AU/AWC/RWP123/97-04

AIR WAR COLLEGE

AIR UNIVERSITY

CYBER TROOPS AND NET WAR

THE PROFESSION OF ARMS IN THE INFORMATION AGE

by

Arsenio T. Gumahad II
Lt Col, USAF

A Research Report Submitted To The Faculty

In Fulfillment Of The Curriculum Requirement

Advisor: Col Richard Szafranski, USAF

Maxwell Air Force Base, Alabama

1 April 1996

DISTRIBUTION A:

Approved for public release; distribution is unlimited.

Air War College
Maxwell AFB, Al 36112

Disclaimer

Contents

Abstract

Information is emerging as the catalyst for a major change. It is redefining wealth and power in modern post-industrial societies. This paper discusses the societal, political, and economic ramifications of this unprecedented technological growth. The military faces the newest revolution in military affairs as it enters the 21st century. The military is affected internally as it evaluates its continued role in the new age. Both the quality of its personnel and its organizational structure are affected to a degree. The external threats are examined and a future military doctrine which accounts for information as a dominant instrument in future wars is discussed.

Chapter 1

Introduction

Victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after the changes occur.

—Guilio Douhet
The Command of the Air

Guilio Douhet appeared prophetic when predicting the contribution of air power to the changing nature of warfare this century. The visionary Douhet, along with his contemporary Brigadier General Billy Mitchell, brought recognition of air power as a powerful military instrument. Today, information and information technology are viewed in a similar fashion. Many think that success in future wars hinges in the ability to exploit information. But, what is "information"?[1] The definition is critical to the analysis of this potential new tool in modern warfare.[2] Information begins as derived data from observable facts or events. Interpreting data leads to the development of information. The ultimate interpreter is the person receiving the data. At times, though, an observed event is too complex for the human mind to dissect. Machines are used, therefore, to reduce the data into a manageable and comprehensible set. These machines are information systems and they come in both hardware and software forms.

Modern society is dependent on the use of information systems. The last three decades of technology growth made such systems more available and affordable.

Televisions, computers, pagers, cellular phones are only a few of the products of information technology. A growing number of people, organizations, and even nations use these devices for business transactions, personal affairs, and government functions. On one hand, information and information systems are becoming an indispensable part of modern life. On the other hand, these systems are increasingly the targets for exploitation. Many see possibilities in using information as a potent instrument in war. The United States Air Force subscribes to this new form of conflict resolution by dubbing it "information warfare." Information warfare is "any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military's information functions."[3]

The military's use of information in war is not new. Information has been a basic war fighting requirement for all of history. Technological advances made information more available than ever before. Information now may be in a position to become an effective weapon in future wars. The military is formulating doctrine for using information as a weapon effectively. This development is crucial if the United States military expects to take full advantage of the power inherent in information. Historically, the military have problems with expedient doctrinal development. It took decades from the time the Wright brothers flew the first airplane in Kitty Hawk to the development of the first usable doctrine for the use of air power. Likewise, the potential of information warfare is not yet fully realized, despite the emergence of information systems about forty years ago.

This paper addresses the ramifications of the unprecedented explosion of information and technology to the US military establishment. The first step is to summarize how information affects the military of the twenty-first century and creates the potential of

using information as an instrument of policy making and war (Chapter II). The paper traces the information revolution back to the development of critical electronic devices several decades ago and discusses the societal, economic, political, and military trends arising from technological advancements (Chapter III). This is followed with a discussion introducing information as the new catalyst for an emerging "revolution in military affairs" and reviews past "revolutions" since the Hundred Years War to provide historical context (Chapter IV). The changes resulting from the information age revolution bring challenges to the United States military with new threats to international stability and complicating future military missions (Chapter V). Legal and moral issues are presented in this chapter, highlighting concerns over the legality of conducting information warfare. The structure of the US military in the twenty-first century is assessed and possible changes in organization, training, and equipment are discussed (Chapter VI). For information and information systems to become effective as weapons in future wars, the development of doctrine is necessary. The application of information warfare is discussed at all levels of war. In the concluding section, the tools of the information warfare trade are examined for both future defensive and offensive applications (Chapter VII).

Notes

[1]*Joint Pub 3-13 (*1995 Draft) defines information as any communication or representation of knowledge such as facts, data, or opinions in any medium or form. *Joint Pub 1-02* defines it as the meaning that a human assigns to data by means of the known convention used in their representation.

[2]John Arquilla and David Ronfeldt, "Information, Power, and Grand Strategy: In Athena's Camp," *Information and National Security*, edited by Stuart Schwartzstein (Center for International and Strategic Studies, Washington DC, forthcoming 1996). In this paper Arquilla and Ronfeldt introduces information as a "physical property—as physical as mass and energy, and inherent in all matters." This view of information treats "all military systems as being based on, if not composed of, information." The concept of using information as a warfare means becomes evident. "If information is a veritably

physical property, then in the information age winning wars may depend on being able to hurl the most information at the enemy, while safeguarding against retaliation."

[3]*Cornerstone of Information Warfare*, foreword by General Ronald R. Fogleman, USAF Chief of Staff and Sheila E. Widnall, Secretary of the Air Force, 1995, 4.

Chapter 2

The Framework

A New Society

According to John Halton "the world is undergoing a major social and economic change, a second Industrial Revolution, through the new information processing technology of communications and computers."[1] High-speed computers can solve some extremely complex technical problem in fractions of a second. Satellite communications are linking remote areas of the globe. Fiber optic cables provide faster, more reliable, and more cost effective transfer of information. Cellular phones allow mobility, freedom and instant connectivity. All of these systems comprise the "information infrastructure."[2] The physical world "shrinks" in this complex high-speed world of electrons and bits. The flow of information, via this infrastructure, is real time—instant data to the users. Physical distance does not matter in this environment. According to Massachusetts Institute of Technology Professor Nicholas Negroponte, "digital living will include less and less dependence upon being in a specific place at a specific time."[3] Today, geographically separated parties conduct business using the information infrastructure of fiber optics, satellites, and video technology. A "uniligual" world, united by an electronic language spoken via a global network of microprocessors and personal computers, is emerging.

Alvin and Heidi Toffler envision a "third wave" in human development consisting of a society dependent on information as the source of power and wealth[4]. This "third wave" society, the Tofflers argue, is rapidly replacing the "second wave" societies formed during the industrial revolution.

Information Dominance[5]

The United States military is increasingly emphasizing "information dominance" as a prerequisite to future operations and contingencies. According to the DOD's 1994 Annual Report, information dominance over an area of operations is "key to achieving success in future crisis or conflicts."[6] Denying, exploiting, corrupting and destroying the enemy's information functions while protecting US information systems result in information dominance. Military space systems have become synonymous with the information age, and thus information warfare. Their ability to direct information flow anywhere on earth, provide weather data, and intelligence is invaluable to US military forces. To some, the 1991 Gulf War portrayed the first "space war"—where space assets were employed at all levels of the operation from real time communications and precision navigation to battle damage assessment.[7] Additionally, precision munitions extracted heavy losses against Iraqi targets. The use of these modern systems reflects a modern warfighting concept. Space systems provided information on troop concentration, weather data, wideband communications, and imagery.[8] This information, in turn, provided precise target coordinates for the "smart" weapons used by coalition forces. This conflict represented the first extensive and effective use of information and

information systems in combat. The Gulf war "drew international attention to the value of information in systematically destroying an enemy's ability to conduct war."[9]

The continuing information revolution will affect the profession of arms over the next several decades. The organization, training, and employment of US military forces remain key elements in conducting future campaigns. The potential influence of the information revolution on the military force structure and its future capabilities is tremendous. The US military must examine its internal makeup[10] for its continued viability in the new age. Future warfare will depend more on information and technology. The Gulf War serves as the harbinger of information age warfare. A revolution in military affairs (RMA)[11] involving information may be on the horizon[12]. The current doctrine and organization of the US military developed based on experiences during the nineteenth and twentieth centuries needs re-evaluation.

Developing Doctrine

To take full advantage of innovations in information technologies, organizational and doctrinal changes are required. Real time communications, effective command and control, and rapid and precise information processing and dissemination provide undeniable offensive and defensive advantages to US operational forces. To Lt Gen. Paul E. Funk, "success in combat can be attributed to the commander who has the clearest picture of the battlefield."[13] Understanding the offensive and defensive nature of using information in warfare requires an analysis of information warfare's total scope. Some see information only in a supporting military role—there to enhance the military's traditional combat missions. To others, information warfare promises to provide a powerful

capability at the strategic level, at the point prior to general escalation and deployment of combat forces for action. According to Air Force Colonel Richard Szafranski "information warfare need not be deferred until hostility becomes open."[14] Conceivably, information warfare can provide rapid and unqualified victory even prior to commencement of physical hostilities between warring parties. R.L. Dinardo and Daniel J. Hughes warn, however, of potential problems with the employment of such weapons. They argue that proponents of information warfare "fail to consider that the same measures might just as easily lead to entirely unanticipated results or even to consequences that would be inconsistent with or counterproductive to the original intent."[15] Nevertheless, the success during the Gulf War stimulated military forces to using information and information technologies in fighting future wars.

When developing strategies and doctrine for employing information warfare, the military must consider certain moral questions and ethical issues.[16] As discussed, the technology innovation triggering the current RMA is the same catalyst for major societal changes. These changes create "new sets of potential operational and strategic targets"[17] —the economy, the computerized air traffic control, subways, and more. The application of a strategic level information warfare may be bloodless, but could ultimately result in the total paralysis of the adversary state, beyond merely rendering its military less effective or even ineffective in combat operations. The resulting human suffering among non-combatants may be unfathomable; the psychological impact too costly to accept for the American people. Colonel Szafranski argues that the decision to develop information weapons or conduct information warfare must "be made consciously and deliberately and with an understanding of the moral and ethical risks of information warfare."[18]

Information and information systems are an undeniable part of life today. The influence of the information revolution is worldwide. However, its full impact on society, politics, the economy, and the military twenty to thirty years from now is hard to foresee. The rise of new information-age challenges to the United States is inevitable. Information is becoming a dominant factor in the evolution of future societies.[19]

Notes

[1]John Halton "The Anatomy of Computers," *The Information Technology Revolution*, edited by Tom Forester (MIT Press, Cambridge, Mass., 1985), 3.

[2]The components of the 'information infrastructure' include scanners, keyboards, TVs, Fax machines, switches, computers, CDs, weather information, cable, wire, satellites, fiber, microwave nets, cameras, people, etc. according to *Information Warfare—Legal, Regulatory, Policy, and Organizational Considerations for Assurance*, July 4, 1995, 2-4.

[3]Nicholas Negroponte, *Being Digital* (Vintage Books, New York, NY, 1995), 165.

[4]Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Little-Brown, Boston, Mass, 1993).

