon Moore, then head of the Research and Development at Fairchild Semiconductor, predicted that "Integrated circuits will lead to such wonders as home computers, or at least terminals connected to a central computer, automatic controls for automobiles, and personal portable communications equipment."[10] He also wrote Moore's Law that stipulates that the numbers of transistors on a chip double every two years. This exponential increase in transistors produces an equal increase in processing power and an inversely proportional decrease in the costs of computation. The result over the last 43 years has been an exponentially staggering increase in computing power and speed, and a corresponding decline in cost. Experts predict that Moore's Law will remain valid well

[9] Peter Constantini, "Technology-Information: Information Warriors Form New Army" (Inter-Press Service: 09 August 1996).
[10] Haim Mendelson, "Moore's Law," Encyclopaedia of Computer Science, n.d., http://www.gsb.stanford.edu/cebc/pdfs/Moore's_Law.pdf (09 May 2002).

into the second decade of the twentieth century.[11] The second principle is Metcalf's Law, written by Roger Metcalf, which states "the value or power of a network increases in proportion to the square number of nodes on the network."[12] Together, these two technological laws work together to produce the revolutionary effects of information technology through computing power and networking.

Another significant factor that cannot be ignored is size. Since 1997, governments and commercial industry have been conducting extensive research and development in the field of nanotechnology in a race to build a molecular computer. Computer speeds increase dramatically as they get smaller. According to NASA's Nanotechnology Team, "studies suggest that it may be possible to build 10^{18} MIPS computers -- about a million times more powerful than the largest supercomputer that exists today (Fall 1997)."[13] It is estimated that the first molecular computer will be built by about 2010 to 2015. Clearly the role of these information systems in the private, commercial, and government sectors has increased dramatically as the speed and power of

information technology continues to increase exponentially.

> "We must build forces that draw upon the revolutionary advances in the technology of war…one that relies more heavily on stealth, precision weaponry, and information technologies"
>
> *George W. Bush*
> *Commander in Chief*

Since the beginning of the information age, military applications for information

---

[11] Haim Mendelson, "Moore's Law," Encyclopaedia of Computer Science, n.d., http://www.gsb.stanford.edu/cebc/pdfs/Moore's_Law.pdf (09 May 2002).
[12] "Metcalf's Law," The Fundamentals of Information Science, n.d., http://www-ec.njit.edu/~robertso/infosci/metcalf.html (09 May 2002).
[13] Al Globus, David Bailey, Jie Han, Richard Jaffe, Creon Levit, Ralph Merkle, and Deepak Srivastava, "NASA applications of molecular nanotechnology." The Journal of the British Interplanetary Society, 1998, < http://www.nas.nasa.gov/Groups/Nanotechnology/publications/1997/applications/#rodLogic> (09 May 2002).

technology have been increasingly adopted. In their book War in the Information Age, the authors state, "The speed, power and miniaturization of information processing components have brought greater lethality and precision; increased stand-off distance of command, forces, and firing platforms; and improved knowledge of the battlespace from intelligence, surveillance, and reconnaissance."[14]

The military manifestation of information age technologies is a concept called network centric warfare (NCW). Captain John T. Locks, USN, says "Network centric warfare simply proposes to disperse weapons, sensors, and decision-makers across a multitude of platforms in a way that achieves greater, and more sustainable, combat power than was previously possible."[15] The network centric warfare concept is a military application of Metcalf's law, using platforms as nodes thereby increasing their power exponentially by interconnecting them through a network.

Considering the exponential rate of development of information technologies, combined with the increasing integration of information technologies in warfighting systems and organizations, the effects on the operational commander must not be underestimated or overlooked.

There is a profound relationship between information technology and IO. Today's global, national, and defense information infrastructures have been built with information age technology, using information systems that consist primarily of computers and computer networks. Since IO strives to affect adversary information systems while defending ones own, the role and significance of IO to the operational

[14] Robert L. Pfaltzgraff, Jr. and Richard H. Shultz, Jr., War in the Information Age (Washington, DC: AUSA, 1997) 198-199.
[15] Captain John T. Locks, "NCW Fundamentals," (NWC 1005, Joint Military Operations Department, U.S. Naval War College, Newport, RI: 2002) 1.

commander increases as well.

