CANADIAN FORCES COLLEGE / COLLEGE DES FORCES

CANADIENNES

NATIONAL SECURITY STUDIES COURSE (NSSC) 5

A/AS/JCO/DOC/S-3

"Warfare in the 21st Century: The Revolution in Information Warfare will dominate the future battlefield

By / par Colonel Darryl Bradley

March 2003

ABSTRACT

Thesis Statement: Information warfare will dominate the battlefield in the 21st Century.

The paper will demonstrate that information warfare used to gain information superiority will dominate the battlefield in the 21st Century. *Joint Vision 2010* describes the ongoing transformation to new capabilities that will allow the Armed forces to be faster, more lethal, and more precise in the 21st Century.[1] Additionally, information technology advances will make dramatic changes in how the United States will conduct military operations, and fight wars in the future.[2] This increased capability of information warfare coupled with precision attack will allow the United States to strike the enemy's decisive points at the critical moment and dominant the battlefield.

The paper begins with a look at the evolution of information warfare, and how it was used during early conflicts and currently being employed in the United States coalition led campaign in Iraq. The paper further examines information warfare as one of the Revolution of Military Affairs (RMAs) Debate, and the major changes in the nature of warfare brought about by the innovative application of new technologies. These changes will have a significant impact on the overall strategic strategy, and the conduct of future military operations. The paper will argue that information warfare combined with dramatic changes in military technology will dominate the battlefield in the 21st Century, over other conventional methods of weapons

[1] Department of Defense, Joint Publication, Joint Vision 2010, May 1996.

[2] Cisco Van Schaik, "Information Warfare in the 21st Century," www.mil.za/CSANDF

employment. The paper concludes that information warfare will dominant the battlefield in the 21st century, and enable the United States to win future wars and conflicts.

INTRODUCTION

> Information is the key to successful military operations; strategically, operationally, tactically, and technically. From war to OOTW, the adversity who wins the Information War prevails.[3]
>
> --Gen(Ret) Glenn Otis, 1991

The evolution of information warfare has been around since the first spoken or written words evolved. Dating back to the first wars, information has played a major role in warfare. In decades past, information was passed between allies on written mediums, spoken works, radio waves, and even smoke-signals. The art of information warfare also dates back in history to these types of communications. Agents were sent into enemy lines to impersonate allies to gather information that may be spoken, or written, between the opposing sides.

During World War II, there were several evolutionary changes in warfare and tactics to include large-scale air-to-air combat, strategic bombing, naval carriers, and the use of the atomic bomb. These changes marked cornerstones in the use of information warfare as a new tactic in defeating your enemy, and were a milestone in communications with the use of radio waves to transmit information over great distances. The transmission of communications also spawned the need for offensive and defensive measures that were necessary to maintain continuity with the forces. The Germans employed an enciphered message over the airwaves to troops on land, sea, and air. The tactics of intercept and deception were employed during World War II against the Enigma cipher, and proved to be key to the Allies success in defeating the German.[4]

---

[3] United States Government, Field Manual 34-1, "Information Operations," Chapter 7, February 1996, 6.

[4] Eric Hrovat, "Information Warfare: "The Unconventional Art In a Digital World," SANS, June 2001, 1.

The time after World War II was described as the time of the theory of mass destruction. The doctrine in the Cold War was not priorizate targets or precise targeting, but to destroy everything in order to win the war.

In the late 1970s and early 1980s, third wave technologies and ideas began to change the industrial wave societies. The mass society became slowly a communication society. With this development, technology in the military began to change rapidly and made a significant impact of the way the United States fought in the Gulf War.

