STRATEGY
RESEARCH
PROJECT

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

LIKE A LIGHTNING BOLT - INFORMATION WARFARE

BY

COLONEL KENNETH BOLL
United States Army

19990608 005

DISTRIBUTION STATEMENT A:
Approved for public release.
Distribution is unlimited.

USAWC CLASS OF 1999

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

DTIC QUALITY INSPECTED 4

USAWC STRATEGY RESEARCH PROJECT

LIKE A LIGHTNING BOLT—INFORMATION WARFARE

by

Colonel Kenneth Boll
United States Army

Professor Mike Morin
Project Advisor

The views expressed in this academic research paper are those of the author and do not necessarily reflect the official policy or position of the U.S. Government, the Department of Defense, or any of its agen

DISTRIBUTION STATEMENT A:
Approved for public release.
Distribution is unlimited.

U.S. Army War College
Carlisle Barracks, Pennsylvania 17013

ABSTRACT

AUTHOR: Colonel Kenneth Boll

TITLE: Like A Lightning Bolt–Information Warfare

FORMAT: Strategy Research Project

DATE: 1 February 1999 PAGES: 41 CLASSIFICATION: Unclassified

Combatant commanders currently do not have the best possible support from information warfare doctrine and capabilities that facilitate organizing forces for offensive and defensive information warfare. A balance of offensive and defensive information power is required and this research project suggests clearer doctrinal command and control relationships, integrated ways of employment, and sufficient information warfare means to enable a joint force commander to project dominant information power. The appropriate organization for combat will include a Joint Information Warfare Task Force to assist the joint force commander's planning effort and execute information operations.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

LIKE A LIGHTNING BOLT—INFORMATION WARFARE

> Those expert in attack consider it fundamental to rely on the seasons and the advantages of the ground; they use inundations and fire according to the situation. They make it impossible for the enemy to know where to prepare. They release the attack like a lightning bolt from above the nine-layered heavens.
>
> —Tu Yu, 735-812

As we near the end of the Twentieth Century, the United States Armed Forces are offered an opportunity to leap ahead in military effectiveness by exploiting an advantage in the conduct of military affairs—information warfare. However, in a time that cries out for rapidly formulating information warfare tactics, techniques and procedures, the U.S. military, instead, is moving with glacial slowness to place information warfare tools in the hands of the warfighter. Only when doctrine and organizations for warfighters are revised to reflect the efficient application of information operations to modern warfare, will the combatant commander be able to fully mobilize dominant information power and win fast with minimum casualties.

Modern materiel capable of executing information missions and soldiers knowledgeable in the constituent aspects of information warfare are already on hand; commanders require only familiarity with the ways to accomplish the appropriate ends.

Joint and service component commanders will gain full capability to wage information warfare only when furnished with a comprehensive doctrine and the type of organizations that can advantage the information age, as we are beginning to comprehend it. Discouragingly, our current slow pace for fielding imaginative uses for information at all levels of combat fails to capture the inherent creativity and resourcefulness of the American soldier, handicapping our abilities to wage war in the Information Age. We are sensing, yet again, the depressing reality that "revolutions in military affairs are perennially held hostage to the narrow, demeaning, and gritty bureaucratic agendas of military organizations that, like the poor, are seemingly with us always."[1] Perhaps it is time to formulate doctrine at the lowest levels and let change percolate up. As a way of doing so, combatant commanders should review the meaningful aspects of the global information infrastructure and begin to apply them to military solutions. The appropriate organization for combat will include a Joint Information Warfare Task Force to assist the joint force commander's planning effort and execute information operations.

THE GLOBAL INFORMATION INFRASTRUCTURE

Our culture increasingly is dependent on the easy access to information and the services provided by information-based systems.[2] Our technology-dependent society is swiftly merging international communications networks, computer databases, and consumer electronics. In the U.S. military alone, an estimated 95 percent of strategic communications travel over commercial data systems.[3]

By the year 2010, theorists anticipate that "cyberwar may be to the twenty-first century what blitzkrieg was to the twentieth century."[4] Indeed, cyberwar, in its aspect of offensive military operations directed against the United States, may be a cheap revolution in military affairs that evens the playing field of international conflict and encourages antagonists to attempt to defeat a military superpower without engaging in conventional military attacks.[5] With such a threat emerging, it is disturbing to note that a White House staffer from the current administration states: "The biggest problem that I see in this whole [information warfare] business is that we do not have anybody in charge, we do not know who is responsible for what piece of this."[6] This despite the fact that our national security thinkers have long debated about the conduct of information warfare.

It is imperative for the conduct of military operations that the organization and chain of command for information operations be clearly delineated and resourced. The military cannot afford confusing lines of authority and responsibility for information warfare because it detracts from effective combat operations. We must conceptualize what the military can do with information in the global information infrastructure and capture those techniques in meaningful doctrine without further delay.

CURRENT DOCTRINE

Current doctrine is grounded in the overarching National Security Strategy, the capstone documents of the Department of Defense and in CJCS policy documents. Our doctrine clearly defines information operations in terms of "information superiority:" that is, "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[7] In turn, this policy requires both offensive and defensive information warfare capabilities.[8] This is an expansion of the definition of information operations articulated in DOD Directive S-3600.1 of 9 December 1996: actions taken to affect adversary information and information systems while defending one's own information and information systems. Clearly, in order to develop campaign plans and organize for combat, combatant commanders and subordinate joint force commanders require doctrine that provides a more concrete statement of what information warfare is supposed to accomplish on the battlefield.

