Summer 1996

Information Warfare: Technology and the Information Advantage

Daniel Matthew Parker
Old Dominion University

INFORMATION WARFARE: TECHNOLOGY AND THE INFORMATION ADVANTAGE

by

Daniel Matthew Parker
Bachelor of Aerospace Engineering, June 1970, Georgia Institute of Technology

A Thesis submitted to the Faculty of
Old Dominion University in Partial Fulfillment of the Requirement for the Degree of

MASTER OF ARTS

INTERNATIONAL STUDIES

OLD DOMINION UNIVERSITY
August 1996

Approved by:

Regina Cowen Karp (Director)

Philip S. Gillette (Member)

Dennis Ray (Member)

ABSTRACT

INFORMATION WARFARE: TECHNOLOGY AND THE INFORMATION ADVANTAGE.

Daniel Matthew Parker
Old Dominion University, 1996
Director: Dr. Regina Cowen Karp

This thesis analyzes information warfare--that emerging form of warfare that attempts to destroy, degrade and exploit the information systems of another, while protecting one's own--in the context of the technology of warfare. Just as one might peel an onion, the analysis proceeds from a general analysis of technology in warfare to the more specific analysis of information warfare as it is currently defined. Information technology is an enabling factor in the emergence of information warfare as a new warfare area. Although it is revolutionizing the way warfare is conducted, the elements of information warfare have been practiced for thousands of years. Information warfare itself appears to be a natural and expected evolution in warfare. Throughout history, though, the technological superiority and excellence of one group have been short-lived. Technology tends to proliferate and balance the weapons available. More importantly, superior organization, training and doctrine often overcome superior technology.

The paper concludes that the nature of warfare is changing radically. The information advantage and its ability to reduce the uncertainty in warfare will play an ever

important role. Since this advantage is just as important prior to hostilities, the reduction in uncertainty for both political and military actions will be affected. Heightened expectations for the role of technology will continue to grow.

The implications are profound. The world environment is finding regional conflict, ethnic violence, and peacemaking the norm for intervention by conventional military forces. This environment presents a tremendous advantage to the asymmetry in the information edge between military forces such as those of the United States and other countries. Yet, this information advantage could be inconsequential against an opponent without a technological base. The challenge will be to develop the technology, along with the organization, training, and doctrine for information warfare that can be applied against the range of threats to our national interests.

TABLE OF CONTENTS

Chapter Page

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

No one has given a precise date to the start of the information revolution. Most observers mark its beginning with the end of the industrial revolution. Nevertheless, there is almost total agreement that we are in the throes of the most significant world change since the industrial revolution began. This transformation will affect everyone's life from job choices and career decisions to travel, investment, and business decisions. This portends not only a shift for the individual from an industrial society to an information society but also a shift in the way nations interact with one another. These changes include the empowerment of the individual, the change in the nature of warfare, and the erosion of the basic rules of inter-state behavior that have existed for three centuries.[1]

Fundamental change is taking place in the way information is gathered, processed, displayed, transferred, and stored; and organizations are changing to take advantage of increased information. According to analysts John Arquilla and Dave Ronfeldt, "Information is becoming a strategic

---

[1]John Naisbitt and Patricia Aburdene, Megatrends 2000 (New York: William Morrow and Company, 1990), 13; for examples of some of the views on the information revolution and its impact on society in general see Alvin Toffler and Heidi Toffler, War and Anti-War (Boston: Little, Brown and Company, 1993); John Naisbitt, Global Paradox (New York: William Morrow and Company, 1994); for impact on national sovereignty see Walter B. Wriston, The Twilight of Sovereignty (New York: Scribner and Sons, 1992).

resource that may prove as valuable and influential in the post-industrial era as capital and labor have been in the industrial age."[2]

Futurists Alvin and Heidi Toffler provide a model for the change caused by the information revolution that they call the "Third Wave." They argue that the agricultural revolution of 10,000 years ago launched the first wave of change in human history. This was followed by the industrial revolution of 300 years ago which triggered a second wave of change. Today we are feeling the impact of a third wave of change.[3]

The implications of the information era are wide-ranging and affect not only the individual and traditional relationships between families, businesses, and the media but also governments and the military.[4] The major impetus for this revolution is the explosion of information technology. New technology is having a transforming effect because it disrupts old ways of thinking and operating, provides capabilities to do things differently, and suggests how some things may be done better if done differently.

RAND analyst Carl Builder calls this fundamental revolution "the first major shift in the control of

---

[2]John Arquilla and David Ronfeldt, "Cyberwar is Coming!" Comparative Strategy, 12 (1993): 143.

[3]Toffler, War and Anti-War, 9.

[4]For a discussion of the role information plays on the economic relationship among states see Robert B. Reich, The Work of Nations (New York: Knopf, 1991).

information since the Renaissance."[5] We are witnessing an explosion in information technology and the result is a recognizable change in the nature of conflict. With this change emerges a different form of warfare--information warfare (IW).

IW is the ability to use information not only to support other operations, but to use it as a weapon. It is the ability to dominate the battlefield by dominating knowledge. IW has the potential to achieve victory, possibly before conflict. Recent experience in Desert Storm provided a preview of this type of warfare. It was a war "where an ounce of silicon in a computer may have had more effect than a ton of depleted uranium."[6]

As war has evolved through the ages, so have the challenges of keeping pace with the increasing volume of information that is available to the decisionmaker. History shows us that change is truly constant. Information technology is indeed changing the way conflict is viewed by national leaders as well as the population at large.

This paper will analyze IW--that emerging form of warfare that attempts to destroy, degrade and exploit the information systems of another, while protecting one's own--in the context of the technology of warfare. Just as one might

---

[5]Carl Builder, "Is It a Transition or a Revolution?" Futures, March 1993: 158.

[6]Alan D. Campen, ed., The First Information War (Fairfax: Armed Forces Communications and Elecrtonics Association International Press, 1992), xi.

peel an onion, the analysis will proceed from a general analysis of technology in warfare to the more specific analysis of IW as it is currently defined. Chapter I will address the broad topic of the technology of warfare and will identify several themes that result from technology's effect on conflict throughout the ages. Chapter II will narrow the focus to address information technology and the revolution in military affairs. Chapter III will establish IW and information technology in the context of military operations. Chapters IV and V will then investigate IW in its relation to historical theories of warfare and discuss its major subset, command and control warfare (C2W).

The explosion in information technology is creating a dramatic change in the nature of weapons, organizations, and warfighting doctrine. This revolution is also affecting the way nations interact, especially as they prepare to conduct IW prior to conflict. However, IW is not a totally new concept. It represents an informed, organized way of thinking about the utility of information.

As a subset of IW, C2W, which is the application of IW in military operations, is well defined, but the military doctrine that will one day guide the development of operating procedures, identification of warfare requirements, and establishment of the organization necessary to achieve the promise that this warfare area portends, is still in development. The Gulf War gave us a preview of the type of warfare that is possible using the elements of C2W. There is

no denying the impact of information technology on the outcome of that conflict. From a theoretical perspective, C2W can be firmly defined within the framework of commonly accepted and approved principles of war.

IW and C2W are not relegated only to the realm of military action during wartime. There is a strategic level of state operation where IW is used to influence the decisions of another state. There is also an area in the realm of tactical operations where it has applicability. As a form of non-lethal warfare, the elements of C2W and IW offer tremendous possibilities. Because of the complexity of these relationships, this paper will concentrate on the operational and tactical levels of conflict and the application of IW and C2W at these levels.

The implication that IW represents a form of warfare that could preserve lives and property hinges on solving serious policy and political issues. Policies for the use of IW short of hostilities, guidelines on the proper role of perception management at the strategic level, and the role of the press in conducting IW beg development.

The message of this thesis is information technology is indeed an enabling factor in the emergence of IW and C2W as a new warfare area. Although information technology is revolutionizing the way warfare is conducted, the elements of this warfare have been practiced for thousands of years. These elements are as valid today as they were in the time of Sun Tzu or von Clausewitz. In sum, the role of information in

warfare has been linked with conflict for thousands of years--in warfare as well as in peace. The current explosion in information technology ensures that this linkage will continue.

CHAPTER II

TECHNOLOGY IN WARFARE--THE HISTORICAL CONTEXT

War and technology have influenced every era of man's history; the literature is rife with examples of this relationship.[1] From the time of Alexander the Great who commanded his troops from atop a hill, shouting orders to the right flank to move forward or to the left flank to hold position, technology has played an ever increasing role in warfare. Alexander commanded his entire army by voice from a central position without ever writing down an order.[2] Likewise, Admiral Horatio Nelson used only three general flag hoist signals to command his fleet at the Battle of Trafalgar.[3] By contrast, General Norman Schwartzkof's frequency spectrum managers assigned over 35,000 frequencies to U.S. and coalition forces for communications during Desert

---

[1]Some of the more notable works that discuss the relationship of technology and warfare include Martin van Creveld, Technology and War (New York: Free Press, 1991) and The Transformation of War (New York: The Free Press, 1991); Merritt Roe Smith, ed., Military Enterprise and Technological Change (Cambridge: MIT Press, 1985); Manuel DeLanda, War in the Age of Intelligent Machines (New York: Zone Books, 1991); and Bernard and Fawn Brodie, From Cross-Bow to H-Bomb (Bloomington: Indiana University Press, 1973).

[2]This provides a colorful allusion. However, Alexander would never have led his forces from any position other than in the van of the wing of his army with the most important strategic goal. He would never have had time for written orders because he was probably too busy fighting for his life. Martin van Creveld makes note of this in Technology and War (39, 236); see also J.F.C. Fuller, Alexander the Great (New Brunswick: Rutgers University Press, 1960).

[3]Michael A. Palmer, "Lord Nelson: Master of Command," Naval War College Review (Winter 1988): 110.

Storm.[4] The technology that each of these commanders possessed was an integral part of his concept of war and influenced the outcome of military operations for each of them.

This chapter examines the relationship between technology and warfare during the period from about 2000 B.C. to the present and focuses on specific advances in technology that have influenced the conduct of warfare. The final section of this chapter analyzes a unique case study of technology insertion in military operations--the adoption of radio by the U.S. Navy during the early years of this century. What are some of the recurring themes that can be identified as technological advances have changed the manner in which warfare has been conducted? Has technology itself produced a profound effect on the nature of warfare, or have there been other influences that have acted to improve the integration of technology in war? This chapter will examine several technologies that have influenced warfare throughout history and draw conclusions on the impact of this technology.

Land Warfare

Throughout history there have been two dominant forms of warfare and two methods of organizing forces to conduct warfare. On the one hand is attrition, or sedentary, warfare

---

[4]Department of Defense, Conduct of the Persian Gulf War (Washington, D.C.: U. S. Government Printing Office, 1992), 571.

and on the other is maneuver, or mobility, warfare.[5] On one side is the lightning-quick mobility of the nomads of the Steppes who invaded Europe in the thirteenth century; on the other is the sedentary war making style of the Assyrian, Greek, and Roman armies from which modern armies evolved.[6]

The tactics of the nomads were based on the mobility of archers and calvary, coupled with intense firepower. They used the entire terrain of the battlefield for ambush and surprise establishing a combination of psychological shock and physical speed.

The armies of sedentary agricultural states developed an entirely different form of warfare. The Greeks, for example, developed the phalanx, a tightly packed and rigid square of spearmen with heavy armor. It was designed specifically to hold terrain against attacking calvary, and to engage opposing infantry in hand-to-hand combat. However, the phalanx had a very limited ability to maneuver, and control by the commander was difficult, if not impossible, once the

---

[5]Manuel DeLanda introduces the concepts of sedentary and mobile forces in War in the Age of Intelligent Machines (11-13). The concepts of attrition and maneuver warfare have been covered by numerous authors. See for example, Gary Hart and William S. Lind, America Can Win: The Case for Military Reform (Bethesda: Alder and Alder, 1986) and William S. Lind, Maneuver Warfare Handbook (Boulder: Westview Press, 1985) for the definitive treatment of maneuver warfare; and Russell F. Weigley, The American Way of War (Bloomington: Indiana University Press, 1977) for a treatment of attrition warfare American style.

[6]DeLanda, War in the Age of Intelligent Machines, 11; see also Julius Caesar, The Conquest of Gaul, trans. S.A. Handford (New York: Penguin Books, 1982); and Graham Webster, The Roman Imperial Army (New York: Funk and Wagnalls, 1969), 19.

battle was engaged. Despite the improvements made to the phalanx by the Romans, the nomad form of warfare remained the accepted successful model until the late fifteenth century. At that point in history, a new form of warfare, driven by the development of gunpowder and mobile artillery, decided the outcome of battles with the mobile forces of the Steppes. The sedentary form of warfare began to dominate warfare.[7]

1494 marks the transition of this phase of competition between sedentary and nomadic armies. Up to that time, castles had used height to stop an invading army. Now, high walls would become a liability as they made easy targets for cannon. In 1494 when Charles VIII invaded Italy, it was the first demonstration of the effect that gunpowder and cannon would have in centuries to come. Charles VIII integrated 150 years of cannon technology to produce an engine of destruction that left a physical and psychological mark on the towns that he encountered.[8] Although the cannon existed since the fourteenth century, it remained inferior to its rival missile-throwing technologies such as the catapult and the trebucket because of its lack of mobility. The cannon was relegated to the role of siege engine.

In the military campaign of 1494, the cannon became mobile and was available as either a siege engine or field artillery. More importantly, the gunners had been trained for

---

[7]Brodie, From Cross-Bow to H-Bomb, 51-53.

[8]DeLanda, War in the Age of Intelligent Machines, 12.

rapid loading and firing. This ensured for the first time the tactical integration of men and weapons. Perhaps the most significant signal that heralded the arrival of a new technology was the level of destruction that was available. The full integration of artillery into warfare destroyed the existing model of military architecture and forced the creation of a new style of fortifications. Hence, a long tradition in defense technology, height, was replaced by a new model, defense-in-depth.[9]

This use of gunpowder created the conditions under which sedentary armies defeated the nomadic armies of the Steppes that had dominated the art of warfare for centuries. Artillery allowed the sedentary armies to neutralize the mobility of the nomads' calvary. Curtains of metallic projectiles produced by volley fire overcame raw speed and surprise.[10]

The year 1494 represents a distinct transition point in

---

[9]For a complimentary view of the impact of gunpowder and artillery on fifteenth century warfare, see Felix Gilbert, "Machiavelli: The Renaissance of the Art of War," in Makers of Modern Strategy, ed. Peter Paret (Princeton: Princeton University Press, 1986), 3-25.

[10]Gunpowder provides only part of the answer for the decline of the nomads. In addition to the destruction that was wrought by this form of warfare, there was also a concentrating of wealth in a few major kingdoms. Since the new cannons and the ability to organize and effectively fight with them required wealth, the kingdoms with the most resources could easily conquer others. This tended to influence social conditions by centralizing power. Both Felix Gilbert in "Machiavelli: The Renaissance of the Art of War," (5); and Manuel DeLanda in War in the Age of Intelligent Machines, (13) make note of this influence.

the history of technology and land warfare. Despite the numerous and complex developments in the two millennia prior, it can be argued that technological innovations were minimal. In the final analysis, a sword was still a sword, a lance a lance, and a shield remained a shield. A Roman bowman in Caesar's time may not have been distinguishable from a Norman bowman in the eleventh, or even an English bowman in the fourteenth or the fifteenth century. Persian horsemen of A.D 500 resembled medieval knights in that they wore armor and used the lance as their principle weapon.[11]

After about 1500, there was continuous and fairly consistent technological change. In general, this meant that there was no periodic return to old weapons. There was a gradual movement from one obsolete weapon to newly invented ones. Over time, only the most wealthy kingdoms could stay in the race and the others dropped out.[12]

On the other hand, a commander tended to spend his whole career employing the same weapons. Besides breeding extremely knowledgeable generals who were adept at the art of war, this period was notable because none of the great warriors of the age possessed any significant margin of technological superiority. It is difficult to attribute the success of one leader over the other to technological considerations. Even Napoleon, who was far from having any margin of technological

---

[11]van Creveld, Technology and War, 20-21.

[12]DeLanda, War in the Age of Intelligent Machines, 13.

superiority, was not above incorporating an entire captured enemy arsenal into his army.[13] Just as importantly, nontechnical issues had a profound affect:

> Where arms and equipment on both sides were approximately the same, as they normally were in encounters between the principal powers, the factor which decided the issue was not technology, but the ability to combine hardware, training, doctrine, and organization into a single decisive whole. This whole had to be perfect, not only in the sense of tailoring the different constituents to match each other, but above all in relation to the specific enemy and circumstances and purpose at hand.[14]

Even though there was consistent military technological change after about 1500, this change was slow and nearly transparent to contemporary commentators.[15] The early 1800s, however, witnessed the emergence of a number of inventions that radically altered the conduct of war.

Most profound of these inventions were the telegraph and the railroad. By 1830, these strictly non-military inventions were becoming more useful as a coordinated system for military operations. Together they provided the means and the control to move large contingents of troops and supplies. For the most part, they were seen as much more useful in a national

---

[13]Bernard and Fawn Brodie discuss Napoleon's use of technology in From Cross-Bow to H-Bomb (83-85).

[14]van Creveld, Technology and War, 97.

[15]Carl von Clausewitz makes the point in On War, ed. and trans. Michael Howard and Peter Paret, (Princeton: Princeton University Press, 1976), 282, "Today armies are so much alike in weapons, training, and equipment that there is little difference in such matters between the best and the worst of them." He makes only passing reference to military technology in his historical case studies and then dismisses its importance.

strategy than in tactical situations where enemy troops were close at hand. Additionally, they required an infrastructure of rail lines and telegraph wires together with rail heads and telegraph stations. This infrastructure was vulnerable to enemy action and, more importantly, tended to drive the formulation of strategy. During the nineteenth century, armies were deployed not where they would do the most good, but where railroads and stations were situated.[16]

Military application of the telegraph and railroads influenced not only the strategy, but also the scope of warfare. While the traditional distance between wings of an army had been 5-6 km, Napoleon increased this to between 25 and 75 km. By the middle of the nineteenth century, however, strategic dispersion of several hundred kilometers was not unusual.[17] The telegraph allowed for the control of forces at these ranges, but, like the railroad, it was not sufficient for tactical control of commanders on the scene of an engagement who needed rapid communications. The technical problems of operating the telegraph made it a much more useful tool for strategic control of forces. As these limitations were better understood, the side with the greatest appreciation of these technologies was likely the more successful on the battlefield. The Prussian-French war of

---

[16]van Creveld, Technology and War, 169.

[17]See, for example, Hajo Holborn, "Molke and Schlieffen: The Prussian-German School," in Makers of Modern Strategy, ed. Peter Paret (Princeton: Princeton University Press, 1986), 177-178.

1870-71 provided an insightful example:

> . . . so superior were the Prussians in utilizing telegraph and rails that the outcome of the conflict was decided almost before the first shot was fired. This was due less to the superiority in hardware--if anything, it was the French who had more and better rails and rolling stock--than to infinitely superior coordination and use.[18]

Just as the affect of military technological innovation on strategy and tactics represented in these few examples in land warfare provides lessons for the integration of technology in general, war at sea also provides some specific lessons.

War At Sea

No one knows exactly when ships came on the historical scene. Man probably began going to sea on logs and eventually developed more complex vessels by strapping several of them together. At some point it became advantageous to hollow out the log and ride inside rather than on top. This progression of techniques led to the trade of shipbuilding and the ever more complex methods of construction using "skin" that covered a system of ribbing. Ships became ever larger as the technical skills and the technology of shipbuilding allowed for stronger and more durable construction. Until modern times, though, there remained basically two methods of propulsion--the oar and the sail.[19]

---

[18]van Creveld, Technology and War, 159.

[19]Some of the histories that cover the periods of galley, sail and steam include Bjorn Landstrom, The Ship (Garden City, NY: Doubleday, 1961); Philip Cowburn, The Warship in History (New York: Macmillan, 1965); R.C. Anderson, Oared Fighting

Oared craft held a dominant position in world navies until at least the 1500s. As late as 1570 at the Battle of Lepanto, all four of the fleets represented--Ottoman, Spanish, Genoese and Papal--consisted entirely of galleys. Using traditional tactics, the ships of each side were arranged into crescents that hurled themselves at each other with cannon, grappling hooks, and boarding parties that fought sword-to-sword. In response to the destruction of his fleet, the Ottoman Sultan reacted by building a new fleet of the same type. Until early in the eighteenth century, galleys continued to represent the standard of naval power, especially for the French and the Spanish.[20]

A significant weakness during this early period was the lack of navigation technology. Although the compass made its appearance around 1150 in China, it was more than a century before it arrived in Europe. Even its users, fearing that they might be accused of practicing the black arts, kept it out of sight thereby hindering its development as a useful navigation tool.[21] In its absence, only astronomical

---

Ships, from Classical Times to the Coming of Steam (London: P. Marshall, 1962); and John F. Guilmartin, Gunpowder and Galleys: Changing Technology and Mediterranean Warfare at Sea in the Sixteenth Century (London: Cambridge University Press, 1974).

[20]van Creveld, Technology and War, 61-62; Timothy Garden, The Technology Trap (London: Brassey's Defense Publishers, 1989), 7.

