From ‘Battle’ to the ‘Battle of Ideas’:

The Meaning and Misunderstanding of Information Operations

A Monograph

by

MAJOR Christopher W Lowe

US Army

School of Advanced Military Studies

United States Army Command and General Staff College

Fort Leavenworth, Kansas

AY 2010

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	12-10-2010	SAMS MONOGRAPH JAN 2010-DEC 2010

4. TITLE AND SUBTITLE
From 'Battle' to the 'Battle of Ideas': the Meaning and Misunderstanding of Information Operations

5. FUNDING NUMBERS

6. AUTHOR(S)
Major Christopher W. Lowe, United States Army

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
School of Advanced Military Studies
250 Gibbon Avenue
Fort Leavenworth KS, 66027-2134

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT ***(Maximum 200 Words)***

There is a common view within the United States Army that Information Operations is a military doctrine designed to win a "battle of ideas" within human populations. This monograph refutes this understanding of Information Operations by tracing the doctrine's underlying design throughout its historical evolution, from its Soviet origins until present. In the late Cold War, increased reliance on both radio-electronic communications and computer automation introduced a new vulnerability: the military command and control function was itself subject to attack through the electromagnetic spectrum. The Soviet military was the first to identify the potential advantage associated with attacking an enemy's command and control function by disrupting its radio-electronic "nervous system." In 1996, the US Army published FM 100-6 *Information Operations.* At the core of this new doctrine was an old concept – the integration of military capabilities to disrupt or degrade an adversary's command and control. However, during the Bosnia and Kosovo peacekeeping operations, and in the counterinsurgencies of Iraq and Afghanistan, Army forces would look to Information Operations as a means to influence the ideas, sentiments, and attitudes of civilian populations. This monograph argues that a discrepancy now exists between Information Operations, *as designed* and Information Operations *as practiced*

14. SUBJECT TERMS	15. NUMBER OF PAGES
Information Operations, Radioelectronic Combat, Command Control Communications Countermeasures, Cybernetics, Doctrine	64
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
		(U)	

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

MAJ Christopher W. Lowe

Title of Monograph: From 'Battle' to the 'Battle of Ideas': The Meaning and Misunderstanding of Information Operations

Approved by:

_____ Matthew J. Schmidt	Monograph Director
_____ Wayne W. Grigsby, Jr., COL, IN	Director, School of Advanced Military Studies
_____ Robert F. Baumann, Ph.D.	Director, Graduate Degree Programs

Abstract

FROM “BATTLE” TO THE “BATTLE OF IDEAS”; THE MEANING AND MISUNDERSTANDING OF INFORMATION OPERATIONS by MAJOR Christopher W. Lowe, USA, 64 pages.

There is a common view within the United States Army that Information Operations is a military doctrine designed to win a “battle of ideas” within human populations. This monograph refutes this understanding of Information Operations by tracing the doctrine’s underlying design throughout its historical evolution, from its Soviet origins until present. In the late Cold War, increased reliance on both radio-electronic communications and computer automation introduced a new vulnerability: the military command and control function was itself subject to attack through the electromagnetic spectrum. The Soviet military was the first to identify the potential advantage associated with attacking an enemy’s command and control function by disrupting its radio-electronic “nervous system.” By 1974, the Soviets embraced a doctrine known as Radio-electronic Combat (REC) to realize this advantage. REC integrated a combination of disruptive and destructive means, to include signal jamming and the physical destruction of critical nodes. The ensuing disruption of radio-electronic information flows was expected to paralyze or misguide adversary military action. In1979 the American military responded to REC with a doctrine of its own, known as Command Control Communication Countermeasures (C3CM.) Comprised of physical destruction, jamming, operations security, and deception, C3CM shared the Soviet doctrine’s essentials, to include its principle elements, its emphasis on operational integration, and its intended effects on enemy command and control. In 1993, the Department of Defense recast C3CM as Command and Control Warfare (C2W), adding psychological operations (PSYOP), an additional capability that proved useful in breaking enemy information flows during the preceding Gulf War. The information revolution and consequent Revolution in Military Affairs (RMA) debate of the 1990s led to further rebranding of the C2W doctrine. In 1996, the US Army published FM 100-6 *Information Operations.* At the core of this new doctrine was an old concept – the integration of military capabilities to disrupt or degrade an adversary’s command and control. However, during the Bosnia and Kosovo peacekeeping operations, and in the counterinsurgencies of Iraq and Afghanistan, Army forces would look to Information Operations as a means to influence the ideas, sentiments, and attitudes of civilian populations. This monograph argues that a discrepancy now exists between Information Operations, *as designed* and Information Operations *as practiced*.

Table of Contents

Introduction

The term Information Operations entered the United States Army's doctrinal lexicon in 1996, with the publication of Field Manual 100-6, *Information Operations*. Since then, Army leaders, military theorists, and others have made competing claims as to the meaning and contribution of Information Operations. Throughout its history, authors have alternatively characterized Information Operations as a combat multiplier, [1]a decisive means to prevent or win wars, a form of statecraft,[2] a non-lethal targeting methodology,[3] or the military use of information technologies.

The most recent and widely accepted claim is that Information Operations is the primary tool to shape the perceptions of civilian populations and win a proverbial 'battle of ideas'.[4] Proponents of this view expect that Information Operations lead to the framing of local

[1] See Robert J. Bunker, "Information Operations and the Conduct of Land Warfare,"*Military Review* LXVIII (September-November 1998). http://cgsc.cdmhost.com/cgi-bin/showfile.exe?CISOROOT=/p124201coll1&CISOPTR=424&filename=425.pdf (accessed April 21, 2010)

[2] For a view of information operations as "an instrument of statecraft" and tool for deterrence, see Roger W. Barnett, "Information Operations, Deterrence, and the Use of Force," *Naval War College Review* (Spring 1998) http://www.au.af.mil/au/awc/awcgate/navy/art1-sp8.htm (accessed November 10, 2010).

[3] In their article concerning tactical targeting and Information Operations, Field Artillery Observer Controllers at the Joint Readiness Center assert that "IO is really targeting with new terminology" in MAJ Matt Anderson, *et al*. "Battalion/Task Force Targeting and the Military Decision-Making Process (MDMP) in the Information Operations (IO) Environment" http://www.iwar.org.uk/iwar/resources/call/00-4ch1.htm (accessed September 14, 2010).

[4] Many view Information Operations as a means to modify the assumptions, perceptions, behaviors, attitudes, beliefs, or second nature of local civilian populations. This 'battle of ideas' view of Information Operations is prevalent within the United States Army, and is reflected in journal articles, such as LTG Thomas F. Metz, US Army and James E. Hutton, "Massing Effects in the Information Domain: A Case Study in Aggressive Information Operations," *Military Review*, 3 (Mar-April 2006) and CPT Leonardo J. Flor, US Army, "Harnessing Information Operations' Potential Energy," *Military Review* 3 (May-Jun 2010). For a similar perspective, emanating from outside of the Army, see Tim Foxley, "Countering Taliban Information Operations in Afghanistan," *Prism* 1, no. 4 (September 2010). For a broader theoretical treatment of the battle of ideas, see Antulio J. Echevarria, *Wars of Ideas and The War of Ideas*, Carlisle, PA: US Army War College, Strategic Studies Institute: 2008. http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=866 (accessed 14 Nov 2010).

interpretations, consistent with US goals and objectives. For much of the Army then, Information Superiority refers to the domination of news cycles, social narratives, and public sentiment.

However, if Information Operations is a tool to win the battle of ideas, why has the military designed Information Operations around a suite of capabilities that includes electronic warfare, operational security, and military deception? In short, does Information Operations design really reflect this purpose? This monograph argues that Information Operations' design[5] is optimal for an altogether different function: the disruption of enemy, and preservation of friendly information flows, and the subsequent establishment of a relative command and control advantage. In other words, Information Operations is designed for battle, not for the battle of ideas.

This monograph will develop this thesis by outlining the continuity of Information Operations' underlying design throughout its doctrinal evolution, from its first expression as Soviet REC doctrine, its successive American reincarnations as Command, Control, Communication Countermeasures (C3CM), Command and Control Warfare (C2W), and most recently, as Information Operations (IO). Doctrines are always artifacts of their time – to help the reader make sense of these doctrines, and to contextualize the continuity of purpose between them, this monograph selectively draws on the writings of contemporary observers, relevant official publications, and documented historical events.

Of specific interest are the historical influences that shaped doctrinal thought and development. These include the field of cybernetics; the growth of what General Westmoreland labeled the "electronic battlefield" and the military's operational dependency on radio-electronic communications; Soviet thought and US policy during the Cold War; the Gulf War and the

[5] Information Operations' design refers to the selection of elements that constitute the Information Operations core capabilities, which are also under the integrating authority of the Information Operations staff. These elements currently include electronic warfare (EW), operational security (OPSEC), military deception (MILDEC), psychological operations (PSYOP), and computer network operations (CNO.) When mutually integrated within operations, these capabilities contribute to an operational effect, which is the purpose of Information Operations.

ensuing Revolution in Military Affairs (RMA) debate; the Balkan peacekeeping operations, and the post-9/11 wars in Afghanistan and Iraq.

This monograph consists of three sections. The first section, "Military Forces as Cybernetic Systems," details the historical and military-technical conditions that led to the Soviet development of Radio-electronic Combat (REC) doctrine, which would later serve as a blueprint for US doctrines (ultimately, for Information Operations.) Specifically, this section will focus on technologically driven changes to the nature of command and control during the Cold War. As militaries grew increasingly reliant on radio-electronic devices for command and control, the electromagnetic spectrum became an important area of military contest. In essence, military forces became cybernetic systems, dependent on radio-electronic "information flows" for self-regulation. The Soviets developed Radioelectronic Combat (REC) to realize the relative information advantage stemming from the disruption of enemy radio-electronic information flows.

The second section, "The Information Battle" charts the evolution of doctrine from Soviet REC in the early 1960s, to Information Operations, in 1996. This section pays particular attention to the overwhelming design consistency between Soviet REC and subsequent US doctrines. This section thereby establishes that defense officials intended US doctrines – to include Information Operations--to essentially achieve the same ends as Soviet REC, namely, a relative advantage in the ability to collect and process information.

The third section, "The Battle of Ideas", details the Army's reinterpretation of Information Operations as means to engage in, and win, a battle of ideas. Driven by its Balkan peacekeeping experience, and enabled by the addition of Psychological Operations to Information Operations core capabilities, the Army no longer saw Information Operations as a means to consistently 'know and control more than the enemy' but as a means to shape the perceptions, change the attitudes, and alter the behavior of civilian populations.

However, despite this shifting focus, the Army did little to change the underlying design of Information Operations. In fact, in 2003, new Information Operations doctrine erased the language that might otherwise point to the design's logic and purpose. An ambiguous new doctrine in tow, the population-centric counterinsurgencies in Afghanistan and Iraq only underscored the Army's interpretation of Information Operations as a means to win the battle of ideas. Finally, a concluding section will summarize the major findings and present several areas that warrant further research.

Military Forces as Cybernetic Systems

> One thing is as certain as death and taxes – communications and electronics are here to stay.
> -General William C. Westmoreland, "The Military Uses of Communications-Electronics"

During the Cold War, both the militaries of the United States and the Soviet Union underwent a massive explosion in the employment of radio-electronic devices for the purpose of commanding forces and controlling weapon systems. While technology expanded the capacity for command and control, it also presented a new vulnerability: military forces were suddenly dependent on the electromagnetic spectrum in order to function.

Information needed to regulate military performance, such as the location of enemy targets or friendly units, now predominantly passed between human decision makers via the electromagnetic spectrum. Therefore, a significant advantage would go to the side that could dominate the use of the electromagnetic spectrum, since that side could ensure the flow of friendly information while denying or disrupting the flow of enemy information.

The Soviets were the first to organize a comprehensive approach to exploit this new condition. This section details this approach, known as Radio-electronic Combat (REC), and expounds on its logic, which is best expressed through cybernetic theories of feedback, communication and control.

Radio-Electronics and Command and Control

In the years following World War II, both the militaries of the Soviet Union and the United States grew increasingly dependent on radio-electronic devices for the purpose of command and control. Evidence of this transformation can be found in a 1969 address by General William C. Westmoreland, in which the Army Chief of Staff famously articulated a high technology, communications-dependent vision of war. According to Westmoreland, the Army in Vietnam had experienced a "quiet" though "not fully understood," "revolution in ground warfare."[6] The first and most obvious component of this revolution was the massive increase in air mobility. The second, not yet fully developed component of the revolution was what Westmoreland termed "the electronic battlefield."[7]

The development and integration of combat helicopters during the Vietnam War meant that ground units were largely freed from the "constrictions of terrain" and distance that have always challenged Armies.[8] As a result, Army forces could rapidly and unexpectedly, concentrate firepower. However, air mobility did not automatically resolve the problem of determining where Army forces should mass, because the very location and disposition of North Vietnamese Army units was often in doubt.

Searching for the enemy was a major focus of US operations. Frequently used terms such as "search and destroy," "combat sweep" and "reconnaissance in force" all point to the significant effort US forces placed on finding NVA units.[9] The task of finding enemy units diverted combat power from a finite pool of forces. Herein lay the second component of Westmoreland's revolution – a network of automated sensors could be developed that would give

---

[7] General William C. Westmoreland, *Addresses by General W. C. Westmoreland, Chief of Staff, United States Army, Volume IV, 3 July 1969 – 16 December 1969.* (Washington DC: 1973), 93.

[8] Ibid.

[9] Robert A. Doughty, *The Evolution of US Army Tactical Doctrine, 1946-197. (*Leavenworth: Combat Studies Institute, U.S. Army Command and General Staff College, 1979), 32.

the American Army the eyes it needed without the force-structure costs. According to Westmoreland:

> "On the battlefield of the future, enemy forces will be located, tracked, and targeted almost instantaneously, through the use of data links, computer assisted intelligence evaluation, and automated fire control. With first round kill probabilities approaching certainty, and with surveillance devices that can continually track the enemy, the need for large forces to fix the enemy will be less important."[10]

Indeed, by the time of Westmoreland's speech, defense engineers had already taken the first step with new surveillance devices. In 1966, Robert McNamara directed the development of a "high technology barrier system," to identify and interdict NVA movements along the Ho Chi Minh trail.[11] The project, later known as the McNamara line, employed some $670 million in unattended sensors.[12] Seismic, chemical, and electromagnetic sensors transmitted data to overflying aircraft, which in turn relayed this information to an operations center in Nakhon Phanom, Thailand. At Nakhon Phanom, raw sensor data was processed, displayed, and turned into targeting data. Nahkon then furnished this information to attack aircraft, which could engage and destroy enemy forces in the field.

Soon after its employment, US forces discovered tactical uses. In 1968, while US forces were emplacing sensors to complete the McNamara line, the NVA attacked the nearby Marine Corps firebase at Khe Sahn. Westmoreland directed that the uninstalled sensors be diverted for use at Khe Sahn.[13] The sensors ringing the firebase may have reduced US casualties at Khe Sahn

[10] Westmoreland, *Addresses*, 96.

[11] Thomas G. Mahnken, *Technology and the American Way of War*, (New York: Columbia University Press, 2008), 108.

[12] Ibid., 109.