While, at the National-level at least, doctrine for broad-based information operations appears to require a balance between offensive and defensive means, this same vision has not yet been articulated throughout the wide range of military operations. Joint doctrine defines command and control warfare as occurring primarily at the operational level,[9] while the Army's basic doctrine for information operations fails to meaningfully describe offensive information operations at the operational and tactical levels. The possibility of non-lethal attack of the enemy's information operating systems is not specified, and the only mention of attack is at the tactical level, where published doctrine envisions a standard approach of active electronic warfare and physical destruction. Indeed, the Army's doctrinally specified means of attack are electro-optical, radio frequencies, infrared, lethal attacks, OPSEC, and deception.[10] In this respect, the Army needs to catch up to the joint community's clear definition of the use of information operations, information warfare and command and control warfare.

One of the great challenges to providing meaningful doctrine for the conduct of information operations is a mindset among many doctrine writers that conducting offensive information warfare requires little in the way of new doctrine. This notion, emanating from such sources as the Joint Warfighting Center, assumes the warfighting systems that will support offensive information warfare, electronic warfare platforms and PSYOPS, for example, are so well understood by field commanders that they need to expend little intellectual effort to understand how these existing systems are integrated into information warfare.[11] This leads to a focus of doctrinal development on defensive efforts, assuming that this is the area of our least understanding and greatest vulnerability. Hence, the joint community, following the national command authority's guidance, places their focus on computer network defense as the area for most doctrinal and organizational emphasis. Creating a standing joint task force for computer network defense without an analogous organization for computer network attack is a recent example of this emphasis on the defense.[12]

As a result of the prevailing defensive mindset among doctrine developers, there is a dearth of effective organization for balanced (offensive and defensive) information operations at the operational and tactical levels.[13] This doctrinal gap is particularly debilitating in a period when the U.S. defense drawdown deprives the U.S. military of overwhelming mass, mandating effective synergy among joint forces in order to advantage all aspects of combat power.[14] This, in turn, requires innovative thinking at tactical, operational and strategic levels to come up with tools to replace mass in its conventional sense. For a start, doctrine developers should note that, from the aspect of organizing for combat, the terms "information operations," "information warfare," and "command and control warfare" all mean the same thing in terms of organizing units for combat in the global information infrastructure—both offensive and defensive information tools are required. It is time to use simple expressions to codify doctrine for information warfare so the services can develop organizations to conduct it.

In another area crying out for simplicity, Army doctrine states that information operations are to be coordinated by "cells" as part of the land component commander's staff.[15] This cell coordinates electronic warfare, operations security (OPSEC), psychological operations (PSYOPS), military deception and, presumably, computer network attack. However, in practice, this low-powered staff structure is likely to inhibit effective information operations. Noting the fact that even the Army's own doctrinal publications confuse acronyms (in one place, even confusing the acronym "STO" as "special tactical operations" rather than "special technical operations")[16], it is clear that staffs are unlikely to even recognize the roles of all the players because of unclear doctrine.

As an example of how little the Army pays attention to existing doctrine that calls for integrated information warfare, Figure 1 shows the organization for combat of one of our most

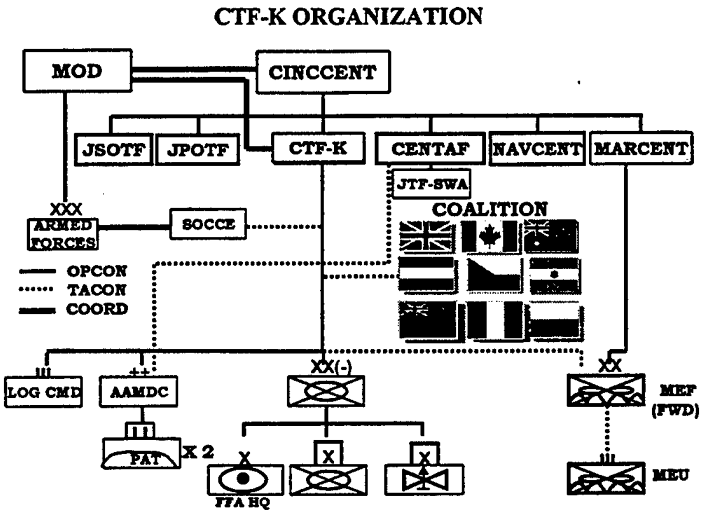


Figure 1 - CTF-K ORGANIZATION

recent endeavors in joint and combined command and control for land forces operations, the structure of Combined/Joint Task Force-Kuwait (CTF-Kuwait).[17] There are evident impediments to coordinating information operations efficiently, most notably the existence of a Joint Psychological Operations Task Force operating directly under the CINC although its operations were designed to take place in the CTF commander's JOA. This separates one information warfare discipline from others by providing a command and control "stovepipe" not applicable to the other elements. Other information warfare elements, such as military deception units, are not similarly represented by commanders, leading to an imbalance in the ability of a single staff to coordinate. Another example, military deception elements are organic to the Military Intelligence battalion of the subordinate 3rd Infantry Division (Mechanized),[18] well below the level of a JTF staff to direct effectively, given intervening command layers.

The notion of a "cell" supervised by a very busy J3 effectively reaching across layers of command to control all elements of information warfare discards some truisms that have stood the test of military logic throughout the ages, including unity of command and economy of force.