[21]The Brodies discuss this aspect of the reluctance of medieval mariners to acknowledge the power of the compass in From Cross-Bow to H-Bomb (34).

observation and dead reckoning were available for navigation. Neither was especially accurate. It was common for a ship at sea or a fleet on a prolonged voyage to proceed until it made landfall and then turn and follow the coast to the intended destination. This made for a most unreliable ability to coordinate land and sea operations. It was impossible to gauge with any degree of accuracy the time required to complete a given course or to estimate the length of a voyage. Alexander discovered this to his great cost while proceeding up the coast of the Persian Gulf. Unopposed troops were reasonably expected to cover a specific distance in a given time. However, a navy was always susceptible to unforeseen happenings.[22]

Although there were probably great changes in maritime technology in the millennia prior to 1500, there were consistent restraints on the use of navies conducting war at sea. The most notable of these was the seaworthiness of the vessels themselves. When a tote of the damage inflicted by opposing navies is weighted against the destruction caused by nature, the elements of nature are the winners by a far margin. In addition to seaworthiness, the inability to sail close to the wind and logistical problems associated with long voyages made it nearly impossible for even a technologically superior country to control the seas. As a result naval

---

[22]See Fuller's analysis of Alexander's campaign along the Persian Gulf and the impact that the timing of his navy had on the operations in Alexander the Great (142, 273); see also Garden, The Technology Trap, 114.

battles were conducted in small, defined spaces of ocean usually within sight of land. Tactics remained virtually the same up until 1400-1500. However, just as great technological changes occurred in land warfare during a similar timeframe, so too did technology advances affect war at sea.[23]

The principal technological advances that occurred in the early modern period involved advances in the technology of ship building. As construction techniques improved, ships became longer and more seaworthy. Bigger ships in turn were able to carry the supplies necessary for prolonged voyages and had the strength to withstand the forces of the sea. These qualities meant that voyages no longer needed to be conducted during the summer months. From the fifteenth century on, far longer voyages were possible than before. Except for the fact that ships needed to take on fresh water and provisions, which they could complete with their small boats, their endurance was almost unlimited. Before the end of the fifteenth century, this endurance allowed America to be discovered and the East Indies to be reached by sea. In 1527, the globe itself was circumnavigated by one of Magellan's ships. As impressive as this feat was in demonstrating the endurance required to make a voyage of such length, the fact that it could be repeated was more remarkable and it soon became

---

[23]van Creveld, Technology and War, 65.

commonplace.[24]

The range and endurance of these ships would have been superfluous had it not been for advances in navigation technology. By 1300 the modern compass was beginning to come into general use but it wasn't until the early eighteenth century that the quadrant allowed an observer to see sun and horizon simultaneously thereby measuring the angle between them regardless of the ship's movement. By 1757 the sextant was developed which finally allowed for latitude to be measured at sea satisfactorily. This method of navigation was not improved upon until the advent of inertial and radio navigation in the twentieth century.[25]

For warfare at sea these technological improvements meant that navies could finally reach the point in endurance, seakeeping and navigation expertise where it was possible to gain control of the sea, a feat which had been impossible up to this period. Fleets could remain at sea for extended periods and chase each other about the oceans so that the string of events that led up to the Battle of Trafalgar in 1805 could occur. Likewise, the increased mobility and seakeeping ability of ships allowed Admiral Nelson's force to maneuver to attack and defeat a French fleet moored in an

---

[24]For a discussion of the technology of ship building during this time period see Gillian Hutchinson, Medieval Ships and Shipping (Rutherford: Fairleigh Dickinson University Press, 1994); and Bjorn Landstrom, Sailing Ships (Garden City, New York: Doubleday and Co., 1969).

[25]Hutchinson, Medieval Ships and Shipping, 170; Cowburn, The Warship in History, 119.

unprotected anchorage at the Battle of Abikur Bay in 1798.[26]

Just as on land, the earliest cannons at sea were made of bronze and designed for use against personnel. They were small and usually mounted high on the ship in order to provide the best fire against the crew of an opposing ship. As the seaborne artillery became larger and heavier, mountings had to be moved below decks to account for the shift in center of gravity which made the platform unstable and susceptible to capsizing. From about 1430 on, cannons were mounted on the centerdecks of sailing ships and fired through ports cut in the sides.[27]

These early cannon were made of bronze and were extremely heavy for their size. Because of this weight, only the larger sailing ships could carry enough firepower to make it worthwhile. This did not matter as long as cannon were scarce, but this scarcity was a matter of price. After 1500, the price of cannon decreased sharply as a result of experimentation by the British during the reign of Henry VIII. They were successfully producing cannon made out of iron rather than bronze. Iron guns were considered substandard and of lesser quality than the bronze guns but were about one-

---

[26]For a discussion of warfare at sea during this time period see for example Ian Friel, The Good Ship (Baltimore: Johns Hopkins University Press, 1995), 139-145; and Brodie, From Cross-Bow to H-Bomb, 111-113. Michael A. Palmer discusses Nelson's command and control techniques in "Lord Nelson: Master of Command" (105-114).

[27]Friel, The Good Ship, 81-85; Landstrom, Sailing Ships, 131-132.

third the price. By the middle of the sixteenth century, despite royal prohibition against export of this technology, countries such as France, the Netherlands, Sweden, and even Russia started their own iron-cannon production. "In the long run, numbers combined with low prices overcame technological excellence as such."[28]

Between 1500 and 1800, naval warfare grew from the technology at hand. Yet it was not only the result of technology. As often happens, naval warfare development was the result of many technical factors, all interacting to bring about new changes.[29] The most important technology that developed included the cannon, the refinement of the steam engine, and the ability to build large vessels out of iron and steel.

One of the major technological developments at the end of the nineteenth century was just such a result of the combination of many factors. The submarine was the fulfillment of an ancient dream. The concept of sailing under the seas dates at least to the designs of Leonardo da Vinci who is said to have produced a design and hidden it for fear that it would be used to develop a weapon. By the time of the

---

[28]van Creveld, Technology and War, 133. This a most important and noteworthy lesson from history, especially when taken in the context of current efforts at counter-proliferation and attempts to limit or control the spread of high-tech weaponry; see also Brodie, From Cross-Bow to H-Bomb, 65.

[29]Garden, The Technology Trap, 7; P.W. Brock, Steam and Sail: In Britain and North America (Princeton: Pyne Press, 1973), 11.

Napoleonic Wars submarines were being produced but were slow and limited in range. During the American Civil War, the Confederates developed miniature submarines that seemed to be more dangerous to their crews than to the enemy. It was not a lack of scientific understanding that slowed the successful development of the submarine, but a lack of technical skill in building and operating the vessels. A suitable engine, a method of finding one's way underwater, and a self-propelled weapon that could be operated under the sea were missing. By the time of the First World War these technological problems had been solved and the submarine had reached a form that would not change for the next 30 years.[30]

Just as each of the previous technological innovations in land and sea warfare had its own unique affect on the conduct of warfare during its period, so too did the introduction of radio into the U.S. Navy at the beginning of twentieth century.

His Master's Voice

At the end of World War I, the U.S. Navy controlled and operated the entire American radio network. It consisted of

---

[30]Brodie, From Cross-Bow to H-Bomb, 133; for a discussion of submarine warfare and American development of the submarine from World War I through the advent of nuclear power see, for example, Weigley, The American Way of War, 180-181, 296-299; for a discussion of the development of submarine warfare in Europe see, for example, Theodore Ropp, "Continental Doctrines of Sea Power," in Makers of Modern Strategy, ed. Peter Paret (Princeton: Princeton University Press, 1986), 451-456; a general discussion of submarine development is found in Kenneth Macksey, Technology in War (New York: Prentice Hall Press, 1986), 8-12.

stations aboard ships, medium-range shore stations, and several high-powered, long range stations capable of signaling thousands of miles. As the United States entered the war, all radio stations were placed under naval control by presidential decree. The navy did not, however, merely maintain custodial control of this national capability, but orchestrated a technological revolution that created an industry. After establishing a technical and organizational infrastructure, Navy officials assumed a central role in negotiations leading to the formulation of our first national radio company, the Radio Corporation of America (RCA).[31] This vision and foresightedness demonstrated by the Navy after World War I belies the fact that just twenty years earlier this new technology was hardly embraced. As late as 1911, naval commanders were writing that wireless technology had no tactical significance for the Navy. The acceptance of radio and its implementation in naval operations were the culmination of a tortuous and lengthy process.[32]

---

[31]John J. Fee provides a brief description of the role the Navy played in the formation of the Radio Corporation of America in "The Declining Years," in Naval Engineering and American Seapower, ed. Randolf W. King (Baltimore: Nautical and Aviation Publishing Company of America, n.d.), 151; see also Hugh G. J. Aitken, The Continuous Wave (Princeton: Princeton University Press, 1985), 302-387.

[32]Susan J. Douglas provides insight into this phase of naval history in her case study of this subject, "The Navy Adopts the Radio," in Military Enterprise and Technological Change, ed. Merritt Roe Smith (Cambridge: MIT Press, 1985), 117-174; see also Erick Barnouw, A Tower in Babel: A History of Broadcasting in the United States (New York: Oxford University Press, 1966) for the early history of radio in the U.S. Navy; and Elting E. Morison, Men, Machines and Modern

Clearly, the Navy's attitude toward the use of radio changed in the two decades between the turn of the century and the aftermath of World War I. Several factors played key roles in this change. One of which, no doubt, was the improvement in the technical capability of the radio. This technological change by itself, though, does not account for the turn-around in the Navy's attitude. Undoubtedly, individual officers were able to influence the way the radio was utilized and contributed to its acceptance. "But possibly the most important factor was the organizational structure of which these men were part and into which this technology had to fit."[33]

Wireless telegraphy, as radio was called, exploded on a fleet that was still adapting to its latest transformation. Having resisted the emergence of steam propulsion and steel hulls for nearly twelve years, the Navy began in 1880 to acquire fast, steel hulled ships. Prodded by Congress, the Navy's transition from wooden to steel hulls and from sail to steam propulsion was nearly complete by 1900. This transformation was traumatic. The new ships had different logistical needs and operating requirements; and demanded fresh thinking about the role of leadership, shore based support infrastructure, and command at sea. The initial

---

Times (Cambridge: The MIT Press, 1966), 17-33, for a discussion of naval operations and changing tactics during this time period.

[33]Douglas, "The Navy Adopts the Radio," 120.

changes were cosmetic. Most of the steam powered ships retained the rigging for sail, and the needed modernization in bureaucratic organization, administration and tactics was lagging.[34]

The Navy's first introduction to wireless came during the America Cup Yacht races of 1899. Guilielmo Marconi brought his new technology to the United States and, as a publicity stunt, arranged for his system to be set up on the press boats covering the race. His arrangement with the New York Herald allowed on-site reporting of the race to reporters on the shore, thus giving the Herald a "scoop" and showcasing Marconi's system. The Navy was aware of the trial and provided officers to evaluate the demonstration. Based on this success, the Navy persuaded Marconi to remain in America longer and to allow a limited test of his system. Follow-on testing received a glowing endorsement from the Bureau of Equipment as a promising technology for the future of the naval service.[35]

Despite successful testing and endorsement, Marconi equipment was never purchased by the Navy. The breakdown between the Navy and Marconi had far-reaching effects not only on the Marconi Company and the Navy but on the new-founded wireless industry in general. The Navy had an extremely

---

[34]Morison, Men, Machines and Modern Times, 34-35, 98-121; Stephen Howarth, To Shining Sea (New York: Random House, 1991), 187-195.

[35]Douglas, "The Navy Adopts the Radio," 128.

difficult time dealing with the contractual and financial needs of the blossoming industry. Every company trying to do business with the Navy encountered an attitude inhospitable to inventors and unappreciative of their requirements to protect and to market their inventions.[36]

Naval officers and inventors were approaching each other from distinct and opposite cultural backgrounds. They had different social values and differing outlooks and orientations. The Navy man was an organizational man. He progressed during his career in an organization that surrounded him and insulated him. Except for wartime, he advanced through diligence and diplomacy and by keeping a low profile. He spent his life both giving and receiving orders within an institutional context. His progression through the ranks was gradual, preserving the status quo, honoring tradition, and defending the organization that provided him security and recognition.[37]

The inventor, on the other hand, had no such organizational loyalty. He was usually a loner whose intelligence and inventive genius were devoted to changing the status quo. Plagued by financial uncertainty usually throughout the life of his invention, his intent was to make his mark on history by facilitating change. An optimist, he

---

[36]Ibid., 131.

[37]For an account of naval culture during the early part of the twentieth century see, for example, E. B. Potter, Nimitz (Annapolis: Naval Institute Press, 1979), 56-65.

usually over-sold his products and exaggerated their capabilities.[38]

The Navy's progress over a twenty-year period to fully integrate radio into naval operations was gradual, shaped by extraordinary external events, and unsettling to the organization. By 1919, when the Navy incited General Electric to purchase American Marconi which led to the founding of RCA, the Navy's vision of radio's value and potential was fully demonstrated.[39] The most critical factor in this process of technical adaptation was organizational realignment. Technical improvements, a European war, and Congressional mandate all pushed the Navy into acceptance and implementation. However, the Navy would not have been able to exploit the invention without restructuring how and where the invention fit into the bureaucracy. In 1899, the Navy was a decentralized organization and the absence of communications links between ships, and between ship and shore, reinforced autonomous action and jealous protection of institutional turf. Radio had the potential to provide invisible, powerful links between previously unconnected segments of the service portending nothing short of structural revolution.[40] The lines of authority aboard ship and on shore were disrupted and

---

[38]Douglas, "The Navy Adopts the Radio," 135.

[39]Hugh Aitken addresses the Navy's distrust of Marconi in The Continuous Wave, (252-255).

[40]Edward L. Beach discusses the institutional environment within the Navy at the turn of the century in The United States Navy (New York: Henry Holt & Co., 1986), 176-185.

redefined as the invention was deployed. The radio was a communications technology and as such defined command and control. It directly affected organizational relationships and who communicated with whom and under what circumstances. Such profound transformations required institutional realignment and the Navy of 1899 could not coordinate or facilitate such a change.[41]

Summary

This chapter has surveyed the history of technology and warfare and highlighted several of the more important advances in technology and the subsequent affect on warfare. There are some conclusions that can be drawn from this very brief survey.

It is apparent that war, and military operations in general, have been completely permeated by technology and governed by it. Even in those instances when commentators have paid little attention to the affect that technology has played in the conduct of warfare, all sides have been influenced by its impact. Technology has influenced the development of tactics, strategy, and the organization of military formations. Additionally, technological superiority has been short-lived. In spite of attempts to control the proliferation of war technology, the record of preventing its spread is unambiguous. Technology proliferation can be

---

[41]Douglas, "The Navy Adopts the Radio," 171; C. Kenneth Allard, Command and Control and the Common Defense (New Haven: Yale University Press, 1990), 69-73.

controlled for a limited time, but can not be completely denied. Whether it is the attempt to prevent the spread of iron cannon or to limit the cross-bow as being a weapon too violent for war, warfare technology eventually spreads to equalize the capabilities of each side of the conflict.

Just as importantly, technology in itself is rarely the determining factor in success on the battlefield. Superior organization, training and doctrine often overcome superior technology. Just as the Prussians were able to defeat the French in 1870-71 through more efficient use of railroad and telegraph technology, superior doctrine and organization prevailed. As well, the most important factor affecting the acceptance of new technology is the organizational structure into which it must fit. The Navy's acceptance of radio is a prime example. Acceptance of the radio in naval operations was as much dependent on proper integration with the organizational structure as it was on technical improvements.

The next chapter will move from this generalization of the technology of warfare to a focus on a specific technology, information technology and the value of the information advantage in warfare.

CHAPTER III

INFORMATION TECHNOLOGY--INFORMATION ADVANTAGE

The two sections of sleek fighters approached each other from the opposite points of the compass.[1] They swooped and soared; turned, banked, and dove, each trying to out maneuver the other to obtain the tactical advantage on the others tail, two miles astern and slightly below. Each pilot reacted instinctively. As his adversary turned, he turned. As his adversary climbed, he climbed. One set of fighters was faster and slightly more maneuverable because of better aircraft design, but the pilot's visibility was hampered by a thick bullet proof glass window in front and high side-rails on either side. His fighter was difficult to control because it took considerable muscle to move the control stick, even thought it was inherently more maneuverable.

The other pilot's aircraft was slower and was designed with more lateral stability making it less maneuverable in pitch and roll maneuvers. Yet his control system was hydraulically boosted and allowed him to more easily maneuver his fighter. His visibility was clear and unobstructed to the forward, side, and rear. He was able to step through a cycle

---

[1]For a discussion of fighter tactics in World War II and the Korean War see, for example, Major General Marion E. Carl, USMC (Ret.), Pushing the Envelope (Annapolis: Naval Institute Press, 1994); and Daniel Ford, Flying Tigers: Claire Chennault and the American Volunteer Group (Washington: Smithsonian Institution Press, 1991).

of observation, orientation, decision, and action (OODA)[2] just slightly faster than his opponent, maintaining the initiative. Clear visibility and sensitive controls gave him an information advantage which more than compensated for a slower speed.[3]

In 1991 the lessons of an overwhelming information advantage were incontestably demonstrated in the desert sands of Kuwait and Iraq. The defeat of Saddam Hussein's army was the result of many factors. The allied coalition had better leadership, and better trained forces; better logistics support and better morale; and better resources and equipment. Most importantly, it possessed the information advantage from a network of communications, surveillance satellites, and high technology weapons that allowed it to speed around the OODA loop far ahead of Iraqi forces.[4]

As was seen in the previous chapter, technology alone seldom wins wars. However, the advent of new technology coupled with innovative tactics and organization can achieve

---

[2]John Boyd, "Organic Design for Command and Control," briefing paper (mimeographed), 1984. John Boyd's considerable contributions to the military reform movement, such as this conceptualized command and control theory of the OODA Loop, are based largely on his unpublished presentations developed since leaving active military service.

[3]For a more technical and mathematical explanation of these observations see for example, Courtland D. Perkins and Robert D. Hogue, Airplane Performance, Stability, and Control (New York: John Wiley and Sons, 1967), 419-475; and Daniel O. Donnasch, Sydney S. Sherby, and Thomas F. Connally, Airplane Aerodynamics (New York: Pitman Publishing, 1967), 480-515.

[4]See for example Campen, The First Information War; and Department of Defense, Conduct of the Persian Gulf War.

an overwhelming advantage. This leaves the other side with only the options of countering the technology or mastering the same tactics and technology. In accomplishing this they revolutionize the way war is fought. Such a revolution is now underway and it involves the ability of countries, armies, commanders, soldiers, and individual weapons to gather, process and use information.[5]

This chapter will analyze information technology as it is enabling what is being referred to as the "revolution in military affairs" and its contribution to the information advantage. Is the revolution in military affairs truly a revolution or is it merely a love affair with advanced technology? If it is a revolution, how is this revolution manifesting itself? And how is information technology providing the information advantage?

Some Attempts to Define the Revolution in Military Affairs

Revolutions in military affairs are nothing new. Advances in technology or changes in strategy and doctrine have always brought changes in the way wars are fought. Some advances have favored the offense while others have favored the defense. Some have been initiated by a new weapon while others have been the result of new ideas about the way wars

---

[5]See for example Oliver Morton, "The Software Revolution, A Survey of Defence Technology," The Economist, 10 June 1995, 5-20; Campen, The First Information War, 171-176.

can be fought.[6]

The current American revolution in military affairs (RMA), as it is being called, has been addressed in joint publications and national journals, as well as, the Service war college journals such as Parameters and the Naval War College Review. A number of thoughtful analysts have wrestled with conceptualizing the RMA. Three of them are presented here: Michael Mazarr, a scholar at the Center for Strategic and International Studies, William Owens, retired Vice Chairman, Joint Chiefs of Staff, and Eliot Cohen, Professor of Strategic Studies at The Johns Hopkins University. These three perspectives suggest something of the universal aspects of the RMA, flavored as always by the authors individual biases.[7]

There have been various advances in military affairs throughout history that have been commonly called revolutions. The advent of gunpowder or nuclear weapons, or the proliferation of mechanization completely reshaped the nature of warfare. Sometimes these advances made offensive warfare

---

[6]Bernard Brodie discusses this phenomenon in War and Politics (New York: Macmillan Publishing Co., 1973), 223-275.

[7]Some other noteworthy thinking on the revolution in military affairs can be found in the following articles: Paul Bracken, "The Military After Next," The Washington Quarterly 16 (Autumn 1993): 27-35; Antulio J. Echevarria and John M. Shaw, "The New Military Revolution: Post-Industrial Change," Parameters 22 (Winter 1992): 17-28; James R. Fitzsimonds and Jan M. van Tol, "Revolutions in Military Affairs," Joint Force Quarterly 4 (Spring 1994): 32-41; and Vladimir I. Slipchenko, "A Russian Analysis of Warfare Leading to the Sixth Generation," Field Artillery (October 1993): 18-23.

obsolete. Whether on the tactical, operational or strategic level, the costs involved became too great while later advances made the battlefield fluid again.[8]

Michael Mazarr believes that revolutions in military affairs have generally shared several aspects in common.[9] These commonalities lead to the central nature of an RMA which has the following elements:

• Fundamental advances in technology, doctrine, or organization that render existing methods of conducting warfare obsolete. The accuracy of the rifled barrel, for example, made massed infantry operations difficult while mechanized warfare did the same for non-mechanized infantry operations. Guerrilla warfare made many conventional tactics ineffective for certain types of war.[10]

• Critical effect on some fundamental aspect of strategy. The classical military strategy expounded by Sun Tzu, Clausewitz, Napoleon, Jomini and others was that concentration of force at a critical point to win a decisive battle leads to

---

[8]See for example Michael Moody, The Dreadful Fury (New York: Praeger Press, 1989).

[9]Michael J. Mazarr, Final Report of the Center for Strategic and International Studies Group on the Military Technical Revolution, (Washington, D.C.: Center for Strategic and International Studies, [1993]), 15-23.

[10]For a discussion of this impact of technology especially in World War I, see for example Hubert C. Johnson, Breakthrough!: Tactics, Technology, and the Search for Victory on the Western Front in World War I (Novato: Presidio Press, 1994); Ed Masey and Kaldor Asbjrn address the issue of technology and guerrilla warfare in The World Military Order: The Impact of Military Technology on the Third World (New York: Macmillan and Co., 1979).

victory. Past military revolutions modified that strategy in basic ways. The advances in firepower in World War I rendered concentration of force a disadvantage to the offense, making large scale offensive operations costly. World War II's mechanized warfare made maneuver, concentration of force and a decisive battle once again possible. This was later dissipated by the nuclear revolution and guerrilla warfare.[11]

• Achieved by a combination of technology, organization, and doctrine. Advances in any one of these three characteristics alone could result in significant advances in warfare but could never generate a revolution. For example, it was more than just the advent of the tank which revolutionized the mechanized warfare of World War II. It was the combination of the technology of the tank plus the doctrine and organization of the blitzkrieg, that revolutionized maneuver warfare.

William Owens defines the elements of a military revolution similarly as ". . . occurring quickly, the changes in the capability will be great and the implications of the changes in military technology will extend through the U.S. military's organization, doctrine, and tactics, and out into the nation's foreign and security policies."[12]

---

[11]See for example Martin L. van Creveld's views on the future of warfare in the nuclear age in Nuclear Proliferation and the Future of Conflict (New York: Free Press, 1993).

[12]Admiral William A. Owens, Vice Chairman, Joint Chiefs of Staff, "System of Systems," Armed Forces Journal International (January 1996): 47.