Today's operational commander must take into account the factors of space, time and force in relation to assigned objectives. In order assess these factors effectively, the commander must have information that is accurate, relevant, timely and usable in addition to being complete and precise.[16] Information technology provides the means to rapidly gather and project a tremendous quantity of information to a large number of personnel simultaneously (the operational commander and those on his staff who need the information), and almost instantaneously. Today, IO uses the OPSEC process to identify critical information, determine which friendly actions might be observed by the enemy and used to derive critical information, and then execute measures that reduce or eliminate vulnerabilities to enemy exploitation.[17] This OPSEC methodology is tailored to each operation and requires considerable manpower to perform. As the military continues to expand the integration of information technology and networks into its infrastructure, the role of OPSEC will become more significant as the volume of information will increase significantly. Fortunately, improvements in IT that facilitate the information process should also assist the OPSEC process, increasing efficiency decreasing the manpower required to perform OPSEC. IO will also need to continuously integrate and update information technology in order to conduct offensive IO against increasingly sophisticated enemy information systems.

Information technology has a significant impact on the factors of both space and time. According to the U.S. government's C4ISR Cooperative Research Program, "The

[16] Dr. Milan Vego, Operational Warfare (n.p., copyright 2000), 96.

[17] Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Pub 3-13 (Washington, DC: 9 October 1998), III-4 -III-5.

information age is making distance less relevant. Information, and the decisions that result, can travel almost instantaneously to the place(s) where they are needed, making the location of those who gather, analyze, make decisions, and possibly those who act on these decisions, largely irrelevant."[18] Linking sensor, weapons and communications systems together in the form of a network provide the operational commander and his staff with near real time information about the operations area, regardless of the size or region, diminishing the effects of factors space and time on both planning and execution of operations. Continuously improving communications networks facilitate the flow of information regardless of distance or location, greatly decreasing the affect of space and time on command and control. A study done for the Office of the Secretary of Defense by Booze, Allen and Hamilton Inc. concludes that "a disaggregated network of sensors, command centers, and weapon systems allows for greater dispersion of combat forces while maintaining situational awareness, thus enabling greater mobility and survivability. Greater dispersion generates increased complexity for the enemy commander and decreases his overall understanding, while networked systems offer simplicity and greater understanding for the friendly force commander. In the past, overcoming the problems associated with space was mainly a factor of physical speed; in the future, space will be measured in terms of information (situational awareness), indirect weapons range, and physical speed of units and platforms. The emphasis is shifting from physical speed and presence to virtual speed and presence."[19]

Regarding factor force, information technology and networks provide the

---

[18] David S. Alberts, John J. Garstka and Frederick P. Stein, Network Centric Warfare - Developing and Leveraging Information Superiority, 2nd ed. (Vienna, VA: CCRP, 1999), 20-21.
[19] Booze, Allen & Hamilton Inc., Measuring the Effects of Network-Centric Warfare, (McLean, VA: 1999), 2-3.

operational commander with improved situational awareness regarding both enemy and friendly force dispositions and status, thereby obtaining a decisive advantage over his opponent and reducing the likelihood that the enemy can achieve surprise.[20] Information technology also "improves the effectiveness of kinetic weapons, especially long-range, GPS-guided ones. Timely and accurate information exchange between sensor and shooter increases the probability of locating, classifying, and hitting the desired target. In turn, the increase in individual weapon effectiveness results in a net increase in potential force. In the past, force was measured in terms of sheer mass; in the future, force will be measured more in terms of precision effects."[21] In essence, the operational commander will be able build more combat power with less forces, which may be dispersed over a large geographic area.

Clearly, IO is integral to the ability of the operational commander to successfully utilize the tremendous space, time and force advantages offered by the information age. Without the ability to perform offensive IO against enemy information systems and networks, while performing defensive IO to protect his own, the tremendous operational advantage could become an equally large disadvantage. The demand for IO to keep pace with technology is underscored in the book *Information Warfare Principles and Operations*, which states, "The current state of the art in information operations is based on core technologies whose performance is rapidly changing, even as information technologies rapidly advance. As new technologies enable more advanced offenses and defense, emerging technologies farther on the horizon will introduce radically new implications for information warfare."[22]

---

[20] Dr. Milan Vego, Operational Warfare (n.p., copyright 2000), 100.
[21] Booze, Allen & Hamilton Inc., Measuring the Effects of Network-Centric Warfare, (McLean, VA: 1999), 2-2.

