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.

THE FUNCTIONAL RELATIONSHIP BETWEEN INFORMATION OPERATIONS AND MILITARY INTELLIGENCE

BY

LIEUTENANT COLONEL CAROL J. ROGERS
United States Army

DISTRIBUTION STATEMENT A:
Approved for Public Release.
Distribution is Unlimited.

USAWC CLASS OF 2001

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

20010605 157

USAWC STRATEGY RESEARCH PROJECT

The Functional Relationship between Information Operations and Military Intelligence

by

Lieutenant Colonel Carol J. Rogers
Department of the Army

Professor Anthony Williams
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 agencies.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

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

ABSTRACT

AUTHOR: Carol J. Rogers

TITLE: The Functional Relationship between Information Operations and Military Intelligence

FORMAT: Strategy Research Project

DATE: 10 April 2001 PAGES: 29 CLASSIFICATION: Unclassified

Information operations are a new approach to managing and manipulating information. Through the ages, the possession of information has won wars, and the lack of it often led to defeat. This paper attempts to define the relationship between information and intelligence, and concludes that military intelligence professionals have the core competencies needed to be effective information operations officers. Focusing on a joint perspective, information operations is defined, using illustrations to clarify the multi-faceted information operations' missions. The impact of new technologies is examined, as it relates to the use of information as a tool for military leaders. The personnel requirements for IO are examined and compared to the core competencies of military intelligence. The findings indicate the redundancy and overlay of the primary personnel capabilities of information operations and military intelligence. The arguments lead to the conclusion that intelligence officers are best suited and qualified to perform the responsibilities of an information operations officer and to manage information operations.

TABLE OF CONTENTS

ABSTRACT III

LIST OF TABLES VII

THE FUNCTIONAL RELATIONSHIP BETWEEN INFORMATION OPERATIONS AND MILITARY INTELLIGENCE 1

BACKGROUND 1

IO DEFINED 2

IO PERSONNEL REQUIREMENTS 6

MI PERSONNEL REQUIREMENTS 7

COMPARISON OF IO AND MI PERSONNEL REQUIREMENTS 9

FINDINGS 12

CONCLUSION 13

ENDNOTES 15

BIBLIOGRAPHY 19

LIST OF TABLES

TABLE 1. COMPARISON OF REQUIRED CAPABILITIES 10

THE FUNCTIONAL RELATIONSHIP BETWEEN INFORMATION OPERATIONS AND MILITARY INTELLIGENCE

> In a world where information is power, a vital element of our national security lies in our intelligence services.
>
> —President Gerald R. Ford

Information Operations (IO) is surrounded by confusion. The very term conjures up a variety of concepts. Even the term *information* is ambiguous, as throughout history into the present day it has been used interchangeably with *intelligence*. There is no standard definition or doctrine within the military services and the Department of Defense (DOD) for IO; consequently there is no clear command and control (C2) delineated. Still, the prevailing sense is that IO has not only utility, it is critical to national security and stability. Information has always been a vital aspect in protecting a nation's security—those who had the best ability to obtain, control and use the information, had the tactical advantage. The major portion of this effort has been traditionally allocated to the intelligence personnel of the armed forces. So what makes IO different from the task that has been done by intelligence throughout the ages? Should it be managed by the military intelligence (MI) community, and are they capable of handling it? Or is IO already so large and complex that it needs a new organization, doctrine, tactics, techniques and procedures to manage it? Is it simply the means by which the information is collected, controlled and used? General Ryan believes that what has changed is "the means and route of attack"[1]—does this explain the IO phenomenon?

This paper will examine these questions. It will describe IO, its mission, capabilities and functions. It will then discuss the personnel requirements of IO as well as MI, and compare the mission requirements of each. Based on these findings and the functions of IO, it will then recommend the most appropriate C2, and discuss the MI corps' ability to handle this additional responsibility. The paper will limit intelligence to the military community, and study the problem in the context of the joint environment.

BACKGROUND

> A strong nation requires a strong intelligence organization.
>
> —George Bush

Throughout history "Information" and "Intelligence" have been interchanged. Often "information" is used to define "intelligence," and even Webster defines "intelligence" as "news