Doctrinally, the information operations "cell" coordinates all information operations, including command and control countermeasures, consisting of offensive and defensive command and control warfare actions. However, in day to day pre-conflict operations, a typical ARFOR headquarters does not have direct access to all elements of the doctrinal "cell." For example, the recent CTF-Kuwait organization had a mechanized infantry division furnishing the ARFOR headquarters for CTF-K. This division has no organic PSYOPS or "information warfare officer" assigned, although the Army plans to provide an information warrior to the division at some time in the future.[19] Both Army and Joint doctrine presuppose that technical expertise in integrating all elements of information operations will show up, "as required," in the form of augmentees from the Army's Land Information Warfare Activity[20] (LIWA) or the Joint Command and Control Warfare Center.[21] In addition, the "Special Technical" aspect of command and control warfare is available to the land component commander only through augmentation from higher headquarters.[22]

But how is this expected to work in practice? The land component commander of a non-standing joint force assembles his information operations "cell" only on the eve of warfare and does not train routinely with all elements of the cell because they are not all organic to his command. Some elements of the information operations functions are compartmented as separate, functional commands and some represent traditional elements of combat power that are reoriented to perform information operations roles. Some functions cross service lines and some represent National agency assets being synchronized into the tactical fight. And the first commander who is responsible for integrating this multi-echelon, multiservice, interagency effort is the joint forces land component commander, who might also have other missions for himself and his staff to worry about. This is the commander expected to coordinate the newly emerging tenets of information operations, on the fly.

It is clear that, at least in the realm of joint operations, there is a school of thought that supports the notion of warfare by committee—after all, the current joint doctrine supports the notion of a J3-sponsored committee running information operations (the "cell"). The most telling argument in support of a committee approach is that the elements of combat power employed in information warfare, e.g. electronic warfare or physical destruction, are means commonly possessed by any number of commanders in a theater.[23] Thus, these multiple means have identities and utilities of their own, separate from the information warfare effort. Since these means are widely applicable to other forms of combat, adherents to this school of thought argue that a commander need not be placed in charge of the overall information warfare effort in a CINC's campaign because information warfare brings nothing unique to the table. Furthermore, they believe any effort to develop "information warfare" as a separate area for study or training expertise, is misguided. In fact, the elements of deception, psychological operations, and operational security are seen as so fundamental to all unit operations that they are inseparable from unit operations of any kind of unit and should not be assigned as a lead responsibility to a single commander.[24]

However, even those who believe that information warfare is nothing new, merely a repackaging of existing means, also note "a job generally doesn't get done unless someone is put in charge of it."[25] This focus on command clearly is the crux of the argument—the CINC should not have to personally fight the information campaign and should have a subordinate commander to orchestrate the planning and execution of the theater information warfare planning and execution effort. An understanding of how to conduct an information warfare campaign is the clearly new facet of warfighting on a battlefield where, admittedly, the elements of information warfare are, and have been for some time, present on the battlefield.

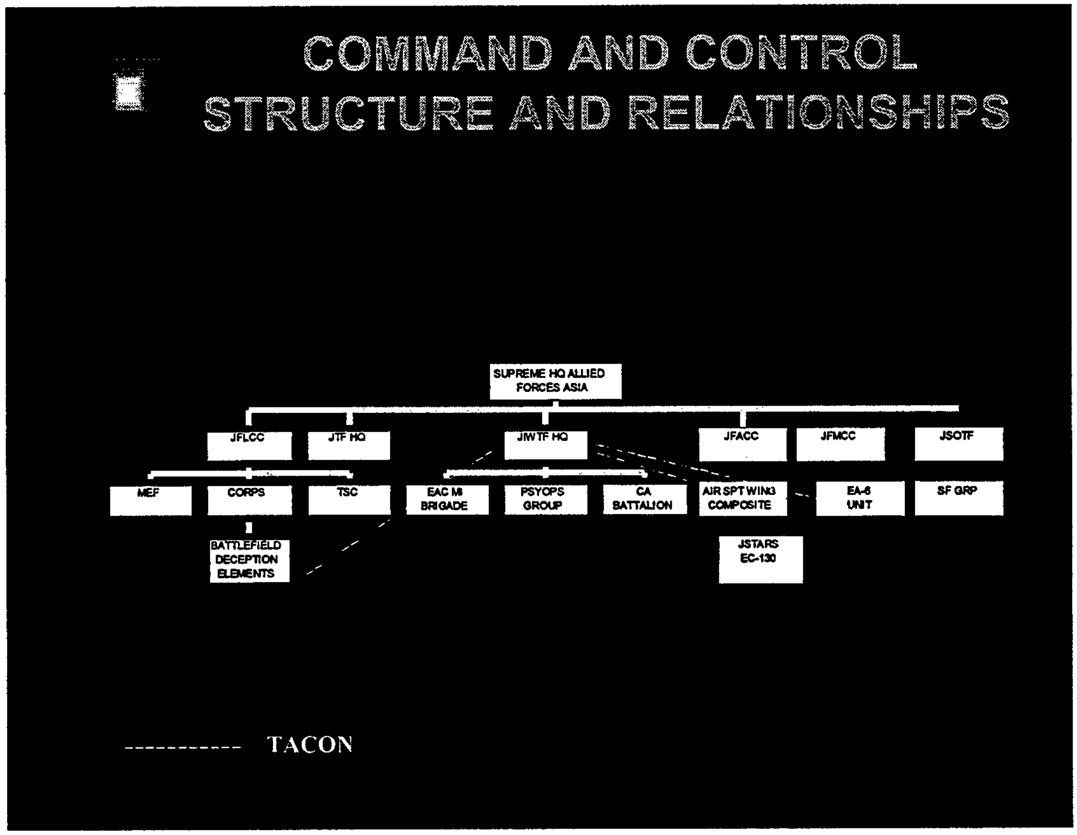
Returning to a focus on command responsibility is worth elaborating here because it is a simple truth. The notion of command responsibility is supposedly so well engrained in our thinking that military doctrine writers tend not to articulate how necessary it is for conducting all military operations. As a result, doctrinal discussions about new areas of warfare, such as information operations, go so far astray from reality as to contemplate conducting warfare by committee. While it is true, as stated in the Army's Operations Field Manual, unity of command may not always be possible in combined and interagency operations, in joint operations, employment of military forces in a matter that best masses combat power requires unity of command.[26] An effective information warfare campaign clearly is the type of effort, requiring concentration of disparate means against an enemy center of gravity over time, which requires the focus of a responsible commander to achieve unity of effort.