As technology advances and is adapted to military purposes, Information systems will play an increasing role in the traditional operational functional areas.

In the area of operational movement and maneuver, information systems will provide enhanced situational awareness (SA) and command and control (C2). As a result, the operational commander will be able to move and maneuver disparate forces, spread over a larger geographic area, with greater speed and precision. These advances will significantly increase his ability to synchronize actions more precisely and effectively, producing higher levels of combat power at the time and place of his choosing.[23] In order to do so, the commander must employ IO to safeguard his own networks, protecting them from destruction or compromise, and to disrupt or destroy the enemy's networks.

Improved SA and C2 will improve the commander's ability to conduct operational fires through enhanced knowledge of enemy movement, maneuver, logistics, order of battle and staging base locations. IO will protect friendly information and penetrate enemy networks in order to gain information regarding enemy plans and operations.

Operational logistics will be increased by orders of magnitude using information systems and will be crucial to maintaining the high operational tempo created by network centric warfare. Information technology and networks will be used to precisely monitor the status of resources, user requirements and available transportation. Indeed, "logisticians will be able to anticipate exact requirements throughout the conduct of operations, and efficiently forward materiel and other resources."[24] Enhanced IO

---

[22] Edward Waltz, Information Warfare Principles and Operations (Boston: Artech House Inc., 1998), 357.
[23] Edward Waltz, Information Warfare Principles and Operations (Boston: Artech House Inc., 1998), 31.
[24] Robert L. Pfaltzgraff, Jr. and Richard H. Shultz, Jr., War in the Information Age (Washington, DC: AUSA, 1997) 184.

capabilities and strategies will be required to protect these networks and disrupt or destroy the enemy's.

Operational force protection capabilities will be greatly enhanced by information technology and networks. Embedded information technologies, increased speed and agility facilitated by enhanced SA and C2, and the dispersion of forces will work together to create ambiguity and confusion for the enemy and increase survivability of forces.[25] Sensors will provide commanders with a clearer picture of threats in all dimensions. Reliance on these systems and networks also pose a liability that can only be eliminated or reduced by the effective use of IO to protect them from attack or compromise.

Technology tremendously increase the commanders ability to leverage the operational intelligence function. Campaign or major operation planning and preparation will be enhanced through rapid mapping of terrain, information infrastructures, electronic orders of battle and decision processes; networked space, air, sea, and ground sensors; all-source data fusion and mining; integration of distributed databases; intelligent agents for search and cueing, recognition, and routing; automated language, syntax, and protocol translation; multimedia distribution networks; collaborative multimedia conferencing; and tactical/mobile networking.[26] As the number of information sources, and sheer quantity of information increases, so to will the role and importance of IO in the operational intelligence function. As technology increases the quality, quantity and timeliness of intelligence, there is a corresponding increase in reliance on that technology, posing an inherent risk of attack. Therefore, the commander must ensure that

[25] Robert L. Pfaltzgraff, Jr. and Richard H. Shultz, Jr., War in the Information Age (Washington, DC: AUSA, 1997) 208-211.
[26] Edward Waltz, Information Warfare Principles and Operations (Boston: Artech House Inc., 1998),113-116.

IO is conducted to the extent required to protect information, and the systems used to collect, analyze and distribute information, from attack or compromise. Fortunately, our enemies will be subject to the same risks, emphasizing the need for developing and evolving offensive IO strategies and tactics in order to destroy, disrupt, or deny the enemy's ability to use his information systems.

Perhaps the most significant link between technology and the increased role and significance of IO is the affect of information age technology on the centers of gravity and culminating point of offense and defense.