[13] Ibid., 112.

by half, according to one officer.[14] Soon thereafter, units tactically deployed sensors along road networks and around installations.[15]

Military Assistance Command Vietnam (MACV) also relied on automation extensively for the analysis of more traditionally derived intelligence. Under Major General Joseph A. McChristian's direction the MACV intelligence staff transformed into "a computerized, automated intelligence processing organization" in which over a thousand US and Republic of Vietnam intelligence workers interrogated, exploited or analyzed enemy prisoners, weapons, documents and other materiel.[16] This "futuristic intelligence system"[17] was "the most elaborate ever organized against a US enemy."[18] According to Lloyd H. Norman, then Pentagon correspondent for Newsweek, "Data on every Viet Cong guerilla or North Vietnamese regular who falls into the clutches of combined U.S. and South Vietnamese intelligence go on an IBM card."[19]

At the same time, automated systems were showing promise for use field use. Under the auspices of the US Army Automatic Data Field Systems Command, formed in 1965, the Tactical Operations System (TOS) was developed and fielded for trial with the US Seventh Army in Germany.[20] Its developers intended that the TOS provide the "field Army commander and his staff with relevant and timely information in selected functions of intelligence, operations, and

---

[14] Ibid.

[15] Ibid.

[16] Lloyd Norman, "Westmoreland's J2," *Army 17* no. 5 (May 1967): 24.

[17] Ibid.

[18] Ibid., 23.

[19] Ibid. On page 24 of the same article Norman also related how the automated intelligence system performed: "Data are cross-indexed and filed on IBM cards or tapes. To process these data, hundreds of Vietnamese IBM operators man three shifts and keep the machines going 22 hours a day … From master tapes, J2 can search for intelligence data at the rate of 6,400 frames of film a minute. By punching a button, a desired frame can be blown up and read in either English or Vietnamese, and a copy can be made of that frame in five seconds by punching another button."

[20] R. H. Scherer, "Data Communications and Field Data Information Handling Systems," *Signal* XXIII, no. 5 (January 1969): 8. The TOS was an improved version of the Army's first tactical operations center, the ARTOC, developed in 1958. Unlike the ARTOC, the TOS was a mobile platform designed for use in the field.

fire support coordination by utilizing an on-line near real-time automatic data processing system."[21]

While the computer processing and sensor technologies that enabled MACV intelligence, the McNamara Line, tactical defensive operations such as Khe Sahn, and the TOS were, by the late 1960s only nascent, they were undoubtedly a significant step toward the "electronic battlefield" advocated by Westmoreland.[22]

However, the Army was realizing the "electronic battlefield" in other ways as well. As Martin Van Creveld relates in *Command in War,* voice communications took a qualitative and quantitative leap during the Vietnam years. By 1971, the standard Army brigade maintained 539 radio sets.[23] This figure represents an 857 percent increase in fielded radios, per brigade, since 1943.[24] In the Korean War, the division headquarters maintained eight channels, in Vietnam, thirty-two -- a three-fold increase.[25] Very High Frequency (VHF) radio sets provided reliable communications at lower tactical echelons, enabling units to operate outside of visual range in disruptive terrain.[26] Furthermore, the American Army in Vietnam, for "the first time in history" enjoyed both "voice encryption at the tactical level"[27] and a "fully automated telephone system" for intra-theater communication.[28] To support the massive communications effort, one of out every five soldiers at the division level were radio operators.[29]

---

[21] Ibid.

[22] See General William C. Westmoreland, *A Soldier Reports*, (New York: Da Capo Press, 1989),418. As Army Chief of Staff, General Westmoreland established a program at Fort Hood Texas, to further develop and exploit sensor technologies.

[23] Martin Van Creveld, *Command in War,* (Cambridge: Harvard University Press, 1985), 238.

[24] Ibid.

[25] Ibid.

[26] Ibid.

[27] General William C. Westmoreland, "The Military Uses of Communications-Electronics," *Signal (*August 1969): 73.

[28] Van Creveld, *Command in War,* 239.

[29] Ibid.

Maintenance figures further underscore how communications intensive American warfighting had grown. Signal units serviced communications devices at 150 maintenance sites in South Vietnam, where over 500,000 stockpiled communications parts were installed.[30] The criticality of voice communications to modern war was most aptly summed up by General Westmoreland himself, who noted that "on the battlefield no plan of operation is given serious consideration without assured communications. Compare this with the shooting and moving of the mob which has no communication – no control."[31]

During the same period, the Soviet military was also increasing its technological sophistication and its overall electronic dependency. Writing in 1964, Soviet Major General I. Kurnosov, chair of the communications department at the Frunze Military Academy, noted that the "role of radioelectronics cannot be overevaluated, easily here."[32] "The use of radioelectronics for controlling weapons and equipment" writes Kurnosov, "is becoming even more widespread. It is difficult to find a means of combat whose effectiveness to some degree is not dependent upon radio-electronics."[33]

As in the US Army, by the 1970s, Soviet Army forces reportedly enjoyed "reliable and really uninterrupted communication while moving in fast motor vehicles, APCs, tanks, aircraft and helicopters."[34] For the Frunze Academy Deputy Chief, Lieutenant General Vasily Gerasimovich Reznichenko, the combination of high mobility platforms and radio-electronic communications meant that battle would be "characterized by vast spatial range, high dynamism

---

[30] Ibid.

[31] Westmoreland, "The Military Uses of Communications-Electronics," 30.

[32] Ivan Kurnosov, "Development of Radioelectronic Means of Troop Control and Methods of Their Application," *Voyennaya mysl'*, No. 9, (September 1964) reprinted in *Selected Readings From Military Thought, 1963-1973*, selected and compiled by Joseph D. Douglas, Jr. and Amoretta M. Hoeber, *Studies in Communist Affairs*, Vol. 5, Part 1 (Washington, DC: U.S. Government Printing Office [GPO], 1982), 1.

[33]Ibid.

[34] A. Belov, "Signal Troops in the Soviet Armed Forces," *Soviet Military Review*, English Edition, (November 1973): 2-4.

and fluidity, quick changes from one form of combat action to another" and "intensification of critical situations."[35]

Overall, this situation posed a dilemma: information flows increased, while, at the same time, commanders enjoyed "less and less time to collect, process, and communicate it."[36] To resolve this dilemma, one option would be to decrease the span of military control, thereby increasing the number of controlling nodes on the battlefield. However, as Lieutenant-Colonel Engineer V. Kulikov noted, "this would require an enormous number of staff personnel which, in turn, would greatly complicate the management of such agencies."[37] In other words, from the Soviet perspective, attempts to put more humans in the loop would merely add more complexity.

This complexity, characterized in the Soviet literature as a problem of "troop control" was manageable only with the assistance of automated systems.[38] In 1972, V. Driuzhinin and D. Kontorov published their groundbreaking monograph *Idea, Algorithm, Decision,* providing the theoretical framework for the problems and opportunities associated with complexity, military decision-making, and troop control.[39] It is with the Soviet military's embrace of automation, the computer, that this monograph turns its attention to Cybernetics to explain the sudden emergence of information as a military resource.[40]

---

[35]V. Reznichenko "Modern Weapons and Troop Control," *Soviet Military Review*, English Edition, (December 1978): 11.

[36] Ibid., 13.

[37] V. Kulikov, review of "Idea, Algorithm, Decision" *Soviet Military Review*, English Edition, (April 1974):56.

[38]Ibid. Kulikov notes that the "only way out of this contradiction is the incorporation on a large scale of automation equipment among which electronic computers are of paramount importance." Lt Col Bokariev similarly diagnoses "the contradiction between steadily rising and dynamic activity in battle and the existing systems of controlling man and weapons." in Lt Col V. Bokariev, "Cybernetics," *Military Review XLIV* no. 11 (November 1964): 69. He states, "As the difficulties of controlling troops grow, the flow of information in military communication links continuously increases. A simple numerical increase in the number of staff officers in a headquarters cannot sufficiently improve the ability of a staff to control subordinate units. It creates only disorder and the duplication of effort."

[39] V. Kulikov, review of "Idea, Algorithm, Decision," 56.

[40] According to Slava Gerovitch, Soviet cybernetic pioneers Liapunov, Sobolev, and Kitov "chose the computer rather than the servomechanism as the archetypal cybernetic machine. They therefore

Cybernetics and Information Flows

During the Second World War a new science of "communication and control" emerged. Norbert Wiener, its American founder, coined this new science 'cybernetics.' Wiener derived the term cybernetics "from the Greek word *kubernetes*, or "steersman," the same Greek word from which we eventually derive our word governor."[41] The wartime challenge that led Wiener to problems of communication and control was the improvement of antiaircraft technology, which aviation technology had outpaced.[42]

Increasing aircraft altitude and faster performance meant that air defenders were often unable to visually acquire and engage enemy aircraft passing overhead.[43] Wiener employed the idea of the servomechanism[44], or feedback loop system, to design a machine that could "predict an airplane's trajectory by making use of information about its previous trajectories."[45] Wiener and colleagues would continue to look to the idea of the servomechanism, or feedback loop system, as a prototype for intelligent machines.[46]

---

broadened the subject of cybernetics to encompass not only feedback models but also computer algorithms." in Slava Gerovitch, *From Newspeak to Cyberspeak, (*Cambridge: The MIT Press, 2002), 178.

[41] Norbert Wiener, *The Human Use of Human Beings: Cybernetics and Society*, Da Capo Series in Science. (1954; repr., Boston: De Capo Series in Science, 1998), 1.

[42] Peter Gallison "The Ontology of the Enemy: Norbert Wiener and the Cybernetic Vision," *Critical Inquiry* 21, no.1. (Autumn, 1994): 234. http://www.jstor.org (accessed 15 September, 2010)

[43] Antoine Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*, (New York: Columbia University Press, 2009), 25.

[44] The servomechanism predates Cybernetics. The first servo-mechanism is credited to James Watt, who invented the steam engine governor in the latter half of the 18th century.

[45] Jennifer Light, *From Warfare to Welfare: Defense Intellectuals and Urban Problems in Cold War America*, (Baltimore: Johns Hopkins University Press, 2003), 37. As Peter Gallison relates, the antiaircraft predictor would ultimately add little to the war effort – simpler mechanisms proved marginally better in trials, in Gallison, "The Ontology of the Enemy," 244.

[46] Ultimately, cybernetic scientists expanded this vision, and saw the feedback loop as an explanation for the behavior of all living organisms, to include humans. As Peter Gallison notes,"Step by step, Wiener came to see the predictor as a prototype not only of the mind of an inaccessible Axis opponent, but of the Allied antiaircraft gunner as well, and then even more widely to include the vast array of human proprioceptive and electro-physiological feedback systems … Finally, the AA predictor, along with associated engineering notions of feedback systems and black boxes, became, for Wiener, the model for a cybernetic understanding of the universe itself." In Gallison, "The Ontology of the Enemy," 229.

The feedback loop is a circular cause-effect process, in which informational feedback regulates 'outputs.' A classic example of a negative (or self-regulating) feedback loop is the thermostat. The thermostat 'senses' temperature information from the environment, causing it to either raise or lower the output of hot or cool air; a new temperature reading results, causing the thermostat to adjust its output again. This process of feedback and response occurs indefinitely, so long as the thermostat continues to 'sense' its environment (in terms of temperature) and can send messages or commands to increase or decrease the flow of heat.

In Wiener's estimation, the "behavior" of the thermostat is little different from the individual human's process of *homeostasis*:

> "our bodily temperature rises or sinks one degree from its normal level of 98.6^{o} we take notice of it, and if it rises or sinks ten degrees, we are all but sure to die. The oxygen and carbon dioxide and salt in our blood, the hormones flowing through our ductless glands, are all regulated by mechanisms, which tend to resist any untoward changes in their levels. These mechanisms constitute what is known as homeostasis, and are negative feedback mechanisms of a type that we may find exemplified in mechanical automata."[47]

With colleagues Arturo Rosenblueth and Julian Bigelow, Wiener described the "behavior" of negative feedback systems, whether man or machine, as purposeful.[48] The common goal of all negative feedback systems, to include mechanical automata as well as living beings, argues the cyberneticist, is to prevent entropy. However, as the thermo-stat and *homeostasis* examples show, cybernetic systems require an uninterrupted flow of information to balance against entropy. Without continuous information flows, a cybernetic system could neither 'sense' the environment appropriately, nor could it command new behaviors.

---

[47] Wiener, *The Human Use of Human Beings*, 96.

[48] "A torpedo with a target-seeking mechanism is an example. The term servo-mechanisms has been coined precisely to designate machines with intrinsic purposeful behavior." See Arturo Rosenblueth, Norbert Wiener, and Julian Bigelow, "Behavior, Purpose and Teleology," *Philosophy of Science* 10, no. 1 (January 1943): 19. http://www.jstor.org/stable/1343893 (accessed 15 September, 2010).

Herein lay one of Cybernetics most important insights, at least at it relates to military affairs: military forces rely on negative feedback to regulate performance and to achieve their ends. In practical terms, military systems too could be treated as cybernetic systems. By the 1960s, Soviet "military specialists" would view military forces in precisely these terms. As Slava Gerovitch contends, Soviet thinkers such as Aleksei Liapunov – one of the Soviet Union's earliest and most prolific cybernetic proponents – saw "weapon systems, including both machines and the people who operate them as cybernetic systems".[49] For Liapunov, the military was analogous to an organism, the brain of which was the commander.

As Jacob Kipp relates, according to Irina Grekova, "one of the leading Soviet specialists in applied mathematics and a long-time professor at the Zhukovsky Academy" the Soviets were discussing cybernetics as early as 1952, only four years following Wiener's publication of *Cybernetics or Control and Communications in the Animal World and the Machine*. In 1953, Soviet Admiral A. I. Berg, the newly appointed Deputy Defense Minister, was given responsibility to develop "Soviet radio electronics and cybernetics." By 1958, the Soviets had translated Wiener's *Cybernetics* into Russian, and a year later, "the Frunze Academy organized a faculty of military cybernetics."[50] Throughout the late 1950s, 1960s, and into the late 1970s, Soviet military publications explored the consequences of military cybernetics relating to troop control, weapons development, modeling and simulation, decision support and operational art.

In 1964, Soviet naval Captain 1st Rank A.L. Lifshits described the "Navy as a system of subsystems"[51] and, in 1965, Iu. V. Chuev published a volume on Operations Research that stressed the importance of systems thinking and the cybernetic principle of feedback and self-regulation.[52] Similarly, in 1963 Lieutenant Colonel V. Bokariev noted the "governing" nature of

---

[49] Slava Gerovitch, *From Newspeak to Cyberspeak*, (Cambridge: The MIT Press, 2002), 265.

[50] Kipp, *From Foresight to Forecasting*,178.

[51] Ibid., 184.

[52] Ibid., 183.

information in military cybernetic systems. "As an example," writes Bokariev, "imagine … an order sent to subordinate units … If, when the information is received by the subordinate unit, it is valuable to the receiver (man, animal, or automat), then it will have an influence upon the recipient's behavior. The ability of the information to affect the condition or behavior of the receiver is called "governing."[53] As with Liapunov, Bokariev goes on to draw an analogy between this process of "governing" in military cybernetic systems and the nervous system of living organisms. "For the first time" writes Bokariev "cybernetics provides the possibility of examining thoroughly the characteristics of the nervous system of man as one link of an automated system of control."[54]

In 1966, another author, detailing the state of cybernetics in Eastern Europe, credited cybernetics as "an important factor in the Soviet "revolution in the military system.' "[55] In 1971, Major General of Artillery Ionov recommended methods to "cause the enemy to make and execute a decision that is favorable to us" and in 1973, Colonel A.F. Shramchenko advocated for the use of disinformation and the systematic electronic jamming and destruction of "troop control points" and "radio-electronic sensors." Jacob Kipp quotes Shramchenko:

> "Systematic strikes upon the troop control points besides the fact that they have an adverse effect on the will of officers also call forth an unpleasant emotional state and rob them of rest. All of this can lead to certain errors, to an overassessment of the capabilities of the other side, to mistakes in decisions and actions.[37]„[56]

The Soviet military's embrace of cybernetics was comprehensive, affecting not only weapons and computer system development, but also operational thought, especially in terms of troop control. The cybernetic influence on American military thinking was perhaps less

---

[53] Lt Col V. Bokariev, "Cybernetics," *Military Review* XLIV, no. 11 (November 1964): 68.