The Gulf War was a historic event in the use of information warfare as a key to winning the war. The use of space assets, both military and commercial, provided Coalition forces with communications, navigation, surveillance, intelligence, and early warning in the victory over the Iraqi forces. This war has been called the first "Information War" because of the advanced information systems used by the coalition for supply, intelligence, analysis, and weaponry, and the general conclusion that it was this technology that greatly limited coalition casualties.[5]

Today, the United States military is in the midst of the initial phase of what is known as a revolution in military affairs led by several former leaders of the military. The Department of Defense's vision of the revolution in military affairs, seeks the application of new technology, particularly digital information technology, to operational and strategic concepts that are less than radical. This vision was also a focus for the first "Quadrennial Strategy Review, a congressionally mandated reassessment of defense policy, began formally in January 1997, and

---

[5] Hrovat, 2.

much of Washington's security policy began to force on the requirements for the military in the 21st century.[6] Additionally, former Chairman of the Chiefs of Staff, General John Shalikashvili published a document entitled *"Joint Vision 2010"* which is a conceptual template describing how United States armed forces should expect to conduct warfare in the early 21st century.

While not focused primarily on information warfare, *Joint Vision 2010 – American's Military: Shaping the Future,* ideas are of direct relevance to the future evolution and role of information warfare. *Joint Vision 2010* begins with a projection of current technological trends assumed to shape the future war-fighting environment.[7] This trend includes both offensive and defensive information warfare required in information supremacy. It correctly recognizes information warfare as one of the most important and necessary condition for future joint warfare, and identified technological innovation as a vital component of the transformation of the joint force.

Additionally, *Joint Vision 2010* asserts that the combination of these technologies will provide an order of magnitude improvement in lethality. Underpinning future operations will be information technology that will provide the ability to see, prioritize, assign, and assess information so that American forces will achieve "dominate battlespace awareness".[8] A key goal, therefore, will be "information superiority", the capability to collect, process, and

---

[6] James R. Blaker, "Understanding the Revolution in Military Affairs (RMA)," New Democrats Online, February 1997, 2.

[7] Joint Vision 2010,

[8] Lothar Ibrugger, "The Revolution in Military Affairs," NATO Parliamentary Assembly, Committee Reports, November 1998, 1.

disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

Joint Vision 2020 continues to build upon and extends the conceptual template established by *Joint Vision 2010* to the continuing transformation of America's armed forces. The evolution of information technology will increasingly permit the United States to integrate the traditional forms of information operations with sophisticated all source intelligence, surveillance, and reconnaissance in a fully synchronized information campaign.[9]

AIM

The aim of this paper is to demonstrate that information warfare used to gain information superiority will dominate the battlefield in the 21st Century. The paper will further examine information as a Revolution of Military Affairs Debate, and the implication of new technologies to support information warfare on the battlefield. The paper argues that information warfare will dominate the battlefield of the 21st century, over other conventional weapons on the battlefield.

DEFINING INFORMATION WARFARE

There are several definitions of information warfare that have been formulated and disseminated throughout the Department of Defense (DOD), and it is important to first

[9] Joint Vision 2020,

understand the meaning of information warfare. Information warfare, in its essence, is about ideas and epistemology – big words meaning that information warfare is about the way humans think and, more important, the way humans make decisions.[10] A common thread amongst all the definitions is the PROTECTION of your information systems and the ATTACK and EXPLOITATION of an adversary's information systems with the goal of attaining the advantage for information operations.[11] The Joint Staff defines information warfare as:

> actions "taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems while leveraging and defending friend information systems. Information warfare constitutes another revolutionary aspect of the new era warfare quickly disrupting or destroying an adversary's command and control system, intelligence, information propaganda abilities, and general situational awareness.

The definition of information warfare has different meanings outside of the Joint Staff and is unique to each Service. Major General Kenneth Minihan, former U.S. Air Force Assistant Chief of Staff for Intelligence, describes information warfare in more objective terms, which he says is really "information dominance."[12] In describing information dominance, he puts it this way:

Information dominance is not "my pile of information is bigger than yours" in some sort of linear sense. It is not just a way to reduce the fog of war on our side or thicken it on the enemy's side. It is not analysis of yesterday's events, although proper application of historical analysis is important to gaining information dominance. It is something that is battled for, like air superiority. It is a way of increasing our capabilities by using that information to make right decisions, (and) apply them faster than the enemy can. It is a way to alter the enemy's entire perception of reality. It is a method of using all information at our disposal to predict (and

---

[10] George J. Stein, "Information Warfare," *Airpower Journal*, Spring 1995, .2.