or *information.*" Clausewitz uses one to define the other, " By Intelligence we mean every sort of *information* about the enemy and his country—the basis, in short, of our own plans and operations."[2] This can be illustrated by examining the definition of *information* as defined in the Joint IO Publication, which is "*Facts, data, or instructions in any medium or form. It is the meaning that a human assigns to data by means of the known conventions used in their representation.*"[3] Compare this to the joint definition for *intelligence*: "The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas."[4] When the two definitions are compared, it appears that various references to *information* in many national documents, really mean *intelligence".* It is clear that *information* is just data, with whatever meaning an individual conjures up in his mind when he hears/sees that data. Whereas *intelligence* requires an assessment or interpretation, adding a human dimension that is not necessary for *information.* Joint Vision 2020 states, "Throughout history, military leaders have regarded information superiority as a key enabler of victory."[5] Data, alone, does not enable victory—it must be analyzed, evaluated and interpreted before it becomes of value. As one researcher noted, *"The tendency to equate information and intelligence probably stems from the dual nature of the term "intelligence" which is both a process and a range of products. Information and intelligence are epistemologically related concepts, but they differ in terms of their scope, content, and ability to create understanding."*[6] The understanding of the relationship between *information* and *intelligence* is crucial as the role of IO at the national, strategic and military levels is sorted out and clarified.

IO DEFINED

> Dominating the information spectrum is as critical to conflict now as occupying the land or controlling the air has been in the past.
>
> —General Ronald R. Fogleman

What is Information Operations? IO derives from the recognition and acceptance that manipulation of information itself can be a key element of the war-winning equation.[7] IO is defined in the Joint Doctrine for Information Operations as "Actions taken to affect adversary information and information systems while defending one's own information and information systems."[8] This and the services' definitions do not clearly delineate to the novice what IO actually is or what it does. The military services' definitions of IO include: collecting information on adversaries and potential adversaries; distributing information beneficial to US missions, as

well as distribution of misinformation to disrupt enemy operations; protection of our information systems; conversely, the ability to disrupt enemy information systems, disrupting their operations; warfighting missions which combine the aspects of PSYOPS, military deception, EW, Signals Intelligence, civil affairs (CA) and public affairs (PA); plus Computer Network Attack (CNA) and Defense (CND).[9] There are many responsibilities listed, which have traditionally been performed by separate branches. Two aspects seem to differentiate IO from these traditional divisions of labor: the technological capability and the coordination function of IO.

It is necessary here to examine the definitions of Information Warfare (IW), a term often used synonymously with IO. JP3-13 defines IW as, "*Information operations* conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries."[10] Most of the documentation suggests that IO is conducted during peacetime, whereas IW is IO conducted during crisis or conflict.[11] There are no specific guidelines, however, to determine when the line is crossed from IO to IW. This begs the question whether the IW subset of IO is necessary. IO could be regarded as an economic sanction, which if used could defer or deter military actions, or conversely, could irritate and alienate the targeted country, forcing them to military action. The line between making a point and pushing the objective country to more drastic actions is vague and unpredictable. If IW remains a subset of IO, it is imperative that documentation delineating the conditions and perimeters of IW be clearly established. If this concept progresses to the debate of whether IW could be considered an act of war, a list of actions that fall into this category would have to be defined by all parties concerned. It would then follow that IO, or at least the IW subset, officially has become an instrument of war, and its use could be construed as an act of war.

"The concept of IO is a new approach to the way we conduct military operations which focus on controlling and exploiting information to support operations to achieve the desired end state."[12] IO coordinates the activities of psychological operations, military deception, electronic warfare, operations security, and physical destruction. These activities are employed in military operations to specifically attack and defend the command and control target set. By bringing all these information-based and information-focused operations under one doctrinal framework, all information operations are synchronized and mutually reinforcing, achieving synergy and unity of effort.[13]

The two most visible functions of IO are psychological operations and cyberwar. The ability to communicate, with precision and discrimination, massive amounts of information to target audiences with the intent of influencing their perceptions and decision-making processes, is an example of the psychological operations subset of IO. This was demonstrated during

Operation JUST CAUSE. Ground units employed loudspeakers to drive Panamanian dictator Manuel Noriega, a fugitive from justice, out of his hiding location and to induce the surrender of thousands of Panamanian Defense Force personnel.[14]

> The use of psychological methods of information operations against the other side's forces offers variations on two traditional themes: fear of death and potential resentment between the trench and the castle (or home front). In the Gulf War, Coalition forces convinced many Iraqis that if they abandoned their vulnerable vehicles they would live longer. The Coalition's persuasiveness was fortified by weapons that had just destroyed such vehicles during the fighting.[15]

Psychological methods of IO use radio shows, television broadcasts, and print operations (newspapers, handbills, posters, magazines, comic books and flyers). CNN taped the poor defenseless Albanians and broadcast them to viewers. What viewers did not know was that those same Albanians were also running black market operations. This left the military confused as to what to do with them.[16] This is an example of an effective IO directed against the American public and its political leadership. The affluence of US society, which supports this information infrastructure (a television in every household) makes the US much more vulnerable to this type of IO attack than some of our poorer competitors, who not only do not have a television in every house, but neither a radio, computer or even a newspaper.