[5]Information dominance is defined in AFDD 1, *Air Force Basic Doctrine* (First Draft, August 15, 1995) as that degree of superiority in information functions that permit friendly forces to operate at a given time and place without prohibitive interference by the opposing force.

[6]Excerpt from the *Strategic Assessment 1995—US Security Challenges in Transition*, prepared by the Institute for National Strategic Studies, published in 1995 but written in mid-1994 and revised to include development through November 1994, 161.

[7]James W. Canan, "Space Support for the Shooting Wars," *Air Force Magazine*, April 1993, Vol. 76, No. 4, 31. Space systems came through for coalition forces in the Persian Gulf War, often with stunning results, in such areas as navigation, weather, surveillance, missile warning, and communications.

[8]Craig Covault, "USAF Urges Greater Use of SPOT Based on Gulf War Experience," *Aviation Week and Space Technology* July 13, 1992, 61—"the use of SPOT imagery was instrumental in the US/Allied air campaign against Iraq. It was used extensively for attack planning, target coordination, and mission execution"

[9]William B. Scott, "Information Warfare Demands New Approach," *Aviation Week and Space Technology*, May 13, 1995, 85.

[10]These include personnel, leadership, and organization.

[11]Jeffrey McKitrick, et al. "Chapter 3: The Revolution in Military Affairs," *Battlefield of the Future—21st Century Warfare Issues*, edited by Barry Schneider and L. E. Grinter (AU Press, Maxwell AFB, 1995), 65—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.

[12]John Arquilla and David Ronfeldt "Cyberwar is Coming," 1992, reprinted in Air War College Handbook on Conflict and Change, Maxwell AFB, 1995, 378.

[13]Lt Gen Paul E. Funk, US Army, "The Army's Digital Revolution," *Army*, Feb. 1994, 33. At the time of this article, Lt Gen Funk served as the Commanding General, US Army III Corps and Ft Hood, TX.

[14]Colonel Richard Szafranski, "A Theory of Information Warfare—Preparing for 2020," *Airpower Journal*, Spring 1995, Vol. 9, No. 1, 58.

[15]R. L. DiNardo and Daniel J. Hughes, "Some Cautionary Thoughts on Information Warfare," *Airpower Journal*, Winter 1995, Vol. 9, No. 4, 69-77.

[16]Douglas Waller, "Onward Cyber Soldiers," *TIME*, August 21, 1995, 38-44.

[17]McKitrick, et al., 66.

[18]Szafranski, 56.

[19]Carl H. Builder and Brian Nichiporuk, *Information Technologies and the Future of Land Warfare* (RAND Corp., Santa Monica, Ca, 1995), 25-45.

Chapter 3

Information—The New Enabler

According to Joseph N. Pelton, author of *Future View*, the information revolution is "changing every aspect of our world. Basic power relationships are changing—militarily, politically, and socially. Our economy and our jobs are being transformed."[1] Computer technology is the centerpiece of the emerging information age. The computer goes back as early as 1930 when Vannebar Bush built the first analog computer.[2] The first digital computer was built in 1945, but was impractical for potential real-world use.[3] It weighed tons and occupied almost an entire building. The two events which took the digital world from obscurity into a common everyday tool were the invention of the transistor in 1948 and the integrated circuit in 1960. The growth of this technology is staggering. In 1960, a single integrated circuit contained one transistor. In 1964, it had 1000 transistors. By 1975, 10000 transistors were in one microprocessor chip. By the turn of the century, about 100 million transistors are expected on a single integrated circuit chip.[4]

Computer systems are more common now that ever before. Their introduction is faster than that of any other system.[5] The technology of miniaturization resulted in greater digitization and computerization of virtually every device and apparatus used. It is hard to find an element of everyday life not affected by micro technology today. Cellular phones,

alarm clocks, even automobiles now use microprocessors to power their functions and guide their performance.

The "Internetted" World

The rapid expansion of information technology creates an environment where information is readily accessible and available to all seeking it. Local area networks linking two or more at one level are rapidly expanding into wide area networks connecting remote areas of one country to the rest of the world. With the Internet, the globalization of information flow and exchange is a reality. The genesis of this capability is the Department of Defense sponsored Advanced Research Projects Agency Network (ARPANET) in 1970, an effort to connect researchers from a distance via computers.[6] The Internet is growing at a rate of 25 percent per month. In the US, the number of Internet users will reach 100 million people by 2000[7]. This trend is not a unique phenomenon limited to the US. The rest of the world is following closely behind. According to one commentator, "Entire countries are being wired. Third World countries, such as Turkey, are beginning projects that will effectively move their country from near medieval conditions into the information age."[8] In *Being Digital*, Negroponte observes that the "fastest growing number of Internet hosts in the third quarter of 1994 were Argentina, Iran, Peru, the Philippines, the Russian Federation, Slovenia, and Indonesia (in that order)."[9] He adds, "the Internet is not North American anymore. Thirty five percent of the hosts are in the rest of the world, and that is the fast-growing part."[10]

Information and Democratization

Information availability and access compare to the initial introduction of mass print in the fourteenth century. The invention of the printing press signaled the move toward a better-informed population. The mass production of newspapers and books educated society in the years that followed. Free and open discussions of ideas and concepts transpired. In the 1830s, newspapers became "the great organ and pivot of government, society, commerce, finance, religion, and all human civilization."[11] To those professing democratic ideals, newspapers and the free flow of information were building blocks toward more democratic thinking. Likewise, in today's environment with computers and the Internet, individuals can freely discuss what is on their minds. These individuals could be from different countries, from a different culture and from divergent religions. It does not matter. Some observers suggest that "as more and more people interact via electronic networks in what is termed 'cyberspace'[12], their thinking about 'the system' and the world in which they live will invariably change."[13] New generations of citizens are raised with the heavy influence of technology in the background. The impact of information which is now readily available to them can not be underestimated. "Information in electronic form is difficult to control, data networks, financial data flows, electronic mail, TV and news broadcasts do not stop at national borders."[14]

Redefining Wealth

According to leading Japanese futurist Yoneji Masuda "the information society will function around the axis of information rather than material values."[15] The Tofflers agree that information is the critical element for power and wealth in the new age. Masuda

envisions the growth of a world society free of overruling power, essentially a classless society, each person exercising total independence and freedom of choice. The hierarchical form of social interaction is no longer dominant in the information age. To Masuda, the society will be "horizontally functional, maintaining social order by autonomous and complementary functions of a voluntary civil society."[16] The financial and economic sectors of many nations rely on the global information infrastructure as well.[17] Digital banking and electronic funds transfer change how money is exchanged and used. The total economic worth of nations or financial organizations is now conveniently expressed in bits and bytes. The global reach of information is redefining present concepts of organizational relationships and dynamics. The characteristics of an information age world is evident today. Thus, the arguments presented by futurists, like Masuda and Toffler, have merit.

The information age will challenge the US military in two areas: internally, in terms of how it organizes, recruits, trains, and leads forces into battle and externally, in the way it handles future conflicts. Information is the catalyst for a new form of warfare. The US military must remain forward-looking. It must plan for possible contingencies in response to these security threats. The military is on the verge of a new revolution in military affairs. The success of US and allied forces in the Gulf heralds the arrival of this new RMA.[18]

Notes

[1]Joseph N. Pelton, *Future View* (Baylin Pub, Boulder, Co. 1992), 10.

[2]Ellis Mount and Barbara A. List, *Milestones in Science and Technology* (Oryx Press, NY, 1987), 4.

[3]Ibid., 25. It contained 18,000 tubes , weighed 30 tons and stood 2 stories high.

Notes

[4]John L. Petersen, *The Road to 2015: Profiles of the Future* (Waite Group Press, Corte Madera, CA. 1994), 30.

[5]Ibid., 32—information systems include televisions, video recorders, cellular phones, etc.

[6]Howard Rheingold, *The Virtual Community: Hometeaching on the Electronic Frontier* (Addison-Wesley Pub., Menlo Park, CA. 1993), 7.

[7]Petersen, 37-38.

[8]Lt Col David M. Komar, USAF, *Information Based Warfare: A Third Wave Perspective*, Air War College Research Report, May 1995, 10.

[9]Negroponte, 182.

[10]Ibid.

[11]Stephen Lubar, *Infoculture* (Houghton Mifflin Co., New York, 1993), 402. Quoting James Gordon Bennet, one time publisher of the New York Herald.

[12]Bob Cotton and Richard Oliver, *The Cyberspace Lexicon* (Phaidon Press, London, UK, 1994), 54. Cyberspace is defined as the virtual space of computer memory and networks, telecommunications and digital media. It is an emerging environment created, on the one hand, by the global network of telephone, satellite communications, and computer networks, interactive cable TV and ISDN, and on the other by the internal quantum space of the microchip, and electromagnetic and digital-optical storage technologies.

[13]LCDR William M. Luoma, USN, *Netwar: The Other Side of Information Warfare*, Naval War College Thesis, February 8, 1994, 8.

[14]Luoma, 9.

[15]Yoneji Masuda, "Computopia," *The Information Technology Revolution*, edited by Tom Forester (MIT Press, Cambridge, Mass, 1986), 620.

[16]Ibid., 623

[17]*Strategic Assessment 1995*, 152—Direct Broadcast Satellites serves European, Japanese, and other Asian audiences. Global cellular communications will offer services not only to remote locations but also under circumstances not dictated by local phone systems. In 1993, the world equaled the US in the number of cellular telephone subscribers.

[18]Thomas A. Keaney and Eliot A. Cohen, *Gulf War Air Power Survey Summary Report* (Washington DC, 1993), 235—There are two schools of thought on the Gulf War. One school argues that the Gulf War confirms the arrival of an RMA driven by advances in information age technologies (micro electronics, telecommunications, satellites, lasers, etc.). The other school sees the Gulf War as evidence that technology has finally enabled airmen to fulfill the expectations that air power advocates advanced in the 1920s and 1930s.

Chapter 4

A New Revolution in the Making

The form of any war—and it is the form which is of primary interest to men of war—depends upon the technical means of war available.