Owens envisions the emergence of what he calls a "system of systems" that is being created as a result of three recent revolutions. The first is the revolution in world affairs caused by the demise of the former Soviet Union and the end of the Cold War. The second revolution is the budget revolution that began with the reduction of the U.S. military budgets in the mid-1980s and accelerated with the implosion of the Soviet Union. The third revolution is the revolution in military affairs.[13]

Owens believes that the U.S. is the first nation to enter this revolution and will be the first to emerge with all of the capabilities that information technology can bring to a nation and its ability to commit forces to military action. The RMA is driving requirements for military capabilities that fall into three broad categories: intelligence, command and control, and precision force.[14]

- The first category consists of intelligence, surveillance, and reconnaissance (ISR) and relates to the way we collect and disseminate intelligence information and the manner in which we keep track of our own forces as well as our adversaries. Advances in this category are allowing us to "maintain awareness" of vast geographical areas.
- The second category is command, control, communication,

---

[13]Admiral William A. Owens, introduction to Dominant Battlespace Knowledge ed. Stuart E. Johnson and Martin C. Libicki (Washington, D.C.: National Defense University Press, 1995), 3.

[14]Ibid., 4.

computers and intelligence processing, or C4I. This relates to the ability to transfer this awareness to widely dispersed forces in near real-time. This awareness includes force disposition and allocation, targeting data, and identification. "In other words, it is the realm in which we convert the understanding of a battlespace to missions and assignments designed to alter, control, and dominate that battlespace."[15]

• The last category is precision force. Many people see this category in terms of precision guided weapons. It includes these weapons, but it is a much broader concept that includes all our forces and their inherent maneuver and firepower. This is the area in which the two previous categories come together to utilize the knowledge and power garnered from superior ISR and the ability to transfer the information. The combination of superior ISR, C4I and precision force results in a uniquely different military potential.[16]

This result is the creation of a system of systems, caused by broad conceptual architectures that merge our capacity to gather continuously real-time information with our increasing capacity to process and transfer this voluminous data. In Owens' view, this is the essence of the American

---

[15]Ibid.

[16]Ibid., 5.

RMA.[17]

Professor Eliot Cohen takes a more historical view of the RMA. In his view "the contemporary revolution in military affairs, like those of the nineteenth century, has its origins in the civilian world."[18] It is based on two specific developments: the rise in information technologies and the emergence of capitalism in the United States and abroad after World War II. The affect of information technologies has included the development of intelligent weapons that can be used for precision strikes and the ability to transfer vast quantities of information to warfighters.[19]

The rise of capitalism is a novel explanation of the RMA. According to Cohen, countries have spent a great deal of their wealth on defense and created vast bureaucracies to provide for military needs. The competition to supply these needs has created a market for military goods and services. Countries have access to military capabilities far more easily than before. With ready cash they can gain access to military hardware as well as skilled personnel to operate and maintain high-technology weapons.[20]

Cohen defines the RMA in terms of four issues that

---

[17]See also Admiral Owens' discussion of this topic in "System-of-Systems," 47.

[18]Eliot A. Cohen, "A Revolution in Warfare," Foreign Affairs 75,(March/April): 42.

[19]Ibid., 43.

[20]Ibid.

describe it. First is the degree to which the appearance of combat is changed; second is the degree to which the structure of armies is changed; third is the rise of a new military elite; and fourth is the degree to which countries' power position is changed. He believes that these issues reflect a fundamental change in warfare that is only dimly visible.[21]

From an analysis of these four issues, Cohen concludes that a revolution in military affairs is indeed underway. But, he cautions that "revolution implies rapid, violent, and, above all, unpredictable change."[22] Even though the RMA represents an opportunity for development of U.S. military power beyond that of any other country in the world, it will require changes that the military is yet to fully understand and that the politicians can not imagine.

Information Technology

Although the above is more a description of a revolution in military affairs than a precise definition, it allows one now to view some of the elements of information technology within the boundary of a set framework. The growth of information technology is profoundly influencing the U.S. military's ability to achieve the information advantage. As we have seen, success on past battlefields has resulted not so much from technological advances but from innovative ways of considering and combining available and sometimes new

---

[21]Ibid., 44.

[22]Ibid., 54.

technologies to warfighting. A number of these technologies dealt with the communication of information. For example, the telegraph led to distributed operational maneuver in the latter part of the nineteenth century. The telephone redefined fire support, resulting in the greatly expanded role of artillery in World War I. The radio led to the coordinated air, ground, mobile, and armored combat operations of World War II. Finally, the coordinated employment of radar and communications allowed Air Marshal Hugh Dowding's Fighter Command to use the unprecedented capabilities of its command and control system to anticipate the Luftwaffe's attacks and move all available fighters to critical points where its pilots surprised and attacked the enemy in the Battle of Britain.[23]

Information technology is expected to make a thousandfold advance over the next 20 years. Today developments in information technology have already begun to revolutionize how nations, organizations, and people interact. Nowhere is the effect greater than on military organizations. The rapid diffusion of information, enabled by these technological advances, challenges the relevance of traditional organizational and management principles. The

---

[23]The U.S. Army has recognized the importance of information in the conduct of military operations. See for example Department of Defense, Department of the Army, Force XXI Operations (TRADOC Pam 525-5), 1 August 1994, 1-5; see Thomas P. Coakley, Command and Control for War and Peace, (Washington, D.C.: National Defense University Press, 1992), (54), for a discussion of the role of command and control in the Battle of Britain.

military implications of new organizational sciences that examine internetted, nonhierarchical versus hierarchical management models are yet to be fully understood. Take, for example, the organizational chart of a modern army corps and compare it with the organizational structure of a 1950s era major corporation. They are similar--a pyramidal command structure with large groups reporting to ever smaller groups. However, the structure of today's modern corporation barely resembles its cousin of the 1950s, while the organizational structure of the corps has changed little. The army corps still relies on a vast hierarchical structure of officers and enlisted, while the modern corporation has a flat organization with much of the middle management gone. As Eliot Cohen has noted, "The radical revision of these structures will be the last manifestation of a revolution in military affairs, and the most difficult to implement."[24]

Clearly, information age technology, and the management ideas it fosters, will greatly influence our capability to engage in information warfare. Improvements in information technology are evolutionary while the management changes they fosters are revolutionary. Future information technology will greatly increase the volume, accuracy, and speed of battlefield information available to commanders. Such technology will allow organizations to operate at levels most adversaries cannot match, while simultaneously protecting that

---

[24]Cohen, "A Revolution in Warfare," 48.

capability.[25]

Moreover, future technology will also require the military to reassess traditional and time-honored means of conducting command and control of forces. They will have to recognize that in the future, military operations will involve the coexistence of both hierarchical and internetted, nonhierarchical processes. Order will be less physically imposed than knowledge-imposed. Combinations of centralized and decentralized means will result in military units being able to decide and act at a tempo enemies simply cannot equal.[26]

There are logical limits to what can be predicted about technological change. Revolutionary advancements are by their nature unforeseeable. That they will occur is a certainty, but what they will be is far less certain. Even less-than-revolutionary changes are difficult to predict as well. Nonetheless, the most profound implications of advances in information technology will probably occur in the areas of communications and psychological warfare, computer processing, and intelligence gathering and dissemination--those areas that can most significantly influence the information advantage.

---

[25]Some basic organizational behavior texts that discuss the phenomenon include Irving L. Janus, Groupthink (Dallas: Houghton Mifflin Co., 1982); and Daniel A. Wren, The Evolution of Management Thought (New York: Roland Press, 1972), 493-527.

[26]Department of the Army, Force XXI Operations, 1-5. This is the core concept in John Boyd's OODA Loop.

Communications and Psychological Warfare

President Bush employed television in a masterful manner to rally U.S. and world support against Saddam Hussein. Boris Yeltsin and his supporters defeated the tanks of the neo-Stalinist coup plotters with the same electronic tool. Both Bush and Yeltsin understood that public opinion is a crucial center of gravity in modern conflicts. In the future, electronic technology will assume an ever-greater role in shaping perceptions. As a result, U.S. military leaders will need to consider television and other communications as means to defend or smash the will of entire populations. Commercial satellite communications are ever present.

Unlike contemporary television satellites, which require ground stations to relay their signals to individual television sets, satellites are now beginning to send programs directly to viewers. Jamming television signals from space will be quite difficult. Many foreign governments will have to choose between abandoning their own television broadcasts or allowing U.S. propaganda free access to their people. Since it will be possible soon to create fraudulent videos and recordings indistinguishable from reality, U.S. psychological warriors could wreak havoc in the minds of Third World audiences. Consider a U.S. video showing a future Saddam Hussein confessing his stupidity and cowardice to his command

council.[27]

Knowledge of the English language and American culture is spreading rapidly, even among non-elite non-western populations. As a result, U.S. news broadcasting may come to dominate world perceptions of events in peace or war. But this development creates a two-edged sword, also increasing the ability of foreign governments to craft effective propaganda for U.S. audiences.

Computer Processing

Tomorrow's field-level computers, besides being very compact, will have much more processing power than today's supercomputers. Mission planning will be largely automated and less centralized. Operators will be able to enter a goal such as attack a given target or targets. The system will automatically formulate the detailed instructions that lead to the result without the operator having to enumerate each step.[28]

---

[27]Dr. Martin Libicki, "Future Technology and National Security," Technology for Economic and National Security (TENS) Conference Vol II, National Defense University, Fort Leslie J. McNair, 14-15 September 1993, A-9. There has been considerable discussion of the role played by the media in Desert Storm; see for example Alan D. Campen, "Information, Truth and War," The First Information War, (87-91), and the nine articles on the subject in Proceeding, August 1991.

[28]Of the elements of information technology that will advance most rapidly, most observers agree that advances in computing power will be most dramatic. See for example David Brown, "Managing Data, to Win the Information War," Aviation Week and Space Technology, January 1996, s-6; and Amy McAuliffe, "Information Warfare: Technology and Beyond," Military and Aerospace Electronics, December 1995, 6.

Limitations in communications, however, will restrict the military's ability to capitalize on this enormous increase in computing power. Fiber optics, although they promise virtually unlimited capacity for carrying information, will not solve the problem entirely. They are not practical for mobile combat because fiber optics would require that the battlefield be pre-wired to carry information back from the sensors in the field to the computers behind the lines. Moreover, there are real limits to the amount of information that can be carried on radio waves. Some increases in capacity may result from focusing signals, as microwaves do now, to different receivers, or using extremely accurate lasers for line-of-sight communications. In general, the ability to send all information that could be collected to a single headquarters to be analyzed is unlikely to be reached.

It is more probable that an increasing percentage of signal and data processing will have to move into the field at intermediate points. This is where artificial intelligence can be used to maximum advantage. "Smart" nodes will collect information from sensors, compress it, analyze it, act on some of it, store some of it, and send the rest back or across to another node.[29]

Organizing and making sense of the data collected by this vast array of sensors creates a difficult command and

---

[29]Arun Netravali addresses some of the advanced concepts in communications in "Technology, Computing and Telecommunications," TENS Conference, I-40.

control problem. Considerable effort is now being devoted to problems of getting processors to work in parallel, together as a team, rather than depending on one central processor. While it is uncertain precisely how efficient such a system of distributed processors can be made, in general, distributed systems should lead to more robust and survivable forces. Military doctrine has stressed the capture or destruction of a strategic core which could immobilize all other forces. In a system in which critical information flows to multiple nodes or centers, there is less vulnerability to a devastating attack. With sufficient computation power available at subordinate commands, essential pieces of command and control can then be scattered. Focusing operations against a nominal strategic core or critical vulnerability will be far less useful against forces that have taken advantage of the information revolution.[30]

In turn, our current sophisticated capabilities to eavesdrop on communications will become decreasingly useful as a result of the use of coding algorithms such as public-key cryptography. This process is called public because the listener gives out the encoder and keeps the decoder. Right now, all of America's supercomputers working together can barely crack one code. The next generation of codes will be longer and thus virtually unbreakable by combinations of future supercomputers, given the low likelihood of

---

[30]Libicki, "Future Technology and National Security," A-6.

breakthroughs in the mathematics of factoring numbers used in the cryptographic codes. By 2025, unbreakable data encryption and decryption chips will be so cheap they will be built into virtually all devices that could possibly carry sensitive information.[31]

Intelligence Collection and Dissemination

The proliferation of objects capable of acquiring intelligence will be part of a "pop-up" battlefield. Forces will be seen only while shooting or while moving over a terrain mined with sensors. These could consist of flying drones, loitering precision guided munitions, autonomous land crawlers, semi-independent submersibles, and small satellites. It will probably be cost-effective to disperse sensors from planes or even cannon tubes. Many of these sensors have already appeared, albeit in rudimentary form. In the future, they will be cheaper, more sensitive, and capable of simultaneously receiving signals from the various parts of the electromagnetic spectrum. In addition, with advances in artificial intelligence and neural-net technologies, sensors will be able not only to sense simple data but also to recognize more sophisticated patterns on the battlefield.[32]

---

[31]Simon L. Garfinkel, "The Manchurian Printer," The Boston Globe, 5 March 1995, sec. F, 83. For a discussion of the current state of the art in commercial and private cryptography, see for example Neil Monroe, "Information Security Gets a Boost," Washington Technology, 9 March 1995, 40-43.

[32]The Tofflers discuss advanced intelligence gathering technologies in War and Anti-War, (143).

It will also be possible to seed the battlefield with cheap, disposable emitters, which can generate confusing signatures, broadcast precise local positioning signals for precise targeting, and illuminate targets with reflected radio waves. All this will be made possible by a combination of miniaturization, reduced costs, and the development of systems for coordinating emitter signals in large numbers.[33]

While these capabilities focus on the technological aspects of intelligence gathering, the role of intelligence is critical for an effective information campaign, and the foundation is not limited to the scientific and technical aspects of various intelligence analyses and systems. In many cases, intelligence must include biographic, cultural, sociological and economic factors, especially in operations-other-than-war where troops will be coming into direct daily contact with a foreign population. The actions and decisions of these troops could have an immediate effect on foreign policy objectives. The basis of daily activities must have a strong intelligence underpinning. Military personnel must be armed with knowledge.[34]

Equally important as gathering intelligence is disseminating it. Again, Desert Storm gives us an unambiguous

---

[33]This concept is primarily espoused by Dr. Martin Libicki. See his comments in "Future Technology and National Security," (A-5); and in What is Information Warfare? (Washington, D.C.: National University Press, 1996), 12-18.

[34]LTGEN James R. Clapper, USAF, and LTC Eben H. Trevino, USAF, "Critical Security Dominates Information Warfare Moves," Signal, March 1995, 72.

projection of the implications of intelligence dissemination on information warfare. Military intelligence received mixed reviews from operational commanders, and the sharpest criticism concerned inability to get current photographs into the hands of targeteers in time to be of use. That turned out to be largely a problem with communication systems. They lacked the capacity to handle data-intensive photographs; they were technically incompatible with each other and could not exchange data; or they lacked the connectivity to lower combat units such as divisions and below, airfields and ships afloat. Those problems are nothing new. The intelligence and communications communities have been squabbling over inadequate support for high data rates for years, and they will not be easily solved.[35]

The Increased Role of Space Based Resources

Next to advances in computing power, the proliferation of spaced-based resources will be most significant. The U.S. and the former Soviet Union will no longer monopolize space. Shrinking budgets, military force reductions, shifting alliances, openly available technologies, and the commercialization of launch facilities will greatly expand the number of nations having access to space. There is evidence today that extremely-high-resolution imagery (<<5 meters) will be readily available from commercial photo satellites, and these products will no longer be limited to superpower

---

[35]Campen, The First Information War, xiv.

nations. Computer enhancement can further improve the resolution. Japan and France will possess this near-real-time imaging capability, other countries can purchase it. Others, such as Israel--and perhaps Brazil and India--are likely to develop their own imagery capabilities although less sophisticated.[36]

Crises will require that satellite communications and observation sensors be focused rapidly in areas where coalition and U. S. forces will act. The geographic coverage requirements of tactical space systems could expand appreciably from those today. Flexible regional coverage with global access will be important in the design of future space systems. Databases compiling the surveillance of potential targets will have to be rapidly accessible to commanders at all levels. Assured delivery of information will be the goal and a key benefit of future support using space-based resources.

---

[36]Ibid. Resolution is defined as a measurement of the smallest detail which can be distinguished by a sensor system under specified conditions, Joint Pub 1-02, 325. As an example of the commercially available imagery from space resources, two are worth noting--LANDSAT and SPOT. LANDSAT satellites are part of a commercially-owned U.S. system. They are in Sun-synchronous polar orbit, which ensures that the Sun is always in the same position for the image. Each LANDSAT passes over every point on the Earth once every 16 days and each image covers approximately 170 sq. km. SPOT is a French owned satellite system that is also in sun-synchronous orbit and covers every point on earth once every 26 days. Both systems utilize a combination of visual photography and infrared detection. The resolution available from these systems ranges from 120 to 20 meters. The satellite imagery product from both these systems is available on the open market. "Multi-Spectral Imagery Space Resources," Space Tracks, September-October, 1994, 4.

Diplomatic and political pressures to share space-derived data among members of a coalition will be greater than ever before. If access is denied, exploitation of open commercial sources may increase. Growth in commercial ventures will provide many nations the ability to deny others the capability to effect a "black out." Information embargoes could become commonplace. U.S. dependence on commercial or foreign sources for space support will likely increase. Information sharing must be managed to further our national interests. Plans and policies will need to evolve to keep pace with commercial developments.[37]

Desert Storm gave us a preview of the ever increasing importance of space-based resources and the implications for information warfare. It proved the true and remarkable importance of the Global Positioning System (GPS) and the blurring of the distinction between civil and military systems. It demonstrated the military potential of commercial communications and earth observation systems. In some cases the commercial variant proved superior. It demonstrated the vulnerability of democracies to the public glare of worldwide space television news reporting. Space has given the media a freedom which may be impossible to withdraw.[38]

---

[37]Gary A. Frederici and Leon S. Straus, Information Warfare-A White Paper (CNA 93-020) (Alexandria: The Center for Naval Analysis, 1993), 4.

[38]Sir Peter Anson and Dennis Cummings, "The First Space War: The Contribution of Satellites to the Gulf War," in Campen, The First Information War, 133.

Summary

What then can be said regarding the contribution of the explosion in information technology to achieving an information advantage? There can be no doubt that advances in information technology are having a profound affect on the way war is planned and fought. Desert Storm gives a preview of how the new information technology is being harnessed to provide the information advantage to those with the resources to invest in the technology. This is being demonstrated in the way information is gathered, processed, and disseminated. But, is it causing a true revolution in military affairs?

Using the combination of elements of an RMA presented earlier--fundamental advances in technology, doctrine, or organization; critical effect on combat and fundamental strategy; achieved by a combination of technology, organization and doctrine; and providing a shift in countries' power position--it can be argued that although there is the appearance of a revolution, in reality, it may be too soon to tell. The fundamental advances in technology are present and the advances in doctrine seem to be contained in the concept of information warfare. Yet, whether there has been a critical effect on a fundamental strategy is still ambiguous. For example, the strategy changes that were demonstrated in Desert Storm could have been precipitated more by the political situation and influence of the news media, than the direct result of technology. Alan Campen notes that "Desert Storm was and future wars will be fought in the unforgiving

glare of public television. What a military commander does may be aimed as much at influencing public opinion as it is at countering the enemy."[39]

There are several factors that permit some useful predictions on the technological implications of information warfare. First, technologies that may eventually be deployed are foreshadowed by existing prototypes, technological developments and research. Second, even if technological research were simply to stop, the application of current technologies, like fiber optics, would result in new uses such as high-speed telecommunications. Third, new products tend to spread inexorably from the point of development to the rest of the world. Fourth, and perhaps most importantly, information technologies, having progressed at a rapid pace over the last 15 years, are likely to continue to do so for the next decade or two. Collectively, these factors indicate that key aspects of the technological future are indeed foreseeable and the revolution in military affairs may be a "work in progress" for several more decades to come.[40]

The next chapter will move from the general topic of information technology and its application on the battlefield and focus on a specific related aspect, information warfare.

---

[39]Campen, The First Information War, xvi.

[40]Libicki, "Future Technology and National Security," A-3.

CHAPTER IV

INFORMATION WARFARE--THE CHANGING NATURE OF CONFLICT

Consider the following scenario set in the year 2000.

The Crisis: A Middle East state decides the time is ripe for a power grab in the Persian Gulf and directs its threat to an oil-rich neighbor that the United States is pledged to protect. Determined not to repeat Saddam Hussein's mistake, the aggressors elect not to challenge America in a head-on military confrontation. Instead they prepare a more insidious assault. In the United States and abroad among U.S. allies, a pattern of computer mayhem begins to emerge in a cascading sequence of events. Actually, the war has already begun but no one in the United States yet realizes it; keyboard mice, logic bombs and computer viruses do not make much noise.

The Attack: A three-hour power blackout in a Mid-Atlantic city has no reasonable explanation; computer-controlled telephone systems in the United States "crash" or are paralyzed for hours; misrouted freight and passenger trains collide, killing and injuring many passenger. Malfunctions of computerized flow-controlled mechanisms trigger oil refinery explosions and fires; electronic "sniffers" sabotage the global financial system by disrupting international fund-transfer networks, causing stocks to plunge on the New York and London exchanges. In America, local automatic teller machines begin randomly crediting or debiting

thousands of dollars to customers' accounts. As news spreads across the country, people panic and rush to make withdrawals. Television stations in the Mid-East lose control of their programming and a misinformation campaign of unknown orchestration sows widespread confusion. Computerized dial-in attacks paralyze the phone systems at bases where U.S. troops are scheduled to begin deployment; various groups flood the Internet calling for massive rallies to protest U.S. war preparations. Computers at U.S. military bases around the world are stricken--slowing down, disconnecting, crashing. More ominous, some of the military's most sophisticated computer-controlled weapon systems are exhibiting flickering screens and other signs of electronic malaise. Even though U.S. intelligence indicates hostile military intent by the aggressor, there is still no solid information on who is behind the events that have undermined the country's ability to respond to the threats. The reluctant conclusion is that unknown "bad actors" have launched an "infowar attack" against the United States.[1]

"Information warfare," as Lieutenant General James R. Clapper, director of the Defense Intelligence Agency states,

---

[1]Adapted from "Information Warfare: A Two-Edged Sword," RAND Research Review (Fall 1995) which describes a series of strategic exercises simulating an information attack on the United States and its allies conducted for the Department of Defense by RAND. Six exercises, aimed at refining the concept of information warfare and its implications for national security, were conducted over the course of five months from January to June, 1995. Mark Thompson relates the same scenario in greater detail in "If War Comes Home," Time, 21 August 1995, 44-45.