[54]Ibid., 69.

[55] Michael Csizmas, "Military Cybernetics in Eastern Europe," *Military Review* XLVII, no. 9 (September 1967): 22. The United States Defense establishment would similarly proclaim a Revolution in Military Affairs (RMA) in the early 1990s.

[56] Kipp, *From Foresight to Forecasting*, 211.

consciously reflected in the professional military literature, at least in terms of its implications for military theory. Nonetheless, cybernetics was informing technological development, and in this way, the discipline was bearing significantly on military officers' imagination and expectations, as General Westmoreland's desire for an automated battlefield reflects.[57]

Army Lieutenant Colonel Charles J. Davis articulated a lucid and highly developed understanding of cybernetics and its implications for military affairs in his 1963 *ARMY* article, "Command Control and Cybernetics." Davis analogizes the automated military force as man himself, and in so doing, relates the life and death importance of information flows in military operations:

> "Picture this "machine-man" on the battlefield. It senses the many events in this environment through the delicate mechanism of sound, light, electromagnetic radiation, and pressure. Myriads of sensory signals, quantitized and at various repetition rates, move down the fine network of "aherent" "nerve fibers" to reflex centers where they stimulate the first of the reflex arcs. Insufficient processing has taken place to result in intelligent instructions to the effectors of muscles of the system. So the "data" enter the central transmission system – the spinal cord and its amazing trunk of communication lines – on its way to the master processor, the brain. Here, masses of information are sorted, correlated, rejected, and arranged in an orderly array of instructions – orders, if you will – to be sent out over the efferent nerve network to the proper effector elements: hands, legs, arms, feet, eyelids, fingers – the soldiers of the battlefield. Some days the system is sick—pain within, or damage to brain or central nervous system and all response ceases. The thing must be protected – or its dies."[58]

Not only did Davis identify the military force as a cybernetic system, dependent on information flows for its very life, he situated this understanding within the context of a military contest. In so doing, Davis articulated an adaptive combat cycle sixteen years ahead of Boyd's presentation of his now famous Orient Observe Decide Act (OODA) loop. [59] As Davis expressed

---

[58] LTC Charles J. Davis, USA., "Command Control and Cybernetics," *ARMY* 13, no. 6 (January 1963): 55.

[59] According to Air Force Captain Paul E. Vanden Dries, retired Air Force Colonel John Boyd presented his "asymmetric fast transient theory," from which the OODA loop derives, at the Air Command and Staff College in 1979 in Capt Paul Vanden Dries, USAF, "C3CM-The Boyd Cycle's Throttle,"

it, "the mission is stated, an estimate of the situation is made, alternative courses of action are considered, a course of action is chosen; orders are issued; the progress of the battle is monitored; and adjustments to the orders are made as time passes."[60]

As Davis notes further, radio-electronic systems play a vital role in this adaptive cycle. "Progress is fed back through the area communications system and its complex network of transmission media and switching centers. Using the control information and *new* battlefield information, another cycle starts – and so on until time is called by defeat of the opposing force or agreement between the national powers."[61] In the 1970s, the Soviets sought to gain a decisive advantage in this interlocking contest of adaptive cycles. It would come by attacking the enemy's central nervous system, which, as David realized, was dependent on a host of radio-electronic devices, and more generally on the electromagnetic spectrum itself. The Soviet approach was termed *radioelektonnaya bor'ba,* or in English, radio-electronic combat (REC.)[62]

The Information Battle

In the years following Vietnam, the US Army returned to a 'conventional' war fighting emphasis and a re-orientation to the Soviet threat in Europe.[63] By the second half of the 1970s, US Army intelligence had uncovered the Soviet concept known as radio-electronic combat."[64] This doctrine was the impetus for later American efforts to protect its radio-electronic communications systems, thereby ensuring the flow of information necessary to command and

---

Proceedings of the 1981 Western Region Technical Symposium, (San Antonio: Western Region of the Association of the Old Crows, 1981): 7.

[60] Davis, "Command Control and Cybernetics," 53.

[61] Ibid., 54.

[62] David G. Chizum, *Soviet Radioelectronic Combat.*Westview, Special Studies in Military Affairs (Boulder: Westview Press, 1985), 3. Chizum asserts that a better translation would be radioelectronic "struggle."

[63] Robert A. Doughty, *The Evolution of US Army Tactical Doctrine, 1946-1976,* Leavenworth Papers No 1. (Fort Leavenworth, KS: Combat Studies Institute, U.S. Army Command and General Staff College, 1979), 40.

[64] Charles F. Smith, "Command, Control and Countermeasures (C3CM)," *Military Review* LXIII, no. 1 (January 1983): 68.

control forces and weapons systems. Furthermore, radio-electronic combat provided the essential blueprint, which US forces would later appropriate, with some modifications, under the name Command Control Communications Countermeasures (C3CM). C3CM would later evolve into Command and Control Warfare (C2W). C2W in turn would evolve into Information Operations. Throughout this evolution Information Operations essential design – the deliberate integration of electromagnetic capabilities with stratagem-related practices, aimed at disrupting enemy and protecting friendly information flows – remained virtually unchanged.

Radio-Electronic Combat (REC)

Beginning in the late 1960s, the Soviets started moving toward integrated approaches to "combating enemy radioelectronic equipment"[65] This occurred as the Soviets grew increasingly aware of modern Armies' radio-electronic dependence, particularly related to Command Control Communications and Intelligence (C3I), and as they monitored the successful employment of Electronic Countermeasures (ECM) against Soviet equipment in the Vietnam and 1973 Arab-Israeli wars. As US Navy CDR Floyd Kennedy argued, to the Soviets the "message was clear …EW developments were moving very fast in the West".[66]

Throughout the early 1970's analysis of Soviet military discourse suggests internal debate over REC's "proper nature".[67] It was not until 1974, however, when Soviet Major General A.I. Paliy, the "most consistent and authoritative writer on the subject,"[68] whom David

[65] David Chizum notes that this "rather wordy term" came into usage sometime after World War II in Chizum, *Soviet Radioelectronic Combat*, 20-21.

[66] Commander Floyd D. Kennedy USN Reserve, "The Evolution of Soviet Thought on "Warfare in the Fourth Dimension'," *Naval War College Review* (March-April 1982): 42.

[67] Chizum, *Soviet Radioelectronic Combat*, 24.

[68] Richard H. Phillips, "Workshop Trends in Soviet Views on Theater War," (Cambridge: MIT Center for International Studies, November 5, 1987): 2.

Chizum refers to as "the Grand old man of Soviet electronic warfare"[69] published *Radioelectronic Combat*, thereby galvanizing Soviet doctrinal consensus.[70]

According to the unclassified 1978 US Army study, Radio-electronic Combat was an "integrated system" that combined "signal intelligence, direction finding, intensive jamming, deception, and suppressive fires to attack enemy organizations and systems throughout their means of control." [71] The overall purpose of REC says the study, was "to limit, delay, or nullify the enemy's use of his command and control systems, while protecting one's own."[72]

As REC expert, David Chizum explains, "Integration stands out as" the concept's "most significant point." According to Chizum's reading of Soviet military writing, "The word integrated… has five specific meanings." Here, it is useful to quote extensively from Chizum's analysis:

> "1. It means that REC has been adopted for use by all the services of the Soviet armed forces, subject to central direction, probably by the General staff.
> 2. It portrays the combination of political ideology and military strategy into one unified concept.
> 3. It signifies that REC is an integral part of overall Soviet military doctrine.
> 4. It means that REC integrates all methods of manipulating radioelectronic emissions throughout the electromagnetic spectrum – including electro-optical and acoustic signals – into one inclusive system of military practice.
> 5. Finally, it indicates that several of the component elements of REC are employed simultaneously for maximum effectiveness." [73]

Aside from integration, the REC concept differed significantly from contemporary Western notions of EW in its emphasis on the "physical destruction of electronic targets."[74]

---

[69] Chizum, *Soviet Radioelectronic Combat,* 24.

[70] Ibid.

[71] Kennedy, "The Evolution of Soviet Thought on "Warfare in the Fourth Dimension' ", 42.

[72] The same year in which the US Army published Department of the Army, *Field Manual 100-2-1: The Soviet Army, Operations and Tactics, (*Washington DC: 16 July, 1984), 5-81. from which this quote was taken, David Chizum reports that the Soviets themselves officially added the term "disruption of command and control" to the Soviet Military Encyclopedia, which he characterizes as "the partial or complete disorganization of enemy command and control and weapons sytems…" in Chizum, *Soviet Radioelectronic Combat*, 46-47.

[73] Chizum, *Soviet Radioelectronic Combat,* 4.

Another important feature of REC was its overall relationship to operations in general. Was REC an enabling function or was it something more?[75] On this, Chizum concludes that REC was undoubtedly construed as "a form of operational, or battle, support."[76] In other words, REC has its "proper place among support measures" and can be considered in American military terms as a combat multiplier or force multiplier.[77]

The Soviets appreciated that, whatever REC's effects, they were not, in themselves decisive. However, REC offered a period of advantage in which a decisive blow was possible.[78] REC doctrine did not hold on to the illusion that this period of advantage could be sustained "for extended periods of time."[79] Therefore, the Soviets intended to employ REC during "critical times" in command and control procedures" to render important yet, "perishable information …obsolete.[80]

---

[74] Ibid., 24.

[75] This very question has divided US military thinkers concerning Information Operations from its very introduction to doctrine. For instance, consider Robert Bunker's statement, made only two years following the publication of FM 100-6 Information Operations that "One school of thought posits that they [Information Operations] represent an adjunct to current operations – the end result of which is to enhance current Army capabilities by making what it has traditionally done better by means of a force multiplier effect. Another school of thought suggests that IO will provide the Army with new capabilities. Instead of being a simple adjunct to current operations, according to this school the influence of the "information revolution" on warfare will result in the redefinition of operations themselves" in Robert J. Bunker, "Information Operations and the Conduct of Land Warfare," *Military Review* LXVIII (September-November 1998): 6. http://cgsc.cdmhost.com/cgi-bin/showfile.exe?CISOROOT=/p124201coll1&CISOPTR=424&filename=425.pdf (accessed April 21, 2010).

[76] Chizum, *Soviet Radioelectronic Combat,* 34.

[77] Ibid.

[78] This is consistent with the American doctrinal understanding that Information Operations contributes to Information Superiority, which is itself expressed in terms of an "an operational advantage" in US Joint Chiefs of Staff, Joint Publication 3-13, *Information Operations*, (Washington DC: 13 February 2006), I-1.

[79] Department of the Army, *Field Manual 100-2-1: The Soviet Army, Operations and Tactics*, 15-1.

[80] Department of the Army, *Soviet Army Operations*, (Arlington, VA: BDM Corporation and the US Army Intelligence and Threat Analysis Center, 1978), 5-81.

In total, the Soviet Army expected REC to render "at least 50 percent of the enemy's command, control, and weapon system communications" either disrupted or destroyed.[81] American analysis of REC doctrine, history, and training suggested that Soviets would concentrate lethal fires at the forward edge of the battle area (FEBA).[82] According to Soviet General-Major N.A. Kostin, "the experience of exercises and the results of scientific studies" suggested that knocking out as much as 40% of NATO command and control would require as much as much as ten percent of rockets, fifteen percent of conventional ammunition, and twenty percent of helicopter flights.[83]

By the late 1980s, the Soviet Military had invested heavily in non-lethal REC force structure. At the Front Level, for instance, EW assets alone consisted of up to twenty-five units, comprising up to 300 ground "jamming stations" and fifty jamming aircraft. In addition, as much as one third of all Soviet combat aircraft were equipped with electronic jammers. According to Kostrin, this ensemble was able "to suppress the most important [short wave] communication lines of a group of Armies…air defense systems and up to 3-4 army corps."[84]

Command Control Communications Countermeasures (C3CM)

The discovery of Soviet Radio Electronic Combat (REC) highlighted the Soviet's plan to dominate the electromagnetic spectrum and disrupt NATO command and control. Although no single element of REC, to include jamming, deception, secrecy, intelligence, or destructive fires, was missing from American capabilities or doctrine, at the time of REC's discovery, the US possessed no single approach to integrate these functions. In fact, it does not appear that the

[81] Ibid.

[82] Department of the Army, *Field Manual 100-2-1: The Soviet Army, Operations and Tactics,*15-4.

[83] N.A. Kostin *Organization and Conduct of Radioelectronic Combat in a Defensive Coalition-Based Front Operation in the Initial Period of a War*, trans. by CRH & Associates (Moscow: Union of Soviet Socialist Republics, 1989), 2.

[84] Ibid., 4.

United States military had considered the prospect of having to fight for the electromagnetic spectrum, except in the tactical sense of electronic countermeasures.

The Department of Defense would ultimately appropriate REC, with only minor changes, under the title Command Control Communication Countermeasures (C3CM). As such, C3CM was the first American instance of the deliberate operational integration of capabilities specifically designed to disrupt enemy decision-making while protecting friendly decision-making.

Between 1975 and 1978, both the Air Force and Department of Defense conducted several studies that further analyzed the implication of Soviet numerical superiority, and the newly discovered REC doctrine.[85] A 1976 Defense Science Board study demonstrated the desirability and logic of US employment of an integrated approach akin to REC, in order to disrupt Soviet command and control, and prevent Soviet attempts to do the same. As later articulated by Lieutenant Colonel Evan H. Parrot, the study determined that "If good C3 is considered a "force multiplier" for NATO … then disruption of the enemy's systems would be a "force-divider" for our adversaries."[86]

Force multiplication and division were important concepts, as they provided the logic for the then nascent "offset strategy," first formulated by Undersecretary of Defense for Research and Engineering, William Perry in 1977.[87] Soviet expenditures in military equipment had outpaced US investment by "$240 billion" in the previous decade, and the principle challenge, evident

[85] Smith, "Command, Control and Countermeasures (C3CM)," 68.

[86] Evan H. Parrot, "C3CM: Theory, Application and Process," Research Report, (Maxwell Air Force Base: Air War College, Air University, February, 1983): 15. The exact extent to which C3 variables affect total military force is inconclusive. The historian and retired Army Colonel Trevor N. Dupuy assessed that completely ineffective C3 degraded combat power by as much as half, leading at least one journalist to surmise that electronic warfare systems could potentially "double a unit's combat capability" in Deborah M. Kyle and Benjamin F. Schemmer, "C^3/EW in Europe – Can NATO Get Its Electrons Together," *Armed Forces Journal* 118, no. 1 (Sepetember 1980): 28.

[87] Lawrence Castro,"Communications for Tactical Signals Intelligence – A Weak Link in the C3I Force Multiplier?," Research Report, (National War College, National Defense University, April, 1984): 3.

since the 1973 Arab Israeli War, was how to fight outnumbered and win.[88] Perry's approach was to "counteract a numerical disadvantage in military equipment" through a technological "offset."[89] The "offset" technologies pursued by the Department of Defense under Perry's strategy included "surveillance systems", data communication systems, "positioning systems", and missile "guidance systems"[90] – all dependent, in some fashion, on the electromagnetic spectrum.

In 1978, Admiral (ret) Daniel Murphy, the Deputy Under Secretary of Defense for Policy, chaired a DOD committee appointed to further consider the DSB report.[91] A year later, Murphy's committee published DOD Directive 4600.4, which introduced an American version of the REC concept, which it termed Command, Control, Communications Countermeasures (C3CM) (see figure 1). DOD Directive 4600.4 defined C3CM as:

> "The integrated use of operations security, military deception, jamming, and physical destruction, supported by intelligence, to deny information, to influence, degrade, or destroy adversary C3 capabilities and to protect friendly C3 against such action."