—Guilio Douhet,

Past RMAs

As many as ten military revolutions were recorded since the thirteenth century[1]. Two significant revolutions occurred during the period of the Hundred Years War (1337-1453) alone: the infantry revolution which peaked in the 1340s and 1350s changed the employment of the infantry in war; and the artillery revolution which changed siege warfare in the 1420s to 1440s.[2]

The cavalry dominated medieval wars before the infantry revolution. The mobility and quickness of the cavalry gave them the advantage and they were generally victorious in combat.[3] Dismounted men-at-arms did not singularly win battles during this time although they played major parts in these engagements.[4] The development of the six-foot long bow, which replaced the standard crossbow, combined with a change in operational doctrine of coordinated attack between dismounted soldiers and archers, changed land warfare during this period. At the battle of Crecy in 1346, the English using foot soldiers and archers overwhelmed a cavalry dominated French army three times their size.[5]

Warfighting shifted from one dominated by the mounted cavalry to the infantry. In the decades to follow, major cavalry actions on the field were rare.[6]

In the second revolution of the Hundred Years War, a major development in the technology of gunpowder artillery made the difference in achieving victory against well-entrenched forces. In siege warfare, the defense usually had the advantage. The attacking army won only after long sieges by starving the defenders of a beleaguered garrison. It was not uncommon, therefore, for sieges to last up to one year. However, a well-defended garrison could still frustrate an attacking army. The offensive momentum was usually lost during long sieges. The battle's Clausewitzian "culminating point"[7] is reached when the attacker can no longer sustain the siege. The defenders mount a counter attack and defeat the now retreating invading army. A technical innovation in artillery changed the form of siege warfare. Innovators realized that greater accuracy and firepower was possible by lengthening the barrels of artillery guns. An operational change was adopted which took advantage of this technological change. Targeting the walls and attacking the supporting infrastructure of fortifications caused once impenetrable garrisons to be overrun more quickly than ever before.

The revolution in fortification around the 1520s was effectively a counter revolution against the earlier successes of the artillery innovation.[8] Also around this time, the Gunpowder revolution materialized with the introduction of armor-piercing muskets coupled with a new operational battlefield concept using linear tactics.[9] The Napoleonic revolution began the mobilization of massive numbers of men-at-arms and fully exploited the technological advancements of the Industrial Revolution. The use of rail and telegraph allowed for greater mobility and troop deployment. The Prussian army perfected the

employment of these capabilities and was rewarded with a reputation for efficiency and effectiveness. In 1866 and again in 1870-1871, the Prussian Army were so superior "in utilizing telegraphs and rails that the outcome of the conflict was decided almost before the first shot was fired."[10] The efficiency displayed by the Prussians during this period was a tribute to the skills of their leader, General Helmuth von Moltke.[11] The proficiency of the Prussians to organize, ship, and equip hundreds of thousands of men convinced many potential adversaries of the futility of engaging war against them. Later, the combination of increased mobility with offensive lethality resulted in the Land Warfare revolution of the late 1800s. Here the innovation involved advancements in musket rifling and artillery technology. A revolution in mechanization and aviation enabled Germany to employ the "blitzkrieg" strategy to quickly envelop Europe at the start of World War II.[12] Lastly, the nuclear revolution at the end of war changed the nature of warfare forever. This revolution remains the most impressive and most lethal in history.

The cold war produced a technological race among the superpowers which fueled the creativity of American industry. National policy during this period contained the Soviet Union using the strategy of deterrence to ensure peace.[13] Military planners devoted their efforts to addressing perceived technological uncertainties. Much of defense programming directed development of new and more technologically advanced systems.[14] This period brought space to the forefront of the superpower technological contest. The single influential moment that marked the beginning of a new technological age was arguably the Soviet launching of Sputnik in 1958.[15] Research and development grew and the race for space supremacy dominated the military and industrial complex. Technology became the centerpiece for human advancement and continued development. This

spawned, among others, a new industry devoted to increased digitization, miniaturization, higher reliability, and lower cost manufacturing.[16]

The Newest RMA

History since the Hundred Years War showed that one who recognizes the advent of a military revolution and employs it to the fullest extent enjoys a significant advantage, perhaps overwhelming in some cases, over an adversary who has failed to do so. In all past revolutions, technological innovation combined with new doctrine and organization resulted in a significant leverage in conducting wars. In studying the Army Air Corps during World War I, Professor I. B. Holley concluded that the war "emphasized the necessity for a conscious recognition of the need for both superior weapons and doctrines to ensure maximum exploitation of their potential."[17] On forming organizations to develop and exploit air power, he adds that there is a "need for administrative agencies to ensure their fulfillment once they have been recognized as requirements." The creation of the United States Air Force in 1947 fulfilled the dreams of early airpower pioneers like Billy Mitchell. The creation of a separate Air Force formally recognized air power as a formidable military force. This was necessary to prosecute the doctrine of strategic bombardment effectively demonstrated at the end of World War II. Another example is the Air Force Strategic Air Command (SAC). SAC's early formation[18] resulted from the doctrine of massive nuclear strike employing both air delivered nuclear weapons and intercontinental ballistic missiles.[19] Today, a new military revolution may be emerging—this one based on exploiting information in warfare.

The era of the digital battlefield and the greater employment of technology in war made its debut in the Gulf War. The Gulf War witnessed the effective use of precision weapons and space technology to defeat the Iraqi military. The war heralded the use of information warfare as an effective tool for the military. During this conflict, computers were as valuable as guns, tanks, and airplanes. To ex-JCS chairman, General Colin L. Powell, "the sight of a soldier going to war with a rifle in one hand and a laptop computer in the other would have been shocking only a few years ago. Yet this is exactly what was seen in the sands of Saudi Arabia in 1990 and 1991."[20]

Quincy Wright argues that revolutions are "initiated by certain physical or social invention and leading to certain military and political consequences."[21] Today that "invention" is information technology and the resulting information revolution causes the rise of the latest revolution in military affairs. But the application of information technology in war alone is insufficient to make a military revolution. Doctrinal and organizational adaptations must accompany it in order to fully exploit the power of this innovation.

Discussions about the information age are no longer confined to academicians and technologists. US policymakers are now quick to embrace its consequence on future US military, political, economic policies. James A. Baker III, formerly President George Bush's secretary of state, declared "the emergence of information as a commodity has altered forever the nature of our domestic economics as well as the terms and intensity of international competition."[22] President Clinton's National Security Strategy of Engagement and Enlargement recognizes the significance of this trend as well.[23] Clinton's national security advisor, Anthony Lake, sums it—"the pulse of the planet has accelerated

dramatically and with it the pace of change in human events. Computers, faxes, fiber optic cables and satellites all speed the flow of information. The measurement of wealth, and increasingly wealth itself, consists in bits of data that move at the speed of light."[24]

Increasingly, modern societies use information as a critical element for both power and wealth.[25] Computers and the global information infrastructure are the tools used to exchange information worldwide. In previous wars, nations battled for control of territory and resources; now the new battleground also involves the information domain. James R. Fitzsimonds' characterization of this phenomenon appears accurate—"evolving technologies may result in a transition from information in warfare—information as a supporting function of the traditional attrition/maneuver operations—to information as warfare—in which attrition and maneuver become supporting elements of military, political, and economic leverage through information control."[26] Information used as an offensive instrument in war may result in the resolution of a conflict prior to use of force and violence.

The assumption made is that future warring states rely on information for conducting their political, economic, and military affairs. Modern strategists often view enemy states as a system of concentric rings representing fielded armies, the population, the enemy infrastructure, its organic essentials, and its leadership.[27] To Colonel Szafranski, "information is the 'bolt' that holds the rings together."[28] Disrupting the information flow by attacking the enemy's internal infrastructure hinders their ability for conducting offensive operations. But, the complexity of the information age brings with it potential challenges to the national interests of the United States. The US military, as protector of American interests, is thrown in the forefront of probable future conflicts once again.

Notes

[1]Andrew F. Krepinevich, "Cavalry to Computers—The Patterns of Military Revolutions," *The National Interest*, No. 33, Fall 1994, 30-42.

[2]Clifford J. Rogers, "The Military Revolutions of the Hundred Years War," *The Journal of Military History*, No. 57, April 1993, 241-278.

[3]Ibid., 245. Early historians described the period of 1066-1346 as the age of the "supremacy of the feudal cavalry." Some now dispute this early concept arguing that the infantry played an equal or greater role on the medieval battlefield. But the fact remains that "medieval warfare was characterized by the dominant role of the heavy cavalry."

[4]Ibid., 247.

[5]Robert L. O'Connell, *Of Arms and Men—A History of War, Weapons, and Aggression* (Oxford University Press, New York, NY, 1989), 104. A crucial element in the British tactic was "the establishment of a narrow-fronted killing zone around two hundred yards deep, into which several thousand arrows could be launched in sheets at approximately ten second intervals."

[6]Ibid., 249.

[7]Carl Von Clausewitz, *On War*, edited and Translated by Michael Howard and Peter Paret (Princeton University Press, Princeton, NJ, 1989), 528.

[8]Martin Van Creveld, *Technology and War: From 2000 BC to the Present* (Free Press, New York. 1989), 103.

[9]To solve the slow rate of fire of Muskets, the Dutch positioned their forces in a series of long lines. As one line fired, the other reloaded. See Krepinevich.

[10]Van Creveld, 159.

[11]General Helmuth Karl Bernhard von Moltke, *On the Art of War—Selected Writings*, edited and translated by Daniel J. Hughes (Presidio Press, Novato, Ca., 1993). On the use of telegraphs, Moltke states, "The telegraph substantially assists the high command in making estimates of the military situation," 113. Hughes points out that Moltke fully exploited the use of railroads in wartime more effectively than any of his predecessors.

[12]Although radios, tanks, and planes were available during World War I, the Germans perfected the integrated employment of these technologies in a lightning quick attack of France, known as "Blitzkrieg."

[13]Terry L. Diebel and John L. Gaddis, *Containing the Soviet Union—A Critique of US Policy* (Pergammon-Brassey's, Washington DC, 1987), 8.

[14]Carl Builder and James A. Dewar, "A Time for Planning? If not now, when?, *Parameters*, Vol. 24 # 2, Summer 1994, 8.

[15]A total surprise to the US; President Kennedy pledged landing a man on the moon before the end of the decade (1960s). This energized the US Space establishment. NASA led the way in the development of 'space age' tools.

[16]From *Aviation Week and Space Technology*, July 18, 1994 , s3. "To accomplish the moon landing objectives, new methods and techniques had to be developed to assure product quality and reliability. Apollo encouraged advances in manufacturing, such as wraparound tooling, multilayer circuit board soldering, cold bonding, and precision hole-drilling through steel, titanium and composite honeycomb materials. Specifications for computer software were far more demanding than those undertaken in previous military or

civilian projects"; "Call them spin-offs, offshoots, technology twice used, whatever . . . going to the moon created thousands of beneficial products and processes."

[17]Holley, I. B. (Maj Gen USAFR Ret), *Ideas and Weapons*, Yale Univ. Press, New Haven, 1953. 175.

[18]David A. Anderton, *Strategic Air Command—Two Thirds of the TRIAD* (Charles Scribner's Sons, New York, 1976), 31. The atom bomb "added a new dimension to air power by fostering the thought that a future war...was unthinkable. Such a war had to be prevented from happening. And there was only one apparent way to prevent future wars: Create a peace keeping force so strong, so well armed, so mobile and flexible, that no nation would think of a direct challenge. This thinking led to the eventual creation of the Strategic Air Command."