"evolved from the ability of computers and communications equipment to influence the outcome of any event or scenario."[2] However, information warfare means different things to different people. For some, it is all about communications and the predominant role played by communications in the command and control of military forces.[3] For others it is about computers, networks and leadership.[4] The only thing on which everyone seems to agree is that information warfare is important.

What is information warfare and what role does it play in our notion of conflict in the information age? How has the explosion in information technology allowed information warfare to take so prominent a role in the revolution in military affairs? This chapter will analyze these questions and address this relationship between information technology and information warfare.

---

[2]LTGen James R. Clapper, Jr., USAF and LTC Eben H. Trevino, Jr., USAF, "Critical Security Dominates Information Warfare Moves," Signal, March 1995, 71.

[3]For discussions of this view of information warfare see, for example, Bryan Ellickson, Gauging the Information Revolution (N-3351-SF) (Santa Monica: The RAND Corporation, 1988); James P. Kahan, D. Robert Worley and Cathleen Stasz, Understanding Commanders' Information Needs (R-3761-A) (Santa Monica: The RAND Corporation, 1989); and LTCOL C. Kenneth Allard, USA, Command, Control, and the Common Defense (New Haven: Yale University Press, 1990).

[4]For this view of information warfare see, for example, Winn Schwartau, Information Warfare--Chaos on the Electronic Superhighway (New York: Thunder's Mouth Press, 1994); and Clifford Stoll, The Cuckoo's Egg (New York: Doubleday, 1989).

What is Information Warfare

While the authoritative description or definition of information warfare has been slow in being promulgated by the Joint Chiefs of Staff or the Office of the Secretary of Defense, each of the military services has one. None are exactly alike, but all are similar.[5] It is not difficult to find various definitions and descriptions of IW. Several of the more noteworthy concepts from different strategists and the U.S. military are presented below.

The National Defense University's School of Information Warfare and Strategy stresses that information warfare is the sum of many things: electronic warfare, psychological operations, deception, intelligence, reconnaissance, and surveillance. Information warfare is understanding an adversary's flow of information. The resulting knowledge allows the effective application of force against the enemy's information links to increase uncertainty and disorder. This knowledge also allows for the protection of friendly information flow. Because of the critical importance that warfighters place on this flow, it becomes a center of gravity, the center of all power, that, if attacked, will hinder operations. Information warfare is a deliberate warfighting method and strategy. It is an integrated methodology employing combinations of missions and operations

---

[5]Amy McAuliffe discusses this phenomenon of various definitions of information warfare in "Information Warfare," 8. See also Stephen M. Hardy, "Should We Fear the Byte Bomb?" Journal of Electronic Defense 19 (January 1996): 42.

with a heavy reliance on intelligence and communications.[6]

While this description explains information warfare at the operational and tactical levels of conflict, it neglects the strategic level of conflict. Dr. Thomas P. Rona has defined information warfare as:

> . . . the sequence of actions undertaken by all sides in a conflict to destroy, degrade and exploit the information systems of their adversaries. Conversely, information warfare also comprises all the actions aimed at protecting information systems against hostile attempts at destruction, degradation and exploitation. Information warfare actions take place in all phases of conflict evolution: peace, crisis, escalation, war, de-escalation and post-conflict periods.[7]

This definition captures the concept of information warfare that has been missing. It includes all aspects of conflict and can be applied in contexts other than military.

One commentator has developed a construct of information warfare which is even broader in its application. Winn Schwartau views it as being available to anyone with an agenda and an attitude and divides it into three distinct levels of intensity, each with its own goals, methods and targets. By this construct, information warfare is inevitable. The incredibly rapid proliferation of high quality, high performance electronic information systems throughout the world has provided the capability to wage information warfare

---

[6]Clapper and Trevino, "Critical Security Dominates Information Warfare Moves," 71.

[7]Thomas P. Rona, "Information Warfare--Presentation to the Information Resources Management College Seminar, Introduction to Information-Based Warfare," Washington, 11 April 1994. (Mimeographed.)

to anyone with a computer, modem, telephone line connection to the international computer networks, such as Internet, and basic computer knowledge.[8]

Since greed is in no short supply there is tremendous gain to the winner and devastation to the loser in information warfare. It is no longer necessary to intrude physically on a victim's turf to conduct this type of warfare. It is a low risk/high reward endeavor.[9]

Schwartau defines three levels of information warfare intensity:

• Class I--an attack against an individual's electronic privacy. Such things as digital records, files or other portions of an individual's electronic history are the targets. This category of information warfare most resembles terrorism and can be successful because there is no such thing as electronic privacy.

• Class II--an attack against a corporation or between corporations. This is more than just industrial or economic espionage and more than stealing secrets, eavesdropping or stealing faxes. It is more that reading corporate secrets via sophisticated technical means. It is all of these things. It is the use of economic and business information in any way possible to improve one company's position relative to another.

---

[8]Schwartau, Information Warfare, 16.

[9]Ibid. See also David C. Gompert, "Keeping Information Warfare in Perspective," Rand Research Review (Fall 1995).

• Class III--an attack against industries, political spheres of influence, global economic forces, or even against entire countries. This is global information warfare conducted at the strategic level of conflict. It requires extensive financial resources to conduct and also requires sufficient motivation. It requires the ability to organize and control a large number of people and a target with substantial reliance upon information processing capability. It requires a highly technical target. Most of all it requires a great deal of patience on the part of the attacker who must realize that this class of information warfare requires many years to develop the tools and methods to be successful.[10]

While this construct for information warfare is broader in scope that the previous description, it is still limited because it addresses only the technical aspects. It could be better described as "computer warfare" since it is devoted almost exclusively to computer-to-computer interactions.

Although no official unclassified definition of information warfare has been published, brief hints of the definition have appeared in open sources. In late 1992, the Department of Defense (DOD) released a grossly overclassified directive on information warfare that contained an official DOD definition. This policy states that:

> . . . U.S. Armed Forces will be organized, manned, equipped and supported in such a manner as to be able to

---

[10]Schwartau, Information Warfare, 20.

> achieve a distinct information advantage over potential adversaries to win quickly, decisively, and with minimum losses and collateral effects.[11]

It further states that IW is:

> . . . competition of opposing information systems . . . includes exploitation, corruption, or destruction of an adversary's information system through such means as . . . while protecting the integrity of one's own information system from such attacks. The objective of IW is . . . attain dominating information advantage . . . enable force overall to predominate . . . do it quickly.[12]

The U.S. National Security Strategy describes information in the framework of the elements of national power. The formal definition of Nation Security Strategy from Joint Chiefs of Staff Publication 1-02 (JCS Pub 1-02)includes information as an element of nation security and defines it as: "The art and science of developing, applying, and coordinating the instruments of national power, diplomatic, economic, military, and informational, to achieve objectives that contribute to the national security."[13]

---

[11]CAPT R.J. Caldarella, USN, "Information Warfare: The Navy Response," Presentation to the Technical Marketing Society of America, Information Warfare Conference, Washington, DC, 8 December 1994.

[12]Ibid. Department of Defense Directive TS3600.1, Information Warfare, of 21 December 1992 is classified TOP SECRET. Abstracts of the unclassified portions have appeared in various open sources. In the abstract quoted here, the classified portions have obviously been removed. See also J. R. Batzler, RADM, USN (Ret) and Gary A. Frederici, "Science and Technology Initiatives: Information Warfare", Alexandria: The Center for Naval Analysis (CAB 93-29, Feb 1994-Annotated Briefing), 1994.

[13]Joint Chiefs of Staff, DOD Dictionary of Military and Associated Terms (JP 1-02) (Washington, D.C.: Government Printing Office, 1994), 187. (hereafter cited as JCS Pub 1-02)

The above definition provides a useful construct for visualizing the role of information in support of national security strategy. Figure 1 depicts the role that the instruments of national power, diplomatic, economic, military and informational, play in supporting national interests. Diplomacy is seen to have a low level of perceived violence with DOD playing a relatively small role. On the other hand, the use of the military as an instrument of national power is seen to have a high perceived level of violence and it falls almost exclusively in the domain of DOD for execution. These divisions are not absolute. It is possible, for example, to use the military in less violent roles such as peace enforcement or in a diplomatic role such as forward presence or naval port visits. Information can be seen as an instrument of national power which provides national decision makers with a much broader range of options with which to influence events.[14]

Information Warfare Terrain

Most of the literature on information warfare has focused on charting information flows and decision making

---

[14]For discussion of the role of information in national security strategy see for example Owens, "Harnessing the Revolution," 55-57; "Infowar Hearings Planned," Washington Technology, 21 December 1995, 6; Pat Cooper and Jason Glaskow, "New U.S. Army Tenet Focuses on Info Control," Defense News, 18-24 December 1995, 12; Pat Cooper, "Information Warfare Sparks Security Affairs Revolution," Defense News, 12-18 June 1995, 1; and William E. Rohde, "What is Info Warfare?" Proceedings, February 1996, 34-38.

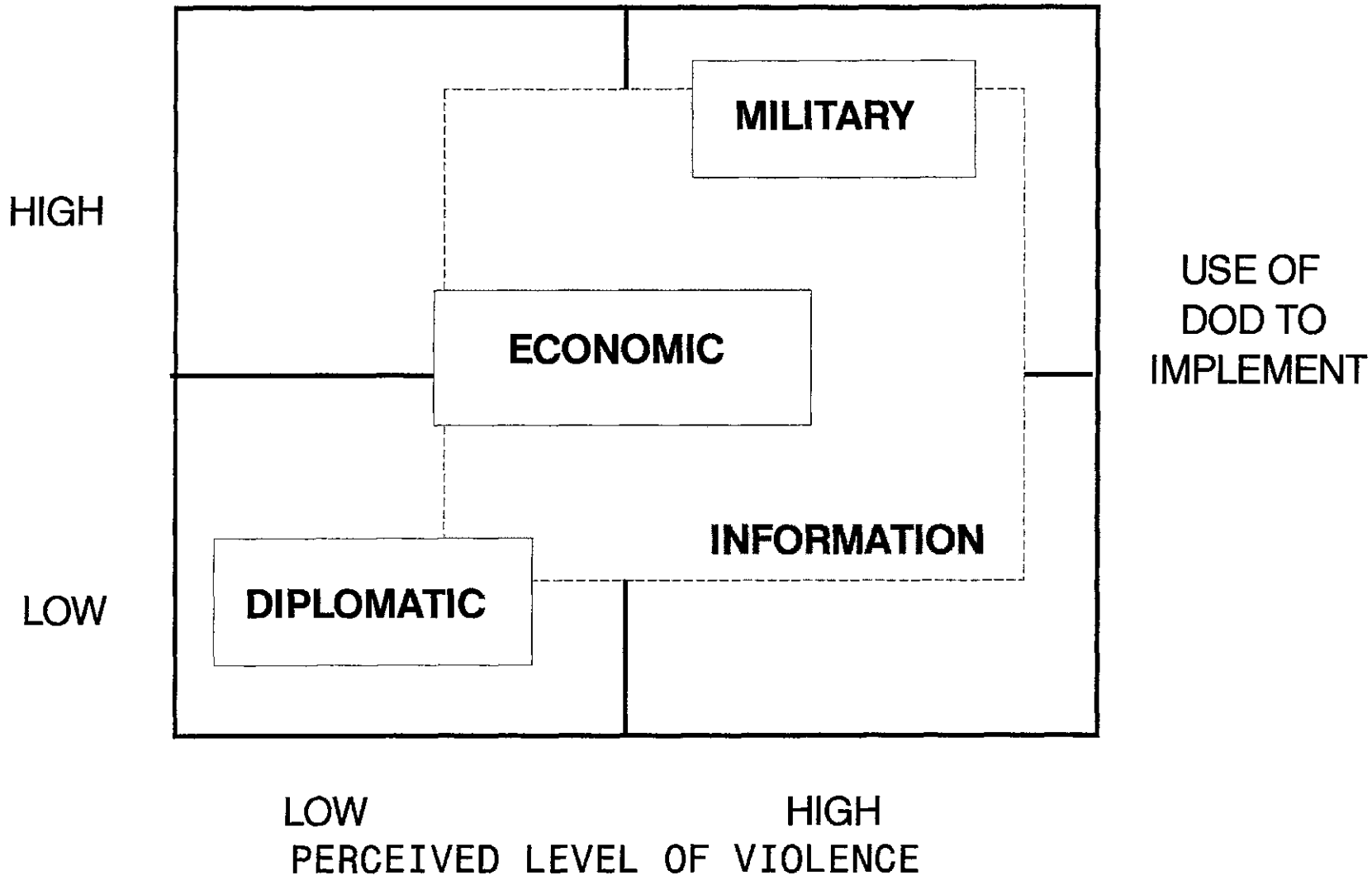

Figure 1: Information as an Instrument of National Power

processes. Little attention has been paid to information as an area or environment of operation or describing the "terrain" of information warfare. One of the problems most associated with the concept of information warfare is that it is viewed as merely a fancy name for intelligence and counterintelligence. It is true that intelligence collection plays an important role in information warfare, as it does in ground, sea or air warfare. Intelligence is, according to the Joint Staff, "the product resulting from the collection, processing, integration, analysis, evaluation and interpretation of available information concerning foreign countries or areas."[15] By this definition, intelligence is a passive affair. Information warfare is an active fight between opposing sides to shape the information battlefield. The information battlefield is an interactive fight between adversaries with one side emerging dominant over the other.[16]

The information battlefield is not a physical battlefield in the sense that Waterloo was in 1815, Midway and the Pacific in 1942, or Britain in 1940. It is, however, fought over a physical dimension, be it the electromagnetic spectrum, fiber or laser optic networks, or through the electronic bits that make up the memory and processing power of the modern computer. These are the features of the terrain

---

[15]JCS Pub 1-02, 205.

[16]Laurence Zuriff, Department of Defense(DOD) intern, to A.W. Marshal, DOD Director of Net Assessment, "Information Warfare", Washington, DC, 13 April 1993.

of the information battlefield. Aside from an operational and tactical dimension, information now has greater strategic value. For example, today, many manufacturing techniques, civilian safety systems, and political-military command structures rely on integrated information processing technologies. All industrialized countries rely on information systems to clear their financial markets, monitor air traffic, collect tax revenue, distribute news and even harvest their food. Just to provide an example of our vulnerability to information systems, the stock market crash of 1987 has been attributed to computer-managed large institutional sales. A similar situation occurred in 1992 when two British speculators were able to devalue the pound in an evening, almost casting the European Monetary System into chaos. The destruction or exploitation of information systems could render a critical function of government inoperable or catastrophically inefficient.[17]

Information Warfare Elements

From the various definitions and descriptions of information warfare it is possible to list at least three components: attack, exploit and protect. In addition it is possible to describe several elements of information warfare. These are:

---

[17]Zuriff, "Information Warfare," 2. See also Walter B. Wriston, The Twilight of Sovereignty (187-200) for a discussion of the affect of information technology on the international monetary system.

• Espionage. Actions directed toward the acquisition of information through clandestine means.[18]

• Propaganda. Any form of communication in support of national objectives designed to influence the opinions, emotions, attitudes or behavior of any group in order to benefit the sponsor, either directly or indirectly.[19]

• Perception Management. Actions to convey and/or deny select information and indications to foreign audiences to influence their emotions, motives, and objective reasoning; and to intelligence systems and leaders at all levels to influence their estimates, ultimately resulting in behaviors and official actions favorable to the organization's objectives. In some ways, perception management combines truth projections, operations security, cover and deception and psychological operations.[20]

• Information Security. Actions taken to protect the integrity of one's own information.

• Computer Warfare. Action taken to deny, destroy, disrupt or exploit the computer systems of another. Usually conducted using computer software, hardware and telecommunications related equipment.[21]

---

[18]JCS Pub 1-02, 192.

[19]Ibid., 285.

[20]Ibid., 273.

[21]Col. Douglas P. Hotard, "Leveraging Technology for the Future," Presentation to the Technical Marketing Society of America, Information Warfare Conference, Washington, DC, 8 December 1994.

For each or these elements of information warfare all three components--attack, exploit and protect--apply. For example the element of espionage has components of attack, exploit and protect where one can attack another's information systems using espionage while protecting against the enemy's espionage and exploiting the enemy's espionage system to provide false or distorted information.[22]

These elements of IW have application throughout the spectrum of conflict from peacetime competition to war.[23] However, espionage, propaganda and perception management and information security would nominally be applied during periods of less violent conflict while computer warfare would likely be applied during more violent conflict.[24]

Why Information Warfare

Information has been an essential element in the successful outcome of conflict from the beginning of history. Knowing the enemy's location, his strengths and his intentions often determine the outcome of battle. Maintaining the secrecy of your own information is just as important as

---

[22]Caldarella, "Information Warfare: The Navy Response."

[23]Current concepts of information warfare are numerous and varied. For example Martin Lubicki defines seven elements of IW which he refers to as "seven forms in search of a function." They are command and control warfare (C2W), intelligence-based warfare (IBW), electronic warfare (EW), psychological warfare, hacker warfare, economic information warfare, and cyberwarfare in What is Information Warfare? 12-38.

[24]Hotard, "Leveraging Technology."

knowing everything possible about the enemy. Information is an equalizer.

One of the earliest examples of this attempt to hide one's own information through the use of ciphers occurred in the fifth century BC. The Spartans employed a device called a "shytale" which was nothing more than a staff of wood around which was wrapped a strip of parchment or leather. The secret message was written on the parchment down the length of the staff. The parchment was them unwound and dispatched to its intended recipient. The letters on the parchment made no sense unless wrapped around a staff the same size as the first. Using the proper sized staff, the message was easily deciphered. Thucydides describes this device as it was used by the rulers of Sparta to order an ambitious prince and general home in about 474 B.C.[25]

Although the technology has changed the intent is still the same--to deny information to the enemy while protecting your own. At the strategic level of conflict, information warfare targets the entire information infrastructure of a nation, not just military targets. Such targets as the banking and financial network of a country as well as the civilian communications infrastructure can be disrupted, manipulated or destroyed. More importantly, information warfare pervades all levels of conflict from normal peacetime competition to total war. But this does not explain why

---

[25]Wriston, The Twilight of Sovereignty, 154.

information warfare has been elevated to the level of other conventional forms of warfare.

There are several indicators. First, information technology is changing the nature of warfare. The industrial form of war used brute force to destroy the economic and battlefield instruments of war--an industrial "broad sword." Information warfare represents a "stiletto to the brain rather than a broad sword to the body."[26] Information warfare is aimed at the information systems of an adversary, the information that is used to make decisions. The goal is to decapitate the enemy and separate the leadership from his forces.[27]

Second, future wars, both state-level and terrorist or tribal, will continue to use the precision weapons developed for industrial forms of warfare, but the primary targets will be the information channels of government, society and the military. And last, priority in targeting will be given to the information systems that enable economic systems such as computers and electrical power and the observation and control

---

[26]RADM J. R. Batzler, USN (Ret) and Gary A. Frederici, "Science and Technology Initiatives: Information Warfare", Alexandria: The Center for Naval Analysis (CAB 93-29, Feb 1994-Annotated Briefing), 1994.

[27]See for example Pat Cooper, "C3I, Data Become Battlefield Targets," Defense News, 4-10 December 1995, 8; and Col. Alan D. Campen, USAF (Ret), "Vulnerability of Info Systems Demands Immediate Action," National Defense, November 1995, 26-27.

of the battlefield.[28]

Few argue the implications of information warfare as a mode of 21st century warfare. The question becomes why is this different from any other form of warfare? The answer seems to lie in four specific areas.

Information warfare is a rapidly changing and relatively uncharted arena. Information technology is changing at an enormous rate. For example, communication bandwidth which equates to the ability to send more information faster is exploding, processor power for computer chips is doubling every 24 months, memory sizes triple every 18 months, and memory density has doubled every 24 months while costs have halved every 18 months.[29]

Most actions in information warfare are designed to be covert and surreptitious. That is, actions taken using information warfare to cause system failures are designed to be ambiguous. Was the system failure the result of deliberate action or was it simply a hardware or software malfunction? Furthermore, information warfare requires "peacetime" involvement. Information sources and data bases must be developed well in advance of any hostilities. And finally,

---

[28]See Bob Brewin, "Info Warfare Goes on Attack," Federal Computer Week, 23 October 1995, 1; and Pat Cooper, "U.S. Wrestles with Info Warfare Enigma," Defense News, 4-10 September 1995, 4,36.

[29]Dr. Aren Netravani, Technology for Economic and National Security (TENS) Conference Vol II, National Defense University, Fort Leslie J. McNair, 14-15 September 1993, I-42.

information warfare inherently possesses possible conflict with civil liberties concepts. Because it must begin very early, prior to any overt hostilities, and because possible targets are strategic information infrastructures such as banking and economics, the legal implications have not yet been fully developed. These legal implications could include violations of international law as well as national restrictions.[30]

The Mixed Gabble of Terminology

Information warfare has become a cottage industry unto itself in attempts to invent words and phrases to define more precisely its meaning. Two of those new words are cyberwar and netwar.

Cyberwar refers to the conduct of information-based warfare. It means disrupting, if not totally destroying, information and communications systems. It means knowing as much about the enemy as possible while denying information on oneself to the adversary.[31]

This form of warfare depends on diverse technologies for command and control, intelligence gathering, tactical communications and accurate positioning for targeting of "smart" weapons. The U. S. Army has recently previewed the

---

[30]BGEN (P) John P. Casciano, "Information Needs and Requirements: An Air Force Perspective," Presentation to the Technical Marketing Society of America, Information Warfare Conference, Washington, DC, 8 December 1994.

[31]Lubicki, What is Information Warfare? 32.

"computer-age" Army of the future. A broad based research program that is developing the computer age Army is designed to prepare the Army for the cyberwar of the next century. Its goal is to prepare the commander to overcome the enemy with superior decision making, maneuvering and applied firepower. This use of digital computer technology is designed to speed the collection and analysis of critical battlefield intelligence, accelerating the decision making process and providing communications and navigational information to mass firepower.[32]

For example, elements of this technology include:

• Precision locating systems--In battle, tanks and other vehicles require exact information on their location and that of the enemy. Tied to the satellite-based Global Positioning System (GPS), and linked by a network of communications data links, all vehicles know exactly where they are in relation to the others. Such a system protects the units from ambush by the enemy and accidental death from friendly fire.