[11] Robert Thompson Jr., "Information Warfare," Kaman Sciences Corporation, www.dacs.dtic.mil, Spring 1998, 5.

[12] Craig L. Johnson, "Information Warfare – Not a Paper War," *Journal of Electronic Defense,* Vol 17, no 8, August 1994, 3.

affect) what happens tomorrow before the enemy even jumps out of bed and thinks about what to do today.[13]

Although information warfare may have different meaning, it has always been a critical factor in war. Clausewitz said " imperfect knowledge of a situation… can bring military action to a standstill," and Sun Tzu indicated information is inherent in war fighting.[14] Information warfare embodies the impact of information on military operations. Sun Tzu recognized the importance dimensions of warfare in which information play a decisive role.

Components of Information Warfare

The information warfare concept has several different components that focus on controlling and exploiting information to support operations, and to achieve a desired end state. These components ensure that all information warfare are synchronized and mutually reinforcing, achieving synergy and unity of effort.

Martin Libicki, a senior fellow at the Institute for National Strategic Studies, National Defense University, notes that information warfare is not "a separate technique of waging war." Rather, there are seven distinct components of information warfare, each involving the protection, manipulation, degradation and denial of information. These forms are:

- Command and control warfare, which is to separate the enemy's head from the body of his forces

[13] Ibid, 2.

[14] James W. McLendon, "Information Warfare: Impacts and Concerns," Battlefield of the Future

- Intelligence-based warfare, which consists of measures and countermeasures that seek knowledge to dominate opponents combat power in the battlespace, and combat power potential outside the battlespace.
- Electronic warfare, such as radio-electronic or cryptographic means.
- Psychological warfare, used to influence the minds of friends, neutrals and foes.
- "Hacker" warfare, in which computer systems are attacked.
- Economic information warfare, blocking or channeling information to pursue economic dominance.
- Cyber warfare, a futuristic collection of ideas that ranges from clever to absurd.

Additionally, there are both offensive and defensive aspects of information warfare. Common links between the two aspects include the target sets involved in information warfare and the dependence upon information to plan operations, deploy forces, and execute missions.[15]

THE REVOLUTION OF MILITARY AFFAIRS (RMAs) DEBATE

> 'A Revolution in Military Affairs is a major change in the nature of warfare brought about by the innovative application of new technologies which, combined with dramatic changes in military doctrine and operational and organizational concepts fundamentally alters the character and conduct of military operations.'[16]

---

[15] United States Government, Joint Publication 3-13, Chapter II, "Offensive Information Operations," February 1996, .2.

[16] The Information Warfare Site

Officer of the Secretary of Defense,
Office of Net Assessment

The Revolution of Military Affairs Debate has been occurring since the Gulf War, and analysts in the United have started calling them RMAs. This change in terminology was meant to capture the nontechnical dimensions of military organization and operations, the sum of which provide a large part of overall military capabilities. This revolution under way in warfare is that associated with information systems, their associated capabilities, and their effects on military organization and operations.[17]

Admiral William Owens, USN (Retired) former vice chairman of the Joint Chiefs of Staff, has been saying for years that the critical "revolution" is informational.[18] In his book *Lifting the Fog of War*, Owens argues that microprocessors were the key element in unmanned aerial vehicle (UAV) development. He defines the ongoing revolution in military affairs as the "the ability to achieve integrated sight – the stage where the raw data gathered from a network of sensors of different types is successfully melded into information."[19]

The Gulf War demonstrated how information could be both a weapon and a target. The RMA – the application of computers and information technology to the conduct of war – had arrived. Additionally, Desert Storm offered a mere first glimpse of what computers and information technology could provide: precision-guided weapons, real-time intelligence data,

---

[17] Ibid,

[18] William A. Owens with Edward Offley, Lifting the Fog of War, (New York: Farrar, Straus and Giroux, 2000).

enhanced situation awareness, more effective command and control, all adding up to a new kind of war … or, as the Joint Chiefs of Staff described it in "Joint Vision 2010," Full Spectrum Dominance.[20]