The second familiar function of IO is cyberwar. Computer hacking, such as viruses, logic bombs, Trojan horses, and sniffers are examples of cyberwar.[17] In the past, the US was protected from hostile attacks on its infrastructures by broad oceans. Today potentially serious cyber attacks can be conceived and planned without detectable logistic preparation. They can be invisibly reconnoitered, clandestinely rehearsed, and then mounted in a matter of minutes or even seconds without revealing the identity and location of the attacker.[18]

The Rome Labs computer intrusion case is one of the most famous and most documented attacks on DoD computer networks.

> Rome Labs was first compromised on 23 March 1994 but was not discovered until five days later. The attackers installed an illegal computer wiretap program called a "sniffer," which captures valid logons and passwords, and subsequently captured over 100 additional user accounts. E-mails were read, copied and deleted, and megabytes of data were downloaded from penetrated systems, including Rome Labs, commercial Internet service providers, HQ NATO, Goddard Space Center, Jet Propulsion Lab, National Aerospace Plan Joint Program Office, Wright- Patterson AFB, missile contractors, and numerous U.S. Army sites . The attackers used the Rome Labs' computers to download megabytes of Korean Atomic Research Institute information and, due to the vast amounts of data, even stored this information on the Rome Labs' servers.[19]

The foregoing examples depict the broad range of IO. For the most part, the effectiveness of the operations cited, as well as other IO conducted, results from the integration of military functions and new technological capabilities. Information, once vulnerable only when in transit, now is even more accessible when in unprotected storage—particularly when it is in indifferent or careless hands.[20] The goal of information operations in many instances is to use the proliferation of information in today's world to our advantage and to prevent our adversaries' ability to disrupt our information flow. Often, the goal of IO is to buy time. "Get a commander more time by condensing his decision cycle or disrupting the opponent's, and he now has command of a new dimension of warfare."[21] Often, time is the critical piece of the puzzle. Additionally, most of these operations were conducted with minimum expenditures, but the outcomes were effective. Cyberwar is an IO tool resulting from new technologies that attempts to disrupt the information flow.

> Cyber warrior weapons are often readily available for download on the Internet. Unlike the tools of conventional warfare, the tools of this trade require no long-term acquisition, training, and fielding process to mount an attack. A comparatively low technology adversary with minimal funding, training, manning, and defense infrastructure is capable of employing these weapons on short notice from anywhere in the world. One key advantage afforded the information warrior is freedom from the burden of time and money needed to field and project a conventional force.[22]

Technology spans the entire spectrum of IO. Technology is revolutionizing every aspect of life in the US. Advances are being made in every field, which were not even conceived of one generation ago. The advances are occurring at an exponential rate. This is a reality that impacts each military function and adaptation is imperative to survive the information revolution. Both protecting our systems and exploiting enemy systems, involves a technical capability that is not readily available within the framework of traditional military schooling. Most of the recently published information on IO recognizes the need for this technical proficiency for effective IO, and this new technology has given rise to the new concept of IO.

The second unique aspect of IO is coordination of a variety of military functions. In a crisis situation, or in a peacekeeping situation, there are a variety of critical as well as routine tasks. IO proponents have recognized the need to synchronize several information-based military operations, such as intelligence, information systems, physical security, psychological operations, deception, electronic warfare, civil affairs, and public affairs, that were previously "stove-piped" and independent of one another.[23] The underlying intent of IO is to modify the enemy's perception of the situation and change his behavior, to get into his decision cycle and influence it.[24] "The planning principles of information operations are knowledge and

synchronization. . . There are a number of principles, but the key is synchronization, getting people moving like a football team where everyone is working together and doing their individual jobs."[25] Orchestration is key to coordination of all kinds of specialties, from the traditional computer geeks to intelligence analysts, communications and electronic equipment experts, the security folks, education and training teams, public affairs specialists, PSYOPS, and civil affairs.[26]

IO PERSONNEL REQUIREMENTS

> The primary object of organization is to shield people from unexpected calls upon their powers of adaptability, judgment, and decisions.
>
> —General Sir Ian Hamilton

Many of the qualities and capabilities required for effectiveness as an IO officer are capabilities that are inherent in the training of MI officers. The limited documentation indicates that the IO officer will require five capabilities: analytical, technological, planning, coordination and integration. Technology has guaranteed no shortage of available information. An IO officer will need discernment to sort through this information for that which is relevant. Information comes in from a variety of sources, and it is often fragmented. He will need analytical skills to determine which information to seek, which to keep, which to discard and which will need further processing to be useful. Without this capability the information is simply useless data.

Additionally, the IO officer will need technological capabilities. Supporting IO, especially information warfare, will require different types of expertise than supporting conventional combat. Emerging technologies across the spectrum will require commensurate abilities.[27] It will be crucial for the IO officer to have a technological understanding of these systems, especially the capabilities and vulnerabilities.