• JSTARS--The Joint Surveillance and Target Attack Radar System (JSTARS) is an airborne, computer enhanced radar system used to track ground targets such as tanks and trucks. On the leading edge of digital radar technology, JSTARS was rushed to Saudi Arabia untested in time for the 100-hour ground war in Operation Desert Storm. The system provided commanders with

---

[32]See for example Neil Monroe, "Pentagon Developing Cyberspace Weapons," Washington Technology 10 (June 22, 1995), 1; and Pat Cooper, "Evolving IW Forces Establish Military Doctrine," Defense News, 4-10 December 1995, 10.

precise movement reports on enemy ground forces. The system is currently flying in support of the peacekeeping efforts in the former Yugoslavia.[33]

• Timely Intelligence--The lack of timely intelligence and the reporting of battle damage assessment in Desert Storm was an acknowledged weakness. Portable systems have been developed that can provide the necessary information to commanders on the battlefield from both local assets and other sources.[34]

Another dimension of cyberwar has been called netwar. Unlike cyberwar which is usually violent and conducted by opposing militaries, netwar refers to information-related conflict at a grand level of strategy between nations or societies. It is usually non-violent and consists of trying to disrupt, damage, or modify what a target population knows or thinks it knows about itself and the world around it. Netwar can take place between rival non-state actors, between governments and between governments and non-state actors. As one example, the governments of the United States and Cuba have been involved in netwar for many years. This is manifest

---

[33]"Joint Surveillance Target Attack Radar Provides Key Data For Bosnian Operation," National Defense, February 1996, 10.

[34]Ed Offley, "Computer-age Army," Seattle Post-Intelligencer, 1 April 1994, 1; for some detailed discussion of JSTARS and the weakness of intelligence reporting in Desert Storm see Thomas S. Swalm, "Joint Stars in Desert Storm," and Timothy J. Gibson, "Rapid Preparation and Distribution of Battlefield Information," in Campen, The First Information War.

by the activities of radio and TV Marti on the one side, and on the international activism of pro-Cuban groups around the world on Castro's side.[35] Among the more impressive examples of government and non-state actor netwar are the running battles between Greenpeace and the industrialized nations over environmental issues. Using advanced communications and information technologies to strengthen their activities, Greenpeace constantly attacks the environmental policies of the major industrial states.[36]

The gabble of terminology such as cyberwar and netwar reflects the immature stage of thought on this subject of "knowledge warfare." Each is simply another term for information warfare. On the one hand, information warfare conducted on the operational and tactical levels of conflict by military forces, and on the other, information warfare conducted at the strategic level between nation-states or between non-government actors and states.[37]

Summary

There is both a military context to information warfare as well as national level policy context. Information warfare can be conducted between nations in all levels of conflict

---

[35]John Arquilla and David Ronfeldt, "Cyberwar is Coming!" Comparative Strategy, 12 (Spring 1993): 145.

[36]See for example Douglas Waller, "Onward Cybersoldiers," Time, 21 August 1995, 38-44.

[37]See also Col. Alan D. Campen, "Rush to Information-Based Warfare Gambles With National Security," Signal, July 1995, 68.

from normal peacetime competition through war. Information warfare can also be conducted among corporations or among state and non-state actors. It is society driven, replete with policy issues. Modern technology has provided the tools to extend the horizon on this new "idea-rich," but still organizationally fragmented, warfare area.

The next chapter will focus on a subset of information warfare, its military application, command and control warfare.

CHAPTER V

INFORMATION WARFARE AND THEORIES OF WAR

History is replete with theories of war. The most enduring of the theorists lived nearly 2000 years apart--Sun Tzu and Carl von Clausewitz. This chapter will discuss IW within the framework of traditional theories of war. How does IW fit within historical theories of warfare and how do the concepts of IW relate to the writings of military strategists of earier times?

Sun Tzu's Military Strategy, traditionally known as the Art of War, has received much exposure in the west. It was first translated by a French missionary about 200 years ago and was reportedly used by Napoleon and certain members of the Nazi High Command. For over 2000 years it remains the most important military treatise in Asia, known at least by name to the common people. Over the centuries the book's concepts have stimulated intense debate and vehement discussion. The Art of War has long been recognized as China's oldest and most profound military treatise. However, scholars continue to debate whether Sun Tzu existed as a military strategist or whether he existed at all.[1]

Carl von Clausewitz' military writings hold a singular position in the history of military thought. His book On War is reverently called a classic, though, as one scholar of

---

[1]Sun Tzu, The Art of War, trans. Ralph D. Sawyer (Boulder: Westview Press, 1994), 79.

Clausewitz has quipped, "one that seems to be more quoted than actually read." It is the first study of war that truly grapples with the fundamentals of its subject, and the first to evolve a pattern of thought adaptable to every stage of military history and practice.[2]

Sun Tzu lived and wrote around 512 BC and Clausewitz' book On War was published posthumously by his widow in 1832, still unfinished. The sheer durability of the principles proffered by these influential military theorist is a testimonial to the enduring nature of their writings.

Information warfare, on the other hand, is a new warfare area. Yet, the concepts supporting IW are not. Many of the basic elements of IW have been a part of warfare since the beginning. Comparing the writings of Sun Tzu and Clausewitz with elements of IW can provide a useful theoretical framework. The elements of deception, surprise, intelligence and command and control are discussed by each of these miliary theorists.

This chapter will analyze IW from two perspectives. On the one hand the elements of IW that can be found in the writings of both von Clausewitz and Sun Tzu will be compared and contrasted to identify the historical impacts that information has had on conflict in these disparate ages. On the other hand, a modern model for conflict that encompasses

---

[2]H. Rothfels, "Clausewitz," in Makers of Modern Strategy, ed. Edward Mead Earle (Princeton: Princeton University Press, 1973), 93.

attrition, and maneuver warfare will be compared with the elements of control warfare for validation.

Deception

In The Art of War, Sun Tzu's military thought has frequently been erroneously identified solely with "deceit and deception" because he advocates employing them to attain military objectives. The principle method of concentrating one's troops while forcing the enemy to disperse his is that of deception. By enabling the deceiver to hide his true objectives, successful deception forces the enemy to concentrate his forces at a place where no attack will actually occur. This weakens him at the decisive point of the real engagement. Deception is also intended to prevent the victim from discovering when and where the real attack will occur, and what methods will be used.[3]

Deception is the most frequently discussed theme in The Art of War, but only two explicit statements actually appear in the book. Sun Tzu's definition of deception is very broad. It includes both active and passive measures from the development of elaborate deception plans, the use of simple diversions to secrecy and concealment. It is employed at all times, before and during war, and on all levels--diplomatic, to drive a wedge between the opponent and his allies,

---

[3]Ralph D. Sawyer, commentary and forward to The Art of War, by Sun Tzu (Boulder: Westview Press, 1994), 136; Michael I. Handel, "Sun Tzu and Clausewitz: The Art of War and On War Compared," Professional Readings in Military Strategy, No. 2, 1991, 39.

political, to plant the seeds of suspicion and discord in his army, or military. Deception is based on a thorough understanding of the enemy's thoughts, expectations and plans. This is derived from good intelligence and the penetration of the opponent's side by one's own spies.[4]

For Sun Tzu, deception is the key to success in war. "Warfare is the Way (Tao) of deception."[5] His list of guiding principles on deception is timeless:

> Although you are capable, display incapability to them. When committed to employing your forces, feign inactivity. When [your objective] is nearby, make it appear as if distant; when far away, create the illusion of being nearby.[6]

Sun Tzu is sensitive to the psychological factors that enable the enemy's perceptions to be manipulated. He understands those convinced of their own superiority and strength are often blind to the need to be on guard against deception. Deceit is not practiced as an end in itself. False measures, feints, prevarications, troop deployments, dragging brush, feigning chaos, and other such acts are designed to manipulate the enemy's perception and cause him to act in a predetermined way thereby providing the army with an exploitable advantage.[7]

On a higher level, false information can be fed to the

---

[4]Handel, "Sun Tzu and Clausewitz," 40; Sawyer, forward to The Art of War, 136.

[5]Sun Tzu, The Art of War, 168.

[6]Ibid.

[7]Ibid.; Handel, "Sun Tzu and Clausewitz," 40.

enemy through double agents or "expendable spies"--those who are deliberately supplied with false information and are allowed to be caught by the enemy. [8]

Sun Tzu is very conscious of deception from double agents and spies in general. While he emphasizes the need to be alert in employing them, he gives no advice on how to distinguish between double agents on the one hand and "real" spies on the other. Of course, the persistent problem of exposing deception is what makes it such a powerful weapon.[9]

In Sun Tzu's broader definition of war, a vital part of deception takes place before the outbreak of hostilities. This type of political and diplomatic deception which sabotages an enemies alliances and internal cohesion is today referred to as disinformation or information warfare. "Thus the highest realization of warfare is to attack the enemy's plans; next is to attack their alliances; next to attack their army; and the lowest is to attack their fortified cities."[10]

Clausewitz, however, does not put much faith in the value of deception operations and diversion.

> To prepare a sham action with sufficient thoroughness to impress an enemy requires a considerable expenditure of time and effort, and the cost increases with the scale of the deception. Normally they call for more than can be spared, and consequently so-called strategic feints rarely have the desired effect. It is dangerous, infact, to use substantial forces over any length of time merely to create an illusion; there is always the risk that

---

[8]Sun Tzu, The Art of War, 231.

[9]Handel, "Sun Tzu and Clausewitz," 41.

[10]Ibid.

> nothing will be gained and that the troops deployed will not be available when they are needed.[11]

Clausewitz does not see deception as a weapon of choice but as the last resort of the weak and desperate.

> Plans and orders issued for appearances only, fake reports designed to confuse the enemy, etc.--have as a rule so little strategic value that they are used only if a ready-made opportunity presents itself. They should not be considered as a significant independent field of action at the disposal of the commander. . . .[12]

> . . . The weaker the forces that are at the disposal of the supreme commander, the more appealing the use of cunning becomes. In a state of weakness and insignificance, when prudence, judgment and ability no longer suffice, cunning may well appear the only choice. The bleaker the situation, with everything concentrating on a single desperate attempt, the more readily cunning is joined to daring. Released from all future considerations, and liberated from thoughts of later retribution, boldness and cunning will be free to augment each other to the point of concentrating faint glimmer of hope into a singlebeam of light which may yet kindle a flame.[13]

The difference between Sun Tzu and Clausewitz on the issue of deception could not be greater. This can be explained based on the level of analysis by each theorist. Sun Tzu is interested in employing deception at all levels including the highest levels of political-strategic and operational. On the other hand, Clausewitz analyzes deception from the viewpoint of the operational and tactical levels where its effect is not only less certain but also less

---

[11]Clausewitz, On War, 203.

[12]Ibid.

[13]Ibid.

effective.[14]

Surprise

Just as he discounted the use of deception, which is the most effective means of achieving surprise, Clausewitz also was convinced that it was practically impossible to achieve surprise at the strategic and higher operational levels.[15]

> The wish to achieve surprise is common and, indeed, indispensable, and while it is true that it will never be completely ineffective, it is equally true that by its very nature surprise can rarely be outstandingly successful.
>
> Basically, surprise is a tactical device, simply because in tactics time and space are limited in scale. Therefore in strategy surprise becomes more feasible the closer it occurs to the tactical realm, and more difficult, the more it approaches the higher levels of policy.
>
> Preparations for war usually take months. Concentrating troops at their main assembly points generally requires the installation of supply dumps and depots, as well as considerable troop movements, whose purpose can be guessed soon enough.
>
> It is very rare therefore that one state surprises another, either by an attack or by preparations for war.[16]
>
> Surprise has lost its usefulness today.[17]
>
> We say this in order to exclude certain vague notions about sudden assaults and surprise attacks which are commonly thought of as bountiful sources of victory. They will only be that under exceptional circumstances.[18]

If surprise cannot be achieved then deception serves no

---

[14]Handel, "Sun Tzu and Clausewitz," 43.

[15]Ibid.

[16]Clausewitz, On War, 198-199.

[17]Ibid., 246.

[18]Ibid., 545.

purpose. Once we move to the lower levels of warfare, surprise may be easier to achieve but its impact is also reduced.[19]

Unlike Clausewitz, Sun Tzu believes that surprise should be on the mind of the military leader at all times and is always a possibility:

> Attack where they are unprepared. Go forth where they will not expect it.[20]
>
> Go forth to positions to which he must race. Race forth where he does not expect it.[21]
>
> The location where we will engage the enemy must not become known to them. If it is not known, then the positions they must prepare to defend will be numerous.[22]

Sun Tzu's confidence in achieving surprise contradicts his faith in the value of intelligence which could be used to prevent surprise from occurring. If one can achieve surprise then so can the enemy which in turn limits the potential contributions from intelligence and calculations or estimates in war. Clausewitz places little faith in the value of intelligence even though he does not believe in the possibility of achieving surprise and is convinced that in many instances intelligence can provide a timely warning. The clue to this inconsistency is again found in the level of analysis. In this instance it has been reversed. When

---

[19]Handel, "Sun Tzu and Clausewitz," 44.

[20]Sun Tzu, The Art of War, 168

[21]Ibid., 191.

[22]Ibid., 192.

Clausewitz refers to the near impossibility of achieving surprise, he is referring to the higher operational or strategic levels. Sun Tzu's high estimate of the utility of surprise is directed at the tactical level of war.[23]

It could be argued that Clausewitz' lack of interest in deception and surprise was right for his own time when it was more difficult to achieve surprise on the higher levels of war. Sun Tzu might have exaggerated the value of deception and surprise in the pre-technology era in which he lived. The achievement of operational and strategic surprise was facilitated by the industrial revolution which made possible unimaginable improvements in mobility, firepower and the availability of real-time communications to coordinate and control troops separated by vast distances. Once surprise became a part of warfare, the value of deception increased. As a result, Sun Tzu's insistence that deception and surprise are a part of all warfare became much more relevant to our own times than Clausewitz' dismissal of its worth. The achievement of surprise at the higher operational level now frequently hinges on the use of deception. In the modern industrial age, concentration of force at the decisive point depends less on the number of troops and more on such elements as mobility, firepower and technological and doctrinal surprise. As demonstrated by the Allies' successful use of deception during the Second World War and, more recently, by

---

[23]Handel, "Sun Tzu and Clausewitz," 44.

the coalition's successful use of it during Desert Storm, the Clausewitzian tradition of underestimating the potential contribution of intelligence and deception is obsolete. Sun Tzu's enthusiastic assessment that they are indispensable remains applicable to modern warfare.[24]

Intelligence

Intelligence is another issue in which Sun Tzu's advice is more relevant for the modern military analyst. Convinced that intelligence is one of the most important multipliers available to political and military leaders, he continuously emphasized the need for meticulous intelligence preparation before the outbreak of war and preceding each campaign and battle. Throughout The Art of War, Sun Tzu makes it clear that an appreciation for the continuous use of intelligence is essential. Good intelligence work can provide more accurate insights into the enemy's mind, intentions, and capabilities as well as into his estimates of one's own dispositions and plans. Sun Tzu's insistence on obtaining the highest quality intelligence must be seen as an ideal that contributes to the educational value of his work. Even if reliable intelligence could never be obtained and uncertainty never eradicated, Sun Tzu's positive attitude toward intelligence would still be important. Clausewitz' negative attitude toward intelligence,

---

[24]Toffler, War and Anti-War, 38; Handel, "Sun Tzu and Clausewitz," 46; for a definitive discussion of deception during World War II, see Seymour Reit, Masquerade--The Amazing Camouflage Deceptions of World War II (New York: Hawthorn Books, 1978).

in contrast, is probably responsible for many of the costly failures of his more dogmatic followers.[25]

Sun Tzu spends an entire chapter on the use of spies to obtain intelligence:

> The means by which enlightened rulers and sagacious generals moved and conquered others, that their achievements surpassed the masses, was advanced knowledge.
>
> Advanced knowledge cannot be gained from ghosts and spirits, inferred from phenomena, or projected from measures of Heaven, but must be gained from men for it is the knowledge of the enemy's true situation.[26]

Given the importance assigned to espionage and intelligence, the leader must reward his agents generously. "The ruler must know the aspects of espionage work. This knowledge inevitably depends on turned spies; therefore, you must be generous to double agents."[27]

One of the most important criteria for evaluating the capability of the commander is his intelligent use of intelligence, with out which he cannot excel.

> Thus enlightened rulers and sagacious generals who are able to get intelligent spies will invariably attain great achievements.[28]
>
> Unless someone has the wisdom of a Sage, he cannot use spies; unless he is benevolent and righteous, he cannot employ spies; unless he is subtle and perspicacious, he cannot perceive the substance in intelligence reports. It is subtle, subtle! There are no areas in which one does

---

[25]Handel, "Sun Tzu and Clausewitz," 46.

[26]Sun Tzu, The Art of War, 231.

[27]Ibid., 232.

[28]Ibid., 233.

not employ spies.[29]

Only through knowledge of the enemy can one defeat his plans. This can only be accomplished through good intelligence. But there are no easy solutions. Agents and spies are notoriously unreliable and may do more harm than good. What can be done to the enemy can also be done by the enemy.

Although Sun Tzu dwells at length on the role of spies, he does not neglect other method of gathering intelligence.

> Someone unfamiliar with the mountains and forests, gorges and defiles, the shape of marshes and wetlands cannot advance the army. One who does not employ local guides cannot gain advantages of terrain.[30]

> Configuration of terrain is an aid to the army. Analyzing the enemy, taking control of victory, estimating ravines and defiles, the distant and near, is the Tao of the superior general. One who knows these and employs them in combat will certainly be victorious.[31]

What we call today "indications and warning" represent another source of direct and indirect information on the enemy's situation and intention. Sun Tzu highlights the following such indicators:

> If an enemy in close proximity remains quiet, they are relying on their tactical occupation of ravines. If large numbers of trees move, they are approaching. If there are many visible obstacles in the heavy grass, it is to make us suspicious. If the birds take flight, there is an ambush. If the animals are afraid, enemy forces are mounting a sudden attack.
>
> If dust rises high up in a sharply defined column, chariots

---

[29]Ibid., 232.

[30]Ibid., 191.

[31]Ibid., 214.

> are coming. If it is low and broad, the infantry is advancing. If it is dispersed in thin shafts, they are gathering firewood.
>
> One who speaks deferentially but increases his preparations will advance. One who speaks belligerently and advances hastily will retreat.
>
> Those who stand about leaning on their weapons are hungry.
>
> One who has emissaries come forth with offerings wants to rest for a while.
>
> If those who draw water drink first, they are thirsty.[32]

Although more reliable than spies, such indicators are subject to manipulation by the enemy and should not be relied upon without corroboration. In gathering the best possible information on the enemy, the commander must also prevent the enemy from doing the same. One way to accomplish this is through security. By not discussing his plans with anyone, the commander denies the information to his enemies:

> It is essential for a general to be tranqil and obscure, upright and self-disciplined, and able to stupefy the eyes and ears of the officers and troops, keeping them ignorant. He alters his management of affairs and changes his strategies to keep other people from recognizing them. He shifts his position and traverses indirect routes to keep other people from being able to anticipate him.[33]

Clausewitz does not concern himself with security because he believes that surprise is virtually impossible and that in most cases attempting to conceal troop movements would be futile. Furthermore, the military genius should be capable of intuitively discerning his opponent's objective despite the

---

[32]Ibid., 208-209.

[33]Ibid., 222.

temporary effects of deception and concealment. Ultimately keeping his troops concentrated and avoiding the temptation to disperse them, the military genius renders the enemy's efforts at security, concealment, and maneuver a waste of energy, if not a form of self-deception.[34]

The obvious question becomes how is one to know, in a world of secrecy, deception, and subjective perceptions, that one's estimates of the enemy's strength are correct? Clausewitz comments, "The difficulty of accurate recognition constitutes one of the most serious sources of friction in war, by making things appear entirely different from what one had expected."[35]

Command and Control

Once the best possible intelligence has been obtained and the estimates taken, the proper plans for war can be prepared. According to Sun Tzu, the outcome can be projected. This is based on the assumption that the commander will be able to implement his plans as they were originally devised. This belief is diametrically opposed by Clausewitz. "In general," suggests Sun Tzu, "commanding a large number is like

---

[34]Handel, "Sun Tzu and Clausewitz," 50.

[35]Clausewitz, On War, 117; modern students of the military art would opine that the command and control process is directed at solving this problem by attempting to reduce uncertainty in the decisionmaking process. See C. Kenneth Allard, Command and Control and the Common Defense (New Haven: Yale University Press, 1990); Coakely, Command and Control for War and Peace; and Frank M. Snyder, Command and Control: The Literature and Commentaries (Washington, D.C.: National Defense University Press, 1993).

commanding a few. It is a question of dividing up the numbers."[36]

Unlike Clausewitz, who saw the battlefield as an uncontrolled and uncontrollable environment, Sun Tzu argues that:

> Simulated chaos is given birth from control; the illusion of fear is given birth from courage; feigned weakness is given birth from strength. Order and disorder are a question of numbers.
>
> One who employs strategic power can command men in battle as if he were rolling logs and stones.[37]

Clausewitz would have found such statements to be unrealistic.

> No other human activity is so continuously or universally bound up with chance. And through the elements of chance, guesswork and luck come to play a great part in war.
>
> The very nature of interactions is bound to make it unpredictable.[38]

Commanders are rarely in control over events on the battlefield. The successful general is not one who carefully implements his original plans, as Sun Tzu idealized, but is the one who can intuitively grasp the chaos on the battlefield and take advantage of its fleeting opportunities.[39]

Clausewitz' discussion of the complexity and unpredictability of war on all levels is perhaps his most

---

[36]Sun Tzu, The Art of War, 187; Handel, "Sun Tzu and Clausewitz," 52.

[37]Sun Tzu, The Art of War, 188.

[38]Clausewitz, On War, 84.

[39]Handel, "Sun Tzu and Clausewitz," 53.

original and important contribution to the study of war. War is permeated by friction, uncertainty and chance, variables whose relationship is unclear and continuously shifting. The sheer complexity of these variables makes any purely rational calculation or planning impossible by definition.[40]

Comparing the writings of Sun Tzu and Clausewitz clearly exemplifies the concept that IW/C2W is not a new phenomenon. The elements have been practiced for thousands of years. The application of these elements has clearly been at both the tactical and the strategic levels of conflict and has encompassed not only offensive aspects but also defensive aspects such as operational security and military deception.

Yet, strategic thinkers offer mixed reviews on the importance of information. Sun Tzu held that dominance in this realm created the necessary conditions for effecting war-winning surprise attacks. Clausewitz, on the other hand, found that friction and the fog of war rendered the influence of superior information negligible. This debate remains unresolved even today.