A year following C3CM's unveiling in DOD Directive 4600.4, the doctrine was put to the test in a training environment, for the first time. This occurred in TEAM SPIRIT 80, a JCS directed exercise, conducted in the Republic of Korea.[92] During TEAM SPIRIT 80, joint forces implemented or, in the case of physical destruction, simulated, all of the C3CM elements. Integration occurred in a "C3CM cell," which furnished recommendations for decision to a

---

[88] United States Department of Defense, *Statement on Technology and Military Manpower*, by William J. Perry, Undersecretary of Defense for Research and Engineering Before the Subcommittee on Armed Services, United States Senate, 96th Cong., Second Sess.(Washington DC, 4 December 1980):1.

[89] Ibid., 9.

[90] Ibid., 1.

[91] Parrot, "C3CM: Theory, Application and Process," 14.

[92] Scott S. Custer, "C3CM: Putting It All Together in Team Spirit 80," Proceedings of the 1981 Western Region Technical Symposium, (San Antonio: Western Region of the Association of the Old Crows, 1981): 3.

"C3CM Director", who "had final authority to …jam, deceive, or exploit C3 targets, or to designate them for destruction."

In addition to the TEAM SPIRIT exercise, 1980 would also witness the 'standup' of the Joint Electronic Warfare Center (JEWC).[93] The JEWC had "an initial cadre of 70 personnel drawn from all four military services."[94] The JEWC was responsible for providing "electronic warfare combat analysis support to U.S. forces; assessing the capabilities and vulnerabilities of U.S. electronic warfare-C3CM equipment and employment concepts; maintaining comprehensive data to satisfy information requirements; providing special research and study support; and assisting joint operations planners in electronic warfare support."[95]

Air Force Major General Doyle Larson, the JEWC's first director, noted considerable interest in the development of C3CM. In the JEWC's inaugural year alone, his staff briefed "more than fifty general and flag officers and flag-equivalent civilians on the missions and functions of the Joint Electronic Warfare Center and its C3CM activities."[96] Nonetheless, Doyle surmised the enormous difficulty in achieving C3CMs most salient feature – the battlefield integration of its elements.[97]

---

[93] Further demonstrating the continuity between C3CM, C2W, and Information Operations, note that the JEWC "later evolved into the Joint Command and Control Warfare Center (JC2WC) and most recently the Joint Information Operations Center" in Mark H. Johnson, "Welcome to the JIOWC," *IO Sphere* (Winter, 2007): 5.

[94] COL Kenneth E. Rexrode, USA, "An Overview of the Joint Electronic Warfare Center," Proceedings of the 1981 Western Region Technical Symposium, (San Antonio: Western Region of the Association of the Old Crows, 1981): 1. Major General Larson also noted that Admiral Murphy, the lead agent in the policy establishment of C3CM, was responsible for recommending that initial cadre include "experts on lethal countermeasures" emphasizing the importance of C3CM's physical destruction component in Major General Doyle E. Larson, "C3CM: Progress and Outlook," *Defense Management Journal*, Vol 18, No.3 (3d Quarter 1982): 7.

[95] Ibid., 8.

[96] Ibid.

[97] Among Doyle's recommendations was the establishment of a single "battle manager" for C3CM in Major General Doyle E. Larson, "C3CM: Let's Get On With It!," *Journal of Electronic Defense* (January 1982): 33.

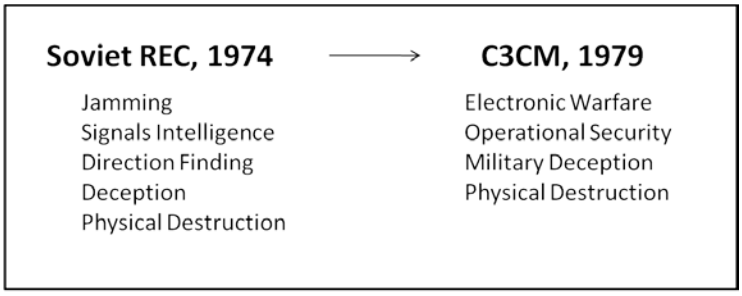

Figure 1. C3CM and the US adaptation of Soviet Radioelectronic Combat. *Sources:* left, adapted from Department of the Army, *Field Manual 100-2-1: The Soviet Army, Operations and Tactics*, (Washington DC, 16 July, 1984), 15-1.; right, adapted from Department of the Army *Field Manual 90-24: C3CM: Multi-Service Procedures for Command, Control, and Communications Countermeasures*, (Washington DC: Government Printing Office, 1991), vii.

One of the immediate challenges associated with C3CM implementation was the alignment of doctrine to ensure, in the potential of war, a unified and self-reinforcing C3CM effort across the battle space. Within the context of already ongoing AirLand Battle coordination, the Army's Training and Doctrine Command (TRADOC) and the Air Force's Tactical Air Command (TAC) sought to develop C3CM doctrine for support to the forward edge of the battle area.[98]

Together, TRADOC and TAC published TRADOC Pam 525-7 "Joint Operational Concept for Command, Control, and Communications Countermeasures (C3CM)" in December 1981. The Joint concept fixed primary joint C3CM responsibility to the Army echelon above corps (EAC), with staff responsibilities to the J3. However, the concept also recognized the requirement for Corps and Division level C3CM planning. TRADOC's Joint Operational Concept for C3CM would remain in service for a period of almost ten years, until it was superseded by the Army's Field Manual 90-24 *C3CM* in May of 1991.

[98] MAJ Roderick J. Isler, USA, "The AirLand Battle—Command, Control, Communications Countermeasures (C3CM) Integration," Student Report, (Air Command and Staff College: March, 1982): 14-15.

The Gulf War and the Revolution in Military Affairs (RMA)

In August 1990, Saddam Hussein's Iraqi Army invaded and occupied neighboring Kuwait. The ensuing Gulf War, in which an American led coalition expelled the Iraqi army from Kuwait and liberated its population, demonstrated the fruit of the US military's technological, doctrinal, and training renaissance of the previous decade. As Robert Citino asserts in *Blitzkrieg to Desert Storm: the Evolution of Operational Warfare,* Desert Storm was both "the most successful campaign in U.S. military history "and one of "the great annihilation battles of all time."[99]

Some also hailed Desert Storm as a proof of concept for a new kind of war, in which information and knowledge played the definitive, if not decisive role. As Alan Campen wrote shortly following the war, "knowledge came to rival weapons and tactics in importance, giving credence to the notion that an enemy might be brought to its knees principally through destruction and disruption of the means for command and control."[100] Indeed, the US military did a great deal to destroy Iraqi command and control during the Gulf War, "utilizing a deadly combination of hard and soft kill."[101]

The destruction or disruption of radar sites, air defense systems, command and control centers, electric power nodes, and communications relays effectively severed vital Iraqi information flows, leading many to employ the metaphors of decapitation, blindness, paralysis, and shock in describing the effects of US targeting against the Iraqi Army. For instance, during the war General Colin Powell characterized the "battle plan" as "first to destroy the Iraqis' air defense system and their command, control, and communications to render the enemy deaf,

---

[99] Robert M. Citino, *Bliztkrieg to Desert Storm: The Evolution of Operational Warfare*, (Lawrence Kansas: University Press of Kansas, 2004): 288.

[100] Alan D. Campen, Contributing Editor, *The First Information War: the Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War,* (Virginia: AFCEA Press, 1992), x.

[101] Ibid., xiv.

dumb, and blind." Powell noted in a press conference that "Our strategy is …very simple … First we are going to cut it off, and then we are going to kill it."[102] In 1993, Air Force First Lieutenant Gary Vincent similarly reflected, "The vulnerability of C2 systems to destruction by air power was demonstrated by the highly centralized Iraqi system. The mixture of Soviet and Western equipment and doctrine was blinded, then paralyzed, then largely destroyed by coalition air attack."[103]

However, it was not only US dominance of the electromagnetic spectrum, whether through physical destruction or electronic warfare, that contributed to Iraqi paralysis. Nearly some 87,000 Iraqi soldiers surrendered as US Psychological Operations forces targeted Iraqi units with leaflets, loudspeaker scripts, and radio broadcasts.[104] Widespread Iraqi surrender or desertion undoubtedly disabled Iraqi command and control (C2), as it robbed Iraqi high command of its 'eyes and ears,' contributed to poor morale, and lowered tactical responsiveness. Whether these effects are principally attributable to PSYOP or to Air Force bombing, is another question. Nonetheless, it is clear that PSYOP products provided Iraqi soldiers with the instructions on how to surrender, even if American bombing provided the motivation.

The Gulf War seemed to validate the logic of viewing military forces as cybernetic systems, dependent on information flows for command and control. As Alvin and Heidi Toffler expressed in *War and AntiWar* "The Iraqi forces, especially after most of their radar and

---

[102] Colin Powell and Joseph Perisco, *My American Journey*, Rev. Ed. (New York: Ballantine Books, 2003), 509- 510.

[103] 1LT Gary A. Vincent, USAF, "A New Approach to Command and Control: The Cybernetic Design," *Airpower Journal*, (Summer 1993): 27. Also, in 2000, Naval Post Graduate Research Associate Professor Jan S. Breemer offered a definition of what he predicted would be the future form of warfare: "Paralytic warfare is aimed at incapacitating the opponents war-making system by causing a complete or partial loss of function involving the power of motion or of sensing in any part of his system. Paralysis-based warfare is precision warfare; it relies on a combination of physical and psychological means to incapacitate critical physical and/or sensory sub-systems in order to immobilize the opponent's war-making system short of its destruction. Whereas implicit in the destruction-based model of warfare is a presumption Jar destruction, paralytic warfare is based on a presumption against destruction" in Jan S. Breemer, "War as We Knew It: The Real revolution in Military Affairs / Understanding Paralysis in Military Operations," Occassional Paper 19, (Maxwell AFB: Air University Press, December 2000): 2.

[104] Kathy J. Perry, "The Use of Psychological Operations as a Strategic Tool," Research Project, (Carlisle: US Army War College, April 2000): 7.

surveillance were excised, were a conventional "military machine"…. By contrast, the allied force was not a machine, but a system with far greater internal feedback, communication, and self-regulatory adjustment capability. It was, in fact, in part at least …a "thinking system.' "[105]

That the US led alliance achieved this relative advantage was not without significant irony. As Alan Campen noted: "It is ironic that the Soviet Union –Iraq's prime mentor—was the first to advance the belief that the balance in war might be tipped by attacking the opponent's control structure."[106] A further irony was that the Soviet Union's political control structure was itself dissolving, virtually concurrent with the American led takedown of the Iraqi command structure. These two events, the near total military success of American forces during the Gulf War and the disintegration of the Warsaw pact (and with it the Cold War) would lead to significant reevaluation of threats, opportunities, and doctrine.

Prior to the Gulf War, the Office of Net Assessment launched an assessment into the claim, long maintained by the Soviet Union, that a military-technical revolution was causing "a major shift in the character of military competitions."[107] The assessment, entitled *Military Technical Revolution: A Preliminary Assessment,* interpreted the "overwhelming U.S. victory in the Gulf War" as evidence that the revolution had in fact arrived.[108] However, the assessment also emphasized that the United States was at the "*beginning* of the revolution."[109] While the United States possessed important technologies, such as precision guided weapons and information and simulations systems, it was only able to capitalize on "a *fraction* of their combat potential."[110]

---

[105] Alvin Toffler and Heidi Toffler, *War and AntiWar: Survival at the Dawn of the 21st Century*, 1st ed. (New York: Little, Brown and Company, 1993), 80.

[106] Campen, *The First Information War,* 173.

[107] Andrew F. Krepinivich Jr., "The Military-Technical Revolution: A Preliminary Assessment," (Washington DC: Center for Strategic and Budgetary Assessments, 2002): iii.

[108] Ibid., 8

[109] Ibid.

[110] Ibid.

This was because "the United States did not come close to its potential to move the most useful information rapidly to those who needed it most."[111]

Introducing language that would later find its way to doctrine, the report asserted, "information dominance could well be the *sine qua non* for effective military operations in future conflicts"[112] and "information superiority could be *the decisive operation* in future conflicts."[113] Furthermore, the report speculated that, since belligerents also understand the decisive nature of information dominance – especially after witnessing the Gulf War -- a zero-sum-game phenomenon would likely ensue. To allow enemy exploitation of information networks during peacetime would risk enemy information dominance, "which would quickly lead to the progressive inability of friendly forces to execute the highly integrated, information-intensive military operations that will be crucial to success in war."[114] In essence, if the United States failed to maintain continuous information dominance, it would lose the deterrent and coercive power of its military force.

The report asserted that during war the United States would likely achieve information dominance through a "full-dimensional operation."[115] "Strategic strikes (to include so called "electronic strikes" and special operations forces strikes) against an adversary's terrestrial information networks would ideally be carried out simultaneously with space control operations."[116] As with Soviet REC & C3CM, dominance comes from the destruction or disruption of information networks, another way to say command and control systems.

On the heels of the Gulf War and the ONA's Military Technical Revolution report, the futurist pair, Alvin and Heidi Toffler, published *War and Anti-War; Survival at the Dawn of the*

---

[111] Ibid.

[112] Ibid., 22.

[113] Ibid., 23.

[114] Ibid., 23.

[115] Ibid., 22.

[116] Ibid.

20th Century. Preceded by the immanently popular *Third Wave*, *War and Anti-War's* essential thesis is that "the way we make wealth is the way we make war, and the way we make anti-war must reflect the way we make war."[117] According to the Toffler's, history has been characterized by "waves", in which wealth generation and war making accorded to specific forms.

The first of these waves, beginning in antiquity and largely terminating with the Industrial revolution, was agrarian. Agrarian war was seasonal, intermittent, unprofessional, and technologically unsophisticated. The Second Wave, brought on by economic industrialization, epitomized mass-production, high lethality, and mechanization. The Third Wave, only emergent at the time of *War and Anti-War*, came with the increasing use of computer technology within the society and the economy. "Knowledge" the Toffler's claimed, "… is now the central resource of destructivity, just as it is the central resource of productivity."[118]

This thesis served as a lens through which the Army would view the Military Technical Revolution proposed by the ONA's report. The Toffler's already enjoyed considerable influence within the Army. In 1982, the Toffler's established contacts with a group of influential Army officers, to include the Chief of TRADOC, Commanding General Don Starry.[119] At the time, Starry was instituting massive doctrinal and educational reforms, to include the development of AirLand Battle and the establishment of the School for Advanced Military Studies (SAMS), both of which later helped to account for the Army's success in the Gulf War. The Toffler's now saw the Gulf War as the opening campaign of the Third Wave: "Something occurred in the night skies and desert sands of the Middle East in 1991 that the world had not seen for three hundred years – the arrival of a new form of warfare that closely mirrors a new form of wealth creation"."[120]

---

[117] Alvin Toffler and Heidi Toffler, *War and AntiWar*, 3.

[118] Ibid., 71.

[119] Ian Curtis, "Misinformed About Information War? The Three-Wave Theory is Under Fire," *Defense and Foreign Affairs Strategic Policy*, (March 1996): 4.

[120] Alvin Toffler and Heidi Toffler, *War and AntiWar*, 64.