General Charles Horner also believes we have entered a period where new technologies can change the manner in which we fight wars and can downgrade the value of possession of nuclear arms.[21] He writes:

> Desert Storm represents a revolution in warfare. Specially, we need to conduct operations in ways that inflict the minimum number of casualties on both sides. Additionally, we must prepare for wars in which ballistic missiles are used against our own troops and as terror weapons…In the end, we should aim to reduce our nuclear arsenals to zero as we substitute missile defenses for nuclear weapons.[22]

The idea of a RMA rests on the view that, sometimes, technological changes, coupled with new organizations and doctrine, transform warfare. It is a war for obtaining, analyzing and disseminating information. But it is above all else an electronic war, both offensive and defensive: it consists of "attacking" the enemy's electronic circuits to jam them, destroy them or alter their content by means of "viruses", "logic bombs" and other "worms"; it also seeks to make its own software secure against enemy incursions.[23] Changes in military technology, organization, and doctrine are not rare. It involves big changes that occur relatively quickly and which tend to spread beyond the profession of arms into the realm of foreign policy, and draws

---

[19] Owens,

[20] Philip Gold, "Rumsfeld's Revolution: Is the Big Shift in Defense Really Happening at Last?" Discover Institute, June 2001.

[21] McLendon, 2.

[22] Ibid, 2.

[23] Le Monde diplomatique, "Developing the weapons of the 21st Century," February 1998, 2.

heavily from ideas, concepts, and suggestions that have circulated inside the Pentagon for several years.

General Gordon Sullivan, former Chief of Staff, United States Army, pointed out: "With this capability, commanders can now blend previously separate and discrete operations into a single and seamless whole.[24] Information technologies are already dramatically improving the ability to gather process, and disseminate information in near real time. Military planners and policymakers, for many years, have advocated the need to increase the interoperability of computer networks for battlefield use.[25]

The RMA's central concept, information warfare, is therefore deployed on all fronts. It is a war for obtaining, analyzing and disseminating information. During a recent speech, Donald H. Rumsfeld, Defense Secretary, stated the military's new dependence on information systems was aimed at refocusing the Pentagon's efforts to change the military to better counter the threats of the 21st century. These threats would be minimize by making use of information warfare to deter new adversaries, and reshaping the armed forces around more sophisticated information and weapon systems.

METHODS OF EMPLOYMENT

> If we used the telegraph to relay mobilization orders quickly and then used railroads to concentrate troops from bases scattered throughout Prussia, we could concentrate the main effort at the key battle location of a campaign. We wouldn't

---

[24] Gordon R. Sullivan and Anthony M. Coroalles, "The Army in the Information Age" (Carlisle Barracks, PA: Strategic Studies Institute, 1995.

[25] Elizabeth G. Book, "Information Warfare Pioneers Take Top Pentagon Positions," *National Defense Magazine*, January 2002, 2.

> have to mobilize the army, then concentrate it, then march it to where we hoped the key battle would occur.[26]

The United States have employed information warfare in order to gain the advantage over the enemies. Many direct capabilities and activities must be integrated to achieve a coherent information warfare strategy. Additionally, intelligence and communicate support are critical to conducting offensive and defensive information.

Employed as an integrating strategy, information warfare focus on the vulnerabilities and opportunities presented by the increasing dependence of the United States and its adversaries or potential adversaries on information and information systems. In the Department of Defense (DOD), the ultimate strategic objective of offensive information warfare is to affect adversary of potential adversary decision makers to the degree that they will cease actions that threaten United States national security interest.[27] Information warfare may have their greatest impact as a deterrent in peace and during the initial states of crisis.

Accurate and timely information has always been eagerly sought by armed forces and defence planers througout history. Today, technology changes have made vast amounts of information virtually available at the click of a mouse. Improved information processing techniques and pattern recognition may soon provide highly effective and automated decision

---

[26] Newt Gingrich, "Information Warfare: Definition, Doctrine and Direction," Address to the National Defense University Washington, DC, May 1994.