The historical record provides support for both views. For example, Hannibal's skillful use of signal mirrors during the Second Punic War, kept him apprised of Roman movements and allowed him to spring decisive tactical surprises on his enemies. Yet Xenophon chronicles the saga of a Greek mercenary force that was trapped leaderless deep inside the

---

[40]Ibid.

Persian empire knowing only that the Black Sea lay far to the north and west. The Greeks nevertheless fought their way to freedom. In more modern times the outgunned Royal Air Force prevailed over the Luftwaffe thanks largely to its information advantage.[41]

Is there a reason why the role of information in warfare has been so mixed? One theory is that knowing more about the enemy has always been necessary to achieving success in battle, but it has rarely been the only condition for winning. Thus, the multitude of surrounding Persian forces failed against Xenophon's hoplites because they could not cope with the Greek phalanx. The German Luftwaffe failed to subdue Great Britain as much because of the tactical disadvantage of fighting at great distance from their bases as to the information differential that existed.[42]

Information Dominance of the Battlefield

As these examples imply, information dominance has been an ever present element in warfare. Recent developments indicate that it is prepared to assume a major role in shaping the course and determining the outcomes of wars to come. This is due to the increasing size of the operational battlefield brought about by the increasing accuracy of weapons, and the emerging ability to command and control large, widely

---

[41]John Arquilla, "The Strategic Implications of Information Dominance," Strategic Review, Summer 1994, 25.

[42]Ibid.; Campen, The First Information War, 172.

distributed forces. Computerization, and its effect on information processing and precision-guided weaponry, will create its own revolution in warfighting. This new paradigm for conflict implies that information dominance will win wars because the uninformed may lose the ability to fight. The Gulf War could be a preview of this style of warfare. Table 1 summarizes various models of conflict.

Table 1

Models of War

Modes	Attrition	Maneuver	Control
Aims	Exhaustion	Annihilation	Paralyzation
Examples: Early	Peloponnesian, Punic Wars	Alexander, Caesar	Mongols
Modern	World War I	World War II	Gulf War
Epitomized by:	Industrialization	Mechanization	Computers

Source: Arquilla, "Information Dominance," 26.

Of the three models, attrition has proved longest-lived. From the Periclean strategy against Sparta to the strategic hamlets policy in Vietnam, attritional wars have aimed at exhausting the opponent. Attrition has often worked, but the side which began the attrition warfare has sometimes been its victim. The carnage and sometimes unintended results of attrition warfare, encouraged by the industrial revolution, led to a search for an alternative model. The advent of the

internal combustion engine provided an avenue for escape.[43]

Mechanization, appearing in late World War I, hinted at a new model for warfare based on maneuver. Between the World Wars, British and German strategist began to develop the fast-paced, combined arms doctrine that became the blitzkrieg of World War II. Based on close coordination between aircraft, tanks and artillery, and often aimed at lines of communication, maneuver campaigns dominated the early years of the War. Eventually all combatants came to employ combined arms maneuver techniques which led to massive and costly battles between mechanized force. Attrition warfare returned in the form of tank warfare.[44]

The pattern from World War II was repeated in Korea where the first year of maneuver gave way to attrition. In Vietnam, the situation reversed itself with attrition dominating until the North's closing blitzkrieg campaign against Saigon in the spring of 1975. The Iran-Iraq war quickly turned from Iraq's early maneuver victories to grinding attrition. Even Israel's advantages in mechanized warfare have faded since the costly tank battles of the 1973 Yom Kippur War. The solution to the problem awaited the arrival of a different model that sought to paralyze rather

---

[43]Toffler, War and Anti-War, 40; Arquilla, "Information Dominance," 26.

[44]Arquilla, "Information Dominance," 26; see also Lind, Maneuver Warfare Handbook and Gary Hart, America Can Win: The Case for Military Reform (Bethesda: Alder and Alder, 1986) for discussions of the impact of maneuver warfare.

than to exhaust or annihilate the enemy.[45]

In Desert Storm, U. S. forces enjoyed almost complete information dominance and a form of command and control warfare emerged. At the tactical level, the Iraqi forces seldom knew the origin or strength of the forces attacking them. At the operational level, almost no capability for coordinated, large-scale maneuver and combat remained after the first hours of the ground campaign.[46]

Summary

This discussion on the role of information from two points in history, one ancient and one more recent, and the indication that information dominance represents a new model of warfare argues that information as a vital component in warfare has always "mattered." A variety of factors are converging to enable information to fulfill its potential to achieve overarching effects in the realm of conflict.

But there are profound implications to these overarching effects. These implications affect the technological development of this warfare area, as well as the political and strategic role that information warfare will play. The next chapter will dissect IW one further step and address its purely military application--command and control warfare.

---

[45]Arquilla, "Information Dominance," 26.

[46]For detailed discussions of command and control in Desert Storm see, for example, James M. Burin, "The Electric Sanctuary," and Alan D. Campen, "Iraqi Command and Control: The Information Differential" in Campen, The First Information War.

CHAPTER VI

COMMAND AND CONTROL WARFARE

In the history of mankind, warfare has evolved from hand-to-hand combat to combined arms operations encompassing well organized land, sea, and air forces. Today, faced with high speed threats and unpredictable political events, military operations rely heavily on the efficient and timely flow of information. The requirement to control, use, deny, and manipulate information can provide major advantages at low cost and risk. As a result, Command and Control Warfare (C2W) has recently been defined as "an application of information warfare in military operations."[1]

The idea of C2W is as old as warfare itself. Destroying an enemy's capability to effectively command and control his forces is, and always has been, a lucrative military target. Protecting own force command and control has historically proven to be just as important to successful military operations. In the past, these efforts have been in support of other warfare areas such as the movement of ground forces towards an objective, opening a limited corridor for air strikes against a specific target, or ensuring effective command of a battle group against numerically superior attacking force. The strategy of C2W is new. No longer is it

---

[1]Joint Chiefs of Staff, Memorandum of Policy No. 30 (MOP30), Command and Control Warfare, (Washington, D.C.: Government Printing Office, 1993), 3. (hereafter cited as JCS MOP 30)

solely actions taken in support of another mission, or self defense. It is the over-arching strategy that has as its objective the leadership of the enemy, the center of gravity in today's information dominated world. This is accomplished by attacking from the top down, going after the decision process vice working from the bottom up, cutting off assets piecemeal, a ridge or beach at a time.[2]

This chapter will define C2W relative to a model of command and control. How does C2W contribute to IW and where does C2W fit within traditional concepts of warfare? How can C2W be viewed within the framework of the time-honored principles of war? And lastly, how is C2W related to IW?

Command and Control Defined

Before describing C2W in more detail, it would be useful to define military command and control and a theory for describing the command and control process.

The principal element of command and control is command. Command is a function of authority, responsibility and accountability. Formally defined, it is:

> The authority that a commander in the military Service lawfully exercises over subordinates by virtue of rank or assignment. Command includes the authority and responsibility for effectively using available resources and for planning the employment of, organizing, directing, coordinating, and controlling military forces for the accomplishment of assigned missions. It also includes responsibility for health, welfare, morale, and

---

[2]Ibid.; targeting individual leaders in time of war is not a novel concept. See, for example, Bruce A. Ross, "The Case for Targeting Leadership in War," Naval War College Review, Summer 1993, 73-93.

discipline of assigned personnel.[3]

Command connotes leadership--the art of motivating people toward a common objective. Leadership is the foremost quality of command, instilling unit cohesion and sense of purpose. It is the catalyst that inspires effort, courage, and commitment. It is the cornerstone of effective command.[4]

The second element of command and control is control. Control is the means by which the commander guides the conduct of operations. Command decides what must be done; control guides the action required to accomplish what must be done. Control gives the commander the means to allocate resources, integrate efforts, and measure performance. It can range from the broad control of military operations--such as the policies issued by a theater commander--to the specific, procedural control of individual weapon systems. We typically think of control as occurring concurrently with the action being controlled, but it may also occur beforehand. For example, a well-conceived plan based on an accurate assessment of the situation, that clearly indicates what needs to be accomplished and why, provides a certain amount of control. Similarly, effective training and education, which make it more likely that subordinates will take the proper action in combat, provide control before the fact. A commander's intent, expressed clearly before the operation begins, also

---

[3]JCS Pub 1-02, 87.

[4]Allard, Command, Control, and the Common Defense, 16.

exerts control.[5]

Many thoughtful analysts have wrestled with the conceptual outlines of the command and control process. As introduced in chapter II, Colonel John Boyd, a retired Air Force Colonel and consultant on command and control matters, provides what has become probably the best known and simplest theoretical treatment of this problem. According to Boyd, command and control is a continuous, cyclical process by which a commander makes decisions and exercises authority over his forces in accomplishing an assigned mission. Each commander's decision and execution cycle has four sequential steps. Figure 2 depicts this process of observation, orientation, decision, and action. Each of these steps is part of a tactical decision loop, the idea being that success in battle often depends on which commander can complete the loop faster. Although this model oversimplifies a complex process, it is useful in showing how command and control functions and how command and control warfare affects the process.[6]

First the model recognizes the commander as the crucial element in the entire process of command and control. Accordingly, a commander first observes the environment, using sensors, information systems, and situation reports from his

---

[5]Ibid., 150; for examples of current thought on both the command and control process and the command and control system see, for example, Snyder, Command and Control: The Literature and Commentaries and Coakley, Command and Control for War and Peace.

[6]Boyd, "An Organic Design for Command and Control."

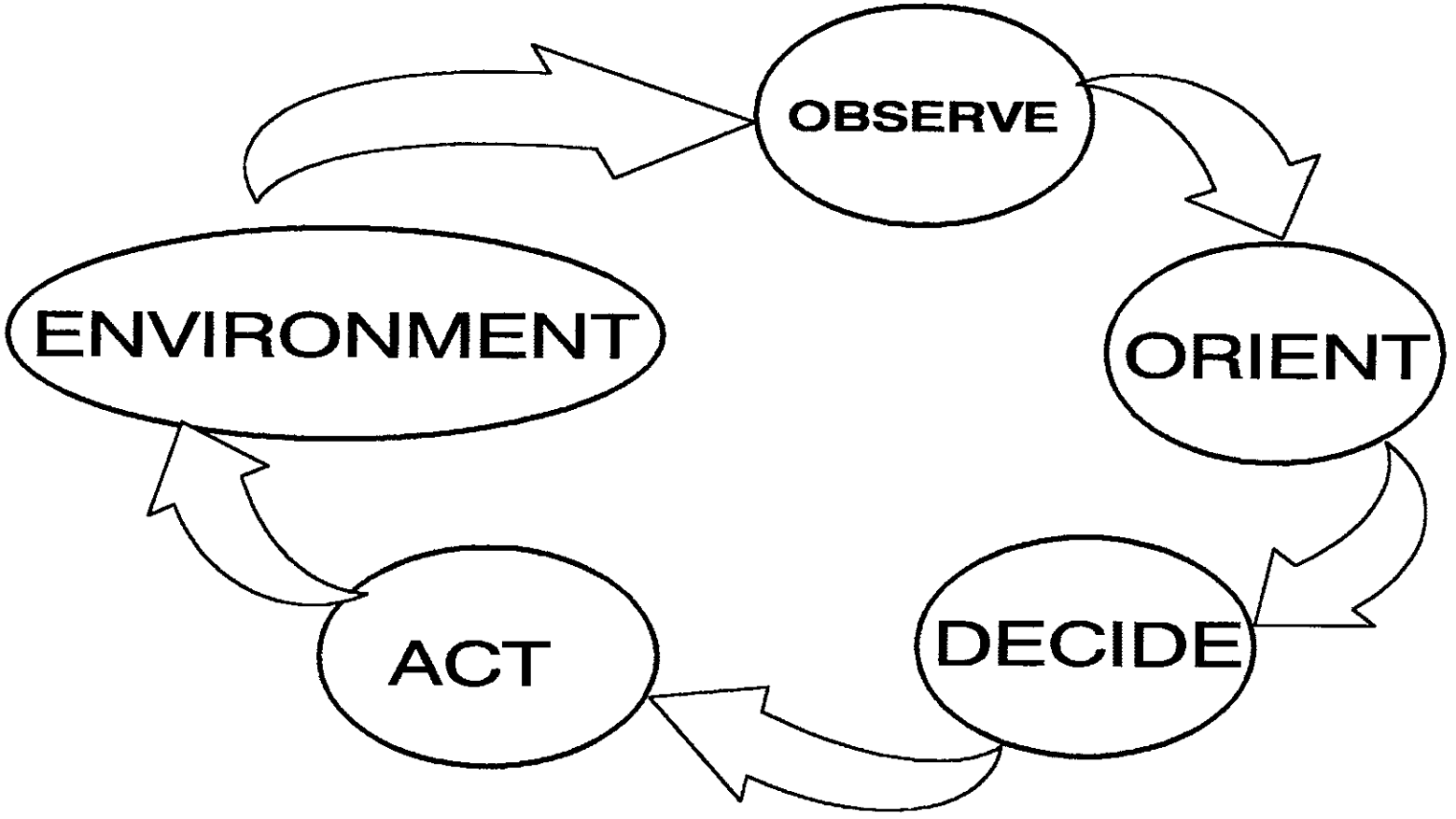

Figure 2: The Observe-Orient-Decide-Act Cycle

Source: Allard, Command, Control and the Common Defense, 151.

subordinates, to gather data about his surroundings and the status of enemy and friendly forces. Next, he orients himself to the environment--that is, he forms a mental image of the situation--by converting sensor data and other information into estimates, assumptions, and judgments about what is happening, Based on his understanding of the situation, he then decides on a course of action and comes up with a plan. Finally, he sets forth his intent and issues orders to put that plan into action. During the action, the commander monitors the execution of operations and gauges their results, bringing him full circle to the observation phase, from which he begins the cycle again. Throughout the entire cycle, the fog and friction of war continually affect the commander's ability to observe, orient, decide, and act.[7]

The enemy's observe-orient-decide-act loops are bounded by these same factors of time and friction. When one effort can increase the friction, it extends the time the adversary needs to execute the cycle. If this effort simultaneously reduces friction and time for the one, the commander will effectively outperform an adversary in combat and will prevail in engagement, crisis or conflict.[8]

What is Command and Control Warfare

Command and control warfare integrates five well

---

[7]Allard, Command, Control and the Common Defense, 151.

[8]Clapper and Trevino, "Critical Security Dominates Information Warfare Moves," 72.

established military tools to achieve information superiority:

- Psychological operations and military deception to replace the information that is being denied to the enemy with tailored information that drives the perception, morale and decision-making of the adversary;
- Operations security to deny adversaries information about friendly capabilities and intentions by identifying, controlling and protecting indicators associated with planning and conducting military operations;
- Electronic warfare to attack an enemy's combat capability using electromagnetic or directed energy to disrupt and deny information; and,
- Physical destruction to permanently or temporarily render the adversary's information infrastructure inoperable for a specific period of time.[9]

The true value of C2W is in the integrated application of these proven military capabilities, supported by intelligence and command, control, communications, computers and intelligence (C4I).

Referring again to Figure 2, it is apparent how the tools of C2W can be applied to disrupt, deceive and deny information to an adversary. Assuming that an enemy's command and control process can also be approximated by this same model, C2W attacks the decision making process. Psychological operations and military deception act primarily on the

---

[9]JCS MOP 30, 5.

observation and orientation phases of the process while electronic warfare and physical destruction inhibit the enemy commander's ability to control his forces in the act phase of the process. Operations security can operate on several phases of the process by denying information required to make decisions.[10]

Command and Control Warfare and the Principles of War

The principles of land, naval, and air warfare are well understood and have become codified in the doctrines of the services that provide forces to operate in each of those media. These separate doctrines have been derived from experience and have withstood the test of actual combat. Each service's doctrine evidences an understanding of the operational environment, accurate descriptions of the characteristics of the forces which operate there, and knowledge of the combat-tested principles which form the basis for operations on land, at sea, and in the air. Many of those combat-tested principles have their genesis in the works of Sun Tzu, von Clausewitz, Mahan, Corbett and Douhet. They are rooted firmly in history and stem from the legacy of actual battles.[11]

---

[10]Ibid.

[11]For a discussion of the principles of war as seen by these theorists see: Allard, Command, Control and the Common Defense, 91-92, 32-33; Russel B. Weigley, The American Way of War (Bloomington: Indiana University Press, 1973), 174-182; Bernard Brodie, War and Politics (New York: MacMillan Publishing Co., 1973), 31, 345, 437, 440-453.

The student of C2W has a tougher chore, for there is very little actual experience with a C2 "battle field", an environment made hostile by deliberate enemy action. Nonetheless, recent war games and exercises, in which one side used the elements of C2W against the other side, suggests that the course and outcome of battle can be influenced by successful attacks against C2 systems. This was reinforced in the Persian Gulf War. Add to this the studies into the ways in which future technologies, including non-lethal technologies, will affect military operations, and there are sufficient insights from which to derive concepts and postulate principles of C2 warfare.[12]

In this section the joint service approved principles of war are used as a frame work to develop C2W concepts. They can be used to stimulate thought, to develop concepts, and, in this case, to discover fundamental tenets about command and

---

[12]Some representative studies that address the subject of future technologies and their possible affect on military operations include Jeffery R. Cooper, "Spectrum Plan--Towards a New Strategic Vision for Future Naval Forces," SRS Technologies, Briefing, October 1993; Final Report of the Center for Strategic and International Studies Group on the Military Technical Revolution, By Michael J. Mazarr, Project Director, (Washington, D.C.: Center for Strategic and International Studies, 1993); Naval Communications Architecture, Task Group 2, Navy Space Panel, Naval Studies Board, Commission on Physical Sciences, Mathematics, and Applications, National Research Council, (Washington, D.C.: National Academy Press, 1994). For an assessment of actions that became C2W in Desert Storm, see Command, Control, and Communications Countermeasures (C3CM) During Desert Shield/Desert Storm(U), By W. J. Barlow, Project Leader, (Alexandria, VA: Institute for Defense Analyses, June 1992).

control warfare.[13]

To this end, the assumption is made that the historical principles of war are applicable to military operation in C2W. The principles of war are a good starting point because they have been proven to be essential elements in successful military operations throughout history. Hence, they offer a solid foundation for operational planning. Given this assumption, the following discussion centers on how the principles of war apply to C2W.

The development, deployment and employment of C2W assets can be guided by fundamental military principles. It is appropriate to use the well-established principles of war as a framework to formulate basic concepts and doctrinal tenets for C2W even though significant experience is lacking. One approach is to make general arguments and draw broad conclusions to gain insight and understanding of what C2 warfare operations may involve, and not to describe them in detail.

An important issue throughout military history has been

---

[13]The nine principles of war approved by the Joint Staff are discussed in such publications as Joint Chiefs of Staff, Joint Pub 0-1, Basic National Defense Doctrine (Washington, D.C.: Government Printing Office, 1994); Joint Chiefs of Staff, Joint Pub 1, Joint Warfare of the U.S. Armed Forces (Washington, D.C.: Government Printing Office, 1993); and Department of the Army, Field Manual 100-5 (FM 100-5) Operations (Washington, D.C.: Government Printing Office, 1993). For a classic discussion of the abuse of the principles of war see Professor Bernard Brodie, "The Worth and Principles of War," United States Naval War College, Operations Department, from a lecture delivered 7 March 1957 to the U.S. Army Command and General Staff College, FT. Leavenworth, Kansas.

the way a military organization addresses the qualities that war demands from its participants. Military leadership has dealt best with the intractable problems of war as a form of military art. Wisdom gained from study of the basic principles of war underscores that war is not the business of managers; it is the art of leaders. Command and control warfare is no less driven by these enduring principles.[14]

• *Principle of the Objective.* Liddel Hart notes that the effective strategist's "true aim is not so much to seek battle as to seek a strategic situation so advantageous that, if it does not of itself produce the decision, its continuation by a battle is sure to achieve this."[15] In the sense of grand strategy, the combination of a sound U.S. economy, a strong national will, and the strength of our military forces support the achievement of a strategic situation which should deter enemy aggression and foster our national aspirations. C2W provides the tools to enforce deterrence by degrading the enemy's capability to conduct war during pre-hostilities. If deterrence fails, however, our military forces must be postured to produce the decision by battle. If battle ensues, what are the objectives of C2W?[16]

C2W has as its strategic goal the separation of the

---

[14]Brodie, War and Politics, 479.

[15]B. H. Liddell Hart, Strategy, 2nd ed. (London: Faber & Faber Ltd., 1967; Signet Books, 1974), 325.

[16]A National Security Strategy of Engagement and Enlargement (Washington, D.C.: The White House, 1995), 1-7.

enemy leader from his forces, to render the leader remote from his people and control his use of the electromagnetic and acoustic spectra. This objective dominates when our quarrel is not with the people but with enemy leadership, when it is highly desirable to limit damage, contain the conflict, and terminate quickly. The key to successful C2W is its integration throughout the planning, execution and termination phases of all operations.[17]

C2W also has a clearly defined target set. This target set consists of those systems, which when destroyed, yield the strategic objective. For C2W the target set consists of the enemy leadership at all levels including the tactical level, its communications systems, both military and civilian, surveillance and targeting systems, information processing, decision and display systems, electronic warfare systems, and weapons guidance systems. An attack on this target set is the epitome of power projection, the ultimate penetration of the enemy. These operations provide a focus of effort to deliver a decisive blow to the enemy's center of gravity and truly enable maneuver warfare.[18]

At the same time, friendly forces are highly dependent upon timely and accurate information conveyed through a resilient command and control (C2) system. Successful C2

---

[17]JCS MOP 30, 5.

[18]For detailed discussion of the history and philosophy of maneuver warfare see William S. Lind, Maneuver Warfare Handbook (Boulder: Westview Press, 1985).

depends upon a rapid flow of accurate information through the arrangement of various components such as personnel, equipment, communications, computers, facilities, and procedures. Protection of friendly C2 capabilities is equally important in C2W. Since command and control of forces is critical to providing the operational and tactical advantage needed by both sides for success in battle, then the objective of a C2W campaign is to deny the enemy the use of his C2 that support his forces while protecting the C2 systems that support friendly forces. This is the essence of C2W. This is the broad objective of a C2W campaign.[19]

What to target, what to protect, when to fire, where to engage, and how best to execute C2W operations are questions with answers that are scenario-dependent. C2W offers an option which may be able to reduce or eliminate threats before the commitment of force. However, insights to generalized answers may be obtained by applying the other principles of war to the C2W campaign, keeping the objective in the forefront.