To better understand the ramifications of the Third Wave, the Army turned to the Toffler's directly, inviting Alvin Toffler to deliver a keynote address at the US Army War College's conference, "The Revolution in Military Affairs: Defining an Army for the 21st Century."[121] Furthermore, no less than the Chief of Staff of the Army, General Gordon R. Sullivan, drew on Toffler's insights in developing internal documents, such as *War in the Information Age*.[122]

War in the Information Age championed Toffler's idea that knowledge – translated by the Army as 'information'- was becoming the central resource of war. In so doing, its authors reiterated the underlying logic of General Westmoreland's "Electronic Battlefield" and William Perry's Offset Strategy – namely, that more perfect information collection and sharing, enabled by the integration of electronic technologies, would provide a marked advantage over larger Armies.[123] Ironically, far from a revolutionary program, *War in the Information Age* proposed to continue the very Cold War approach that its authors eulogized.[124]

Command and Control Warfare (C2W)

In the early 1990s, with the Defense community abuzz about MTR, RMA, the Information Revolution, or Third Wave warfare, the DOD went about revisiting its existing

---

[121] Robert J. Bunker, "The Tofflerian Paradox," *Military Review* LXVV, no. 3 (May-June 1995): 99.

[122] Ibid.

[123] For instance, notice the unmistakable symmetry between the content of General Westmoreland's electronic battlefield speech in Westmoreland, *Addresses,* 93. and the following excerpt from *War in the Information Age*: "First, an information age army will be able to locate enemy forces quickly and precisely, whether those enemies are agrarian warlords, industrial armies, or an information age peer. Second, information age armies will know where their own forces are, much more accurately than before while denying that kind of information to their foes." In GEN Gordon R. Sullivan, USA and COL James M. Dubik, USA, *War in the Information Age,* (Carlisle Barracks: Strategic Studies Institute, US Army War College, 1994), 14.

[124] For additional arguments that the RMA, contrary to its name, was in fact a continuation of the *status quo* see A. J. Bacevich, "Preserving the Well Bred Horse," *National Interest* (Fall 1994): 43-49.; Harvey M. Saplonsky, Benjamin H., Green, and Brendan Rittenhouse, editors, *US Military Innovation since the Cold War: Creation without Destruction,* (New York: Routledge, 2009). and Antoine Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity,* (New York: Columbia University Press, 2009).

C3CM policy. In December of 1992, the Department of Defense issued DOD Directive TS-3600.1 "Information Warfare." This classified directive officially defined Information Warfare for the purposes of joint and service doctrine. In 1996, Martin Hill, a worker in the Office of the Assistant Secretary of Defense for C3I (OASD/C3I) provided an unclassified rendering of Information Warfare. According to Hill, the directive essentially defined Information Warfare as "Actions to achieve information superiority by affecting adversary information, information-based processes, and information systems, while defending one's own information, information-based processes, and information systems."[125]

In response to this directive, the Chairman of the Joint Chiefs of Staff issued its first revision of Memorandum of Policy (MOP) 30 in March of 1993. The policy included three major changes. First, it directed that joint doctrine recast C3CM as Command and Control Warfare (C2W).[126] Second, it designated C2W as the "military strategy that implements Information Warfare." Third, the policy added psychological operations to the list of capabilities previously held by C3CM, bringing C2W's "principle military actions" to a total of five (see figure 2).[127] The policy defined C2W as:

> "The integrated use of Operations Security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW) and physical

[125] Stephen M Hardy, "Should We Fear the Byte Bomb?," *Journal of Electronic Defense* (January 1996): 42.

[126] MOP 30's shift to the acronym C2 (in C2W) from C3 also has its roots in the understanding that command and control depends on more than electromagnetic spectrum. For instance, in the previous year the Army dropped "communications" from C3CM and instead employed the term Command and Control Countermeasures (C2CM). As the 1993, Army Regulation 525-20 C2CM argued that "Communications are not the focus of the Army C2CM strategy whereas command and control targets are … Command and control functions are performed through an arrangement of personnel, equipment, facilities, and procedures employed … Communications are one means to maintain C2 of forces." In Department of the Army, *Army Regulation 525-20 Command and Control Countermeasures (C2CM)*, (Washington DC: 31 July, 1992).

[127] US Joint Chiefs of Staff, Memorandum of Policy #30, *Command and Control Warfare*, (17 July1990, 1st Revision, Washington DC: 8 March, 1993). http://www.dod.gov/pubs/foi/reading_room/732.pdf (accessed 22 April, 2010).

destruction, mutually supported by intelligence, to deny information to, influence, degrade or destroy adversary C2 capabilities against such actions."[128]

MOP 30 noted that Gulf War success stemmed from separating the "the enemy's command structure from its body of combat forces." That PSYOP's primary operational contribution was in breaking information flows between the head and the body, by inducing enemy soldiers' surrender, noncompliance, or hesitation, meant that it was a contributor to the decline of enemy C2. This logic appears to have been the basis for PSYOP's inclusion in the C2W list of capabilities.

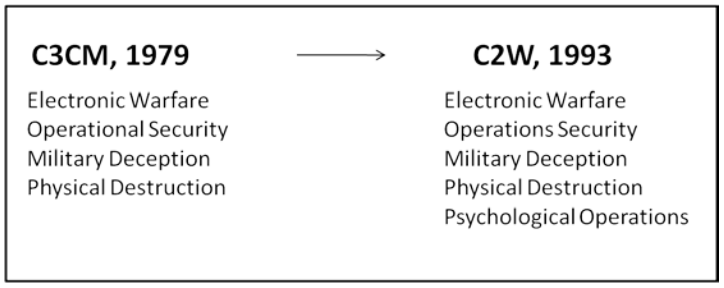

Figure 2. The addition of psychological operations and the establishment of Command and Control Warfare (C2W). *Sources*: left, adapted from Department of the Army, *Field Manual 90-24: C3CM: Multi-Service Procedures for Command, Control, and Communications Countermeasures*, (Washington DC: Government Printing Office, 1991), vii.; right, adapted from US Joint Chiefs of Staff Memorandum of Policy #30, *Command and Control Warfare*, 17 July1990, 1st Revision,(Washington DC: 8 March, 1993), 2.

Only a few months following the release of MOP 30, the National Defense University (NDU) began to develop and teach "a discipline in information-based warfare."[129] In the Spring of 1994 NDU expanded the program, officially establishing a "School of Information Warfare and Strategy."[130] Dr. Fred Giessler, NDU's Information Warfare Course Director described Information Warfare in characteristically cybernetic terms, while participating in the Naval Post

[128]Ibid., 2.

[129] LTG Paul G. Cerjan, USA and COL Robert B. Clarke, USA, "NDU Develops a Discipline in Information-Based Warfare," *ARMY* 44, no. 5, (May 1994): 19.

[130] Ibid.

Graduate School's "Information Warfare Delphi." For instance, when asked to define Information Warfare's characteristics, Giessler echoed Rosenblueth, Wiener, and Bigelow:

> "Competing and conflicting information, control and communication in complex adaptive systems – which all have teleological goals with the ultimate being survival … All systems are involved in information warfare … IW is all about decisions and the use of information, energy and material resources to offset disturbances that may drive your system away from the attainment of its objectives – especially the one about survival."[131]

In August 1995, the Army released a new *Concept for Information Operations* in TRADOC Pamphlet 525-69.[132] In keeping with the Third Wave and RMA discourse, the Information Operations Concept announced revolutionary change. In the pamphlet's forward, General William Hartzog, then TRADOC Commander proclaimed, "The information age paradigm will … change the way wars are fought."[133]

Revolutionary proclamations aside, the Information Operations concept confirmed and programmatically endorsed the logic underlying Soviet REC, C3CM, and C2W. Statements such as "…by denying the adversary's view of friendly battlespace, and exploiting the use of the spectrum, commanders can dominate the battlefield"[134] and the "future C2 system is predicated

---

[131] Roger Dean Thrasher, "Information Warfare Deplhi: Raw Results," (Monterey: Naval Postgraduate School, June 1996): 5. On page 24, when asked, "What can be considered an "information warfare system?" Giessler responded, "Any set of elements related to one another with a goal of survival in the information age. Such a system has input, process, output, and feedback. It is a complex adaptive system that is teleological – goal oriented. So—a commander and his trusted agents (sometimes known as staff) who is trying to defeat, deter, influence the competitor is a IWS [Information Warfare System]…IW Systems are everywhere."

[132] See Department of the Army, "TRADOC Pamphlet 525-69: Concept for Information Operations," (1 August, 1995). http://iwar.org.uk/iwar/resources/tradoc/p525-69.htm (accessed 17 June, 2010). The Information Operations concept defined Information Operations as "Continuous military operations within the Military Information Environment that enable, enhance, and protect the commander's decision cycle and mission execution to achieve an information advantage across the full range of military operations. IO includes interacting with the GIE and, as required, exploiting or degrading and adversary's information and decision systems"

[133] Ibid., Foreward. On page 4, after opening with a quote citation from John Arquilla and David Ronfeldt, the concept affirms, "The Information Age has irreversibly impacted the fundamental approach to warfare."

[134] Department of the Army, "Army Regulation 525-20 Command and Control Countermeasures (C2CM)," (Washington DC: 31 July, 1992): 7.

upon our exercising electromagnetic spectrum supremacy or superiority"[135] echo thirty years worth of theory, doctrine, and practice.

Furthermore, the future digitized battlefield articulated in the Information Operations concept, is strikingly similar in concept to General Westmoreland's Electronic Battlefield. [136] The TRADOC Pamphlet states:

> "Digitization will also assist in combat identification and enhance situational awareness through precise friendly and threat signature definition and updating of weapon system recognition software programs. The direct connection between the global grid of communications and the digitized battlefield will allow precision strike operations against high-value targets."[137]

The following year the Joint Chiefs of Staff published Joint Vision 2010, a "conceptual template" for the future of joint warfighting.[138] Joint Vision 2010 established four operational concepts to guide future development: "dominant maneuver; precision engagement; full dimensional protection; and focused logistics."[139] The document further recognizes that the "basis for this framework is found in the improved command, control, and intelligence which can be assured by information superiority."[140] The document defines information superiority as "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[141] Joint forces achieve information superiority through offensive and defensive Information Warfare which, according to MOP 30,

---

[135] Ibid.

[136] A year after the North Vietnamese Tet Offensive, General Westmoreland envisioned a "battlefield of the future" … in which " enemy forces will be located, tracked, and targeted almost instantaneously, through the use of data links, computer assisted intelligence evaluation, and automated fire control." in Westmoreland, *Addresses*, 96.

[137] Department of the Army, "TRADOC Pamphlet 525-69," 12.

[138] US Joint Chiefs of Staff, *Joint Vision 2010. (*Washington DC: 1996):1.

[139] Ibid., 14.

[140] Ibid., 19.

[141] Ibid.

C2W implements. In other words, the joint operational concept articulated in Joint Vision 2010 depended on effective C2W.

FM 100-6 *Information Operations*

In August 1996, a year following the introduction of TRADOC's concept, the Army published FM 100-6 *Information Operations*. In keeping with the concept, the new doctrine included Public Affairs (PA) and Civil Affairs (CA) as complementary Information Operations elements. Did this adjustment reflect a more significant departure from earlier doctrines? Most importantly, did the new doctrine have in mind a battle of ideas playing out within local civilian populations? Or were these additions aimed to better guarantee a relative command and control advantage?

As with the earlier inclusion of PSYOP within C2W, the addition of PA and CA to Information Operations seems rooted in the institutionally accepted lessons of the Gulf War. As doctrine notes, the Gulf War demonstrated the ubiquity of media on the battlefield, the explosion in telecommunications, and the consequent dissolution of informational boundaries. During the war, media coverage reached global audiences, principally via English language satellite news. This, the doctrine recognized "can dramatically affect strategic direction and the range of military operations."[142]

Spelling out a causal chain, the doctrine suggests that media coverage can profoundly influence military operational decision-making: "Soldier actions" cause a public response that drives Presidential reaction and new strategic or operational directions. FM 100-6 animates this observation with a Gulf War historical vignette, in which "In the space of 11 hours, a press conference that included unguarded opinions about the past and future course of a war profoundly

[142] Department of the Army, *Field Manual 100-6: Information Operations (*Washington DC: August, 1996), 1-3.

affected the strategic, operational, and tactical levels of that war."[143] In other words, the doctrine identified PA as necessary to safeguard friendly decision-making.

Similarly, CA was deemed important to Information Operations because "of its ability to interface with key organizations and individuals in the GIE [Global Information Environment]; for example, CA's traditional relationship with NGOs and PVOs such as the International Committee of the Red Cross."[144] Furthermore, CA's access to local and international actors, as well as with civilian populations, meant that it could serve as a valuable collector of useful information. As with PA's inclusion, CA affords the opportunity to preserve negative entropic information flows – it is both a means to communicate negative entropic information that will ultimately re-enter the military decision making system and, it is a means to gain new information about the local environment.[145]

FM 3-13 *Information Operations*

In 2003, as Army forces were engaged in Afghanistan and Iraq, the Army published an updated version of its Information Operations doctrine under the title FM 3-13 *Information Operations*.[146] The doctrinal content focused on "tactics, techniques, and procedures". As a 'how to' manual, it represented a break from the more philosophical and theoretical FM 100-6.

---

[143] Ibid., 3-16.

[144] Ibid., 3-10.

[145] While doctrinal developers may have viewed PA and CA contributions to Information Operations in terms of enabling superior command and control, they did recognize the importance of nonmilitary information systems. To be sure, the Information Operations doctrine did grasp the significance of civilian populations, an absent factor in REC, C3CM, and C2W doctrines. As such, the doctrine notes in the Operations Other than War section that "PSYOP is a vital force employed to optimize the influence of US national policy on target audiences, whether neutral, hostile, or friendly" in Department of the Army, *Field Manual 100-6*, 6-19. However, nowhere does the doctrine suggest that population influence is a primary aim of Information Operations, even if its most recently included sub-elements may have independent effects in this regard. For instance, Figure 6-2 on page 6-9 depicts an example Information Operations synchronization matrix that exemplifies the battle focus inherent in Information Operations design. In it, the "IO CENTRAL OBJECTIVE" is stated as "Influence, disrupt, or delay the adversary's military decision cycle while protecting US/coalition decision cycles."

[146] The numerical identifier '3-13,' brought the Army in compliance with the Joint doctrinal numbering system.

However, the doctrine continued the essential design of previous Information Operations, C2W, and C3CM doctrines. Nonetheless, it cloaked Information Operations design in a new language, which obscured its origins and therefore, obscured its very function. According to FM 3-13, the Army now defined Information Operations:

> "the employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to affect or defend information and information systems, and to influence decisionmaking."[147]

1996's FM 100-6 held that Information Operations comprised three activities, C2W, Public Affairs, and Civil Affairs. FM 3-13 re-grouped most of the elements historically comprising C2W under the title, "core elements." While this change effectively rendered C2W the "core" of Information Operations, in doing away with the highly descriptive term C2W, it drew attention *away* from this very purpose. Furthermore, additional capabilities were clustered under the heading "supporting elements" while public affairs and civil affairs were carried forward as "related activities" (see figure 3).[148]

[147] See Department of the Army, Field Manual 3-13 *Information Operations,(* Washington DC: November, 2003), 1-13. The reader should note that this definition is strikingly similar to the joint definition of command and control warfare carried in FM 100-6: "the integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary C2 capabilities, while protecting friendly C2 capabilities against such actions; command and control warfare applies across the operational continuum and all levels of conflict (Joint Pub 1-02)" in Department of the Army, *Field Manual 100-6,*Glossary 3.

[148] In addition, to the "core elements", the doctrine added Computer Network Operations, reflecting the importance of automation to the maintenance and processing of information flows. However, without the descriptive label C2W, the reason for computer network operations' inclusion is not entirely obvious. Furthermore, the doctrine did not carry over physical destruction as a core capability, in effect, rendering Information Operations an essentially non-lethal approach to C2W.