[19]Aaron L. Friedberg, "A History of the US Strategic Doctrine 1945 to 1980," *Journal of Strategic Studies*, Vol. 3, No. 3, December 1980, 46—The post World War II strategy in the event of war with the USSR was for the United States to unleash "the largest atomic air offensive feasible" against the Soviets "in the shortest possible period of time."

[20]General Colin L. Powell, US Army (Ret) "Information age Warriors," *Byte*, July 1992, 370.

[21]Quincy Wright, "Technique of Modern War," *A Study of War* (University of Chicago Press, Chicago, IL, 1942), 291-328.

[22]James A. Baker III, address before the International Human Gnome Summit meeting and the James A. Baker II Institute for Public Policy, Rice University, Houston, TX January 21, 1994—"Selective Engagement—Principles for American Foreign Policy in a New Era."

[23]National Security Strategy of Engagement and Enlargement, 1995.

[24]Anthony Lake, address to the Johns Hopkins University School of Advanced International Studies, Washington DC, September 21, 1993—"From Containment to Enlargement—Current Foreign Policy Debates in Perspective."

[25]Komar, 7.

[26]James R. Fitzsimonds, "Intelligence and the Revolution in Military Affairs," *US Intelligence at the Crossroads*, edited by Roy Goodson, Ernest R. May, and Gary Schmitt (Brassy's, Washington DC, 1995), 375.

[27]Colonel John A. Warden, "The Enemy as a System," *Airpower Journal*, Spring 1995, 44.

[28]Colonel Richard Szafranski, "Parallel War—Promise and Problems," *US Naval Institute Proceedings*, Vol. 121, No. 8, August 1995, 57.

Chapter 5

Security Concerns In the Information Age

The United States faces new challenges as it enters the information age. Societal changes combined with the continued growth of technology produce an uncertain future. Industrial age nation-states and the institutions established to support them must now assess the viability of their continued existence. The current day military establishment is a product of the industrial age. Their understanding of the factors shaping their future is therefore vital for surviving in the new age. In this chapter some of the security concerns facing the 21st century military are examined.

The Have and Have Nots

Following the end of the cold war is the emergence of a world of "haves and have nots."[1] The advanced nations are the "haves" but they only represent 25 percent of the world.[2] Information is easily accessible by the "have nots" within the framework of the global network. On one hand, information about the advanced societies of the world strengthens the resolve of third world states to press for modernization and sophistication. On the other hand, the same "have nots" may view the economic prosperity enjoyed by the advanced nations as a widening gap that is not easily bridged. They may think of the "haves," with the US at the centerpiece, as targets for exploitation and attack. At the

extreme, the more radical states may pursue drastic methods to bring down the economy or the government of the United States through sabotage and terrorism.

There is disturbing evidence that some view the information technology gap between the "haves" and the "have nots" as simply an extension of the imperialistic tendencies of past Western colonial empires to force their will on the world's disadvantaged—slavery and repression in the information dimension. One of Egypt's prominent newspaper columnist, Mohamed Sid-Ahmed, also a member of the General Secretariat of the Opposition National Progressive Unionist Party in Egypt, concludes that "the Islamic upsurge in many Arab countries bordering on the Mediterranean is a phenomenon that is linked, somehow or other, to the deep sense of frustration felt by wide sections of Arab society at the way their destinies are being manipulated within the framework of the cybernatic realities of the new world order."[3] Mohamed believes that a view increasingly shared among Arabs is the growth of an information-age "privileged-class" of Western nations linked via the global network. Some of them view the "information superhighway" as a Western concoction designed to pressure the "have nots" and promote the continued subjugation of Arabs by former colonial powers. As menacing as these charges sound, these beliefs are attracting some to turn to radical Islamic fundamentalism to counter the perceived Western plot. This view, when promulgated by radical "have not" societies, could trigger violent reprisals and terrorist activities against United States' interests and other advanced nations. The military must remain vigilant against the potential for such unprovoked aggression.

Global Democratization and Chaos

Futurists like Toffler and Masuda also warn of the potential for a chaotic environment during the transition from the industrial age to the information age. Information availability drives greater democratization, as previously discussed, but leading to greater political instability worldwide. There is evidence showing states that transition to democracies, especially from autocratic rule, are twice as likely to engage in wars as those states which remain autocratic[4]. The violent breakup of the former Yugoslavia in the early '90s reflects the chaotic transition of former totalitarian states. The US military must come prepared for any contingencies involving the deployment of US troops to help stabilize international order. Carl H. Builder and Brian Nichiporuk of RAND observe that "the opponent of the future will present challenges because the new geopolitical environment is fostering types of contingencies and opponents for which the US Army may not be doctrinally prepared."[5] The information revolution will change future missions of the military, expanding the military's spectrum of involvement.[6] The case of US troop deployment in Bosnia in 1995 to support the United Nation's peacekeeping mandate is an example of this emerging military role.[7]

The Rise of Non State Actors

The global network allows for greater discourse between individuals and groups without regard for political boundaries and geography. Satellites cross geo-political lines and are insensitive to physical borders. At higher orbits, half the earth is visible from one satellite.[8] Casual conversations or "electronic chatting" between users of the Internet around the world are popular and common. Interest groups with political, cultural, and

economic agendas use the "World Wide Web" as a means to communicate and promote ideas. Organizations are forming as transnational groups with no direct association with traditional sovereign nations.[9] In the world of commerce, corporations are taking advantage of the free-flow of information to form international alliances and ventures. Pelton in *Future View* suggests a move "beyond the nation state to global markets."[10] In some cases growing cooperation between states in a region is creating an alliance of nations sharing common military, political, economic, and even cultural interests.[11]

The rise of ethnic nationalism during this period is predicted by futurists Toffler and Masuda. John Petersen in his book *The Road to 2015* calls this "growing tribalism"—an act where segments of society are highlighting "minorities at the expense of the whole."[12] Nations with historically large ethnic diasporas may fall apart with groups forming based on ethnic identification. This breakup results in a potential increase of violence between minorities and among ethnic groups.[13]

The recent chemical attack on a Tokyo subway by the Japanese cult Aum Supreme Truth may be a precursor of things to come in the transitory period of the information age. According to Nathan Gardels, editor of *New Perspectives Quarterly*, the act "marked the ultimate devolution of power in the information age: the demassification of mass destruction weapons. The broad 'third wave' dispersion of power and information, including lethal knowledge, has at last undermined the founding basis of the state by depriving it of its monopoly over mass violence."[14] Nation-states no longer have monopoly on organized violence. Groups and non-state actors are increasingly becoming modern day purveyors of weapons of mass destruction.

Hostile Information Warfare against United States Interests

A problem with most advanced societies is their dependence on modern systems and infrastructures like subways, airports, telephone networks, electrical power grids, and so forth. Potential terrorist groups, knowledgeable of these built-in national vulnerabilities, need only target these systems to wreak havoc and confusion within a target country. The Internet is now a popular and convenient vehicle for terrorists and rogue nations for exchanging techniques for the production of crude, but effective, weapons.[15]

Two forms of sabotage or terrorist attack are possible: the first one being the traditional disruption of society and order through violence; and the second more sophisticated in the form of electronic or information-based terrorism. The US relies on technology and information systems to conduct its affairs. Targeting these systems creates widespread terror and confusion. In industry and government the threat of intrusion and attack is all too real. According to the National Computer Security Association, sixty-nine percent of corporations they recently surveyed in 1993 were infected by a malicious virus.[16] The cost to US business is a staggering $3 billion per year.[17] The government is not immune to these types of attack. The May 1990 attack on the Internet by a 24-year-old graduate student disrupted computer installations nationwide.[18] In the spring of 1990 three Australian hackers were charged with damaging data on US government computers. The talent pool for potentially hostile information warriors is large. According to Peter E. Sakkas the pool includes "ex-members of Soviet and Warsaw Pact intelligence agencies (*Stasi, Spetsnaz, and Osnaz*), mercenaries, unemployed technical specialists, Third World technological specialists, etc."[19] Interestingly, Eastern Europe, particularly Bulgaria, is the leading exporter of viruses today.[20]

According to Richard Power of the *Computer Security Journal*, the top ten infrastructure warfare targets which appeared in the July/August 1993 publication of *Wired* magazine are: (1) Culpepper Switch in Culpepper, VA. This electronic switch handles all federal funds and transactions; (2) Alaska Pipeline which carries 10 percent of domestic oil for the US; (3) the Electronic Switching System which manages all telephony; (4) Internet; (5) Time Distribution System; (6) Panama Canal; (7) Worldwide Military Command and Control System (WMCSS); (8) Air Force Satellite Control Network; (9) Moluccan Straits, Singapore, maritime link between Europe-Arabia and the Western Pacific; and (10) the National Photographic Interpretation Center, Washington DC.[21] Imagine the disruption in society, the military, the government, and the economy of a successful attack against any of these targets. The economic paralysis resulting from an operation against the Culpepper Switch is sure to go beyond the borders of the United States. An attack against the Air Force Satellite control network would seriously threaten the US early warning network and paralyze the military communications infrastructure.

The Laws of Information Warfare

General Ronald R. Fogleman, Air Force Chief of Staff, suggests that "because exploiting [information systems] will readily cross international borders, we must be cognizant of what the laws allows and will not allow." He is correct in taking issue with the proper and moral application of information warfare. This new form of warfare raises questions that are difficult to address. Among them are: (1) in an electronic environment, when does war begin?; (2) how does one measure damage and define victory?; (3) does a malicious probe of a US computer system warrant a quid pro quo response or a traditional

combat response?; (4) who decides to deploy offensive information weapons; and (5) would a systems attack by the US require congressional approval?[22] In a recent article in *TIME*, Douglas Waller discussed a meeting of Army chaplains to discuss the moral implications of information warfare. In a lightning quick information attack, an enemy wanting to surrender may not be able to do so.[23] One case in the waning moments of World War II in the Pacific highlights this concern. Japanese General Tomayuti Yamashita, during his war crimes trial at the end of the war, argued that he lost control of his troops in the Philippines due to the successful US campaign which took out his communications infrastructure. He appealed, unsuccessfully, that he could not have been responsible for his troop's actions since his ability to command and control his retreating army was taken away.[24]

In information warfare the vulnerabilities of traditional non-military targets are heightened. Since one of the potential targets for information warfare is the enemy's civilian infrastructure, *Time*'s Waller argues that "infowar may only refine the way modern warfare has shifted toward civilian targets. Taking down a country's air-traffic control or phone systems might be done cleanly with computers—but it still represents an attack on civilians."[25] As with nuclear weapons, Clausewitz's vision of "absolute war" appears real in conducting information warfare. The attack is clean but the resulting human suffering may be too devastating and morally unjustifiable. To Colonel Szafranski "the principles of just war and just conduct in warfare need to be evaluated whenever strategic information warfare is contemplated."[26]

Major General Nolan Sklute, the former USAF Judge Advocate General, asserts the obvious when he says that information warfare will "raise important new legal issues."[27]

He is concerned that the "development of the laws concerning information warfare has lagged somewhat behind innovations in technology and doctrine." To understand the legal implications of information warfare, the Air Force Judge Advocate General's School sponsored a symposium at Maxwell AFB, AL in November 1995. The information warfare arena is large and it spans the entire legal spectrum including intelligence, space law, use of force issues, neutrality, and more. The conduct of information warfare requires new thinking, but legal experts agree that "the legal principles that will govern information warfare will probably be derived by extending law to these new activities."[28] The realm of information warfare is new. Legal issues arise with employing this type of war, but the current US military legal system have limited basis to create laws and regulations. Their only recourse is to extend the statutes of current laws to cover information warfare. Without definitive information warfare laws, however, the legal boundaries of this new form of war remain vague and controversial.