• *Principle of the Offensive.* Since the days of sail--racing an opponent for the upwind advantage to take the initiative--offensive action has allowed military forces to set the terms and select the place of confrontation, exploit

---

[19]Joint Chiefs of Staff, Joint Doctrine for Command and Control Warfare (C2W) (2nd Draft) (JCS Pub 3-13) (Washington, D.C.: Government Printing Office, 1994), I-5. (hereafter cited as JCS Pub 3-13)

vulnerabilities and seize opportunities from unexpected developments. Taking the offensive through initiative is a philosophy that is used to employ available forces intelligently to deny an enemy his freedom of action.

The offensive in C2W is characterized by timely operations which deny the enemy the use of C2 in support of the battlefield. The offensive spirit must be aimed to defeat or disrupt the enemy's center of gravity, the source of strength and balance, for C2 support for the battlefield. If the enemy's center of gravity for surveillance and targeting, for example, is a satellite system, then the focus of offensive operations should be the surveillance satellites. If the satellites are impotent without the use of their ground station, then the center of gravity, the "hub of all power and movement on which everything depends,"[20] may be the ground station. In addition to attacking the enemy's center of gravity, offensive operations must be aimed at attacking the enemy's weaknesses.[21]

Different adversaries require differing command and control schemes. Despotic regimes are characterized by centralized leadership; hierarchical command and control structures; and control of the press and information infrastructure. In the face of new technologies, these

---

[20]Clausewitz, On War, 595-596.

[21]Department of Defense, Department of the Navy, Naval Warfare (NDP 1) (Washington, D.C.: Government Printing Office, 1994), 35.

features--however modern and redundant--are vulnerable.[22]

The timing and tempo of offensive actions in C2W can spell success or failure on the battlefield. C2W operations must be timed to best support the combined operations of the land, sea, and air campaign. The essence of tempo is to maintain a sequence of actions at such a pace that the enemy soon becomes incapable of effective reaction. What is the best sequence of actions at such a pace that the enemy soon becomes incapable of effective reaction? What is the best sequence of actions for C2W? Understanding the enemies capabilities and possible intentions will help direct the focus of effort most efficiently with reduced assets. Future battles will be fast paced due to rapid decision cycles, quick response and highly mobile forces. The C2W commander must control the timing and tempo by acting quickly on the offensive. Sun Tzu says, "Attack where they are unprepared; go forth where they will not expect it"[23]

• *Principle of Mass.* The application of the principle of mass to C2W centers around determining the decisive place and time at which to concentrate this combat power. Is there, in general, a decisive place and decisive time in C2W?

Commanders designate a point of main effort and focus

---

[22]Department of Defense, Department of the Navy, Warfighting (FMFM 1) (Washington, D.C.: Government Printing Office, 1989), 31.

[23]Sun Tzu, The Art of War, 168; FMFM-1, Warfighting and FM 100-5 Operations, discuss the concepts of timing and tempo in some detail.

resources to support it. They are ready to shift it rapidly without losing synchronization of effects as the attack unfolds. C2W supports this concept but its success depends on the ability to mass effects without massing large formations or concentrations of platforms and personnel.[24]

Perhaps more important than concentrating firepower at a decisive place, C2W concepts should be more concerned with concentrating firepower at a decisive time. That is, rather than focus on operations designed to neutralize the enemy's C2 capability at a particular place, C2W operations should be designed to focus on neutralizing all (most) of the enemy's capabilities in the minimum time at the optimum hour of the campaign or prior to actual hostilities. Neutralizing the enemy's C2 capability can include denying, deceiving, disrupting, destroying or exploiting this capability while protecting our own capability.[25]

Suggesting concentration in time is not to say there are no decisive places in C2W. Recalling that the overall objective, the central aim of C2W, is to separate the enemy leadership from his forces. It stands to reason that decisive C2W operations are those that have maximum effect on the battle. Whether this leadership is at the operational or tactical level, separating him from his forces depends on the

---

[24]Joint Chiefs of Staff, Joint Warfare of the U.S. Armed Forces discusses main effort; FM 100-5, Operations discusses the concept of synchronization.

[25]JCS MOP 30, 4.

primary focus of effort defined by the commanders intent. Concentration requires careful, prior coordination with other services and multi-national forces.

• *Principle of Economy of Force.* This principle is to employ all combat power available in the most effective way possible, allocating minimum essential combat power to secondary efforts. What are the secondary effort in C2W? If primary efforts are to exploit or deceive the enemy's information systems, then secondary efforts might be the systematic attrition of his C2 capability by denying or destroying those capabilities not immediately supporting the battlefield.

More importantly, the most effective use of C2W could be prior to actual hostilities. C2W offers the commander the potential to deliver a "technical knock-out" before the outbreak of traditional hostilities. Clearly, the enemy's capabilities need to be understood as completely as possible. Integrated intelligence and counterintelligence support is absolutely critical to C2W. This support requires the fusion of all-source intelligence and is fully dependent upon interagency cooperation.[26]

• *Principle of Maneuver.* The application of maneuver to C2W operations is more than just position relative to our adversary. It is the exploiting of our superior agility in the synergistic application of all five elements of C2W:

---

[26]Ibid., 7.

operational security, psychological operations, military deception, electronic warfare and destruction. It is our ability to effectively apply all of these elements across the spectrum of our adversary's C2, either independently or in coordinated application of many of these elements at once, while preserving our own capability to operate unhindered.

Keys to successful maneuver in C2W are the command, control, communications, computers and intelligence (C4I) connectivity and the common tactical picture which are absolutely essential to the success of C2W in providing as complete a picture as possible to the decision-maker. C4I connectivity is more than a minor supporting actor. It is the means to the end of command and control. It provides for the delegation of forces, information management and intelligence dissemination.

Just as C4I connectivity is essential to C2W, the common tactical picture for all forces provides the reference for maneuver operations. The common tactical picture also includes the tactical management of all technical surveillance as a force system across the entire multi-dimensional battle space, including all sensors, regardless of location (whether national, theater, or platform) or ownership (whether component, joint, or combined.)[27]

• *Principle of Unity of Command.* Whether in a combat direction center or in an amphibious landing, unity in forces

---

[27]Ibid., 8.

is achieved by assigning a single commander. After he expresses his intent and provides an overall focus, he permits subordinate commanders to make timely, critical decisions and focus their strengths in support of a unified objective. The result is success, compounded by unity in purpose, unit cohesion, and flexibility in responding to the uncertainties of combat. For C2W, forces are organized and manned to provide unity of command through a C2W Commander who is responsible for the application of the various tools of C2W as an integrated function. The C2W Commander provides the single focus of effort for C2W.[28]

• *Principle of Security.* C2W contains the elements of operations security, military deception and psychological operations which are primarily concerned with the achievement of security. These element must be executed with close coordination. The first line of defense is to minimize detection and targeting by the enemy. If the enemy can not see you, the enemy can not attack. Security is enhanced by concealment. C2W provides concealment of force maneuver and intentions through deception, disruption, exploitation or destroying the enemy's information infrastructure.

The second line of defense in C2W is to apply C2-protection. One element of C2-protection is to eliminate single critical nodes and "cheap shot" opportunities. C2 systems must be robust, not thin. They must have the ability

---

[28]For a discussion of the organization of the Joint Force Commander for conducting C2W see JCS Pub 3-13.

to take hits and degrade gracefully over time, not allowing a rapid catastrophic loss of the capability they provide. And, although the fog of war will always be present, it is important in C2W to eliminate the ambiguity associated with uncertain knowledge as to whether a C2 system has been attacked or is malfunctioning due to other causes. The enemy can acquire an unexpected advantage if the enemy is unwittingly presented the opportunity for cheap shots.

Another aspect of C2-protection is to provide active and passive survivability. Electronic attack as well Electronic Support and Electronic Protect must be integral to our C2 systems and platforms. C2-protection can also be achieved offensively as well as defensively.

• *Principle of Surprise.* Surprise lies at the root of all successful combat operations and C2W is no exception. Furthermore, the principle of surprise can be applied effectively to defensive as well as offensive operations.

Clausewitz writes that the two factors that produce surprise are secrecy and speed. The need for secrecy in C2W operation plans, C2 vulnerabilities, defensive countermeasures and special capabilities is the same, or greater, than other military operations. Successful application of the principle of surprise is contingent on successful application of secrecy so as not to allow the enemy an advantage in the attack. Surprise is achieved by the direction, timing, boldness, and

force of the C2W attack.[29]

Speed comes from preparation before the battle and from decisive action during the battle. The C2W commander can disrupt the enemy's plans through rapid execution of initiatives. Such initiatives could be attacking advanced communications grids driving the adversary into using more easily exploitable C2 systems or integrating psychological operations, military deception, and operations security to deceive the adversary into a false perception of friendly intentions. And, of course, the quicker C2W can be executed, the greater will be the shock effect to the enemy.

• *Principle of Simplicity.* The broad objectives of the C2W campaign are simple and clear: Separate the enemy leadership from his forces and control his use of the electromagnetic spectrum while protecting our own C2 capability. Both offensive and defensive operations described previously comprise the C2W campaign. In C2W, as in all forms of warfare, the application of simplicity requires that plans conceived by geniuses must be executable by personnel who are not.

The plan must provide coordination among all C2W operations, and the targeting for primary and secondary objectives must be straightforward to reduce confusion. This is not to imply that C2W will be straight forward and easily managed. C2W plans, like all military plans, must incorporate

---

[29]Clausewitz, On War, 624.

enough tolerance to absorb the inevitable fog and friction of war.

Simplicity also applies to the ease with which the objective can be accomplished. For example, attacking choke points in the enemy's homeland, such as vital C2 nodes, may be easier than destroying all of the individual C2 sites. The concerns over conflict escalation, however, would have to be weighed by the national decision makers.

Command and control for C2W operations must also be simple and have the necessary redundant systems. It must include the planning tools, the C4I connectivity, the surveillance control and ability to provide the common tactical picture to all forces involved in C2W.

The Relationship Between IW and C2W

From the definitions of C2W and the descriptions of IW that have been identified, it is possible to develop a relational model of information warfare and command and control warfare based on the levels of conflict, a specific target set and a domain of activity.

Strategic Level of Conflict

Conflict can be defined simply as the clash of ideas. This clash of ideas can take place during normal peacetime competition between nations or during war. The strategic level of conflict is that level at which a nation or group of nations determines national or alliance security objectives

and develops and uses national resources to accomplish those objectives. Activities at this level establish national and alliance military objectives, sequence initiatives, define limits and assess risks for the use of military and other instruments of power, develop global or theater plans to achieve those objectives, and provide armed forces and other capabilities in accordance with the strategic plan.[30]

From this definition it is possible to derive a group of targets, or a target set, which are appropriate at the strategic level of conflict. This target set consists of the following types of targets:

- National Economic Infrastructure--such targets as a country's banking and financial systems, stock market information system or national telephone system, public transportation system or air traffic system, or trading system. All of these targets are dependent on information and computerized systems and require national resources to be successful.

- National Military Organization/C4I--such targets as strategic military communications systems and command and control links connecting the top level of civilian and military leadership, national intelligence and reconnaissance links. These targets are also highly dependent on computer systems and provide information for national level decision making.

---

[30]This definition of the strategic level of conflict is adapted from JCS Pub 1-02, 363.

This level of conflict is normally conducted in the global domain.[31]

Operational Level of Conflict

The operational level of conflict is that level at which campaigns and major operations are planned, conducted, and sustained to accomplish strategic objectives within theaters or areas of operations. Activities at this level link tactics and strategy by establishing objectives, sequencing events to achieve the operational objectives, initiating actions, and applying resources to bring about and sustain these events. These activities imply a broader dimension of time or space than do tactics. They ensure the logistic and administrative support of tactical forces, and provide the means by which tactical successes are exploited to achieve strategic objectives.[32]

From this definition it is possible to define a target set that is appropriate at the operational level. This target set consists of mainly military target but can also consist of limited national targets such as:

- Theater Military Infrastructure--such targets as specific area of operation military command and control links to the national civilian authority, power grids that provide power to both military and civil area operations, civil police and national guard troop communications.

---

[31]ISC, "Information Based Operations."

[32]JCS Pub 1-02, 275.

• Operational Military Commanders/C4I--such targets as command and control links for area commanders to their forces or civil police communications and information systems.

This level of conflict is usually conducted in a specific theater or area of operations.[33]

Tactical Level of Conflict

The tactical level of conflict is that level at which battles and engagements are planned and executed to accomplish military objectives assigned to tactical units or task forces. Activities at this level focus on the ordered arrangement and maneuver of combat elements in relation to each other and to the enemy to achieve combat objectives. The tactical level is related almost entirely to military action on the battlefield.[34]

The target set that defines this level includes:

• Tactical Military Commanders--such targets as command and control links between tactical commanders or logistic and administrative communications among units.

• Units C4I--such targets as individual radio communications and data links between units and command and control links between tactical commanders and their forces.

The domain for this level of conflict is the local

---

[33]ISC, "Information Based Operations."

[34]JCS Pub 1-02, 376.

battlefield or battlespace.[35] Table 2 presents a tabular display of this environment.

Based on this environment and the definition of C2W and the descriptions of IW, figure 3 depicts a relationship between IW and C2W. In this depiction, C2W is a subset of IW and operates at the tactical and operational levels of conflict while IW operates across the entire spectrum from tactical to strategic and from the local battlespace to the global domain. Taken together, IW/C2W can be further defined in terms of the dimensions of policy and legal constraints.

Table 2

IW/C2W Conflict Environment

LEVEL OF CONFLICT	**DOMAIN**	**TARGET SET**
STRATEGIC	GLOBAL	- NATIONAL ECONOMIC INFRASTRUCTURE - NATIONAL MILITARY ORGANIZATION/C4I
OPERATIONAL	THEATER	- THEATER MILITARY INFRASTRUCTURE - OPERATIONAL MILITARY COMMANDERS/C4I
TACTICAL	BATTLESPACE	- TACTICAL MILITARY COMMANDERS - UNITS C4I

Source: Integrated Systems Control, Inc., "Information Based Warfare," Virginia Beach, 1994. (Mimeographed.)

[35]ISC, "Information Based Operations."

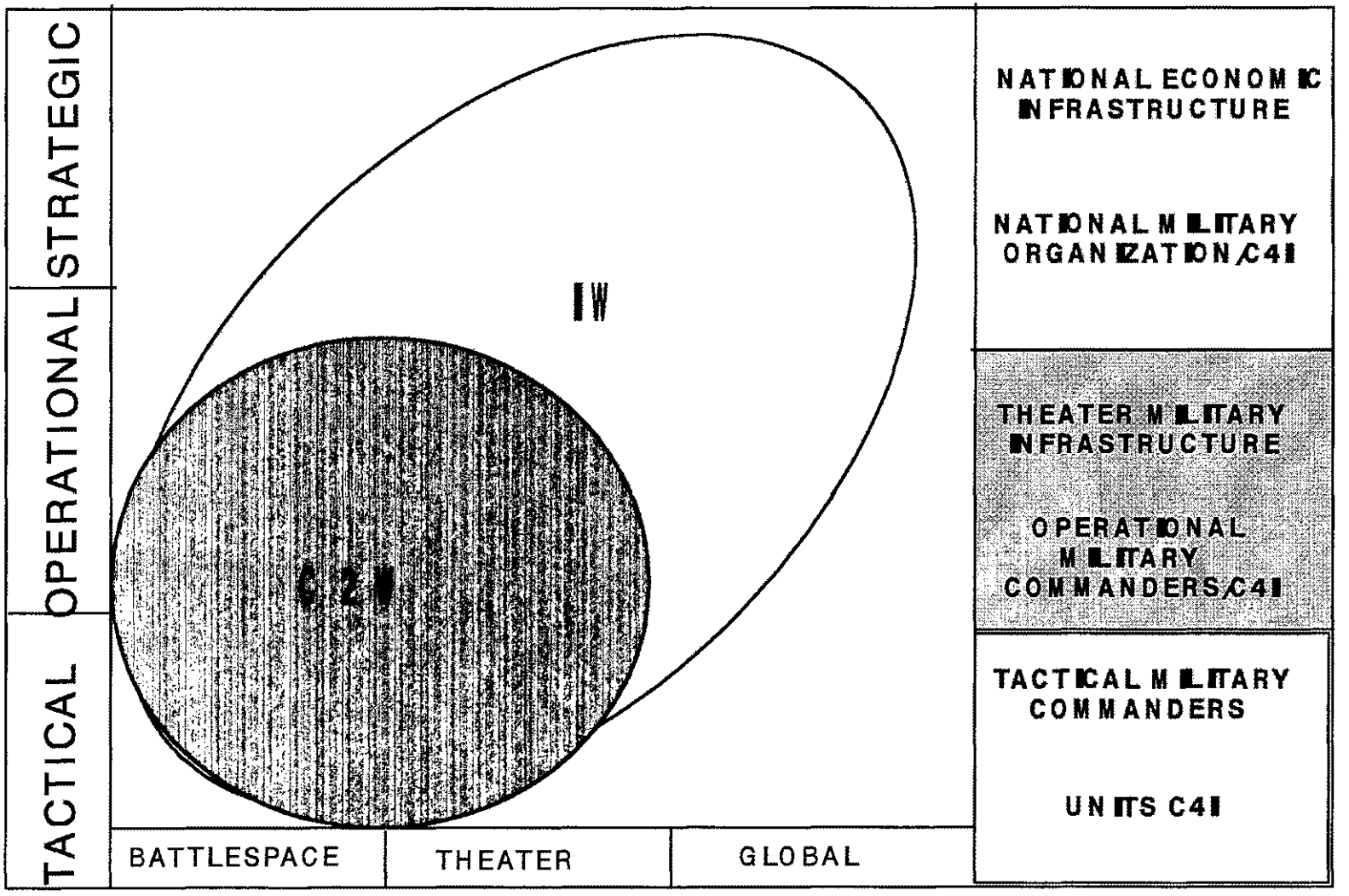

Figure 3: The Relationship of IW to C2W

Source: Integrated Systems Control, Inc, "Information Based Operations," Virginia Beach, 1994. (Mimeographed.)

Dimensions of Policy and Legal Constraints

Unfortunately, a national policy on information warfare strategy has been slow in coming. Many of the political issues associated with IW have crippled an ambitious effort by the Pentagon to win White House approval for a national information warfare strategy, designed to protect military, federal and commercial information systems from attacks during a war or crisis. A draft Presidential Review Decision Directive titled "Policy on IW for Presidential Decision Directive" has not won final approval within the Pentagon, delaying its formal review by White House Officials. The information warfare strategy raises many difficult technical, legal and even constitutional problems.[36]

Summary

The relationship between information warfare and command and control warfare has more than minor importance. We have seen that IW has application at the strategic level of conflict and use in all phases of conflict from peace time competition to war. On the other hand, C2W has been defined as the application of information warfare in military operations. It is a joint warfighting strategy that integrates the concepts of operations security, deception, psychological operations, electronic warfare and the traditional combat role of physical destruction against C2

---

[36]Neil Munro, "White House Security Panels Raise Hackles," Washington Technology, 23 February 1995, 8.

targets. C2W's objectives are achieved by influencing, degrading, denying or destroying an adversary's command and control capabilities. An equally important element of the concept is its defensive nature--the protection of command and control capabilities using operational security, deception operations and protection measures built into information systems.[37]

C2W is defined in both policy and in evolving military doctrine. C2W can also be firmly anchored as a warfighting discipline within the framework of the principles of war as they are currently defined. When analyzed with respect to a simple model of command and control, the power and effectiveness of C2W is apparent. By slowing an adversary's decision cycle and exploiting the information advantage of one's own decision cycle, a style of warfare which is unique from attrition and maneuver warfare can be envisioned.

---

[37]JCS MOP 30 and JCS Pub 3-13 discuss C2W and define it as "a military strategy for implementing IW on the battlefield." The final Draft of JCS Pub 3-13 (scheduled for publication in summer, 1995) modifies this definition slightly to be "an application of IW in military operations."

CHAPTER VII

FINDINGS AND INTERPRETATIONS

One of the central points of this paper is that fundamental change is taking place in the role of information in conflict. The information advantage and its ability to reduce the uncertainty in warfare will play an ever important role. This is being manifest in the way information is gathered, processed, displayed, transferred, and stored, as well as in the way military organizations are changing to take advantage of increased information. The explosion in information technology is truly an enabling factor in the emergence of IW as a new warfare area. Although it has the potential to revolutionize the way warfare is conducted, the elements of IW have been practiced for thousands of years. These elements are reflected in the writings of various commentators on military strategy from Sun Tzu, to von Clausewitz and Jomini, to the modern writing of de Landa and Brodie. IW itself appears to be a natural and expected evolution in warfare. Before settling on the conclusions from this inquiry, several of the more important findings are worth summarizing.

First, there is no doubt that warfare has been completely permeated by technology. It seems that warfare throughout the ages has been a continuous attempt by one side or the other to develop, steal, adapt, or conceal technology. Second, technological superiority and excellence are short-

lived. Technology tends to proliferate in spite of the best efforts of those who wish to control it. Third, technology in itself is rarely the determining factor in military success. Such elements as superior organization, training, doctrine, and even the political process often overcome superior technology. Last, the current revolution in military affairs, with which IW is so closely aligned, may not be so revolutionary. The explosion in information technology that is enabling IW could simply be the evolutionary development of technology applied to military operations. Taken to extreme, it could be suggested that the RMA has run its course and is over. It is over because of information technology's limited effectiveness against the prevailing world threat of regional thugs, religious terrorists, and militarist drug cartels.

This inquiry suggests that the nature of conflict, over the next ten to fifteen years, is fundamentally changing. The U.S. military possesses a lead in adapting information technology to warfare that far outdistances any rival. However, the absence of a peer competitor does not mean that this lead can be sustained indefinitely. Just as the technology inherent in the bronze cannon and the cross bow proliferated to every country that wanted the weapons, so also will information technology and the means to conduct IW proliferate to any country that desires to pursue them. With this proliferation will come the type of universal warfare envisioned by the RMA--information dominance, precision

targeting and weaponry, and total battlefield visibility. This model of conflict will be far more selective, if not less violent, in inflicting damage. It can be likened to the difference between a saber duel and a rugby match.

It will also bring with it a blurring of what we have known as the traditional battlefield. The new infosphere battlefield will no longer be defined by conventional military forces, their weapons, and command infrastructure, but by the information used by these forces. This information can be centrally located or, more likely, widely distributed. The battlefield will no longer be bounded by national or geographic boundaries, nor will it be bounded by the separation of tactical, operational, or strategic targets. With the intermingling of military, governmental, economic, and financial computers and communications, purely military targets on the information battlefield will no longer exist.