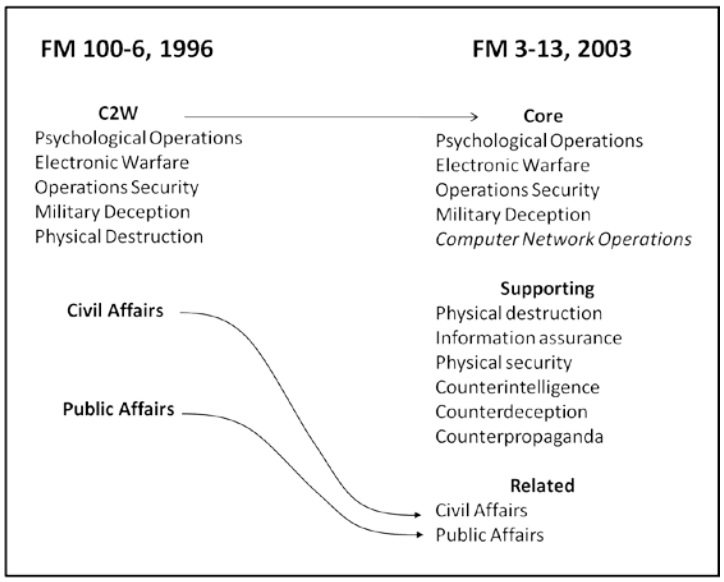

Figure 3. Information Operations, from C2W to the 'Core' elements. *Sources:* left, adapted from Department of the Army, *Field Manual 100-6: Information Operations*, (Washington DC: August, 1996), 3-0.; right, adapted from Department of the Army, *Field Manual 3-13: Information Operations*, (Washington DC: November, 2003), 1-14.

The Battle of Ideas

In the 1990s, peacekeeping operations in Bosnia and Kosovo would profoundly alter the US Army's interpretation of Information Operations. Following these operations, the Army would no longer primarily view Information Operations as a means to achieve a relative C2 advantage. Instead, the Army would view Information Operations as a means to win a battle of ideas. The Army would carry this understanding of Information Operations to the post 9/11 population-focused operations in Afghanistan and Iraq. However, even as the Army reinterpreted the role of Information Operations, it did nothing to alter Information Operations doctrinal design.

The Balkans

On 16 December 1995, NATO began *Operation Joint Endeavor* in Bosnia. The Dayton Peace Accords (DPA), which "brought about a cessation of hostilities in the Bosnian civil war,"

precipitated the operation.[149] The United Nations Security Council authorized member states, under the mantle of the North Atlantic Treaty Organization (NATO) to enforce the DPA. NATO in turn formed a coalition under the respective titles Implementation Forces (IFOR) and later, Stabilization Forces (SFOR.)

With a basic mission to implement and uphold the DPA, NATO forces did not seek to disrupt enemy information flows and C2. Rather, NATO forces primarily combined PSYOP and Public Affairs to influence media-driven social narratives. There are at least two reasons for this. First, if the Former Warring Factions (FWFs) were to comply with the peace agreement, they would require sufficient command and control to maintain the cease-fire, withdraw forces from separation zones, and turn in heavy weapons. Therefore, NATO's mission to maintain the peace depended in part on the maintenance of FWF information flows. This rendered C2W an inappropriate, if not entirely self-defeating tool.

Second, NATO forces sensed the need to reinforce the FWF commitment to the DPA from the bottom up, by directly shaping local popular perceptions. As one analyst put it, "The "battlefield" in Bosnia-Herzogovina is one of a struggle of ideas competing for legitimacy and supremacy."[150] In Bosnia, the media – rather than radio-electronic command and control systems of the Cold War—was the primary domain of military competition. As one contemporary observer related, the "media … suffused the entire Bosnian mission, provoking ambitious efforts by NATO and U.S. public affairs officers to make full use of information for peace."[151] Speaking to the military's sensitivity to media coverage, Pascale Combelles Siegel noted that "many

[149] US Army Training and Doctrine Command, Center for Army Lessons Learned, "CALL Newsletter No 99-2: Task Force Eagle Information Operations; "IO in a Peace Enforcement Environment' " (Fort Leavenworth KS: January 1999): 7.

[150] MAJ Arthur Tulak, USA, "PSYOP C2W Information Operations in Bosnia," Center for Army Lessons Learned Report, (June 1999): 1. http://www.iwar.org.uk/iwar/resources/call/ll.htm (accessed 17 June, 2010).

[151] Larry K Wentz. ed., *Lessons From Bosnia: The IFOR Experience*, (Washington, DC: Institute for National Strategic Studies, 1997), 266.

officers" serving in Bosnia "are convinced that victory is no longer determined on the ground, but in media reporting."[152]

For these reasons, NATO's 'information war' was principally a blend of psychological operations and public affairs, informally dubbed 'information activities'. Confirming this, a military analyst for the Center for Army Lessons Learned stated, "In Bosnia-Herzogivina (BiH), psychological operations (PSYOP) and public affairs (PA) have been the primary vehicles by which the informational IOP [instrument of power] has been wielded in theater."[153]

NATO forces also sought to mitigate the consequences of civil disturbance or other media spectacles that could heighten popular dissent or lead to a cycle of violence. For instance, the goal of Task Force Eagle's "Counter-Demonstration Working Group"[154] was to "beat the factions to the media with the correct information before the factions could launch a propaganda campaign of biased or erroneous reports."[155] Furthermore, Information Operations planners developed "IO messages and themes"[156] to be deployed in media engagements, face-to-face encounters, or negotiations.

Army units employed many of these same practices later during Kosovo's peacekeeping phase, and Information Operations again concerned itself with dominating the media storyline, whereby coalition forces could "maintain credibility with the populace and quickly disseminate

---

[152] Pascalle Combelles Siegel, *Target Bosnia: Integrating Information Activities in Peace Operations*, (Washington DC: DOD Command and Control Research Program, 1998), 1. http://www.dodccrp.org/files/Siegel_Target.pdf (accessed 12 NOV 2010).

[153] Tulak, "PSYOP C2W Information Operations in Bosnia," 1.

[154] CPT Fred Johnson, USA, "Synchronizing the Response to Civil Disturbances: (Task Force Eagle's Staff Coordination)," Center for Army Lessons Learned Report, (December 1996): 1 http://www.iwar.org.uk/iwar/resources/call/sec2.htm (accessed 17 June, 2010).

[155] Ibid.

[156] LTC Robert Algermissen, USA, *et al*., "Task Force Eagle Information Operations Planning," Center for Army Lessons Learned Report, (April 1999). http://www.iwar.org.uk/iwar/resources/call/ll.htm (accessed 17 June 2010).

truthful, factual information."[157] Information Operations practitioners of the time believed that "disseminating timely, truthful information to key local leaders and populace groups"[158] likely "defused several potentially volatile situations."[159]

What both the Bosnian and Kosovo missions reflect, is a turning point in the way Army officers perceived the value and contribution of Information Operations. The US-led wars following the 9/11 terrorist attacks would further entrench the view that Information Operations is a tool to win the battle of ideas. However, even as the operational Army was reinterpreting Information Operations' operational contribution, the institutional army was preserving Information Operations' essential doctrinal design.

Afghanistan and Iraq

Initial invasions of both Afghanistan and Iraq utilized Information Operations as a tool to disrupt enemy information flows. For instance, according to one Combined Forces Land Component Commander (CFLLC) Information Operations targeting officer, US forces had executed nearly 500 C2 physical destruction missions before ground units reached Baghdad.[160] As a result, Iraqi forces could neither effectively concentrate forces nor execute national command and control.

Furthermore, this activity continued, but with "lesser intensity" following the transition to "Phase IV" operations in both Afghanistan and Iraq.[161] However, as the Army's history of Operation Iraqi Freedom points out, after the phase transition "most US leaders believed" that the

---

[157] MAJ Marc J. Romanych, USA Retired and LTC Kenneth Krumm, USA, "Tactical Information Operations in Kosovo," *Military Review* LXXXIV, no. 5 (September-October 2004): 58.

[158] Ibid., 56.

[159] Ibid., 61.

[160] COL Gregory Fontenot, USA Retired, *et al*., *On Point: The United States Army in Operation Iraqi Freedom*, (Fort Leavenworth: Combat Studies Institute Press, 2004), 248.

[161] Donald Wright and LTC Timothy Reese, USA, *On Point II: Transition to a New Campaign*, Fort Leavenworth: Combat Studies Institute Press, 2008), 273.

so called "soft power" side of IO was more important than the "hard" side because it had the potential to win over the Iraqi population and the international community."[162] Army forces now perceived that they were in a "battle of ideas."[163] "If this battle of ideas was successful, commanders believed most Iraqis would willingly embrace the Coalition's efforts to provide security and remake Iraq into a unified, stable, prosperous, and free nation."[164] As *On Point II* notes, "The Army's chief means of fighting the battle of ideas was a group of related actions and processes, collectively called information operations (IO)."[165] In other words, as in the Bosnia and Kosovo peacekeeping operations, Information Operations in Iraq primarily concerned the proverbial "hearts and minds" rather than the disruption of enemy information flows, for which the doctrine was designed. This emphasis is evident from both the Operation Enduring Freedom (OEF) and Operation Iraqi Freedom (OIF) campaign plans.

According to *A Different Kind of War*, which covers OEF in Afghanistan, both Combined Forces Command Afghanistan (CFC-A) and Combined Joint Task Force-180 (CJTF-180) "maintained that information operations was at the center of the strategy to defeat the Taliban and al-Qaeda." Accordingly, for CJTF-180, Information Operations was a line of effort, describing "the Coalition's use of information to build support for the Coalition and the ATA while undermining the Taliban and al-Qaeda."[166] Likewise, in OIF, Combined Joint Task Force -7 maintained an Information Operations logical line of operation, which "drew attention to the need for Soldiers to find ways of using ideas and information to win support within the Iraqi

[162] Ibid., 274.

[163] Ibid., 273.

[164] Ibid.

[165] Ibid.

[166] Donald Wright, *et al*., *A Different Kind of War*, Fort Leavenworth: Combat Studies Institute Press, 2010), 192.

population."[167] The experience of COL Rob Nettles, an Information Operations officer with CFC-A, may serve to illustrate how these lines of effort were translated into action:

> "CFC-A maintained a six-person information operations team that coordinated the various Coalition information efforts. Lieutenant Colonel Nettles, an information operations specialist and a team leader in 2003, used a variety of methods for strategic communications. His team coordinated radio shows hosted by local commanders and established a program that handed out radios powered by an attached hand crank to Afghans. Nettles' team also launched an initiative that built bulletin boards in villages that posted messages promoting the local and national governments. [112] Nettles even convinced the commercial airline carrier, Ariana Afghan Airlines, to distribute to passengers a newspaper highlighting the economic and social accomplishments of the new Afghanistan."[168]

Writing in the Army's Military Review, Captain Leonardo J. Flor recently noted that at the tactical level "vernacular" definitions of IO embrace an Information Operations very different from that of doctrine.[169] "For tactical maneuver units executing counter-insurgency, the term *information operations* has a vernacular definition roughly equivalent to *public affairs* or *public relations*."[170] Recent military professional journal articles also testify that this vernacular understanding is by no means limited to the tactical level. For instance, in their respective Military Review articles, both Lieutenant General Metz and Colonel Rob Baker, representing both theater and tactical level perspectives, relate their experiences with IO in terms of perception management, a function more clearly described by the terms strategic communication, public relations, or influence activities.

Interviews and public statements reinforce the notion that Information Operations is primarily a means to win a battle of ideas. Brigadier General Mark T. Kimmitt, who served as

---

[167] Donald Wright and LTC Timothy Reese, USA, *On Point II*, 120.

[168] Donald Wright, *et al*., *A Different Kind of War*, 261.

[169] CPT Leonardo J. Flor, USA, "Harnessing Information Operations' Potential Energy," *Military Review* XC, no. 3 (May-Jun 2010): 59.

[170] Ibid.

"deputy director of operations and chief military spokesman in Baghdad"[171] commented during a 2006 interview that future inquiries should concern the military's use of "information as a weapon" during phase four operations in Iraq.[172] Kimmitt suggested that the interviewer inquire into "The Army's response to the hearts and minds campaign: did we get the information campaign right?"[173]

COL Ralph Baker echoed this interpretation of Information Operations as a means to win a battle of ideas. Baker explained the approach to Information Operations he adopted while serving as the commander of the 2nd Brigade, 1st Armored Division, in Baghdad of 2003-4, as follows:

> "…I learned and spent a great deal of my time on information operations. […] I ended up developing two themes that we were going to use in the use in the brigade while we were there for information purposes. One theme was to convince the Iraqis that their personal livelihood and their nation's interests were better served working with the coalition forces in the short term. The second theme was to discredit the insurgency. With those two themes, those were the focal points of the talking points that the soldiers, leaders, senior leaders in the brigade, would discuss with Iraqis, governmental officials, reporters, and so forth. So every week we developed metrics to measure that. … Any derogatory statistic that we could attribute to insurgent or terrorist actions, we tracked. Of course in terms of the other theme, which is you had to convince the Iraqis that they had both a personal and national interest in a better Iraq, we copiously tracked the number of insurgents that we were able to capture and put into prison as a result of community involvement. So I would compile that we would put these talking points out every week to all of my commanders. So we were all speaking on the same sheet of music and we weren't contradicting each other."[174]

---

[171] BG Mark T. Kimmitt, USA, interviewed by Pete Connors, 12 January 2006, transcript, Contemporary Operations Studies Team, Combat Studies Institute, Fort Leavenworth, 3. http://www.cgsc.edu/carl/contentdm/home.htm (accessed 12 NOV 2010).

[172] Ibid., 6.

[173] Ibid.

[174] COL Ralph Baker, USA, interviewed by Pete Connors, 1 November 2005, transcript, Contemporary Operations Studies Team, Combat Studies Institute, Fort Leavenworth, 17. http://www.cgsc.edu/carl/contentdm/home.htm (accessed 12 NOV 2010).

Conclusion

There is a common view within the United States Army that Information Operations is a military doctrine designed to win a battle of ideas occurring within human populations. However, an examination of Information Operations underlying structure, its properties, and its genealogy, suggests that the true object of its design is to win military battles.

In the late Cold War, increased reliance on both radio-electronic communications and computer automation for the command and control of forces and weapons introduced a new vulnerability: the military command and control function was itself subject to attack through a disruption of information flows. The multidisciplinary science known as "cybernetics" established the positive link between information flows and command and control. Cybernetics held that all self-regulating or goal-seeking systems – from the thermostat to the biological organism-- depended on an uninterrupted flow of information to adjust performance and fend off entropy. In this way, by the 1960s it was possible to view military forces as self-regulating, information dependent systems. Anthropomorphic comparisons provided the insight that the "nervous system" through which vital information flows passed was largely comprised of radio-electronic components operating within and through the electromagnetic spectrum.

The Soviet military was the first to identify the potential advantage associated with attacking an enemy's command and control function by disrupting its radio-electronic "nervous system." By 1974, the Soviets embraced a doctrine known as Radio-electronic Combat (REC) to realize this advantage. REC integrated a combination of disruptive and destructive means, to include signal jamming and the physical destruction of critical nodes. The ensuing disruption of radio-electronic information flows was expected to paralyze or misguide adversary military action. In1979 the American military responded to REC with a doctrine of its own, known as Command Control Communication Countermeasures (C3CM.) Comprised of physical

destruction, jamming, operations security, and deception, C3CM shared the Soviet doctrine's essentials, to include its principle elements, its emphasis on operational integration, and its intended effects on enemy command and control. In 1993, the Department of Defense recast C3CM as Command and Control Warfare (C2W), adding psychological operations (PSYOP), an additional capability that proved useful in breaking enemy information flows during the preceding Gulf War.

In the 1990s, the defense community hailed the integrated use of information and information technologies demonstrated in the Gulf War as evidence of an ensuing Revolution in Military Affairs (RMA). During this period, American military discourse took on a futurist orientation, spurred by expectations of a digitized battlefield, the Information Age, and the theoretical musings of Toffler's Third Wave perspective on war.