The Future is Uncertain

The world in the information age is facing uncertainties threatening international order and stability. The United States military is confronted with new challenges demanding a review of strategy and doctrine to ensure the armed forces' continued superiority. The threats are both diverse and distributed. Information is the commodity shared by future actors and, as presented so far, it becomes the new basis for power and influence. The United States must take an active part in exploiting information offensively and defensively, therefore, ensuring military, political, and economic dominance over future adversaries in the twenty-first century.

Notes

[1]Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway*, (Thunder Mouth Press, NY, 1994), 432.

[2]Ibid.

[3]Mohamed Sid-Ahmed, "Cybernetic Colonialism and the Moral Search," *New Perspectives Quarterly*, Vol. 11, Issue 2, Spring 1994, 18.

[4]Edward D. Mansfield and Jack Snyder, "Democratization and War," *Foreign Affairs*, Vol. 74, No. 3, May/June 1995, 79-97.

[5]Builder and Nichiporuk, 47.

[6]Ibid., 57.

[7]Others include security assistance, humanitarian assistance, anti-terrorism, counter-drug, peace enforcement, and more.

[8]At geosynchronous altitudes (22,000 NM from the earth's surface), satellites stare at the earth 24 hours in a day. Communications systems which require continuous and complete coverage are typically located at these orbits.

[9]Greenpeace, the international environmental group, is an example of such organization.

[10]Pelton, 160.

[11]The Association of Southeast Asian Nations (ASEAN) is an excellent example. The Bangkok summit declaration of 1995, signed by the Heads of State and Government of the member nations on December 15, 1995 calls for greater inter-ASEAN economic, cultural, political, scientific, and security cooperation.

[12]Petersen, 240.

[13]The breakup of Yugoslavia after the death of Tito into separate states provide the clearest example of the power struggle along ethnic lines.

[14]Nathan Gardels, "Third Wave Terrorism," *New Perspectives Quarterly*, Vol. 12, Issue 3, Summer 1995, 2-3.

[15]Debra Gersh Hernandez, "Bomb Making on the Internet," *Editor and Publisher*, Vol. 128, Issue 25, June 24, 1995, 38-40.

[16]Gary H. Anthes, "Viruses Continue to Wreak Havoc at Many US Companies," *Computerworld*, June 28, 1993, 52.

[17]Stephen A. Booth, "Doom Virus," *Popular Mechanics*, June 1995, 52.

[18]Peter E. Sakkas, "Espionage and Sabotage in the Computer World," *International Journal of Intelligence and Counter Intelligence*, Vol. 5, No. 2, Summer 92, 160.

[19]Sakkas, 163.

[20]Andrew E. Serwer, "Why Bulgarian Bugs Us so Much," *Fortune, Vol.* 131, No. 9, May 15, 1995, 32.

[21]Richard Power, "CSI Special report on Information Warfare," *Computer Security Journal*, Vol. 11, No. 2, 1995, 63-73.

[22]Gary H. Anthes, "New Laws Sought for Information Warfare," *Computerworld*, Vol.29, No. 23, June 5, 1995, 55.

[23]Waller, 44.

[24]Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations* (Basic Books, New York, 1977), 320.

Notes

[25]Waller, 44.

[26]Szafranski, "A Theory of Information Warfare," 64.

[27]Foreword from notes included at the JAG School Symposium on "Legal Issues in Information Warfare," held at Maxwell AFB from November 1-3, 1995.

[28]Ibid., "Primer on Legal Issues in Information Warfare," notes of conference.

Chapter 6

The Cyber Force—The Military in the 21st Century

This description of the future cyber warrior appeared in the August 21, 1995 issue of *Time.*[1] The future soldier's standard gear will include the following advanced systems:

1. **Integrated Headgear**. Collects information for analysis as well as funnels the latest intelligence to soldiers in the field;
2. **The Lightweight Helmet.** Provides greater protection from munitions and projectiles. Its mounted display includes night-vision sensors, a miniature flat video panel and voice activation for a computer built into the soldier's body armor.
3. **The Body Armor**. Allows room for a computer in the lumbar area while protecting the soldier against nuclear and chemical hazards.
4. **The Thermal Sight.** Can send multiple still-frames back to the high command, providing battlefield intelligence and damage assessment.
5. **The Computer.** Embedded in the lumbar region of the armor, runs the soldier's technology, gives him friend-or-foe identification, detects mines and chemicals and tells him exactly where he is.
6. **Wireless Connection.** Links the weapon to the helmet monitor, allowing the soldier to aim at targets without exposing his body to the enemy.

Imagine an army with such a capability. This is no longer confined to the imagination of science fiction. Technology advancement and systematic development of these systems are underway. "Many of the major efforts have been initiated as advanced technology demonstrations within the scope of the Army science and technology master plan."[2] Included are multisensor-aided technology, digital battlefield communications, intelligent minefield, precision munitions, advanced night imaging devices and sensors, and to "win the information war through a comprehensive, integrated multimedia information transport

system."[3] It is only a matter of time before these systems leave the strict confines of the laboratory and enter the field of combat operations. The advantage of these capabilities is significant. The future soldier is almost completely autonomous; the tools are configured to provide the warrior with maximum information about the combat environment. As an integrated capability, the warrior's combat gear provides the collection, processing, analysis, and interpretation of information critical to the soldier's mission. Two and a half thousand years ago, the great Chinese strategist Sun Tzu wrote "If you know your enemy and know yourself, you need not fear the result of a hundred battles."[4] Sun Tzu was speaking of what is now known as "situational awareness." The vast array of available information systems enhances the performance of the future soldier in combat. Superior knowledge of the situation gains the future warrior a clear advantage over the enemy.

In this chapter, the internal makeup of the future military is discussed. As the military enters the information age in earnest its organizational structure is considered. The traditional methods for training and organizing the military may undergo changes. This chapter introduces several military areas for consideration. Some elements that hold the military function as an effective institution are examined.

Organizational Paradigms

Hierarchical organizations were the trademark of the industrial age. The need to respond to the innovations resulting from the Industrial Revolution produced a highly hierarchical society.[5] This strong structure was necessary to attain strict organizational harmony and discipline. A centralized form of government controlled the way of life of the people through laws and regulations. The military more than any other industrial age

institution required strong command organizations to prosecute its unique mission of organized violence. It is self-evident that order and discipline characterize the actions of a professional military, especially during combat operations.

In the information age, futurists predict a major shift in societal behavior. Masuda, for one, envisions a new society where the individual is the centerpiece—personal autonomy as the common element of future social interaction. The information society becomes "multi centered and multi functional."[6] A person no longer requires a great degree of social and even physical interaction with others in society. Individuals can now isolate themselves and still maintain some contact via the vast network of information systems available.[7] To Negroponte, "we will socialize in digital neighborhoods in which physical space will be irrelevant and time will play a different role."[8] According to Michael Marien, editor of *Future Survey*, "the new abundance of information, and its further fragmentation to meet the needs and interests of myriad racial, ethnic, religious, intellectual, political, commercial, and leisure interests is unlikely to advance intergroup harmony and sharing."[9] US Army General Frederick M. Franks concluded that "as information proliferates at faster speeds and is available to a wider array of individuals, hierarchical organizations evolve into networks and power is shifted more to individuals and groups."[10]

The future challenge of military leadership is integrating the disparate interests and varied emotional levels of individuals. The traditional collective and corporate nature of an armed force is affected by the trend towards individualism. For an army to succeed in war it must have a cohesive, integrated, and common objective. The military is built around the "team concept" where the well being of the whole unit supersedes that of the

individual member. When members begin functioning strictly as individuals it undermines the integrity of a military unit and threatens mission success. The military institution suffers if the highly hierarchical military organization it is accustomed to collapses from the weight of the information revolution. Even the middle management levels may become extinct.[11] The force structure will change with the current rank arrangement even becoming obsolete. While this transition is more evolutionary over a period of twenty to thirty years, the planning for this change and the analysis and understanding of its consequences must be done now.

The Military Chain of Command

Dinardo and Hughes warn that the "improvement of communications at the disposal of political leaders and military commanders has always carried the dangers of disrupting the chain of command."[12] With the stroke of a key and knowledge of one's electronic mail address, one easily bypasses the normal structure of the chain of command. The President of the United States, as an example, has a personal Internet address. Anyone, anywhere, anytime can send messages to him directly, unfiltered and unedited. The democratic principles of the US encourage free speech, but when taken to the extreme could damage the effectiveness of the military chain of command. But is the chain of command still a relevant necessity for the military in the information age? In a greatly hierarchical organization, the chain of command endured for the military to succeed in battle. If central bureaucracies and classes disappear then it is questionable whether the class structure of the military profession will survive in its wake. Some experts even expect that by 2020 "the requirements of the battlefield will be such that traditional

hierarchical command and control arrangements will be obsolete."[13] However, the principle of unity of command must remain intact. This basic tenet of command in war must not be compromised. It is the one principle which remained intact in all successful wars in history. Greater discipline among the military is therefore a requirement to preserve command unity and control in future wars.

Training

Information technology is shaping how the military is trained in the future. Using state-of-the art technology promises to make future training systems more cost effective without sacrificing performance and, perhaps, even improving it. Operational cost limits the amount of real-world training afforded the military in the future. The wider use of simulators defrays some of this cost. Simulators are now capable of greater levels of realism with recent technological advancements. "US tank commanders of the 21st century will train in a virtual world more than in the real one. The result will be soldiers who are better prepared—by computer simulators integrated into their vehicles that will enable them to practice just hours before combat."[14] The Army is experimenting with "battle laboratories," the concept of using advanced technologies and systems to simulate the complex interaction of diverse elements in the future battlefield.[15] An Army exercise, *Atlantic Resolve*, held in the fall of 1994 focused on the "use of live, virtual, and constructive simulations for training and experimentation." Their experience with this approach was positive. These battle laboratories paid dividends for the Army in only three years of existence. This method conditioned Army decisions in resource allocation and weapons acquisition in recent years.[16]

The need for high-tech warriors requires an inspection of the current method for recruitment. Education and training must emphasize continued technical competence and know-how for these warriors. The maintenance of expertise in a rapidly evolving technological world is of primary import. Service academies must require from future military leaders proficiency in engineering and the hard sciences. Service professional military schools, including Command and Staff and War Colleges must familiarize senior officers with the process of weapons systems procurement and technology development. The emphasis here is on the interaction of the inseparable mixture of doctrine, organization, and technology—key ingredients for successful revolutions in military affairs.