THOUGHTS ON CURRENT DOCTRINE

It is time to propose another way to organize for conducting information operations at the operational and tactical levels--one that might be a little more recognizable to the joint force land component commander and might be a little more effective in terms of commanding and controlling disparate assets. This approach calls for a Joint Information Warfare Task Force commander who, under the control of the joint force land component commander, is charged with integrating all aspects of offensive and defensive information warfare at the operational level. This responsible commander, in turn, ensures information operations at the tactical level contribute to the overall theater campaign plan.

A "cell" embedded in the land component commander's staff is unable to control subordinate information operations assets directly. On the other hand, a joint information warfare task force commander could be assigned operational control of joint assets as it makes sense within the joint force. This Joint Information Warfare Task Force commander could direct operations and coordinate with other elements of a joint force, as shown by the example in figure 2.

To illustrate the importance of the principle of unity of command, effective information operations require that all forces be under one responsible commander. This commander would control the means of information warfare assets to achieve the ends assigned by the Joint Task Force commander, including both defensive and offensive command and control warfare.



COMMAND AND CONTROL
STRUCTURE AND RELATIONSHIPS

SUPREME HQ ALLIED FORCES ASIA

JFLCC
JTF HQ
JIWTF HQ
JFACC
JFMCC
JSOTF

MEF
CORPS
TSC
EAC MI BRIGADE
PSYOPS GROUP
CA BATTALION
AIR SPT WING COMPOSITE
EA-6 UNIT
SF GRP

BATTLEFIELD DECEPTION ELEMENTS
JSTARS EC-130

----------- TACON

Figure 2 - COMMAND AND CONTROL

DEFENSIVE COMMAND AND CONTROL WARFARE

As stated earlier, the preoccupation of our national security strategy makers lies in defending against a perilous threat against our national information infrastructure—asymmetrical information operations in the hands of terrorists, criminals, or hostile states.[27] While these opposing forces are indeed a threat to our national information infrastructure, a greater danger is that we will fail to conceptualize how to go about defending, even though we have the technical means of defense. Indeed, the technical aspects of defense are familiar techniques. One leading theorist even discounts the threat of such attacks to our infrastructure, pointing out that computer hosts could easily require digital signature codes to sort out the remote computers authorized to enter operational codes.[28] But what is needed most is an overarching mind-set to guide network administrators. One excellent security concept is to employ the guiding principles by which insurgent organizations historically defend their vital information infrastructures successfully.

One of the characteristics of an underground organization is that it operates in an environment of constant threat from police and espionage activities. As a result, the basic underground unit is a cell that is designed to limit the number of members vulnerable to arrest at any time. As the underground organization grows, new cells are added rather than expanding existing cells.[29] Each cell is compartmented, with cutouts to higher and lateral connections (see fig. 3).[30] Any one particular cell is knowledgeable about its own operations, but can be isolated in case of intrusion. The organization is based on a fail-safe principle so that, if one cell is compromised, the consequences to the entire movement are minimized.[31]

Although the techniques of computer programming are different, a similar mentality can easily protect military computer networks from any but the most sophisticated attacks.

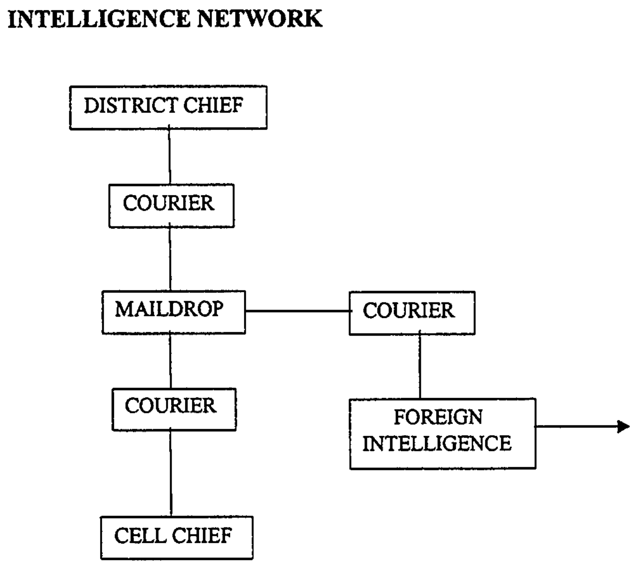


Figure 3 - INTELLIGENCE NETWORK

Extending the analogy, the ability of a revolutionary movement to extend its ranks throughout the populace while maintaining security is a blueprint for the way military information networks should be structured. Computers at all levels of military organization should be linked to the same operations/intelligence network, sharing databases and providing redundant communications and capabilities. Indeed, large mainframe computers that are accessed by a multitude of computers could become a thing of the past—replaced by multiple smaller computers linked in a wide area network without sacrificing security. This redundancy is a tremendous force multiplier in staving off information attacks from inimical third parties. With no mainframe in particular to target, and databases being spread among thousands of smaller computers, each with security cutouts, an enemy would be hard pressed to produce major damage to our military network.

Although the United States military increasingly is dependent on information means for command and control, the United States also possesses the most robust and multi-tiered information environment in the global information environment, capable of enormous redundancy.[32] Although it is a worthwhile effort to ensure our information environment is protected, this effort should be balanced by intellectual and organizational energy expended to support the capability to conduct offensive command and control warfare. Again, we must return to the time-tested principles articulated in FM 100-5, Operations: "Commanders adopt the defensive only as a temporary expedient and must seek every opportunity to seize the initiative."[33]

OFFENSIVE COMMAND AND CONTROL WARFARE

An effective military organization must be capable of assuming the offensive at all levels of operations, tactical, operational, and strategic. To compliment these operations, information warfare organizations must be prepared to assume the offense in support of a Joint Force Commander's combat mission. Clearly, the U.S. military has not yet moved out along this lane.