[27] United States Government, Joint Publication 3-13, "Joint Doctrine for Information Operations," February 1996.

support systems. Combined with technologies that provide dominant battlefield knowledge, such systems offer to the military commander exactly what he seeks.[28]

During the Kosovo War, an information operations (IO) cell was used by the military and it had great success. It was the first time a Joint Task Force staff was organized with an information cell, which was composed of military personnel with expertise in various facets of information operation. Offensive information operations included a wide range of actions, from destroying an enemy's information infrastructure to more traditional electronic warfare attacks, such as jamming an enemy's radar and attacking computer networks.[29] The secret new arts of disrupting enemy capabilities through cyber-space attacks appeared to have been a big part of the campaign.

The Afghanistan conflict brought home to the armed forces another method of war, which was built around an unprecedented dependence on information. The Pentagon relied on a global umbrella of new information systems, ranging from satellites far overhead to surveillance drones circling the battlefield to Special Forces troops with laser designators on the ground, to find targets, transmit information about them and their attack.[30] Most importantly, a communication network that permitted gigabytes of information to rocket from Afghanistan to key leaders in Saudi Arabia, on ships at sea and even as far as Tampa, where the commander of the campaign, General Franks, spent most of the war.

---

[28] Kapil Kak, "Revolution in Military Affairs – An Appraisal"

[29] Bob Brewin, "Kosovo Ushered in Cyberwar," *Federal Computer Week*, September 1999. 2.

[30] Veron Loeb and Thomas E. Ricks, "1's and O's Replacing Bullets in United States Arsenal," *Washington Post*, February 2002.

In Iraq, the United States military and other government agencies initiated a surreptitious email campaign inside Iraq prior to the beginning of the current war. This was just the beginning of a "psychological warfare campaign" to convince the Iraqi leadership they cannot win a war against the United States and its allies. Thousands of email messages were sent out to senior military personnel. This type of information warfare is a method of "psychological warfare campaign" to convince the Iraqi leadership they cannot win a war against the United States and its allies. These messages were being sent by radio broadcast in the days ahead from United States airborne and ground platforms.

A second wave of messages was sent to private cell phone numbers of specially selected officials. The disguised emails, being sent to key Iraqi leaders, urge them to give up, to dissent and to defect. Additionally, the United States for months have been dropping leaflets over the no-fly" zones, warning Iraqi soldiers not to fire at American aircraft and stressing Saddam's suppression of the Iraqi people.

Retired Navy Rear Admiral Stephen Baker, a senior fellow at the Center for Defense Information, notes the e-mail campaign represents a "new and emerging part of the [psychological operations] strategy.[31] It is considered one of the most important phases of the conflict – the psychological operations leading up to the war. By informing Iraqi military

through leaflet drops, radio broadcasts, personal telephone calls and e-mails that they will sustain

---

[31] Dan Caterinicchia, "DOD Confirms Iraq E-mail Campaign," *Federal Computer Week*, January 2003.

heavy losses unless they defy Saddam Hussein, the United States and it allies are hoping to ensure a quick victory.

The United States Air Force has also play a signification in the employment of information warfare, and is prepared to employ a man-made bolt of lightning powerful enough to fry sophisticated computer and electronic components in weapons. Additionally, the Air Force is looking at ways of putting so-called High-Powered Microwave (HPM) beams on aircraft and cruise missiles. These devices are designed to destroy electronic equipment in command, control, communications, computer targets, and zapping the circuitry of everything from jet fighters to television sets while leaving people unscathed.[32] They produce an electromagnetic field of such intensity that their effect can be far more devastating than a lighting strike.

Additionally, the employment of UAVs (unmanned/unpiloted aerial vehicles) were used for investigation, observation, long-distance reconnaissance, and remotely guided attacks. They brought major advantages to the forces and many technical benefits beyond that of satellites. Some of the reports indicate that the military can maneuver some of its fleet of spy satellites to provide pictures of a target every two hours, but UAVs provide continuous watching without interruptions.