> "We are now seeing a tendency toward a shift in the center of gravity away from traditional methods of force and means of combat toward non-traditional methods, including information. Their impact is imperceptible and appears gradually. It is less burdensome economically and is not dangerous ecologically. . . . Thus today information and information technologies are becoming a real weapon. A weapon not just in a metaphoric sense but in a direct sense as well."[27]

A report by the U.S. Air Force determined that "information is now considered a center of gravity for the military."[28] Joint doctrine defines centers of gravity (COGs) as "Those characteristics, capabilities, or sources of power from which a military force derives its freedom of action, physical strength, or will to fight."[29] As militaries continue to integrate information systems and networks into their warfighting infrastructure, the dependence on technology as a source of combat power increases as well. In the case of network centric warfare, where the operational commander uses information and networks to control and leverage combat power from a wide range of disparate,

---

[27] Timothy L. Thomas, "Deterring Information Warfare: A New Strategic Challenge," Parameters, Winter 1996-97, pp. 81-91, < http://carlisle-www.army.mil/usawc/Parameters/96winter/thomas.htm> (12 May 2002).

[28] Lt Col Alfred M. Coffman, Jr., "Strategic Environmental Assessment for Modernization Planning," Report of the Strategic Planning Division, Directorate of Plans, Headquarters United States Air Force, 6 June 1994.

[29] Joint Chiefs of Staff, Department of Defense Dictionary of Military and Associated Terms, Joint Pub 1-02 (Washington, DC: 12 April 2001), 65.

geographically separated units and platforms, the information and networks will be the COG. There may be many cases where information or networks are not the COG, such as the case when troops on the ground are the source of combat power. However, it is probable that C2 and intelligence, logistics and fire support of those troops will be heavily dependent on information systems. In this case, the information systems are a critical factor that the enemy can use to indirectly attack the COG. In either case, the operational commander must recognize the critical role that IO plays in protecting his own COG. Conversely, when an operational commander determines that information systems are the enemy's COG, or the means to attack his COG indirectly, the operational commander will attain victory through the effective use of IO against enemy information systems.

Culminating point is defined as "The point at which a force no longer has the capability to continue its form of operations, offense or defense."[30] The destruction or degradation of any network (sensors, shooters, command and control, logistics, etc.) necessary to mass the combat power required to conduct offensive operations will, by default, mean that an attacker no longer has sufficient combat power to successfully continue the attack. In other words, he will have passed the culminating point of attack. This applies to the culminating point of defense as well. The implication is that even the "best" operational commander can make the right plans and decisions, have superior forces and still lose the offensive, or worse defensive, if he cannot protect his own information systems and attack the enemy's (IO by definition).

[30] Joint Chiefs of Staff, Department of Defense Dictionary of Military and Associated Terms, Joint Pub 1-02 (Washington, DC: 12 April 2001), 112.

In summary, the information age, characterized by digitization, computers, and information technologies, is producing socio-economic changes similar to those produced by the agrarian and industrial ages.[31] Thus far, the information age has produced an information based global economy (globalization). The military is also adapting to the information age through an ongoing revolution in military affairs (RMA) aimed at shifting the focus from individual units or platforms to networks. The RMA is described by Vice Admiral Cebrowski, USN (ret), as "unlike any seen since the Napoleonic Age, when France transformed warfare with the concept of levee en masse."[32]

The future prospects for the RMA are linked to the predicted exponential increases in computer processing power and speed, decreasing computing costs, and increased computer power through networking and miniaturization.

The exponential advancement of information systems and their integration into warfighting infrastructures have a significant impact on the operational commander and his ability to plan and execute operations and campaigns. The operational factors of space and time will be compressed. Enhanced situational awareness will allow the commander to make knowledgeable decisions in a much shorter time span. Orders based on decisions can be communicated instantly worldwide. Network connectivity between sensors, units and platforms, and command will allow forces to disperse over a wider area yet maintain their combat power, making it more difficult for the enemy to anticipate your actions. Improved awareness of the enemy's locations, status and intentions reduce probability of being surprised. Weapons precision and range will be improved. When combined, these technological advances provide the operational commander with an exponential net increase in the ability to mass more combat power at the time and place of his choosing than ever before.

---

[31] Alvin Toffler, The Third Wave (New York: Bantam Books, 1991); Alvin and Heidi Toffler, War and Anti-War: Survival at the Dawn of the 21st Century (New York: Warner Books, 1995).