On the heels of the Gulf War and the RMA debate, a new "information" lexicon entered military use. Superior command and control was reconceived as "information dominance" or "information superiority." And the doctrine aimed at attacking enemy command and control – C2W – was re-cast in terms of Information Warfare (IW) and later, Information Operations (IO). Ultimately, with the 2003 publication of FM 3-13 *Information Operations*, the very term C2W would disappear, subsumed within the "core elements" of Information Operations. Thereby, Information Operations design shares tremendous continuity with REC, C3CM, and C2W, even as its "information age" language suggests that it is something radically new.

During the Bosnia and Kosovo peacekeeping operations, and in the counterinsurgencies of Iraq and Afghanistan, Army forces would look to Information Operations to provide an advantage in a struggle for which the doctrine was never designed, what this monograph has termed the "battle of ideas."

Information Operations application to this battle of ideas seems to stem from three convergent and self-reinforcing factors. First, imbued with the RMA "information age" lexicon (and its suggestion of revolutionary discontinuity) the underlying design of Information Operations was removed from its historical context. As a result, the logic of its design is no longer apparent from the language that describes the design. Rich terms such as C3CM or C2W, which situate the design's functionality firmly on the battlefield, and which clearly articulate the design's relationship to military command and control have not survived the RMA newspeak. Superior command and control is relabeled information superiority. The electromagnetic environment becomes the military information environment and later, simply, the information environment. C2W becomes Information Operations. Unfortunately, regardless of whatever theoretical sophistication the Information labels add, they have widened the range of interpretation beyond the design's intended functionality. Taking the terms at face value, what operations are not "information operations" and what, save perhaps the minerals of the earth, cannot be included in the "information environment?"

Second, the addition of PSYOP and PA to Information Operations has shifted perceptions of the doctrine's focus. Both PSYOP and PA have a significant and vital involvement in the realm of civilian populations, public sentiments, and the flow of ideas. It seems probable that commanders and practitioners have uncritically associated these population-focused missions with Information Operations. As in the Indian legend of the six blind men and the elephant, Army forces have tended to define Information Operations by its parts. Blindfolded by the ambiguities of Information Operations doctrine, Army forces have identified the whole of PSYOP and PA's missions – both of which are readily within the 'grasp' of tactical Army echelons – as Information Operations' real substance.

Third, ever since the Army introduced Information Operations doctrine, Army forces have been deeply engrossed in what Rupert Smith refers to as "war amongst the people."[175] The operational requirement to gain the support of civilian populations has been particularly intense in the post-9/11 environment. The counterinsurgency turn in American war fighting has placed population security at the center. At the same time, enemy forces have adopted deliberate strategies that seem to offset or mitigate the very utility of doctrines like C2W. Insurgents, terrorists, and criminal elements, operating in small, decentralized networks, below the so-called "threshold of discrimination," challenge both the practicality and the reward of breaking information flows.

This monograph has argued that a discrepancy exists between Information Operations *as practiced* and Information Operations *as designed*. However, does this discrepancy matter? Is this merely a terminological problem? Alternatively, has the field simply adapted beyond doctrinal literature? Is this situation an example of innovation, which the Army should recognize and further propagate through doctrine? In any case, is a different use of Information Operations necessarily a misuse of Information Operations?

This monograph proposes no definitive answers to these questions. Merely it has sought to identify and explain a contradiction that exists between design and practice, between intended purpose and actual application. At most, exposing this divergence might help to illuminate an area of unexamined risk, in as much as few leaders seem genuinely aware that such a contradiction exists. What does this risk likely concern?

On the one hand, it likely concerns the possibility that Army forces have unknowingly operated in the battle of ideas with inappropriate or irrelevant concepts taken from Information

[175] Rupert Smith, *The Utility of Force: The Art of War in the Modern World,* (New York: First Vintage Books, 2007), 19.

Operations. On the other hand, in focusing Information Operations toward a battle of ideas, there is the risk that Army forces have or will neglect opportunities to execute the doctrine as intended, and thereby fail to capitalize on its important effects. What follows are some final considerations related to these points.

Incomplete or Misleading Concepts in the Battle of Ideas?

In conceiving of Information Operations as a tool designed to win a the battle of ideas, have Army forces limited their conception of 'influence' to an overly narrow range of activities, for instance, those elements contained within the Information Operations design, such as PSYOP and PA? Moreover, has the Army overestimated the potential of "information" and "information flows" in winning a battle of ideas, leading it to both incorrectly appraise the costs and requirements of fighting a battle of ideas, and to undervalue the role of physical approaches?

It is certainly true that mass media and the internet are important means of popular communication and are important to the exchange of ideas. However, it is equally true that information and ideas flow through populations in many other ways. Here one may think of the inter-weave of the traditional "lines of communication" and the traditional centers of exchange. Highways, rail lines, and rivers converge on cities. Sidewalks and roads converge on markets and places of worship. Even in the so-called Information Age, humans carry information about, in taxis, horse-carts, on foot, exchanging news and speculating on the future as they always have.

Affecting a population's information flows entails more than the use of Information Operations capabilities and elements, to include PSYOP and PA. Surely, a major concern is the management of human movement and exchange. This may involve building or closing roads, securing market spaces, enforcing curfews, separating neighborhoods – and simply interacting with the population. All of these actions are done by Army forces today, under the auspices of a deliberately population focused counterinsurgency doctrine. Nonetheless, it is difficult to know

how fully leaders at every level have made the connection between human movement and the movement of ideas. Have Army forces missed important opportunities to influence the exchange of ideas, especially if, inspired by Information Operations' concern for disembodied "information flows", they have unduly focused on developing clever communications plans?

How important are disembodied "information flows", in the form of PSYOP messages or other communications in the overall battle of ideas? John Arquilla and David Ronfelt have noted the distinction between informational structure and process (flow) in their book *In Athena's Camp*. These theorists propose a "structural information" approach to complement the cybernetic-based information processing view that dominates US defense doctrines.[176] Arquilla states that "much information may just be residing somewhere, embedded, doing little or nothing in the way of processing, while doing a lot to define a particular structure, give it shape, and hold it together—be it a physical, biological , or social structure. Such information is engaged less in "processing" than in "structuring." [177]

Lewis Mumford expresses a somewhat similar idea in a different context, emphasizing both storage and transmission in *The City in History.* As Mumford observed, "From its origins onward … the city may be described as a structure specially equipped to store and transmit the goods of civilization."[178] According to Mumford, the city, "By means of its storage facilities (buildings, vaults, archives, monuments, tablets, books) … became capable of transmitting a complex culture from generation to generation, for it marshaled together not only the physical means but the human agents needed to pass on and enlarge this heritage."[179]

---

[176] John Arquilla and David Ronfeldt, ed., *In Athena's Camp: Preparing for Conflict in the Information Age,* (Santa Monica: RAND, MR-880-OSD, 1997): 443.

[177] Ibid.

[178] Lewis Mumford, *The City in History*, (New York: Harcourt, Brace & World, 1961), 30.

[179] Ibid., 569. For a thorough description of the city's information structuring function, see Steven Johnson, *Emergence; The Connected Lives of Ants, Brains, Cities, and Software*, (New York: Simon and Schuster, 2001), 101-129.

In Mumford's view of the city, embedded information acts as a kind of memory -- a rule-set governing a population's internal flow and processing of information. Political scientist Karl Deutsch echoes this idea when identifying the necessity for any "complex network" to maintain "stable operating rules" that help it "distribute its "attention" and "its priorities in expediting competing messages." In human societies, these "operating rules" manifest as "cultural or institutional preferences, obstacles, and "values." They fundamentally derive from experience, and because of this, populations are "not wholly subject to the present."[180]

Man reifies his "operating rules" or "cultural preferences", which act to prioritize and screen incoming messages, by surrounding himself with his artifacts. Does it follow that altering the arrangement of these artifacts – that is, reordering and restructuring a population's physical environment --is in fact a necessary requirement to change a population's "operating rules?"

Obviously, substantively reordering (rather than purely disordering) the physical environment almost by definition presupposes territorial control. Hence, the political scientist Stathis Kalyvas, whose claim that "control has a decisive impact on the population's collaboration with a political actor" in an irregular war, seems justified.[181] To Kalyvas, one of the benefits that accrues from control, and which leads to the population's collaboration is the opportunity to establish a "dominant cultural message."[182] "Long-lasting control spawns robust informational monopolies that socialize populations accordingly."[183] This in turn, argues Kalyvas, leads to a wider or "exclusive" "recruitment pool" which "generates cascades of support

[180] Karl W. Deutsch, "Mechanism, Teleology, and Mind," *Philosophy and Phenomenological Research* 12, no. 2 (December 1951): 210.

[181] Stathis Kalyvas, *The Logic of Violence in Civil War,* (New York: Cambridge University Press, 2006), 111.

[182] Ibid., 125.

[183] Ibid.

because the families of fighters tend to support the armed factions where their younger members are fighting."[184]

All of this suggests the relative importance of "facts on ground" rather than the psychological sleight of hand characteristic of external messaging. It suggests the essential inadequacy of any population influence scheme that is principally reliant on the communication of disembodied messages – for populations are more than equipped to ignore them, either consciously or unconsciously. It remains an open question whether the Army's expectation that Information Operations can deliver "influence" in the battle of ideas, primarily through a combination of PA and PSYOP, has or continues to lead Army forces away from this realization.

Forgetting Information Operations' True Functionality?

If a generation of officers have associated Information Operations as a tool to win a battle of ideas, it seems likely that Army forces are not disposed to employ Information Operations as designed. More troubling, one may wonder whether the operational problem for which Information Operations was developed, is today a blind spot on the consciousness of many commanders and practitioners. Is superior command and control assumed, a *fait accompli*? Who on the average General Staff today thinks it his primary responsibility to help the commander achieve a relative command and control advantage, if those doctrinally responsible are busy managing the "information campaign"?

Of course, many are prone to consider a C2 advantage a largely irrelevant concern in today's operational environment. However, if no one is exploring the issue, as Information

[184] Ibid., 125-126. The immense military requirements for controlling large population conflicts with the efficiency logic of Westmoreland's Electronic Battlefield, Perry's Offset Strategy, and the RMA. These ideas, which have greatly shaped the US military's design, force structure, and doctrine, maintain the assumption that superior information processing – what doctrine labels "information superiority"-- obviates the requirement for large standing Armies.

Operations specialists might otherwise do, there is no real way to assess the merits of disrupting adversary information flows. In any case, will future assessments be so dismissive of the need to degrade enemy command and control?

Unfortunately, the future practice of Information Operations will largely depend on the meaning that commanders and practitioners ascribe to the doctrine today. Success at Information Operations seems to demand a wealth of technical knowledge concerning command and control means and methods, leadership philosophies, and foreign doctrines. Do the officers responsible to integrate counter command and control efforts into the overall operation possess this knowledge? Will they in the future, if they do not begin to gain this knowledge in the present? Can they, if they are busy now, waging a battle of ideas?

BIBLIOGRAPHY

"Aircraft and Automation Enhance Field Army Effectiveness." *Armed Forces Management* 13, no. 10 (July 1967): 124-129.

Alberts, David S. and Hayes Richard E. *Power to the Edge: Command and Control in the Information Age*. Washington DC: DOD Command and Control Research Program, 2005. http://www.dodccrp.org/files/Alberts_Power.pdf (accessed 22 April, 2010).

Algermissen, LTC Robert M., USA, MAJ Robert Koehler, USA, MAJ Cecil Miller, USA, MAJ Arthur Tulak, USA. "Task Force Eagle Information Operations Planning." Center for Army Lessons Learned Report, (April 1999). http://www.iwar.org.uk/iwar/resources/call/ll.htm (accessed 17 June 2010).

Arnold, LTC E. R., USA. "The Increasing Importance of Military Communications." *Signal* XX, no. 10 (June 1966): 12-15.

Arquilla, John and David Ronfeldt, ed. *In Athena's Camp: Preparing for Conflict in the Information Age.* Santa Monica: RAND, MR-880-OSD, 1997.

Bacevich, A.J. "Preserving the Well Bred Horse." *National Interest* (Fall 1994): 43-49.

Barnett, Roger W. "Information Operations, Deterrence, and the Use of Force." *Naval War College Review* (Spring 1998).

Belov, A. "Signal Troops in the Soviet Armed Forces." *Soviet Military Review.* English Edition. (November 1973): 2-4.

Belov, M. "New Factors in the Development of Modern Armies." *Soviet Military Review.* English Edition. (February 1974): 10-13.

Bokariev, Lt Col V. Soviet Army. "Cybernetics." *Military Review* XLIV, no. 11 (November 1964): 66-70.

Bousquet, Antoine. *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*. New York: Columbia University Press, 2009.

Breemer, Jan S. “War as We Knew It: The Real Revolution in Military Affairs / Understanding Paralysis in Military Operations.” Occassional Paper 19. Maxwell AFB: Air University Press December, 2000.

Bunker, Robert J. “Information Operations and the Conduct of Land Warfare.” *Military Review* LXVIII (September-November 1998). http://cgsc.cdmhost.com/cgi-bin/showfile.exe?CISOROOT=/p124201coll1&CISOPTR=424&filename=425.pdf (accessed April 21, 2010).

Bunker, Robert J. “The Tofflerian Paradox.” *Military Review* LXVV, no. 3 (May-June 1995) 99-102.

Campen, Alan D. Contributing Editor. *The First Information War: the Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War.* Virginia: AFCEA Press, 1992.

Castro, Lawrence. “Communications for Tactical Signals Intelligence – A Weak Link in the C3I Force Multiplier?” Research Report, National War College, National Defense University: April, 1984.

Cerjan, LTG Paul G., USA and COL Robert B. Clarke USA. “NDU Develops a Discipline in Information-Based Warfare.” *ARMY* 44, no. 5 (May 1994): 18-19.

Chizum, David G. *Soviet Radioelectronic Combat.* Westview Special Studies in Military Affairs Boulder: Westview Press, 1985.

Citino, Robert M. *Bliztkrieg to Desert Storm: The Evolution of Operational Warfare*. Lawrence: University Press of Kansas, 2004.

Curtis, Ian. “Misinformed About Information War? The Three-Wave Theory is Under Fire.” *Defense and Foreign Affairs Strategic Policy* (March 1996): 4-5.

Custer, Scott S. “C3CM: Putting It All Together in Team Spirit 80.” Proceedings of the 1981 Western Region Technical Symposium. San Antonio: Western Region of the Association of the Old Crows, 1981, 3-5.

Csizmas, Michael. “Military Cybernetics in Eastern Europe.” *Military Review* XLVII, no. 9 (September 1967): 20-26.

Davis, LTC Charles J. USA. “Command Control and Cybernetics.” *ARMY* 13, no. 6 (January 1963): 51-55.

Department of the Army. *Soviet Army Operations.* Arlington: BDM Corporation and the US Army Intelligence and Threat Analysis Center, 1978.

Department of the Army. *Field Manual 100-2-1: The Soviet Army, Operations and Tactics.* Washington DC, 16 July, 1984.

Department of the Army. *Field Manual 100-6: Information Operations.* Washington DC: August, 1996.

Department of the Army. *Field Manual 3-13*: *Information Operations.* Washington DC: November, 2003.

Department of the Army. *Field Manual 90-24: C3CM: Multi-Service Procedures for Command, Control, and Communications Countermeasures.* Washington DC: Government Printing Office, 1991.

Department of the Army. “Army Regulation 525-20 Command and Control Countermeasures (C2CM).” Washington DC: 31 July, 1992.