Military planners at the United States Central Command are currently using the burgeoning field of information warfare – including electronic attacks on power grids, communications systems and computer networks, as well as deception and psychological

---

[32] David Windle, "E-bomb" May See First Combat Use In Iraq," *New Scientist*, August 2002.

operation to sway Iraqi public opinion. James Wilkinson, US Central Command, notes, "The goal of information warfare is to win without ever firing a shot."[33]

Further, the United States will increasingly rely on sensors to collect information on the battlefield and thereby find targets. There are currently six secret National Reconnaissance Office high-resolution imaging satellites, each costing $1 billion, maintaining an almost hourly watch on Iraqi facilities.[34] Future architectures include a mixture of imagery, radar, infrared, and electronic intelligence sensors in space, on aircraft (e.g., AWACS, JSTARS, Rivet Joint, Cobra Ball), on unmannaerial vehicles, on ship (e.g., Aegis radars), and in ground facilities (e.g., counter-battery radar) supplemented by a wider array scattered on the terrain (e.g., microphones), in the terrain (e.g., seismic sensors) or in the water (e.g., sonobuoys). Over the next 20 years the various data streams produced by theses sensors will be networked, merged, and intelligently fused so as to be able to see more things, faster, and in greater detail.[35] The combination of sensors, networks, and weapons has been referred to as a "System of Systems." When integrated it would reify the RMA as much as any other single innovation.

[33] Thomas Shanker and Eric Schmitt, "Cyber-Warfare in Iraq Already Has Broken Out," New York Times, February 2003.

[34] Craog Cpvai, "Secret NRO Recons Eye Iraqi Threats," Aviation Week & Space Technology, September 2002.

[35] Martin C. Libicki, "Information Dominance," National Defense University, Institute for National Strategic Studies, Number 132, November 1997.

INFORMATION WARFARE DOMINANCE OF THE BATTLEFIELD

> We live in an information-dominate era. Technological discoveries…are changing the nature of war and the way we prepare for it.[36]
>
> William Perry,
> Former United States Secretary of Defense

As the world enters the information age, the United States must stay ahead of changes in warfare. The future force of the United States must be prepared to conduct quick, decisive, highly sophisticated operations. Decisive victory in the 21st century will be achieved by dominating the enemy in speed, space and time, and by achieving and sustaining a high pace of continuous operations in all types of environments. Emerging information and digital technologies will significantly enhance the armed forces capabilities by creating a synergistic effect among weapons and organization.

Conventional warfare with the use of tanks, aircraft, ground-troops, submarines, missiles, and defense systems, is starting to be replaced by the firing of binary digits across a vastly different battlefield then in decades past. Information is the new art of subverting the enemy in the new battles of the 20th century and beyond.[37] Information warfare will also be used to disrupt the use of precision bombs, and means to break into computer systems that control a country's infrastructure, with the result that the civilian infrastructure of a nation would be held hostage.

---

[36] Nunes, Paulo Fernando, "The Impact of New Technologies in the Military Arena: Information Warfare," The Information Warfare Site, March 2001.

Command and Control

The use of process data will dominate the battlefield and will play a significant role in the Global Command and Control System (GCCS). This system is the Department of Defense's computerized system of record for strategic feedback, and execute more demanding, higher precision requirements in fast moving operations.[38]

The GCCS will provide combatant commanders on the battlefield one predominant source for generating, receiving, sharing and using information securely. Additionally, it will provide surveillance and reconnaissance information and access to global intelligence sources as well as data on the precise location of dispersed friendly forces. The GCCS will enable the warfighters to plan, execute and manage military operations. The system helps joint force commanders synchronize the actions of air, land, sea, space, and special operations forces.[39]

Army Force XXI

In the Army, Force XXI process will be a versatile force with the capabilities America will need in the next century. Force XXI draws on rigorous experimentation and leverages the power of information from the foxhole to the industrial base. Additionally, Force XXI will maximize the science of modern digital technology, the art of integrating doctrine and

---

[37] Eriv Hrovat, 3.