One notion evidently lacking in accounts of contemporary combat operations is that of synchronized, offensive command and control warfare that employs all the elements available to the joint force commander. Particularly absent are accounts of non-lethal information attack. Perhaps the only account in current history is the story that U.S. intelligence operatives inserted a computer virus into the Iraqi integrated air defense system by means of a microchip placed in a peripheral printer used by the Iraqi's computer network. Supposedly, the virus then devoured air defense displays, causing information to vanish and disabling the Iraqi network.[34] However, a leading analyst discounts this story in its entirety, pointing out that a printer is designed to send control codes, not the operational codes that would reprogram computers.[35]

In order to produce effective operational-level information attack efforts, the Joint Information Warfare Task Force (JIWTF) Commander needs to centralize operational control of the assets that tend to support the JTF in the context of today's operations. These assets, while residing under the command of the service components of the Joint Force Commander or Special

Operations Commander, would take priority for their operational tasking from the Joint Information Warfare Task Force Commander, including naval, air and ground assets.

NAVAL ASSETS FOR THE JOINT INFORMATION WARFARE TASK FORCE

The principal naval information attack asset that should operate under the control of the Joint Information Warfare Task Force Commander is the EA-6B electronic warfare aircraft organic to the carrier battle group. With its AN/ALQ-99 pods, the EA-6B possesses a powerful offensive electronic warfare capability that should be integrated into the overall attack on the enemy's command and control systems.[36]

AIR FORCE INFORMATION WARFARE OFFENSIVE ASSETS

Similar to the EA-6B's capabilities, Air Force electronic warfare aircraft would be under the operational control of the Joint Information Warfare Task Force Commander to conduct electronic attack, including the COMFY LEVI and other jamming aircraft. Particularly important for situational awareness during the information warfare campaign would be the JSTARS surveillance aircraft, a primary information warfare asset.[37]

The COMMANDO SOLO aircraft would perform psychological operations for the Joint Information Warfare Task Force, integrated into the overall offensive plan.

GROUND IW OFFENSIVE ASSETS

The land component commander would place offensive Information Warfare assets under the control of the Joint Information Warfare Task Force. These assets would include the battlefield deception capabilities of subordinate military intelligence units, as well as their organic electronic attack assets. Furthermore, assigned military intelligence analysis and control elements would be tasked to perform priority technical control and analysis functions in support of the Joint Information Warfare Task Force Commander to facilitate the overall Joint Force Commander's electronic attack plan. These analysis centers also analyze enemy information networks and attack them using special technical means, including computer viruses and intrusion. The theater commander should have a better-integrated, organic capability to attack opposing command and control systems, through the enemy's information network, at the time of maximum impact in conjunction with other elements of combat power.

Special operations elements, to include, psychological operations units, would be under the control of the Joint Information Warfare Task Force Commander for integration into the theater or Joint Task Force Commander's information attack plan.

OPERATIONS SECURITY

Operations security actions should be coordinated, in support of the Joint Force Commander, by the Joint Information Warfare Task Force Commander and his staff. The reconnaissance and security plans of ground maneuver units must be coordinated with the intent of the overall information attack plan. Assets from the Joint Task Force for Computer Network Defense and the Army's Land Information Warfare Activity are particularly well suited to support OPSEC requirements.

DECEPTION

Command and control of deception operations is a critical function of information warfare. A tactical deception plan that is not carefully integrated into a centrally-coordinated, strategic deception plan runs the grave risk of calling the enemy's attention to a move which may actually be the one the Joint Force Commander wants to make when the time comes, as noted by the British Joint Planning Staff during the Second World War.[38]

The Joint Information Warfare Task Force Commander would be responsible for coordinating deception planning and monitoring deception execution by subordinate component commanders. In turn, the Joint Information Warfare Task Force Commander takes his guidance from the theater deception annex. The theater deception strategy should be based on a strategic deception plan formulated by the National Command Authority. The United States government would be wise to establish a national-level deception planning entity, similar to the "London Controlling Section" during the Second World War,[39] to formulate and coordinate the strategic deception plan executed by theater commanders. In particular, the commander must take advantage of the fact that the Information Age offers unparalleled technological means, such as the INTERNET, to bypass opposing government controls and affect opinion leaders in a target country.

ILLUSTRATIVE SCENARIO

For illustrative purposes, consider the following scenario. A southeastern Asian nation, densely populated and with a large, industrial-age army, undertakes offensive operations against Australia. Appeals for assistance leads the United States into offensive operations against the Aggressor State. A Joint Task Force is committed into offensive operations against the main islands of the Aggressor State, supported by a Joint Information Warfare Task Force under CINCPAC.

The CINC reviews the military options available to repel the aggression and ensure that removing the aggressor regime from power terminates the sources of conflict. Examining the use of information warfare in support of this mission, and based on competent legal review, the commander determines: the defeat of the enemy through information warfare will minimize the expenditure of life, time and physical resources; disrupting and incapacitating public information transfer means will not inflict unnecessary suffering on the civilian populace of the aggressor; and the principle of military necessity permits employing information warfare in this context.[40]

The CINC designates the Commander of the supporting echelons-above-corps Army military intelligence brigade as the Commander, Joint Information Warfare Task Force. The supporting MI Brigade contains a commander and staff who are familiar with electronic warfare, deception and OPSEC through the exercise of their doctrinal mission.[41] The Joint Force Commander augments the brigade staff with PSYOPS and physical attack planners to constitute a headquarters capable of planning and executing the entire range of information operations.

In constituting the Joint Information Warfare Task Force, the Joint Force Commander considers the principles of unity of command and simplicity[42] as the driving factors.