Department of the Army. “TRADOC Pamphlet 525-69: Concept for Information Operations.” (1 August, 1995). http://iwar.org.uk/iwar/resources/tradoc/p525-69.htm (accessed 17 June, 2010).

Deutsch, Karl W. “Mechanism, Teleology, and Mind.” *Philosophy and Phenomenological Research* 12, No., 2 (December 1951): 185-223.

Dominique, Michael J. “Information Operations: The Military’s Role in Gaining Information Superiority.” Carlisle Barracks: United States Army War College, 2009.

Doughty, Robert A. *The Evolution of US Army Tactical Doctrine, 1946-1976.* Leavenworth Papers No 1. Fort Leavenworth: Combat Studies Institute, U.S. Army Command and General Staff College, 1979.

Druzhinin, V.V. and D. S. Kontorov. *Concept Algorithm, Decision.* Translated by the United States Airforce. Washington, DC: US Government Printing Office, 1975.

Eassa, Charles N. “US Armed Forces Information Operations – Is the Doctrine Adequate?” Monograph, School of Advanced Military Studies. Fort Leavenworth: U.S. Army Command and General Staff College, 1999.

Eassa, Charles N. “The Friction of Joint Information Operations” Monograph, School of Advanced Military Studies. Fort Leavenworth: U.S. Army Command and General Staff College, 2000.

Echevarria, Antulio J. *Wars of Ideas and The War of Ideas* Carlisle Barracks: US Army War College, Strategic Studies Institute, 2008. http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=866 (accessed 14 Nov 2010).

Fontenot, COL Gregory, USA Retired, LTC E.J. Degen, USA, and LTC David Tohn, USA. *On Point: The United States Army in Operation Iraqi Freedom*. Fort Leavenworth: Combat Studies Institute Press, 2004.

Foxley, Tim. “Countering Taliban Information Operations in Afghanistan.” *Prism* 1, no. 4 (September 2010).

Flor, CPT Leonardo J., USA. “Harnessing Information Operations’ Potential Energy” *Military Review* XC, no. 3 (May-Jun 2010): 58-64.

Gallison, Peter. “The Ontology of the Enemy: Norbert Wiener and the Cybernetic Vision.” *Critical Inquiry* 21, no.1. (Autumn 1994): 228-266. http://www.jstor.org (accessed 15 September, 2010).

“General Westmoreland Foresees New Concept of Combat: Automated Battlefield in Less Than a Decade.” *Army* (November 1969).

Gerovitch, Slava. *From Newspeak to Cyberspeak.* Cambridge: The MIT Press, 2002.

Hardy, Stephen M. “Should We Fear the Byte Bomb?” *Journal of Electronic Defense* (January 1996) 42-28.

Henry, Ryan and C. Edward Peartree. “Military Theory and Information Warfare.” *Parameters* (Autumn 1999): 121-135.

Holloway, David "Soviet Military Cybernetics: Social and Political Problems of Troop Control." *Journal of the Royal United Services Institute for Defense Studies* CXVI, no. 664 (December 1971): 59-64.

Isler, MAJ Roderick J., USA, "The AirLand Battle—Command, Control, Communications Countermeasures (C3CM) Integration" Student Report, Air Command and Staff College: March, 1982.

Johnson, CPT Fred, USA. "Synchronizing the Response to Civil Disturbances: (Task Force Eagle's Staff Coordination.)" Center for Army Lessons Learned Report, December 1996. http://www.iwar.org.uk/iwar/resources/call/sec2.htm (accessed 17 June, 2010).

Johnson, Mark H. "Welcome to the JIOWC." *IO Sphere* (Winter 2007):5-6.

Johnson, Steven. *Emergence; The Connected Lives of Ants, Brains, Cities, and Software*. New York: Simon and Schuster, 2001.

Kipp, Jacob. *From Foresight to Forecasting: The Russian and Soviet Military Experience*. College Station: Center for Strategic Technology, Texas A&M University, 1988.

Kalyvas, Stathis. *The Logic of Violence in Civil War*. New York: Cambridge University Press, 2006.

Kennedy, Commander Floyd D. Jr., USN Reserve. "The Evolution of Soviet Thought on "Warfare in the Fourth Dimension'." *Naval War College Review.* (March-April 1982): 1-2.

Kondakov, G. "Communications in Troop Control." *Soviet Military Review*. English Edition. (March 1976):18-19.

Kostin, N.A. *Organization and Conduct of Radioelectronic Combat in a Defensive Coalition-Based Front Operation in the Initial Period of a War*, trans. by CRH & Associates Moscow: Union of Soviet Socialist Republics, 1989.

Knowles, John. "A Wider View and a Bigger Bite: EW in Information Operations." *Journal of Electronic Defense* (October 1997) 51-57.

Krepinivich, Andrew F. Jr. "The Military-Technical Revolution: A Preliminary Assessment." Washington DC: Center for Strategic and Budgetary Assessments, 2002.

Kulikov, V. review of "Idea, Algorithm, Decision" *Soviet Military Review*. English Edition. (April 1974): 56-57.

Kurnosov, Ivan. "Development of Radioelectronic Means of Troop Control and Methods of Their Application" *Voyennaya mysl'*, No. 9, September 1964, FPD 896, 2 March 1965 reprinted in "Selected Readings From Military Thought, 1963-1973" selected and compiled by Joseph D. Douglas, Jr. and Amoretta M. Hoeber, *Studies in Communist Affairs*, Vol. 5, Part 1.Washington, DC: U.S. Government Printing Office [GPO], 1982.

Kyle, Deborah M. and Benjamin F. Schemmer. "C^3/EW in Europe – Can NATO Get Its Electrons Together." *Armed Forces Journal* 118, no. 1 (September 1980): 24-28.

Larson, Major General Doyle E. USAF. "C3CM: Progress and Outlook." *Defense Management Journal* 18, no. 3 (Third Quarter 1982) 6-10.

Larson, Major General Doyle E. USAF. "C3CM: Let's Get On With It!" *Journal of Electronic Defense* (January 1982).

Libicki, Martin C., David C. Gombert, David R. Frelinger, and Raymond Smith. *Byting Back: Regaining Information Superiority Against 21st-Century Insurgents*. Santa Monica: The RAND Corporation, 2007.

Light, Jennifer. *From Warfare to Welfare: Defense Intellectuals and Urban Problems in Cold War America*. Baltimore: Johns Hopkins University Press, 2003.

Mahnken, Thomas G. *Technology and the American Way of War*. New York: Columbia University Press, 2008.

Metz, LTG Thomas F., USA and James E. Hutton, "Massing Effects in the Information Domain: A Case Study in Aggressive Information Operations." *Military Review, 3* (Mar-April 2006).

Mumford, Lewis. *The City in History*. New York: Harcourt, Brace & World, 1961.

Norman, Lloyd. "Westmoreland's J2" *Army* 17, no. 5 (May 1967): 21-25.

Parrot, Evan H. "C3CM: Theory, Application and Process." Research Report, Air War College, Air University: February, 1983.

Perry, Kathy J. “The Use of Psychological Operations as a Strategic Tool.” Research Project, US Army War College: April 2000.

Petukhov, D. “Types and Means of Communication” *Soviet Military Review*. English Edition. (November 1973): 5-8.

Petukhov, D. “For Reliable and Uninterrupted Communication.” *Soviet Military Review*. English Edition. (August 1974): 28-33.

Phillips, Richard H. “Workshop Trends in Soviet Views on Theater War.” Cambridge: MIT Center for International Studies, November 5, 1987.

Powell, Colin and Joseph Perisco. *My American Journey*. Rev. Ed. New York: Ballantine Books, 2003.

Rexrode, COL Kenneth E., USA. “An Overview of the Joint Electronic Warfare Center” Proceedings of the 1981 Western Region Technical Symposium. San Antonio: Western Region of the Association of the Old Crows, 1981, 1.

Reznichenko, V. “Modern Weapons and Troop Control.” *Soviet Military Review*. English Edition. (December 1978): 10-13.

Romanych, MAJ Marc J., USA Retired and Kenneth Krumm, LTC, USA. “Tactical Information Operations in Kosovo.” *Military Review* LXXXIV, no. 5 (September-October 2004): 56-61.

Rosak, Theodore. *The Cult of Information: The Folklore of Computers and the True Art of Thinking*. New York: Pantheon Books, 1986.

Rosenblueth, Arturo, Norbert Wiener, and Julian Bigelow. “Behavior, Purpose and Teleology.” *Philosophy of Science* 10, no. 1 (January 1943): 18-24. http://www.jstor.org/stable/1343893 (accessed 15 September, 2010).

Rosin, Randolph. “To Kill A Mockingbird: The Deconstruction of Information Operations.” *SmallWars Journal Online* (August 2009). http://smallwarsjournal.com/blog/2009/08/the-deconstruction-of-informat/ (accessed 21 April, 2010).

Romjue, John L. *American Army Doctrine for the Post-Cold War*. Virginia: Military History Office, United States Army Training and Doctrine Command, 1996.

Sapolsky, Harvey M., Benjamin H. Friedman, Brendan Rittenhouse Green, editors. *US Military Innovation since the Cold War: Creation without Destruction.* New York: Routledge, 2009.

Scherer, R.H. "Data Communications and Field Data Information Handling Systems." *Signal* XXIII, no. 5 (January 1969): 8-14.

Shanahan, Stephen W. and Gary J. Beavers. "Information Operations in Bosnia." *Military Review* LXXVII, no. 6 (November-December 1997). http://cgsc.cdmhost.com/cdm4/item_viewer.php?CISOROOT=/p124201coll1&CISOPTR=430&CISOBOX=1&REC=2 (accessed 21 April, 2010).

Sholokhov, A. "Academician Berg." *Soviet Military Review*. English Edition. (July 1981): 27-28.

Siegel, Pascale Combelles. *Target Bosnia: Integrating Information Activities in Peace Operations.* Washington DC: DOD Command and Control Research Program, 1998. http://www.dodccrp.org/files/Siegel_Target.pdf (accessed 12 NOV 2010).

Slayton, Barney F. " 'War in the Ether": Soviet Radio-Electronic Warfare." *Military Review* LX, no. 1 (January 1980). http://cgsc.contentdm.oclc.org/cdm4/item_viewer.php?CISOROOT=/p124201coll1&CISOPTR=344&CISOBOX=1&REC=3 (accessed 15 September, 2010).

Sleeper, Colonel Raymond S. USAF. "Cybernetics in the Service of Communism." *Air University Review* XVIII, no. 3 (March-April 1967): 2-13.

Smith, Charles F. "Command, Control and Countermeasures (C3CM)." *Military Review* LXIII, no. 1 (January 1983).

Smith, Rupert. *The Utility of Force: The Art of War in the Modern World*. New York: First Vintage Books, 2007.

Starry, Michael D. and Charles W. Arneson. "*FM 100-6: Information Operations*." *Military Review* LXXVI, no. 6 (November-December 1996). http://cgsc.cdmhost.com/cdm4/item_viewer.php?CISOROOT=/p124201coll1&CISOPTR=439&CISOBOX=1&REC=1 (accessed 21 April, 2010).

Sullivan, GEN Gordon R., USA and COL James M. Dubik, USA. *War in the Information Age*. Carlisle Barracks: Strategic Studies Institute, US Army War College, 1994.

Thomas, Lieutenant Commander G. Guy, USN., "Warfare in the Fourth Dimension – Is the Navy Ready for it? How can the Navy Prepare for it?" *Naval War College Review* (January-February 1983)*:* 16-23.

Thomas, Timothy L. "Kosovo and the Current Myth of Information Superiority." *Parameters, US Army War College Quarterly* XXX, no. 1 (Spring 2000). http://www.usamhi.army.mil/USAWC/Parameters/00spring/contents.htm (accessed 22 April, 2010).

Thrasher, Roger Dean. "Information Warfare Deplhi: Raw Results." Monterey: Naval Postgraduate School, June 1996.

Toffler, Alvin. *The Third Wave.* New York: Bantam Books, 1990.

Toffler, Alvin and Heidi Toffler. *War and AntiWar: Survival at the Dawn of the 21st Century*. 1st ed. New York: Little, Brown and Company, 1993.

Tulak, MAJ Arthur, USA. "PSYOP C2W Information Operations in Bosnia" Center for Army Lessons Learned Report, June 1999. http://www.iwar.org.uk/iwar/resources/call/ll.htm (accessed 17 June, 2010).

US Army Training and Doctrine Command, Center for Army Lessons Learned. "CALL Newsletter No 99-2: Task Force Eagle Information Operations, "IO in a Peace Enforcement Environment" Fort Leavenworth KS: January 1999.

US Joint Chiefs of Staff. Joint Publication 3-13, *Information Operations*. Washington DC: 13 February 2006.

US Joint Chiefs of Staff Memorandum of Policy #30, *Command and Control Warfare.* (17 July1990, 1st Revision, Washington DC: 8 March, 1993). http://www.dod.gov/pubs/foi/reading_room/732.pdf (accessed 22 April, 2010).

US Joint Chiefs of Staff, *Joint Vision 2010*. Washington DC: 1996.

US Joint Chiefs of Staff *Concept for Future Joint Operations: Expanding Joint Vision 2010.* Washington DC: May, 1997.

United States Department of Defense, *Statement on Technology and Military Manpower*, by William J. Perry, Undersecretary of Defense for Research and Engineering Before the

Subcommittee on Armed Services, United States Senate, 96th Cong., Second Sess.,Washington DC: 4 December 1980.

Van Creveld, Martin. *Command in War*. Cambridge MA: Harvard University Press, 1985.

Vincent, 1Lt Gary A., USAF. "A New Approach to Command and Control: The Cybernetic Design." *Airpower Journal* (Summer 1993): 24-37.

Waltz, Edward. "The US Transition to Information Warfare." *Journal of Electronic Defense* (December 1998): 35-42.

Weiss, Geoffrey F. "Exposing the Information Domain Myth: a New Concept for the Air Force and Information Operations Doctrine." *Air and Space Power Journal* XXII, no. 1 (Spring 2008). http://www.airpower.maxwell.af.mil/airchronicles/apj/apj08/spr08.htm (accessed 22 April, 2010).

Wentz, Larry, K. ed. *Lessons From Bosnia: The IFOR Experience.* Washington, DC: Institute for National Strategic Studies, 1997.

Westmoreland, GEN William C., USA. *Addresses by General W. C. Westmoreland, Chief of Staff, United States Army. Volume IV, 3 July 1969 – 16 December 1969.* Washington DC: 1973.

Westmoreland, GEN W. C., USA. "The Military Uses of Communications-Electronics." *Signal* (August 1969).

Westmoreland, GEN William C. USA. *A Soldier Reports.* New York: Da Capo Press, 1989.

Wiener, Norbert. *The Human Use of Human Beings: Cybernetics and Society*. Da Capo Series in Science. 1954; repr., Boston: De Capo Series in Science, 1998.

Williamson, John R. "The Effects of Soviet Army Communications Jamming on the AIM Division Signal Battalion." master's thesis, US Army Command and General Staff College, 1980.

Wright, Donald and LTC Timothy Reese. USA. *On Point II: Transition to a New Campaign*. Fort Leavenworth: Combat Studies Institute Press, 2008.

Wright, Donald, James R. Bird, Steven E. Clay, Peter W. Connors, LTC Scott C. Farquhar, USA, Lynne Chandler Garcia, and Dennis F. Van Wey. *A Different Kind of War*. Fort Leavenworth: Combat Studies Institute Press, 2010.

Valisyev, S. "Communications in an Offensive" *Soviet Military Review*. English Edition. (September 1975): 5-8.

Vanden Dries, Capt Paul. USAF. "C3CM-The Boyd Cycle's Throttle." Proceedings of the 1981 Western Region Technical Symposium. San Antonio: Western Region of the Association of the Old Crows, 1981: 7.