The high-tech military of the 21st century will be smaller but more sophisticated and specialized than today's military. In twenty to thirty years the organizational structure is changed favoring more direct lines of command with the middle grades eliminated. The future military will comprise well-trained and skilled warrior-technicians comfortable in operating with advanced electronic combat gadgetry. Wars and conflicts in the information age will not be less common or less violent. On the contrary, the transition period between the industrial and information ages is likely to be more chaotic and unstable. If committed to war, future "cyber-warriors" will fight with the same ferocity and force as demonstrated by their predecessors. Using information warfare enhances their approach to war and the way they operate in the battlefield. The commanding general of the US Army Training and Doctrine Command (TRADOC), General William W. Hartzog, postulates a "future in which information plays a central role in battle success."[17] Future warriors will quickly and decisively outflank and outmaneuver the enemy with foreknowledge of the adversary's position and combat situation. With

information age weapons at their disposal they would engage the enemy precisely and decisively. The military employing information age technology to the fullest has the advantage in combat over one who does not. Today's military must prepare and plan now in preparation for the high-tech battleground of tomorrow.

For information to become the catalyst for a new revolution in military affairs, doctrinal and organizational changes must follow. Technology enables the application of a new RMA in war. To sustain the RMA's power and confirm its worth as a potent strategic and operational weapon, however, require a modified organizational structure supported by doctrine articulating its efficient and proper employment at every level of warfare.

Notes

[1]*Time*, August 21, 1995, 42.

[2]General Leon Salomon, US Army, "Technological Edge," *Army*, February 1995, 26.

[3]Ibid., 28

[4]Sun Tzu, *The Art of War*, edited by James Clavell (Delacorte Press, New York, 1983), 18.

[5]Masuda, 621-623.

[6]Ibid., 623.

[7]Such is the case with the growing trend towards the "virtual office," where employees stay at home but still conduct normal business using a personal computer and a modem.

[8]Negroponte, 7.

[9]Michael Marien, "Some Questions of the Information Society," *The Information Technology Revolution*, edited by Tom Forester (MIT Press, Cambridge, Mass. 1985), 654.

[10]General Frederick M. Franks, US Army, address to the Association of the US Army Symposium, Orlando, Fla., Feb. 8, 1994.

[11]Builder and Nichiporuk, 54.

[12]Dinardo and Hughes, 75.

[13]McKitrick, 84.

[14]Judith Gunther, Suzanne Kantra, and Robert Langreth. "Digital Warrior," *Popular Science*, September 1994, 63.

[15]Hartzog, 58.

[16]Ibid., 59.

Notes

[17] General William W. Hartzog, US Army, "A 'Lighthouse of Ideas' on the Road to Force XXI," *Army*, October 1995, 55-59.

Chapter 7

The Need for Doctrine in the Information Age

The following scenario may describe future combat in the information age:

> After months of preparation, all equipment and personnel are in place. The theater commander and his immediate staff are located in the command center where large computer screens show the location of forces on the battlefield. At the push of a button, the screen zooms in to show individual soldiers and equipment with microwave transponders. Another button brings up an overlay of logistics information showing stocks of munitions available in each sector, as well as fuel supplies, food, potable water and other consumable. Other overlays show the size and types of enemy units and equipment, as well as known quantities of munitions, fuels and other supplies available to the opposing forces. Other computer screens project digital video images from cameras on unmanned aerial vehicles and ground vehicles, and small cameras carried by individual soldiers. Tank crews, helicopter pilots and artillery fire control officers are equipped with individual computers and small computer screens that display similar information on the location of enemy and friendly forces in the immediate vicinity. At H-hour, the theater commander gives the signal to begin ground operations. Satellites are turned on to provide global position information, and digitized voice and video communications between and among all levels of the theater operations. Computer screens come alive with activity as the movement of units and equipment is displayed on the computer screens. Video cameras on orbiting satellites are activated to provide continuous photographs of the ground combat operations. Projections of fuel and ammunition consumption rates are displayed for commanders and logisticians.[1]

History is replete with examples of wars won by the superior application of technology and doctrine. Studies of past wars yielded insights into how technology is used to ensure success in war. One thread seems common in most of these studies—formulating doctrine to exploit the full potential of technological innovation is a slow and

tedious process. In his book, *Ideas and Weapons*, Dr. I.B. Holley underscored the critical interaction between innovation, organization, and doctrine in winning wars.[2] His study of the use of American air power in World War I depicts a military leadership unable to realize the power of what they have because of deficiencies in organization and ignorance of the airplanes' purpose and mission. The same predicament suffered by these early military leaders must not encumber the introduction of information as an instrument of winning wars into the military institution. Formulating doctrine early is important to guarantee the expert use of this new capability. An organizational structure, formed on the basis of doctrine, guarantees the orderly development and effective employment of information age weapon systems in the future.

Air Force Doctrine Document #5[3] provides the initial basis for the development of future strategic and operational plans involving information warfare. Air Force defines information warfare as "any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against these actions and exploiting our own military information functions."[4] To some, information warfare is "simply the use of information to achieve our national objectives."[5] It is a form of war "about knowledge—about who knows what, when, where, and why, and about how secure a society or a military is regarding its knowledge of itself and its adversaries."[6] In short, the target of information warfare it seems is the human mind.[7]

At the strategic level the United States seeks to acquire, exploit, and protect information in support of national objectives. The areas for exploitation and protection include the economic, political, and military sectors. Cultural as well as social information may also be required to support US interests and strategic goals. At the operational level

information warfare consists of attacking and defending information as well as exploiting information in support of military operations. Since information is critical to the enemy and US military forces alike, the objective of information warfare is denial, deception, destruction, and attack of the adversary's information-critical systems.

Doctrinal Development

Military doctrine codifies the belief about the best way to conduct military affairs.[8] Doctrine is drawn from experience more than anything else. But past military experience may not be relevant in the age of information. Current Air Force efforts at creating doctrine tend to treat information warfare as merely a new tool to enhance current missions.[9] It is not generally viewed as a weapon on its own accord. Since experience in information warfare is limited, the doctrine for its use is not easily derived. Developing information warfare doctrine results from an analysis of all the likely use of information at all levels of war. In other words, an examination of how it is used as a national strategy mechanism is critical in addition to how it is employed at the lower levels of operational art and tactics. In all cases, both the offensive and defensive nature of information warfare requires detailed examination.

Clausewitz said that war "is a continuation of political intercourse, carried on with other means."[10] It is the last resort when diplomatic and economic alternatives fail. Its premise lies in the maturity of conflicting nations to conduct political dialogue. Wars commence when diplomacy fails to produce a mutual agreement. But are the strategies promoted by Clausewitz still valid in the information age? He emphasized the inter-relationship between industrial age states in politics and war. The enemy in the twenty-

first century may be as ambiguous as Clausewitz's depiction of the "fog of war." When nation-states are giving way to transnational interest groups, who would the military fight? In the next twenty to thirty years the US military faces a diversified set of threats. The potential for armed conflict with advanced states ought to be as likely as wars against non-state actors like terrorists and radical groups. Knowing the enemy remains a timeless imperative in conducting future wars. What must be prevented in the development of future doctrine is the tendency for strategy to be inflexible. Recent US military history reflects the danger of the blind application of doctrine and ignorance about the enemy.

In Vietnam, the use of strategic bombardment as the means to end the war did very little to change the course of this conflict. Mark Clodfelter in his book, *The Limits of Air Power—The American Bombing of North Vietnam* writes of the American failure to apply the right doctrine in Vietnam. His book shows "how the indelible stamp of Air Force strategic bombing doctrine affected the air war against the North, and how doctrinal convictions established long before Vietnam colored air commander's perceptions of bombing effectiveness."[11] The lesson in Vietnam is important—the love of technology must not blind nations and their leaders in searching for more effective and proper strategic alternatives for fighting wars. In the next century, doctrine and strategy must account for the diverse mix of potential adversaries the US could face. The spectrum of probable adversaries ranges from the one extreme, a very sophisticated enemy employing information technologies to the same degree as the US; and to the other extreme, an adversary (a nation or even a group) devoid of high-tech weaponry and capabilities fighting a different kind of war.

Against a Sophisticated Enemy

The Gulf War taught others of the effectiveness and power of information age technologies and weaponry. Since the war, some regional powers are now "looking for ways to use and counter precision guided weapons, computers, and space-based communications."[12] An information warfare attack on an information-advanced state could devastate its national infrastructure. Targeting an enemy's vital financial, electrical, telecommunications, and transportation nerve centers seriously impedes their ability to conduct war. Theoretically, even without firing a single shot, victory is achieved—at least a psychological victory demonstrating the will and the resources of the attacker. To many proponents of information war this is the scenario most discussed. Sun Tzu wrote "to fight and conquer in all your battle is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting."[13]

At the operational art level of war the objective of information warfare is to distort and control the "adversary's perception of the battlespace by controlling or corrupting the information he uses, while providing the friendly commander with an unambiguous picture of his battlespace."[14] Techniques are employed to defeat the adversary's information capability within the constraints of the battlespace. This includes attacks on the enemy's command and control network—the enemy's ability to maintain situational awareness and decision making in the face of uncertainty; and their intelligence apparatus—the enemy's ability to anticipate and predict friendly forces' actions and intentions. The destruction of these key elements is mandatory at first opportunity. Space-based systems when used by foreign adversaries provide a significant command, control and intelligence capability, perhaps even equal to that of the United States.[15] A top-priority target of information

warfare is therefore first strike against the adversary's space systems. "Future wars might become a contest for domination of space, as both sides try to deploy and preserve communications and surveillance satellites."[16] Emphasis in taking out the enemy's space based assets with speed and precision is foremost in war planning. Technology and weapons development in the near term must concentrate in the acquisition of capabilities to neutralize the enemy's "ears and eyes" in air and space. Hardware and software weapons are candidates for use and they include anti-satellite weapons, precision bombs in strikes against ground stations, software attacks using "virus" to infect computers and networks, and more.[17] At the tactical level information warfare consists of electronic measures and physical destruction of key information nodes.[18]

Force Enhancement

Information technology provides the US military with new opportunities. Advanced systems enhance the fighting capability of US forces by providing superior command and control, communications, and intelligence networks. The contribution of space systems during the Gulf War whetted the military's appetite for high-tech systems, thus intensifying the demand for state-of-the art technologies. The technologies which are available today are routinely used in operations such as jamming of enemy radars, monitoring enemy communications, and tracking their movements. Tomorrow's technologies "might enable air forces to conduct electronic embargoes, or detect and identify vehicles or even personnel in combat."[19]

Today's and tomorrow's information systems are an indispensable part of military operations. Real-time or near real-time information on enemy locations, dispositions,

capabilities, and indicators of intentions from surveillance and reconnaissance assets provide the commanders in the field situational awareness of the battlefield. Wide bandwidth digital communication systems give forces real-time command and control links between commanders and fielded units. These systems also offer US National Command Authorities instantaneous communications with globally dispersed US forces. Precision navigation systems, like the twenty-four-satellite constellation comprising the Global Positioning System, enhance the accuracy of weapons and delivery systems. Weather systems sending accurate weather data to commanders enable the direction of combat forces at the right time in support of tactical, operational, and strategic operations.