The Joint Information Warfare Task Force Commander recommends the following actions in support of Joint Forces combat operations. To support forcible entry operations, the aggressor state's stock exchange computer system will be attacked with deceptive information insertion on D-21, causing devaluation of the opponent's currency and undermining public confidence in the regime's policies. This attack would be conducted by the JIWTF, supported by available national resources tasked by the JCS. On D-18, the aggressor state's banking computer network will be attacked with a computer virus, erasing individual account records and further causing public unrest. At the same time, Joint Force-sponsored information broadcasts will overwhelm the aggressor state's television and radio frequencies in the outlying islands, employing a carefully orchestrated information effort designed to cause disaffection with the regime. The Joint Task Force will destroy radio and television transmitters in the outlying areas through a combination of air attack and special operations.

As the opponent's military increasingly is committed against their own nation's internal unrest, cognitive dissonance within the enemy's command and control structure can be exploited through selected electronic attack that undermines confidence in the enemy's capability to communicate timely and accurate information. In conjunction with lethal attack of the enemy air defense operations centers, cyber attacks on the enemy's air traffic control computers will collapse their capability to oppose the Joint Task Force's air assets.

Simultaneously, the Joint Information Warfare Task Force will commence an e-mail effort targeting all known mailboxes for opinion leaders in the Aggressor State. A psychological operations and public information effort identifying specific aggressor leaders as "war criminals" will serve to further isolate the opposing leadership from their own supporters. In addition, opinion leaders will be concerned that their identities and whereabouts will be known when combat operations commence in the main islands. E-mail messages also will refer opinion leaders to an unclassified Joint Information Warfare Task Force web site containing information designed to evoke fear and disaffection among opinion leaders. Regime attempts to retaliate by limiting INTERNET access will be followed immediately by Joint Task Force physical attacks on the telecommunications backbone.

In this particular example, the Joint Information Warfare Task Force would best be organized as a separate unit operating in support of the Joint Task Force Commander who is given the mission of employing combat forces to defend the allied state and to defeat the aggressor state.

COMMAND RELATIONSHIPS

Subordination of the Joint Information Warfare Task Force is an issue that depends upon the theater commander's intent for phased operations. Most probably, the Joint Information Warfare Task Force would be organized as a separate, stand-alone organization capable of supporting multiple "combatant" commanders during the "softening-up" phase of a campaign against an aggressor.

Central to the notion of information warfare, however, is the mental agility necessary for leaders to understand the potential in this new form of warfare. This may be easier said than done. During our recent intervention in Bosnia, one of the greatest barriers to gathering a correct battlefield picture was our sensor-based technology that was hampered by the compartmented physical relief of the Balkans.[43] In the absence of military sensors, inputs from the local society and open source information were more vital to the correct assessment, and a key obstacle to information-based military operations were inflexible leaders.[44] One intelligence analyst pointed out: "The key lessons of IFOR's misuse and lack of information suggest a systemic American military cultural deficiency that new battlefield technologies will not overcome."[45] Clearly, our fixation on automated data storage and retrieval systems alone do not enable commanders or analysts to reach the correct conclusions automatically—training and intuition are as important as ever.[46]

BUILDING THE JOINT INFORMATION WARFARE TASK FORCE COMMAND

When designating the Joint Information Warfare Task Force Commander, a consideration should be selecting the commander who already has the most competent staff for dealing with the aspects of information warfare. As noted above, an Army Military Intelligence Brigade headquarters is structured to deal routinely in three of the six elements of information warfare, making it among the first choices when structuring command and control for information operations.

Most importantly, the commander of an information warfare task force must be trained at a service War College that, as one seasoned observer remarks, stresses:

> the nonmilitary—that is, the political, social, and economic—aspects of war, including the structure of industry, mobilization, finance, and public relations and also including corresponding problems as they affect the United States' main opponents.[47]

RECOMMENDATION

Clearly, the United States military continues to fail to fully exploit the Nation's capabilities to employ offensive information warfare capabilities in pursuit of national ends.

This is largely due to a mind-set that relegates information operations to a supporting role in reinforcing traditional elements of power, rather than recognizing the emergence of an entirely new paradigm. An appropriate organization for combat, including a Joint Information Warfare Task Force, would better address warfare in the Information Age when the means of attack and defense in the global information infrastructure are present, but not yet truly integrated as an awesome weapon. Our leadership must put form and substance to what is currently only a glimmering of doctrinal precepts. It is time to treat information warfare as a practical tool, wielded by specific organizations, surprising the enemy. Perhaps Major-General J.F.C. Fuller put it best when, in his book, Generalship: Its Diseases and Their Cure, he noted:

> Originality, not conventionality, is one of the main pillars of generalship. To do something that the enemy does not expect, is not prepared for, something which will surprise him and disarm him morally. To be always thinking ahead and to be always peeping around corners. To spy out the soul of one's adversary, and to act in a manner which will astonish and bewilder him, this is generalship…This is the foundation of success.

WORD COUNT = 5267

ENDNOTES

[1] C. Kenneth Allard, "Information Warfare: The Burden of History and the Risk of Hubris," in The Information Revolution and National Security, ed. Stuart J.D. Schwartzstein (Washington, D.C., The Center for Strategic and International Studies, 1996), 235.

[2] Ryan Henry and C. Edward Peartree, "Military Theory and Information Warfare," Parameters XXVIII (Autumn 1998): 129.

[3] Ibid.

[4] John Arquilla and David Ronfeldt, "Information, Power, and Grand Strategy: In Athena's Camp," in The Information Revolution and National Security, ed. Stuart J.D. Schwartzstein (Washington, D.C., The Center for Strategic and International Studies, 1996), 147.

[5] William J. Clinton, A National Security Strategy for a New Century (Washington, D.C.: The White House, May 1997), 12.