[38] The Global Command & Control System (GCCS), www.gccs.disa.mil/gccs

[39] United States Department of Defense, Defense Link, "Global Command and Control System Adopted," September 1996.

organization, and skills of the Army's quality people. With information age systems, Army intelligence will do much more than merely collect and process data. Information age technology creates the opportunity to detect, target, and attack enemy forces throughout the depth of the battlefield rapidly. Army intelligence operations will be a critical force multiplier, with requirements to simultaneously deny our potential adversaries access to our critical information, to gain intelligence through access and analysis of enemy information, and to engage in operations that will deny enemy use of command and control.

The digitized battlefield is the cornerstone of the horizontal technology integration initiative and is critical as the Army progresses with the Force XXI process. Digitization is the application of information technologies to acquire, exchange, and employ timely battlefield information. It will enhance situational awareness and provide the means for information dominance by enabling friendly forces to share a common picture of the battlefield while communication and targeting in real or near-real time. Digitization will reduce the "fog of war" and decrease decision-making time by optimizing the flow of information. It will allow the synchronization of combat power at critical times and places faster than an adversary can.[40]

Additionally, the product of the Force XXI process will be Army XXI – a versatile force with the capabilities to win the nation's wars, prevent conflict, and sustain operations. Army XXI will use digital technology to optimize the flow of information and enhance situational awareness. Commanders and soldiers will have a much clearer picture of where friendly and enemy forces are located. When this concept was taken to the National Training Center in

[40] Into the 21st Century

March 1997, observers reported that operations could be planned and carried out in half the time.[41]

Navy

The Navy has possibly more personnel engaged in "nuts and bolts" information warfare than any other Service and has for decades practiced some of the elements of Command and Control Warfare, defined as "military strategy that implements information warfare on the battlefield."[42] The Navy's emerging network-centric concepts holds that the conjunction of communications, sensors, and weapons systems is more important than the individual aircraft, ships, or submarines on which they are deployed. It was noted that "carrier operations in March 1996 off Taiwan were executed with only three written orders; everything else was communicated in real time.[43]

Air Force

The Air Force has taken dramatic steps to move into information age warfare. The new expeditionary warfare concept seeks the ability to conduct distributed collaborative planning literally across the world even up to the point that the missions of entire air wings could be reprogrammed even as aircraft are warming up for takeoff. Other initiatives, such as sensor-to-shooter, permit imagery from space and airborne assets to be conveyed to pilots in real time.

[41] Martin C. Libicki, "Information Dominance," National Defense University, Institute for National Strategic Studies, Number 132, November 1997.

[42] Daniel Kuehl, "Joint Information Warfare," *Defence Journal*, March 1998.

Dr. Sheila Widnall, Secretary of the Air Force, and General Ron fogleman, Chief of Staff, expresses the broadest view of information warfare of any of the Services, stating information is a "realm" to be dominated in a manner alike to air or space.[44]

CONCLUSION

Information Warfare is here to stay, and will dominate the battlefield in the 21st Century. There are many challenges that will face the United States forces, and will continue to do so in the years ahead. However, the United States military is preparing for those challenges every day; the evolution into a 21st century force with the capabilities for continued full spectrum dominance is an attempt to meet head-on the warfighting and affordability challenges of the new century.

The future forces will provide American soldiers with unprecedented advantages, combining the latest technology with those elements of character that have long made America's Army a formidable foe.[45] The Army has and will always command the ground aspect of warfare. The information revolution will provide battlefield awareness unimaginable today. The fog of war will be greatly reduced if eliminated. The enemy's fog will be extended to a completed blindness.

---

[43] Libicki.

[44] Kuehl.

[45] Into the 21st Century, 21st Century Force of Decision

The Navy and Marine Corps will continue to control the seas and provide the heavy strategic reach capability that the United States currently enjoys. Global sensory networks will ensure the Navy has the capability. The Air Force and its command of the skies will continue. Tomorrow's air defense weaponry and electronic warfare will be unrecognizable to today's military leaders.