[32] Vice Admiral Arthur K. Cebrowski, USN (ret), and John J. Garstka, "Network-Centric Warfare: Its Origin and Future," U.S. Naval Institute Proceedings (January 1998): 29.

However, the liabilities of integrating information technology into our warfighting systems and concepts can be just as great as the advantages. When relied upon as the principle means to mass combat power, information systems can become the center of gravity or a critical factor, becoming the object of enemy attack.

The key to safeguarding our ability to conduct successful operations and campaigns lies in information operations. Both offensive and defensive information operations strategies and capabilities must keep pace with technological advancement and its integration throughout the military. If we develop network centric warfare capabilities without the corresponding ability to successfully defend information and networks, we are building a formula for defeat.

As our enemies also become more reliant on information systems, so to will the importance of developing advanced offensive information operations capabilities. Using enhanced IO technological capabilities, strategies and tactics, the operational commander will be able to attain strategic, operational, and tactical level victories through IO directed at the enemy's defense information infrastructure, national information infrastructure or the global information infrastructure.[33]

We must not fail to recognize the importance of information operations to the success of information age operational art.

BIBLIOGRAPHY

Alberts, David S., John J. Garstka and Frederick P. Stein. Network Centric Warfare - Developing and Leveraging Information Superiority. 2nd ed. Vienna, VA: CCRP, 1999.

Booze, Allen & Hamilton Inc. Measuring the Effects of Network-Centric Warfare. McLean, VA: 1999.

Cebrowski, Vice Admiral Arthur K., USN (ret) and John J. Garstka. "Network-Centric Warfare: Its Origin and Future." U.S. Naval Institute Proceedings. January 1998: 29.

[33] Edward Waltz, Information Warfare Principles and Operations (Boston: Artech House Inc., 1998),27-31.

Coffman, Lt Col Alfred M. Jr. "Strategic Environmental Assessment for Modernization Planning." Report of the Strategic Planning Division, Directorate of Plans, Headquarters United States Air Force. 6 June 1994.

Constantini, Peter. "Technology-Information: Information Warriors Form New Army." Inter-Press Service. 09 (August 1996).

Globus, Al, David Bailey, Jie Han, Richard Jaffe, Creon Levit, Ralph Merkle, and Deepak Srivastava. "NASA applications of molecular nanotechnology." The Journal of the British Interplanetary Society. 1998. <http://www.nas.nasa.gov/Groups/Nanotechnology/publications/1997/applications/#rodLogic> (09 May 2002).

Locks, Captain John T. "NCW Fundamentals." NWC 1005, Joint Military Operations Department, U.S. Naval War College, Newport, RI: 2002.

Marshall, Andrew W., foreword to Zalmay Khalilzad and John P. White. The Changing Role of Information in Warfare. Santa Monica, CA: RAND, 1999.

Mendelson, Haim. "Moore's Law." Encyclopaedia of Computer Science. n.d. http://www.gsb.stanford.edu/cebc/pdfs/Moore's_Law.pdf (09 May 2002).

"Metcalf's Law." The Fundamentals of Information Science. n.d. http://www-ec.njit.edu/~robertso/infosci/metcalf.html (09 May 2002).

Pfaltzgraff, Robert L. Jr. and Richard H. Shultz Jr. War in the Information Age. Washington, DC: AUSA, 1997.

Thomas, Timothy L. "Deterring Information Warfare: A New Strategic Challenge." Parameters. Winter 1996-97. 81-91. < http://carlisle-www.army.mil/usawc/Parameters/96winter/thomas.htm> (12 May 2002).

Toffler, Alvin. The Third Wave. New York: Bantam Books, 1991

Toffler, Alvin and Heidi. War and Anti-War: Survival at the Dawn of the 21st Century. New York: Warner Books, 1995.

U.S. Joint Chiefs of Staff. Department of Defense Dictionary of Military and Associated Terms (Joint Pub 1-02). Washington, DC: 12 April 2001.

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

U.S. Joint Chiefs of Staff. Joint Vision 2020. Washington, DC: June 2000.

Vego, Milan. Operational Warfare. n.p., copyright 2000.

Waltz, Edward. Information Warfare Principles and Operations. Boston: Artech House Inc., 1998.