[6] Michael Nelson, "The View from the White House: A Public Policy Perspective," in The Information Revolution and National Security, ed. Stuart J.D. Schwartzstein (Washington, D.C.: The Center for Strategic and International Studies, 1996), 66.

[7] Department of Defense, "Joint Vision 2010." Washington, D.C.: Office of the Chairman, Joint Chiefs of Staff, July 1996); quoted in U.S. Army War College Selected Readings AY99, Course I, Volume II (Carlisle, PA: U.S. Army War College, 1998), 340.

[8] Ibid.

[9] Department of Defense, Joint Doctrine for Command and Control Warfare, Joint Publication 3-13.1, 7 February 1996, i; available from <http: //www.dtic.mil/doctrine/jel/new_pubs/jp3_13_1.pdf> Internet; accessed 2 October 1998.

[10] Department of the Army, Information Operations, Field Manual 100-6 (Washington, D.C.: U.S. Department of the Army, 27 August 1996), 6-2,3.

[11] LCDR Andy Wilde, "Update: Information Operations," A Common Perspective 6, No. 2 (October 1998): 8.

[12] Ibid, 9.

[13] The ideas in this paragraph are based on remarks made by a speaker participating in the Commandant's Lecture Series.

[14] Jeffrey Cooper, "Dominant Battlespace Awareness and Future Warfare," in Dominant Battlespace Knowledge, The Winning Edge, ed. Stuart E. Johnson and Martin C. Libicki (Washington, D.C.: NDU Press, 19xx), 113.

[15] FM 100-6, D-0.

[16] Ibid.

[17] COL Bill R. Moore and LTC K.H. Boll, "Intelligence for the Coalition: The Story of Support to Coalition Task Force-Kuwait," memorandum for Commander, Third U.S. Army, Atlanta, GA, 26 May 1998.

[18] Department of the Army, Division Intelligence and Electronic Warfare Operations, Field Manual 34-10 (Washington, D.C.: U.S. Department of the Army, 25 November 1986), 2-7.

[19] The ideas in this paragraph are based on a series of remarks made by a speaker participating in the Commandant's Lecture Series.

[20] FM 100-6, B-3 to B-4.

[21] Ibid, B-1 to B-2.

[22] Ibid, D-0.

[23] CDR Erik J. Dahl, "We Don't Need an IW Commander," U.S. Naval Institute Proceedings 125 (January 1999): 49.

[24] Ibid.

[25] Ibid, 48.

[26] Department of the Army, Operations, Field Manual 100-5 (Washington, D.C.: U.S. Department of the Army, 14 June 1993), 2-10.

[27] William J. Clinton, "A National Security Strategy for a New Century," October 1998; available from <http: //www.whitehouse. gov/WH/EOP/NSC/html/documents/nssr.pdf>; Internet; accessed 7 November 1998, 6.

[28] Martin C. Libicki, What is Information Warfare? (Washington, D.C.: U.S. Government Printing Office, 1995), 54.

[29] Andrew R. Molnar et al., Undergrounds in Insurgent, Revolutionary, and Resistance Warfare (Washington, D.C.: The American University, 1963), 53.

[30] Ibid., 54.

[31] Ibid.

[32] The ideas in this paragraph are based on a series of remarks made by a speaker participating in the Commandant's Lecture Series.

[33] FM 100-5, 2-8.

[34] U.S. News and World Report, Triumph Without Victory (New York: Random House, 1992), 224-225.

[35] Libicki, 50.

[36] Military Aircraft Database; available from <http://www.csd.uwo.ca/~pettypi/elevon/gustin_military/us/A6INTRUD.html>; Internet; accessed 13 November 1998.

[37] Sheila E. Widnall, "Information Technology Vital to Battlefield Success," 22 September 1995; available from <http://www.af.mil/cgi-bin/multigate/retrieve?u=z3950r://dtics11:1024/airforce!F598%3a910958974%3a%28JSTARS%29;esn=FT%5fTEXT%20HTML%200;ct=text/html>; Internet; accessed 13 November 1998.

[38] Michael Howard, Strategic Deception in the Second World War (New York: W.W. Norton and Company, 1995), 26.

[39] Ibid, 27.

[40] Richard W. Aldrich, The International Legal Implications of Information Warfare (Colorado Springs, CO: U.S. Air Force Institute for National Security Studies, 1996), 9.

[41] Department of the Army, Echelons Above Corps Intelligence and Electronic Warfare Operations, Field Manual 34-37 (Washington, D.C.: U.S. Department of the Army, 15 January 1991), 4-3.

[42] FM 100-5, 2-11.

[43] LTC John A. Gentry, "Knowledge-Based 'Warfare:' Lessons from Bosnia," American Intelligence Journal, 18, nos. 1 and 2, (1998), 79.

[44] Ibid.

[45] Ibid., 74.

[46] Jerome K. Clauser and Sandra M. Weir, Intelligence Research Methodology, (State College, PA: HRB-Singer, Inc., 1975), 16.

[47] Martin van Creveld, The Training of Officers, (New York: The Free Press, 1990), 108.

BIBLIOGRAPHY

Aldrich, Richard W. The International Legal Implications of Information Warfare. Colorado Springs, CO: U.S. Air Force Institute for National Security Studies, 1996.

Allard, C. Kenneth. "Information Warfare: The Burden of History and the Risk of Hubris." In The Information Revolution and National Security, ed. Stuart J.D. Schwartzstein, 233-250. Washington, D.C.: The Center for Strategic and International Studies, 1996.

Arquilla, John, and David Ronfeldt. "Cyberwar is Coming!" Comparative Strategy 12, no. 2 (1993): 141-165.