The RMA debate is an intriguing but complex concept, subject to multiple definitions, and with many possible implications for United States force planning and security. There are arguments to defend each major proposal, to be sure; none of the major RMA concepts that have been articulated are unintelligent or unworthy of debate. The cost of the information warfare RMA is not cheap, and will greatly enhance the capabilities and initiatives that are proposed by the *Joint Vision 2010* and *Joint Vision 2020*.

BIBLIOGRAPHY

Blaker, James R., Understanding the Revolution in Military Affairs (RMA), New Democrats Online, (February 1997):

Book, Elizabeth G., "Information Warfare Pioneers Take Top Pentagon Positions," *National Defense Magazine*, (January 2002):

Brewin, Bob, "Kosovo Ushered in Cyberwar*," Federal Computer Week*, (September 1999):

Cpvai, Craog, Secret NRO Recons Eye Iraqi Threats, *Aviation Week & Space Technology*, (September 2002):

Caterinicchia, Dan, "DOD Confirms Ira E-mail Campaign," *Federal Computer Week*," (January 2003):

Diplomatique, Le Monde, "Developing The Weapons of the 21st Century," (February 1998):

Epstein, Edward, "United States Has New Weapon Ready. It Could Kill Circuits But Spare People," *Chronicle Washington Bureau*, (February 2003):

Gingrich, Newt, "Information Warfare: Definition, Doctrine and Direction," Address to the National Defense University Washington, DC, (May 1994):

Gold, Philip, "Rumsfeld's Revolution: Is the Big Sift in Defense Really Happening at Last?" Discover Institute, (June 2001):

Johnson, Craig L., "Information Warfare – Not a Paper War," *Journal of Electronic Defense* 17, Number 8, (August 1994):

Hrovat, Eric, "Information Warfare: The Unconventional Art in a Digital World," *SANS*, (June 2001):

Ibrugger, Lothar, "The Revolution in Military Affairs," NATO Parliamentary Committee Reports, (November 1998):

Kak, Kapil, "Revolution in Military Affairs – An Appraisal"

Kuehl, Daniel, "Joint Information Warfare," Special Report, *Defence Journal*, (March 1998): p2.

Loeb, Vernon and Ricks, Thomas, 1's and O's Replacing Bullets in U.S. Arsenal, *Washington Post*, (February 2002):

Libicki, Martin C., "Information Dominance," National Defense University, Institute for National Strategic Studies, Number 132, (November 1997):

McLendon, James W., "Information Warfare: Impacts and Concerns," Battlefield of the Future"

Miller, John H., "Information: Warfare: Issues and Perspectives," Institute for National Strategic Studies, (March 1995):

Nunes, Paulo Fernando Viegas, "The Impact of New Technologies in the Military Arena: Information Warfare," The Information Warfare Site, (March 2001): p1.

Owens, Willam with Offley, Edward, "Lifting the Fog of War," Farrar, Straus and Giroux, New York: (2000)

Shanker Thomas, and Schmitt, Eric, "Cyber-warfare in Iraq already has broken out," *New York Times*, (February 2003):

Stein, George J., Information Warfare, *Airpower Journal*, (Spring 1995):

Sullivan, Gordon R. and Coroalles, Anthony M., "The Army in the Information Age" (Carlisle Barracks, PA: Strategic Studies Institute, 1995.

Windle, David, "E-bomb" May See First Combat Use In Iraq," *New Scientist*, (August 2002):

BBC News, "United States is Working on Lighting Weapon," BBC New, (January 2003):

Government Publications

United States Government, *Field Manual 34-1,* "Information Operations, Chapter 7

United States Government, Department of Defense, *Joint Publication 3-13,* "Joint Doctrine for Information Operations,"

United States Government, Department of Defense, *Joint Vision 2010,*

United States Government, Department of Defense, *Joint Vision 2020,*

IWS – Information Warfare Site

New Scientist, "E-bomb" may see first combat use in Iraq, August 2002.

Web Sites

Schaik, Cisco Van, "Information Warfare in the 21st Century," www.mil.za/CSANDF

Thompson Jr., Robert, "Information Warfare," Kaman Sciences Corporation, www.dacs.dtic.mil, Spring 1998