This model of the future information battlefield works well for a peer competitor or other high-tech country or non-state actor. However, it fits poorly for a less technically developed opponent who relies on low-tech weaponry and communications. Nevertheless, the advantages of information technology and IW can be successfully adapted to match low-tech opponents. The preparatory phases of conflict become especially important. This is the phase that begins months and even years prior to conflict. Here the development of data related to the cultural, economic, financial, and

governing environment must be pursued so that appropriate IW targets can be developed well in advance. When the time comes, the appropriate groups can then be targeted with the most effective IW weapons such as perception management and psychological operations. Whether the target group is the general population, the social elites, or the ruling class, the application of information technology and IW to these targets represents another dimension of the infosphere battlefield.

The implications of this changing nature of conflict are not inconsequential. One of the more important is that heightened expectations for the role of technology will continue to grow. The world environment is finding regional conflict, ethnic violence, and peacemaking the norm for requiring intervention by conventional military forces. This environment presents a tremendous advantage to military forces such as those of the U.S. whose information edge is so advanced. Yet, this information advantage is unproven against an opponent whose political objectives may be ethnic purity and who lacks a clear military objective. The challenge will be to develop the technology, along with the organization, training, and doctrine for information warfare that can be applied against the range of threats to our national interests.

BIBLIOGRAPHY

BOOKS

Aitken, Hugh G.J. The Continuous Wave. Princeton: Princeton University Press, 1985.

Allard, C. Kenneth, LTCOL, USA. Command, Control, and the Common Defense. New Haven: Yale University Press, 1990.

Anderson, R.C. Oared Fighting Ships, From Classical Times to the Coming of Steam. London: P. Marshall, 1962.

Anson, Sir Peter, and Dennis Cummings. "The First Space War: The Contribution of Satellites to the Gulf War." In The First Information War, ed. Alan D. Campen, 121-134. Fairfax: Armed Forces Communications and Electronics Association International Press, 1992.

Barnouw, Erick. A Tower in Babel: A History of Broadcasting in the United States. New York: Oxford University Press, 1966.

Beach, Edward L. The United States Navy. New York: Henry Holt and Company, 1986.

Brock, P. W. Steam and Sail: In Britain and North America. Princeton: Pyne Press, 1973.

Brodie, Bernard. War and Politics. New York: Macmillan Publishing Co., 1973.

Brodie, Bernard, and Fawn Brodie. From Cross-Bow to H-Bomb. Bloomington: Indiana University Press, 1973.

Burin, James M. "The Electronic Sanctuary." In The First Information War, ed. Alan D. Campen, 47-50. Fairfax: Armed Forces Communications and Electronics Association International Press, 1992.

Caesar, Julius. The Conquest of Gaul. Translated by S. A. Handford. New York: Penguin Books, 1982.

Campen, Alan D, "Iraqi Command and Control: The Information Differential." In The First Information War. Fairfax: Armed Forces Communications and Electronics Association International Press, 1992.

_____, ed. The First Information War. Fairfax: Armed Forces Communications and Electronics Association International Press, 1992.

Carl, Marion E. Pushing the Envelope. Annapolis: Naval Institute Press, 1994.

Chacko, George K. Technology Management: Applications to Corporate Markets and Military Missions. New York: Praeger, 1989.

Coakley, Thomas P., Command and Control for War and Peace, Washington, D.C.: National Defense University Press, 1992.

Cowburn, Philip. The Warship in History. New York: The Macmillan Co., 1967.

Delanda, Manuel. War in the Age of Intelligent Machines. New York: Zone Books, 1991.

Donnasch, Daniel O., Sydney S. Sherby, and Thomas F. Connally. Airplane Aerodynamics. New York: Pitman Publishing, 1967.

Dougherty, James E., and Robert L. Pfaltzgraff. Contending Theories of International Relations. New York: Harper and Row, 1981.

Fasching, Darrell J. Ethical Challenge of Auschwitz and Hiroshima: Apocalypse or Utopia? Albany: State University of New York Press, 1993.

Fee, John J. "The Declining Years." In Naval Engineering and American Seapower, ed. Randolf W. King, 142-168. Baltimore: Nautical and Aviation Publishing Company of America, n.d.

Foertel, Herbert N. Secret Science: Federal Control of American Science and Technology. Westport: Praeger, 1993.

Ford, Daniel. Flying Tigers: Claire Chennault and the American Volunteer Group. Washington, D.C.: Smithsonian Institution Press, 1991.

Friel, Ian. The Good Ship. Baltimore: Johns Hopkins University Press, 1995.

Fuller, J. F. C., Alexander the Great. New Brunswick: Rutgers University Press, 1960.

Garden, Timothy. The Technology Trap: Science and the Military. Washington: Brassey's Defense Publishers, 1989.

Gilbert, Felix. "Machiavelli: The Renaissance of the Art of

War." In Makers of Modern Strategy, ed. Peter Paret, 3-25. Princeton: Princeton University Press, 1986.

Guilmartin, John F. Gunpowder and Galleys: Changing Technology and Mediterranean Warfare at Sea in the Sixteenth Centruy. London: Compridge University Press, 1974.

Hart, Gary and William S. Lind. America Can Win: The Case for Military Reform. Bethesda: Alder and Alder, 1986.

Holborn, Hajo. "Molke and Schlieffen: The Prussian-German School." In Makers of Modern Strategy, ed. Peter Paret, 172-205. Princeton: Princeton University Press, 1986.

Howarth, Stephen. To Shining Sea. New York: Random House, 1991.

Hutchinson, Gillian. Medieval Ships and Shipping. Rutherford: Fairleigh Dickinson University Press, 1994.

Janus, Irving L. Groupthink. Dallas: Houghton Mifflin Co., 1982.

Johnson, Hubert C. Breakthrough!: Tactics, Technology, and the Search for Victory on the Western Front in World War I. Novato: Presidio Press, 1994.

Johnson, Stuart E. and Martin C. Libicki, ed. Dominant Battlespace Knowledge. Washington, D.C.: National Defense University Press, 1995.

Landstrom, Bjorn. Sailing Ships. Garden City, NY: Doubleday and Co., 1969.

_____. The Ship. Garden City, NY: Doubleday and Co., 1961.

Libicki, Martin C. What is Information Warfare? Washington, D.C.: National Defense University Press, 1996.

Liddell Hart, B. H. Strategy. 2nd ed. London: Faber & Faber; Signet Books, 1974.

Lind, William S. Maneuver Warfare Handbook. Boulder: Westview Press, 1985.

Macksey, Kenneth. Technology in War. New York: Prentice Hall Press, 1986.

Masy, Ed, and Kaldor Asbjrn. The World Military Order: The

Impact of Military Technology on the Third World. New York: MacMillan, 1979.

Moodie, Michael. The Dreadful Fury: Advanced Military Technology and the Atlantic Alliance. New York: Praeger Press, 1989.

Morison, Elting E. Men, Machines and Modern Times. Cambridge, MA: The MIT Press, 1966.

Naisbitt, John. Global Paradox. New York: Willian Morrow and Company, Inc., 1994.

Naisbitt, John, and Patricia Aburdene. Megatrends 2000. New York: William Morrow and Company, Inc.,1990.

Olson, William C., David S. McLellan, and Fred A. Sondermann. The Theory and Practice of International Relations. New Jersey: Prentice-Hall, Inc., 1983.

O'Neill, Robert, ed. New Technology and Western Security Policy. Hamden: Archon Books, 1985.

Perkins, Courtland D. and Robert D. Hogue. Airplane Performance, Stability, and Control. New York: John Wiley and Sons, 1967.

Pfaltzgraff, Robert, ed. Emerging Doctrines and Technology. Lexington: Lexington Books, 1988.

Potter, E.B. Nimitz. Annapolis: Naval Institute Press, 1979.

Price, Alfred. The History of U.S. Electronic Warfare, Vol.1, Westford: The Association of Old Crows, 1984.

Reich, Robert B. The Work of Nations, New York: Knopf, 1991.

Reit, Seymour. Masquerade--The Amazing Camouflage Deceptions of World War II, New York: Hawthorn Books, Inc., 1978.

Rosen, Steven J., and Walter S. Jones. The Logic of International Relations, Cambridge: Winthrop Publishers, Inc., 1977.

Rothfels, H. "Clausewitz." In Makers of Modern Strategy, ed. Peter Paret, 93-116. Princeton: Princeton University Press, 1986.

Schwartau, Winn. Information Warfare--Chaos on the Electronic Superhighway. New York: Thunder's Mouth

Press, 1994.

Slatalla, Michelle, and Joshua Quittner. Masters of Deception. New York: HarperCollins, 1995.

Smith, Merritt Roe, ed. Military Enterprise and Technological Change. Cambridge: MIT Press, 1985.

Snyder, Frank M. Command and Control: The Literature and Commentaries. Washington, D.C.: National Defense University Press, 1993.

Stoll, Clifford. The Cuckoo's Egg. New York: Doubleday, 1989.

Sun Tzu. The Art of War. Translated by Ralph D. Sawyer. Boulder: Weatview Press, 1994.

Thucydides. History of the Peloponnesian War. Translated by Rex Warner. New York: Penguin Books, 1972.

Toffler, Alvin, and Heidi Toffler. War and Anti-War. Boston: Little, Brown and Company, 1993.

van Creveld, Martin L. Command in War. Cambridge: Harvard University Press, 1985.

_____. Nuclear Proliferation and the Future of Conflict. New York: Free Press, 1993.

_____. Technology and War. New York: Free Press, 1991.

_____. The Transformation of War, New York: The Free Press, 1991.

Vernon, Raymond. Sovereignty at Bay. New York: Basic Books, 1971.

von Clausewitz, Carl, On War. Edited and translated by Michael Howard and Peter Paret. Princeton: Princeton University Press, 1976.

Watson, G. R. The Roman Soldier. Ithaca: Cornell University Press, 1969.

Webster, Graham. The Roman Imperial Army. New York: Funk and Wagnalls, 1969.

Weigley, Russell F. The American Way of War. Bloomington: Indiana University Press, 1977.

Wren, Daniel A. The Evolution of Management Thought. New York: Roland Press, 1972.

Wriston, Walter B. The Twilight of Sovereignty. New York: Scribner and Sons, 1992.

REPORTS

Batzler, J. R., RADM, USN (Ret) and Frederici, Gary A., Science and Technology Initiatives: Information Warfare, Alexandria: The Center for Naval Analysis (CAB 93-29, Feb 1994-Annotated Briefing), 1994.

Boyd, John R., COL, USAF, (Ret). "An Organic Design for Command and Control," 1984, (Mimeographed.)

Builder, Carl H., The Focus of Air Power in the Nineties--On Broken Dreams or Neglected Nightmares?, Santa Monica: Rand, 1994.

Caldarella, R.J., CAPT, USN, "Information Warfare: The Navy Response," Presentation to the Technical Marketing Society of America, Information Warfare Conference, Washington, DC, 8 December 1994.

Command, Control, and Communications Coutermeasures (C3CM) During Desert Shield/Desert Storm(U), By W. J. Barlow, Project Leader, Alexandria, VA: Institute for Defense Analyses, June 1992.

Cooper, Jeffrey R., "Spectrum Plan--Towards a New Strategic Vision for Future Naval Forces," SRS Technologies, Briefing, October 1993.

Department of Defense. Conduct of the Persian Gulf War. Washington, D.C.: U.S. Government Printing Office, 1992.

_____. Department of the Army, Force XXI Operations (TRADOC Pam 525-5). Washington, D.C.: Government Printing Office, 1994.

_____. Marine Corps Order 3430.5A Policy for Command and Control Warfare (C2W). Washington, D.C.: Government Printing Office 1994.

Ellickson, Bryan, Gauging the Information Revolution (N-3351-SF), Santa Monica: The RAND Corporation, [1988].

Final Report of the Center for Strategic and International Studies Group on the Military Technical Revolution, By Michael J. Mazarr, Project Director, Washington, D.C.: Center for Strategic and International Studies, 1993.

Frederici, G. A., Information Warfare: Issues, (CNA 94-1074/8)

Alexandria: The Center for Naval Analysis, 1994.

Frederici, Gary A. and Straus, Leon S., Information Warfare-A White Paper(CNA 93-020). Alexandria: The Center for Naval Analysis, 1993.

Information War in the 1990s and Beyond, By Dr. Thomas P. Rona, Project Director, Washington, D.C.: Directorate of Net Assessment Office of the Secretary of Defense, 1991.

Integrated Systems Control, Inc., "Information Based Operations," Virginia Beach, 1994. (Mimeographed.)

Joint Chiefs of Staff, Memorandum of Policy No. 30 (MOP30), Command and Control Warfare, Washington, D.C.: Government Printing Office, 1993.

Joint Chiefs of Staff, Joint Doctrine for Command and Control Warfare (C2W) Operations (2nd Draft)(JCS Pub 3-13), Washington, D.C.: Government Printing Office, 1994.

Kahan, James P., Worley, D. Robert, and Stasz, Cathleen, Understanding Commanders' Information Needs (R-3761-A), Santa Monica: The RAND Corporation, [1989].

Libicki, Dr. Martin, "Future Technology and National Security," Technology for Economic and National Security (TENS) Conference Vol II, National Defense University, Fort Leslie J. McNair, 14-15 September 1993, A3-18.

Naval Communications Architecture, Task Group 2, Navy Space Panel, Naval Studies Board, Commission on Physical Sciences, Mathematics, and Applications, National Research Council. Washingon, D.C.: National Academy Press, 1994.

Netravali, Dr. Aren, "Technology, Computing and Telecommunications." Technology for Economic and National Security (TENS) Conference Vol II, National Defense University, Fort Leslie J. McNair, 14-15 September 1993, I39-54.

Parker, Daniel M., Captain, U. S. Navy, "Space and Electronic Warfare Technology and Telecommunications." Technology for Economic and National Security (TENS) Conference Vol II, National Defense University, Fort Leslie J. McNair, 14-15 September 1993, I17-38.

Rona, Thomas, P., "Information Warfare--Presentation to the Information Resources Management College Seminar,

Introdution to Information-Based Warfare," Washington, 11 April 1994. (Mimeographed.)

Ryan, Julie, Frederici, Gary and Thorley, Tom, Information Support to Military Operations in the Year 2000 and Beyond: Security Implications (CIM 324/Nov 93), Alexandria: The Center for Naval Analysis, 1993.

Smith, Douglas V., Military Deception and Operational Art (Strategic Research Department Research Report 8-93), Newport: U.S. Naval War College, 1993.

Wald, Bruce, Information Warfare Catalog--A White Paper (CNA 93-0203), Alexandria: The Center for Naval Analysis, 1993.

Whitney-Smith, Elin, "Analysis for Information Revolutions: Dynamic Analogy Analysis," Proceeding, Second Open Source Solutions Symposium, (2-4 November 1993).

Zuriff, Laurence, Department of Defense(DOD) intern, to A.W. Marshal, DOD Director of Net Assessment, "Information Warfare", Washington, DC, 13 April 1993.

ARTICLES

Ackerman, Robert K. "Military Planners Gird for Information Revolution." Signal, May 1995, 71-76.

Arquilla, John. "The Strategic Implications of Information Dominance." Strategic Review, Summer 1994, 24-30.

Arquilla, John, and Ronfeldt, David. "Cyberwar is Coming!" Comparative Strategy 12 (1993): 141-165.

Bodnar, Captain John W. "The Military Technical Revolution-From Hardware to Information." Naval War College Review, Winter 1993, 7-21.

Bracken, Paul. "The Military After Next." The Washington Quarterly 16 (Autumn 1993): 27-35.

Brewin, Bob. "Info Warfare Goes On Attack." Federal Computer Week, 23 October 1995, 1.

Brown, David. "Managing Data, to Win the Information War." Aviation Week and Space Technology, January 1996, s-6.

Builder, Carl H. "Looking in All the Wrong Places?" Armed Forces Journal International (May 1995): 38-39.

_____. "Is It a Transition or a Revolution?" Futures,

March 1993, 153-164.

Busey, James B., ADM, USN (Ret.). "Information Advantage Offsets Declining U.S. Force Structure." Signal, August 1994, 15-16.

Campen, Colonel Alan D., USAF (Ret). "Rush to Information-Based Warfare Gambles With National Security." Signal, July 1995, 67-68.

_____. "Vulnerability of Info Systems Demands Immediate Action." National Defense, November 1995, 26-27.

Cebrowski, Arthur K., VADM, USN. "Address Before Tidewater Mini-Symposium on Naval Aviation." Naval Engineers Journal (November 1994): 17-20.

Cetron, Marvin. "An American Renaissance in the Year 2000." The Futurist, March-April 1994, 27-38.

Clapper, James R., LTGEN, USAF, and Trevino, Eben H., LTC, USAF. "Critical Security Dominates Information Warfare Moves." Signal, March 1995, 71-72.

Cohen, Eliot A. "A Revolution in Warfare." Foreign Affairs 75, (March/April 1996): 37-54.

Cooper, Pat. "U.S. Wrestles with Info Warfare Enigma." Defense News, 4-10 September 1995, 4.

_____. "Information Warfare Sparks Security Affairs Revolution." Defense News, 12-18 June 1995, 1.

Cooper, Pat and Robert Holzer. "America Lacks Reaction Plan for Info War." Defense Weekly, 2-8 October 1995, 3.

Cooper, Pat and Frank Oliveri. "Air Force Carves Operational Edge In Info Warfare." Defense News, 21-27 August 1995, 1.

Cronin, Patrick M. "Clausewitz Condensed." Military Review, August 1985, 40-49.

Echevarria, Antulio J. and John M. Shaw. "The New Military Revolution: Post-Industrial Change." Parameters 22 (Winter 1992): 17-28.

Fitzsimonds, James R. and Jan M. van Tol. "Revolutions in Military Affairs." Joint Force Quarterly 4 (Spring 1994): 32-41

Fogleman, General Ronald R., Chief of Staff. "Fundamentals of Information Warfare--An Airman's View." Speech

presented to the National Security Industry Association--National Defense University Foundation Conference on The Global Information Explosion, Washington, D.C., 16 May 1995.

Garfinkel, Simon L. "The Manchurian Printer." The Boston Globe, 5 March 1995, sec. F, 83.

Gompert, David C. "Keeping Information Warfare in Perspective." Rand Research Review (Fall 1995): 5.

Handel, Michael I. "Sun Tzu and Clausewitz: The Art of War and On War Compared." Professional Readings in Military Strategy, No. 2, 1991, 38-59.

Hardy, Stephen M. "Should We Fear the Byte Bomb?" Journal of Electronic Defense 19 (January 1996): 39-43.

"Information Warfare: A Two-Edged Sword." RAND Research Review (Fall 1995): 4-5.

MacGregor, Douglas A. "Future Battle: The Merging Levels of War." Parameters 22 (Winter 1992): 33-47.

McAuliffe, Amy. "Information Warfare: Technology and Beyond." Military and Aerospace Electronics, December 1995, 6-9.

Morton, Oliver. "The Software Revolution, A Survey of Defence Technology." The Economist, 10 June 1995, 5-20.

"Multi-Spectral Imagery Space Resources." Space Tracks, September-October 1994, 4-5.

Munro, Neil. "White House Security Panels Raise Hackles." Washington Technology, 23 February 1995, 6-8.

_____. "Information Security Gets a Boost." Washington Technology, 9 March 1995, 40-43.

_____. "Pentagon Developing Cyberspace Weapons." Washington Technology, 22 June 1995, 1.

_____. "Information Warfare Policies Emerge." Washington Technology, 27 July 1995, 27.

"New Squadron Will Build USAF's IW Capability." Jane's Defence Weekly, 30 September 1995, 6.

Nye, Joseph and William Owens. "America's Information Edge." Foreign Affairs 75 (March/April 1996): 20-36.

Offley, Ed. "Computer-age Army--High-tech gear opens up

information suerhighway." Seattle Post-Intelligencer, 1 April 1994, 1.

Owens, William A. "System of Systems." Armed Forces Journal International (January 1996): 47.

Palmer, Michael A. "Lord Nelson: Master of Command." Naval War College Review (Winter 1988): 105-116.

Rohde, William E. "What is Info Warfare?" Proceedings, February 1996, 34-38.

Ross, Bruce A., Lieutenant Commander. "The Case for Targeting Leadership in War," Naval War College Review, Summer 1993, 73-93.

Ryan, Donald E., Jr. "Implications of Information-Based Warfare." Joint Forces Quarterly (Autumn/Winter, 1994-95): 114-116.

Sikorovsky, Elizabeth. "Report: Security Policy Inadequate." Federal Computer Week, 28 August 1995, 8.

Slipchenko, Vladimir I. "A Russian Analysis of Warfare Leading to the Sixth Generation." Field Artillery (October 1993): 18-23.

Sussman, Vic. "Policing Cyberspace." U.S. News and World Report, 23 January 1995, 55-60

Thompson, Mark. "If War Comes Home." Time, 21 August 1995, 44-45.

Waller, Douglas. "Onward Cyber Soldiers." Time, 21 August 1995. 38-46.

VITA

Daniel Matthew Parker
5329 Bagpipers Lane
Virginia Beach, Virginia 23464

Mr. Parker was reared in Savannah, Georgia, and attended Savannah High School. He graduated from the Georgia Institute of Technology with a Bachelor of Aerospace Engineering in 1970. Following graduation, he entered the U.S. Navy and was commissioned an Ensign in 1971. After completing flight training in Pensacola, FL, he was designated a Naval Flight Officer and flew Navy E-2 aircraft from various Navy aircraft carriers. Mr. Parker flew combat missions in Vietnam, served in several E-2 squadrons and in various staff and Pentagon positions. He commanded a Navy E-2C squadron, VAW-126, aboard USS John F. Kennedy. He retired from the Navy as a Captain in 1994 after 24 years of service. His personal decorations include the Legion of Merit, two Meritorious Service Medals, four Air Medals, and the Vietnamese Air Gallantry Cross.

Educational Background

Bachelor of Aerospace Engineering, Georgia Institute of Technology, 1970.

Master of Arts, International Studies, Old Dominion University, 1996.

Mr. Parker's articles have appeared in Proceedings and Campus Magazine; and his book reviews have appeared in Defense Review and The Virginia Pilot. He is currently employed by Integrated Systems Control, Inc. (ISC) in Virginia Beach as an analyst and engineer.