Defensive Information Warfare

The impact if the enemy wages a successful information warfare offensive on the United States is disastrous. An element of information dominance is ensuring that US and allied systems are free of attacks. The government, military, and even industry must remain alert to any attempts of interrupting US operations. The consequence of enemy software penetration of the vast US intelligence network or an operational commander's communications infrastructure could prove fatal in war. Many countries with emerging technological capabilities are known to target US systems today.[20] In addition to the threats by other nations, terrorist groups and multinational organizations including businesses have keen interests in information sabotage. The Internet attack in 1990 was perpetrated by an amateur. Professional computer hackers when sponsored by hostile nations or groups can do so much more damage. As discussed earlier, there is an abundance of computer experts around the world today willing to sell their knowledge and

capabilities to prospective buyers regardless of purpose and intent. Since the playing field of these hackers is the global network of interlinked computers and communications, attacks are done at a great distance from the target. Unlike the terrorist agent planting a bomb inside a building, the information attacker may be as far from the objective as possible. The covert nature of this endeavor is what is especially threatening about such an attack.

Another trend which is impacting the US ability to achieve information dominance in war is the proliferation of military relevant technologies outside the United States. According to the *Strategic Assessment 1995* report, "precise navigation and imagery in the wrong hands can imperil US forces. Space-based communication reduces the US advantage in military command and control. Cryptologic capabilities could permit terrorists to plan havoc undetected."[21] Economically strong nations or groups now purchase advanced technologies in the open market freely. However, controlling the flow of these technologies outside the US or into the hands of radical nations or groups is difficult to achieve. Most of these advanced systems have legitimate civilian application and use. Such is the nature of information age technologies. Their application goes beyond that of the military. The military is increasingly moving towards the "commercialization" of their basic support due to the continuing reduction in the defense budget and the growing emphasis on the use of commercial products. The use or sharing of commercial systems, particularly communications satellites, to support military operations may be the norm of future engagements. The fear lies in the vulnerability of these civilian systems to attack and exploitation. Military systems are usually designed for

security and survivability. Civilian systems are generally built without these provisions because of the high cost associated with their implementation.

Information as a Weapon

Sun Tzu said that "All warfare is based on deception. Hence when able to attack, we must seem unable; when using our forces, we must seem inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near."[22] Deception has played a major part in past wars. In the twenty-first century deception is information manipulation. Targeting an enemy's information infrastructure, however complex or simple, to create misinformation, confusion, and panic is an objective. The disruption of the enemy's way of life, the collapse of the enemy's economic structure, elimination of the enemy's decision making capability, and reduction of the effectiveness of the enemy's military forces can be the results of successful attacks. Information warfare is an effective tool for war making at all levels and it can also be a promising weapon of choice in covert actions during peacetime. Clausewitz's pronouncement that war is simply an extension of politics is also applicable to activities involving covert action. The post-World War II years witnessed the promotion of covert action as a major political arm used by policymakers to further United States' aims and objectives worldwide. The overthrow of Mossadeq and Arbenz during the Eisenhower years[23] did plenty to arouse the fascination of Presidents to the utility of covert action. The medium of cyber space is conducive for conducting information-based covert action activities. Far from physical harm, information warriors using the global network can attack information systems worldwide. According to Winn Schwartau the strategic goal of such an

information warrior includes: (1) theft of information—stealing an enemy's war plans, economic strategy, etc.; (2) modification of information—changing information or inserting malicious information in databases; (3) destruction of information—wiping out databases containing financial, military, and government information; and (4) destruction of the information infrastructure—through introduction of insidious software such as virus and software bugs.[24] With these tools the information warrior conducting covert action could change the course of action a potential adversary may take to one favoring United States' policy.

An effective information warfare campaign depends on the formulation of proper doctrine and the formation of an organization to fully exploit its potential. At the national level, a covert information warfare attack against an adversary helps in meeting US objectives before committing forces to action. At the operational and tactical levels of war, information warfare incapacitates the enemy's information based systems. The enemy is left confused in the battlefield with US forces gaining an overwhelming advantage in combat. The use of information technologies enhances the capabilities of US forces with superior command and control, communications, and intelligence. At all levels of war, defensive information warfare to protect US information systems is a prerequisite to achieve total information dominance. However potent information warfare is against a technologically advanced adversary, its use must remain judicious and calculated. Information warfare is not a panacea for all future conflicts. This type of warfare will not replace the use of arms in combat. As in past conflicts, knowing the enemy and the nature of how best to defeat this enemy are most important. Past lessons showed the futility of

using advanced technology against an ill-defined enemy center of gravity. Objectivity is paramount when using information warfare—its employment must be highly selective.

Notes

[1]General Leon E. Salomon, US Army, "Army Materiel Command: Relevant, Responsive, and Ready," *Army*, October 1995, 61-67.

[2]Holley, *Ideas and Weapons*.

[3]First draft of AFDD 5 made available on 18 November 1995.

[4]*Cornerstones of Information Warfare*, 3.

[5]George Stein, "Information Warfare," *Air Power Journal*, Vol. 9, No. 1, Spring 1995, 30-39.

[6]Arquilla and Ronfeldt, 380.

[7]George Stein, "Information War—Cyber War—Net War," *Battlefield of the Future*, 155.

[8]Col Dennis Drew, USAF and Dr. D. Snow, "Military Doctrine," *Making Strategy, an Introduction to National Security Process and Problems* (Air University Press, Maxwell AFB, AL., August 1988), 163-174.

[9]*Cornerstone of Information Warfare*, 8: "information warfare cannot be pigeon-holed as a single mission. To do so would fail to completely integrate information into Air Force doctrine." Also in AFDD 5, 9: "within Air Force doctrine, Information Warfare is not a mission, in itself, but like air and space warfare, it is a means for executing USAF missions defined by the environment.

[10]Clausewitz, 87.

[11]Mark Clodfelter, *The Limits of Air Power—The American Bombing of North Vietnam* (Free Press, New York, 1989), xii.

[12]Gary Stix, "Fighting Future Wars," *Scientific American*, December 1995, 92-98.

[13]Sun Tzu , 15.

[14]TRADOC Pamphlet 525-63, 9.

[15]*Strategic Assessment 1995*, 153. The Commerce Department has licensed four US groups to sell surveillance "bitstreams." Other like France's Matra, builders of surveillance satellites, has "publicly mulled selling one meter imaging on the commercial market." Additionally, many nations are now embarking on acquiring space based surveillance systems some with capabilities nearing US performance.

[16]Stix, 95.

[17]*Cornerstones of Information Warfare*, 4. "Information Warfare is any attack against an information function regardless of the means." Example: Bombing a telephone switching facility is information warfare. So is destroying the switching facility's software. Neutralizing enemy air and space assets involves more than a direct attack on the air and space platforms. Ground control stations can be attacked physically from the ground. Its computer systems can be penetrated and destroyed using malicious programs.

[18]TRADOC Pamphlet 525-6, 9.

[19]AFDD 5, 2.

[20]Ibid., 9.

Notes

[21]*Strategic Assessment 1995*, 155.

[22]Sun Tzu, 11.

[23]Christopher Andrew, Christopher. *For the President's Eyes Only* (Harper Collins, New York, 199, 199-256—from "Chapter 6 Dwight Eisenhower (1963-1961): Mossadeq was the Iranian Prime Minister in 1951 but drew the wrath of the West for some of his actions. The objective of the covert action was his removal and the reinstatement of the Shah, exiled at the time. Arbenz was the Guatemalan President and was suspected of being a communist sympathizer.

[24]Schwartau, 82-85.

Chapter 8

Conclusions

The information age began with the invention of the computer and device technology in the 1940s. The cold war era after World War II triggered a superpower race in weapons and space exploration. The research and development fervor that followed produced advances in information technology and systems. Today, many of these products are widely available in the commercial market.

The information age is popularized by futurists like Toffler and Masuda claiming the arrival of a "Third Wave" society dependent on information as a source of power and wealth replacing the outmoded societies of the industrial age. They predict societal, economic, political, and cultural changes resulting from the new age. Evidence exists today supporting some of their contentions. The proliferation of free information and the increasing digitization of national economies and financial practices portend an information dependent 21st century world. The growth of the global network of interconnected computers and information systems further gives credence to the notion of an information age. Challenges arise, however, during the transition period between the industrial and information ages resulting in the rise of new threats to United States' national interests.

The Gulf War demonstrated how decisive the effective employment of information is in war. A new RMA is emerging with information at the center. Past revolutions showed the efficacy of technological innovations in war when used with proper doctrine and an effective organization. Information is the catalyst of the newest form of warfare. When applied at the strategic level, information warfare results in success even prior to committing combat forces to battle. Information warfare is a tool in policy making. Covert information warfare can produce unequaled results in peacetime to advance American interests without resorting to violence. The targets of exploitation include the adversary's information-based economic, political, and military systems.

At the operational and tactical levels, information dominance exploits the enemy's information systems while enhancing US capabilities. Controlling information offensively and defensively destroys the adversary's potential and will for waging combat. In all cases, defensive information warfare is imperative. The result of a successful attack on US systems could seriously disrupt American military operations.

The US military recognizes the importance of formulating doctrine for information warfare. AFDD5 represents a good beginning for doctrinal development. However, part of this doctrine must consider the legal and moral issues associated with this new warfare form. Additionally, once created this doctrine can help define an effective organizational structure for exploiting and employing this tool.

The advent of information warfare does not end the traditional missions of the United States' military. The future spectrum of conflict for the military ranges from a highly sophisticated information based adversary to one barely existing as an industrial society.

Information warfare is not the final solution for all future conflicts, but it provides the United States with a new and powerful instrument for policy making.

Bibliography

Books

Anderton, David A. *Strategic Air Command—Two Thirds of the TRIAD. New York: Charles Scribner's Sons, 1976.*

Arquilla, John and David Ronfeldt. *Cyberwar is Coming.* Santa Monica, Ca., 1992.

Builder, Carl H. and Brian Nichiporuk. *Information Technologies and the Future of Land Warfare.* Santa Monica, Ca.: RAND Corp., 1995.