Arquilla, John, and David Ronfeldt. "Information, Power and Grand Strategy: In Athena's Camp." In The Information Revolution and National Security, ed. Stuart J.D. Schwartzstein, 132-180. Washington, D.C.: The Center for Strategic and International Studies, 1996.

Briney, Andy. "1998 Annual Industry Survey." June 1998. Available from <http: //www.Infosecuritymag.com>. Internet. Accessed 5 October 1998.

Clinton, William J. A National Security Strategy for a New Century. Washington, D.C.: The White House, 1997.

Clinton, William J. "A National Security Strategy for a New Century." October 1998. Available from <http: //www. Whitehouse.gov/WH/EOP/NSC/html/documents/nssr.pdf>. Internet. Accessed 7 November 1998.

Clauser, Jerome K. and Sandra M. Weir. Intelligence Research Methodology. State College, PA: HRB-Singer, Inc., 1975.

Cooper, Jeffrey. "Dominant Battlespace Awareness and Future Warfare." In Dominant Battlespace Knowledge, The Winning Edge, ed. Stuart E. Johnson and Martin C. Libicki, 103-119. Washington, D.C.: NDU Press, 1995.

Dahl, CDR Erik J. "We Don't Need an IW Commander." U.S. Naval Institute Proceedings 125 (January 1999): 48-49.

Gentry, John A. "Knowledge-Based 'Warfare:' Lessons from Bosnia." American Intelligence Journal 18, no. 1 (1998): 73-80.

Henry, Ryan and C. Edward Peartree. "Military Theory and Information Warfare." Parameters 28 (Autumn 1998): 121-135.

Howard, Michael. Strategic Deception in the Second World War. New York: W.W. Norton and Company, 1995.

Kennedy, Kevin J., Bruce M. Lawlor, and Arne J. Nelson. Grand Strategy for Information Age National Security, Information Assurance for the Twenty-first Century. Maxwell Air Force Base, AL: Air University Press, 1997.

Libicki, Martin C. What is Information Warfare? Washington, D.C.: U.S. Government Printing Office, 1995.

Military Aircraft Database. Available from <http: //www. csd. Uwo.ca/~pettypi/elevon/gustin_military/us/A6INTRUD.html>. Internet. Accessed 13 November 1998.

Molnar, Andrew R., William A. Lybrand, Lorna Hahn, James L. Kirkman, and Peter B. Riddleberger. Undergrounds in Insurgent, Revolutionary, and Resistance Warfare. Washington, D.C.: The American University, 1963.

Moore, COL Bill R. and LTC K. H. Boll. "Intelligence for the Coalition: The Story of Support to Coalition Task Force-Kuwait." Memorandum for Commander, Third U.S. Army. Fort McPherson, GA, 26 May 1998.

Nelson, Michael. "The View from the White House: A Public Policy Perspective." In The Information Revolution and National Security, ed. Stuart J.D. Schwartzstein, 63-67. Washington, D.C.: The Center for Strategic and International Studies, 1996.

O'Neill, Bard E. Insurgency and Terrorism. Washington, D.C.: Brassey's Inc., 1990.

Stewart, John F. Jr. "Operation DESERT STORM: The Military Intelligence Story." Memorandum for Commander, Third U.S. Army. Riyadh, Saudi Arabia, 1991.

U.S. Department of Defense. Doctrine for Joint Psychological Operations. Joint Publication 3-53. Washington, D.C.: U.S. Department of Defense, 10 July 1996.

U.S. Department of Defense. Joint Doctrine for Command and Control Warfare, Joint Publication 3-13.1, 7 February 1996; available from <http: //www.dtic.mil/doctrine/jel/new_pubs/jp3_13_1.pdf>. Internet. Accessed 2 October 1998.

U.S. Department of Defense. Joint Doctrine for Information Operations. Joint Publication 3-13. Washington, D.C.: U.S. Department of Defense, 9 October 1998.

U.S. Department of Defense. "Joint Vision 2010." Washington, D.C.: U.S. Department of Defense. Quoted in U.S. Army War College Selected Readings AY99, Course I, Volume II, 322-358. Carlisle, PA: U.S. Army War College, 1998.

U.S. Department of Defense Joint Warfighting Center. "Expanding Joint Vision 2010." Fort Monroe, VA: U.S. Department of Defense, 1997.

U.S. Department of the Army. Command and Control Countermeasures. Army Regulation 525-50. Washington, D.C.: U.S. Department of the Army, 31 July 1992.

U.S. Department of the Army. Division Intelligence and Electronic Warfare Operations. Field Manual 34-10. Washington, D.C.: U.S. Department of the Army, 25 November 1986.

U.S. Department of the Army. Echelons Above Corps Intelligence and Electronic Warfare Operations. Field Manual 34-37. Washington, D.C.: U.S. Department of the Army, 15 January 1991.

U.S. Department of the Army. Information Operations. Field Manual 100-6. Washington, D.C.: U.S. Department of the Army, 27 August 1996.

U.S. Department of the Army (DAMO-ODI). Information Operations. Monograph. Washington, D.C.: U.S. Department of the Army, 1998.

U.S. Department of the Army. Operations. Field Manual 100-5. Washington, D.C.: U.S. Department of the Army, 14 June 1993.

U.S. News and World Report. Triumph Without Victory. New York: Random House, 1992.

Van Creveld, Martin. The Training of Officers. New York: The Free Press, 1990.

Widnall, Sheila E. "Information Technology Vital to Battlefield Success." 22 September 1995. Available from <http: //www.af.mil/cgi-bin/multigate/retrieve?u=z3950r://dtics11:1024/airforce!F598%3a910958974%3a%28JSTARS%29;esn=FT%5fTEXT%20HTML%200;ct=text/html>. Internet. Accessed 13 November 1998.

Wilde, LCDR Andy. "Update: Information Operations." A Common Perspective 6, no. 2 (October 1998): 7-10.