Christopher, Andrew. *For the President's Eyes Only: Secret Intelligence and the American Presidency from Washington to Bush.* New York, NY: Harper Collins, 1995.

Clausewitz, Carl von. *On War*, edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1989.

Clodfelter, Mark. *The Limits of Air Power—The American Bombing of North Vietnam.* New York, NY: Free Press, 1989.

Cotton, Bob and Richard Oliver. *The Cyberspace Lexicon.* London, UK: Phaidon Press, 1994.

Deibel, Terry L. and John L. Gaddis. *Containing the Soviet Union—A Critique of US Policy.* Washington DC: Pergammon-Brassey's, 1987.

Drew, Dennis (Col) and Dr. D. Snow. *Making Strategy, an Introduction to National Security Process and Problems.* Maxwell AFB, Al: Air University Press, August 1988.

Douhet, Guilio. *The Command of the Air*, translated by Dino Ferrari. Washington DC: Office of Air Force History, 1983.

Dunn, Richard J. *From Gettysburg to the Gulf and Beyond.* Washington DC: National Defense University, 1992.

Forester, Tom *The Information Technology Revolution.* Cambridge, Ma: MIT Press, 1985.

The Global Positioning System: Changing the Future—Summary Report. National Academy of Public Administration, May 1995.

Goodson, Roy, Ernest R. May, and Gary Schmitt. *US Intelligence at the Crossroads.* Washington DC: Brassy's, 1995.

Hackett, Sir John *The Profession of Arms.* New York, NY: Macmillan Pub Co., 1983.

Holley, I. B. *Ideas and Weapons.* New Haven, Conn.: Yale University Press, 1953.

Hutchinson, Norman B (Lt Col). *Command and Control Warfare—Putting Another Tool in the War-fighter's Database.* Maxwell AFB, Al: Air University Press, 1994.

Keaney, Thomas A. and Eliot A. Cohen. *Gulf War Air Power Survey Summary Report.* Washington DC, 1993.

Lubar, Steven. *Infoculture.* Boston, Ma.: Houghton Mifflin Co., 1993.

Moltke, Helmuth Karl Bernhard. *On the Art of War—Selected Writings*, edited and translated by Daniel J. Hughes. Novato, Ca: Presidio Press, 1993.

Mount, Ellis and Barbara A. List. *Milestones in Science and Technology.* New York, NY: Oryx Press, 1987.

Negroponte, Nicholas. *Being Digital.* New York, NY: Vintage Books, 1995.

Petersen, John L. *The Road to 2015: Profiles of the Future.* Corte Madera, Ca.: Waite Group Press, 1994.

Pelton, Joseph N. *Future View.* Boulder, Co.: Baylin Pub, 1992.

Rheingold, Howard. *The Virtual Community: Hometeaching on the Electronic Frontier.* Menlo Park, Ca.: Addison-Wesley Pub, 1993.

Schneider, Barry and L. E. Grinter. *Battlefield of the Future—21st Century Warfare Issues.* Maxwell AFB, Al: Air University Press, 1995.

Schwartau, Winn. *Information Warfare: Chaos on the Electronic Superhighway.* New York, NY: Thunder Mouth Press, 1994.

Strategic Assessment 1995—US Security Challenges in Transition. The Institute for National Strategic Studies, 1995.

Sun Tzu. *The Art of War*, edited and with foreword by James Clavell. New York, NY: Delacorte Press, 1983.

Toffler, Alvin and Heidi. *War and Anti-War: Survival at the Dawn of the 21st Century.* Boston, Ma.: Little-Brown, 1993.

Walzer, Michael. *Just and Unjust Wars: A moral Argument with Historical Illustrations.* New York, NY: Basic Books, 1977.

Wright, Quincy. *A Study of War.* Chicago, IL.: University of Chicago Press, 1942.

Van Creveld, Martin. *Technology and War: From 2000 to the Present.* New York, NY: Free Press, 1989.

Articles and Other Publications

AFDD 1. *Air Force Basic Doctrine*, First Draft August 15, 1995.

AFDD 5. *Information Warfare*, First Draft November 18, 1995.

AFM 1-1. *Basic Aerospace Doctrine of the United States Air Force*, March 1992.

Anonymous. "Apollo 11." *Aviation Week and Space Technology"* (July 18, 1994), s3-s22.

Anonymous. "Virtual Reality for Soldiers, Cops." *The Futurist* (Nov./Dec. 1995), 44.

Anthes, Gary H. "New Laws Sought for Information Warfare." *Computerworld* (June 5, 1995), 55.

Anthes, Gary H. "Viruses Continue to Wreak Havoc at Many US Companies." *Computerworld* (June 28, 1993), 52.

Arquilla, John and David Ronfeldt. "Cyberwar is Coming," reprinted in Air War College Handbook on Conflict and Change (1995), 377-410.

Arquilla, John and David Ronfledt. "Information, Power, and Grand Strategy: In Athena's Camp" (Draft), being presented at the Catigny Conference on "The Information Revolution and National Security," Wheaton, IL, July 20-21, 1995.

Booth, Stephen A. "Doom Virus," *Popular Mechanics* (June 1995), 51-54, 128.
Builder, Carl and James A. Dewar. "A Time for Planning? If Not Now, When?." *Parameters* 24, no. 2 (Summer 1994), 4-15.
Canan, James W. :Space Support for the Shooting Wars." *Air Force Magazine* 76, no. 4 (April 1993), 30-34.
Chilcoat, Richard (Maj Gen). "Preparing Strategic Leaders in the Age of Information." *ARMY* (October 1995), 163-169.
Cornerstone of Information Warfare. Foreword from General Ronald R. Fogleman, USAF Chief of Staff and Sheila E. Widnall, Secretary of the Air Force, 1995.
Covault, Craig. "Desert Storm Reinforces Military Space Directions." *Aviation Week and Space Technology* (April 8, 1991), 42-45.
Covault, Craig. "USAF Urges Greater Use of SPOT Based on Gulf War Experience." *Aviation Week and Space Technology* (July 13, 1992), 61.
Denning, Dorothy E. "The Case for 'Clipper'." *Technology Review* (July 1995), 48-55.
DiNardo, R. L. and Daniel J. Hughes. "Some Cautionary Thoughts on Information Warfare." *Airpower Journal* 9 , no. 4 (Winter 1995), 69-77.
Friedberg, Aaron L. "A History of the US Strategic Doctrine 1945 to 1980." *Journal of Strategic Studies* 3, no. 3 (December 1980).
Funk, Paul E. (Lt Gen). "Army's Digital Revolution." *Army* (February 1994), 33.
Gardels, Nathan. "Third Wave Terrorism." *New Perspectives Quarterly* 12, no. 3 (Summer 1995), 2-3.
Goodson, Roy. "International Terrorism." *Vital Speeches of the Day* 61, issue 17 (July 15, 1995), 520-525.
Gray, Colin S. "The Changing Nature of Warfare?." *The Officer* (August 1995), 36-39.
Hartzog, William W. (General). "A Lighthouse of Ideas on the Road to Force XXI." *ARMY* (October 1995), 55-59.
Hernandez, Debra Gersh. "Bomb Making on the Internet." *Editor and Publisher* 128, issue 25 (June 24, 1995), 38-40.
Isensee, Ernst K. (Major). *Impacts on the Operational Commander in the Information Age*. Naval War College Report (Newport, RI., 1995).
Joint Pub 1-0. *Joint Warfare of the Armed Forces of the United States* (January 10, 1995).
Joint Pub 2-0. *Joint Doctrine for Intelligence Support to Operations* (May 5, 1995).
Joint Pub 3-13. *Joint Doctrine for Command and Control Warfare* (1995 draft).
Kabay, M. E. "Prepare Yourself for Information Warfare." *Computerworld* (March 30, 1995), 2-7.
Komar, David M. (Lt Col). *Information Based Warfare: A Third Wave Perspective*. Air War College Research Report (Maxwell AFB, Al., 1995).
Krepinevich, Andrew F. "Cavalry to Computers—The Patterns of Military Revolutions." *The National Interest* 33 (Fall 1994), 30-42.
Luoma, William M. (LCDR). *Netwar: The Other Side of Information Warfare*. Naval War College Thesis (Newport, RI., 1995).
Mansfield, Edward D. and Jack Snyder. "Democratization and War." *Foreign Affairs* 74, no. 3 (May/June 1995), 79-97.

Mohamed, Sid-Ahmed. "Cybernetic Colonialism and the Moral Search." *New Perspectives Quarterly* 11, no. 2 (Spring 1994), 15-19.

National Military Strategy of the United States: A Strategy of Flexible and Selective Engagement. 1995.

Peterson, A. Padgett. "Tactical Computers Vulnerable to Malicious Software Attacks." *Signal* (November 1993), 74-75.

Powell, Colin (General, Ret.). "Information Age Warriors." *Byte* (July 1992), 370.

Power, Richard. "CSI Special Report on Information Warfare." *Computer Security Journal* 11, no. 2 (1995), 63-73.

Rogers, Clifford J. "The Military Revolution of the Hundred Years War." *The Journal of Military History* 57 (April 1993), 241-278.

Ross, Jimmy D. "Winning the Information War." *Army* (February 1994), 27-32.

Sakkas, Peter E. "Espionage and Sabotage in the Computer World." *International Journal of Intelligence and Counter Intelligence* 5, no. 2 (Summer 1992), 155-192.

Salomon, Leon E. (Gen). "Army Materiel Command: Relevant, Responsive, and Ready." *Army* (October 1995), 61-67.

Schneider, Michael W. (Major). *Electronic Spectrum Domination: 21st Century Center of Gravity or Achilles Heel?* Army Command and General Staff College Report (Ft Leavenworth, Ks., 1995).

Scott, William B. "Information Warfare Demands New Approach." *Aviation Week and Space Technology* 142, no. 11 (March 13, 1995), 85.

Serwer, Andrew E. "Why Bulgarian Bugs Us So Much." *Fortune* 131, no. 9 (May 15, 1995), 32.

Stein, George. "Information Warfare." *Airpower Journal* 9, no. 1 (Spring 1995), 30-39.

Stix, Gary. "Fighting Future Wars," *Scientific American* (December 1995), 92-98.

Szafranski, Richard (Colonel). "A Theory of Information Warfare—Preparing for 2020," *Airpower Journal* 9, no. 1 (Spring 1995), 56-65.

Szafranski, Richard (Colonel). "Parallel War—Promises and Problems," *US Naval Institute Proceedings* 121, no. 8 (August 1995), 57-61.

TRADOC Pamphlet 525-5. *Force XXI Operations*.

TRADOC Pamphlet 525-69. *Concepts for Information Operations*, August 1, 1995.

Waller, Douglas. "Onward Cyber Soldiers." *Time* (August 21, 1995), 38-44.

Zelizer, Barbie. "CNN, The Gulf War, and Journalistic Practice." *Technology Review* (July 1995), 48-55.