The next three capabilities required of an IO officer are found in JP 3-13, which states, "The primary function of the IO officer is to supervise the IO cell to ensure capabilities and activities are planned, coordinated, and integrated within the joint force staff and with higher echelon, adjacent, subordinate, and multinational staffs."[28]

An IO officer must be a planner. During planning phases of an operation, the IO officer plans the activities and directs the capabilities of the IO cell components, based on guidance from the commander. Often, he is responsible for deconfliction of the many demands for IO as well as insuring unity of effort within his AOR. In addition, the IO officer should also participate in critical planning meetings during the planning phases of any anticipated operation. More

explicitly, he should participate in campaign plans, concept plans (CONPLANS) as well as operations plans (OPLANS).[29]

An IO officer will be required to coordinate all the various aspects of IO. The IO cell merges capabilities from numerous sections, including but not limited to Public Affairs Office, Staff Judge Advocate, Civil Affairs, Service and functional components, targeting, special technical operations, signal and communications, imagery personnel, the various human intelligence personnel, EW, military deception and Joint Special Operations Task Force (JSOTF).[30] Because many of these staff members are full-time staff personnel for their respective staff cells, the IO Officer must carefully coordinate their efforts and manage time and people wisely. He/she must coordinate the capabilities and activities of these various elements into a synergistic plan.

Finally, the IO Officer will need to integrate the various specialties and capabilities that compose the IO cell. JV 2020 states that IO will require "specialists in the field." The IO cell is formed from select representatives from each staff element, component, and supporting agencies. IO is

> "An integrating strategy of actions taken to affect an adversary's decision cycle, information and information systems while defending one's own information and information systems. .The trick is to manage behavior through perception management. We want to modify the enemy's perception of the situation and change his behavior, to get into his decision cycle and influence it."[31]

The IO Officer must "integrate all the different activities of IO to gain information and knowledge and improve friendly execution of operations while denying an adversary similar capabilities by whatever means possible."[32] It is crucial for the IO officer to integrate these capabilities and related activities in support of a given objective.

In short, the IO Officer will need to be a specialist, a creative thinker, who can analyze not only the information, but the situation, who has the technological knowledge to know how to exploit it using the various capabilities within the IO cell, devise a plan, coordinate the plan with all relevant elements and integrate the plan to support the designated objective.

MI PERSONNEL REQUIREMENTS

> Nothing should be as favorably regarded as intelligence; nothing should be as generously rewarded as intelligence; nothing should be as confidential as the work of intelligence.
>
> —Sun Tzu, The Art of War

How do these IO officer requirements compare to the training and requirements of a MI officer? MI officers are trained in a variety of tasks, which are reflected in the five phases of the Intelligence Cycle: planning, collection, processing, analysis and dissemination/integration. A critical look at the MI capabilities in these five phases will show a definite correlation between the capabilities of an MI officer and those of the IO officer.

The first trained capability of a MI officer is planning. Conducted continuously, intelligence planning involves task-organizing intelligence assets; developing a collection plan; issuing requests for collection and production; and monitoring the availability of collected information.[33] The increased number of missions and threats to the United States places an added responsibility on intelligence professionals to prioritize the requests and demands for intelligence, to maximize the limited personnel resources in support of national interests. Unfortunately, the executive guidance is not always clear on what the priorities are. The NSS states, "We place the highest priority on monitoring the most serious threats to US security: states hostile to the US; countries or other entities that possess strategic nuclear forcer or control nuclear weapons, other WMD or nuclear fissile materials; transnational threats, including terrorism, drug trafficking and other international crime; potential regional conflicts that might affect Us national security interests; and threats to US forces and citizens abroad.[34] This prioritization does not sufficiently limit the focus, so the MI officer will be required to use discretion in planning intelligence support to military missions.

The next intelligence capability is collection. Technology in the contemporary world has enabled collectors in all of the intelligence disciplines (except HUMINT) to increase the accuracy and volume of intelligence collected. Still, these improvements still have not maintained the pace of growing numbers of new targets and areas of instability, transnational issues and other topics.[35] Despite the volumes being collected, consumers continue to task for more or different intelligence. The MI officer will need to balance these collection efforts with the capability of his/her counterparts to process and analyze this information.

Processing is necessary to correlate and convert collected data into forms suitable for analysis and production. This includes initial imagery interpretation, data conversion and correlation, document translation, and decryption, as well as reporting these results to production elements.[36] This requires greater technical expertise of the MI officer. The MI officer is trained to maintain these skills through formal military courses, as well as on the job training, where he/she can learn and constantly practice these perishable skills.

Analysis is perhaps the most crucial capability of the MI officer. "Analysis shows why sensor output and other information collected on the battlefield are important."[37]

"Comprehensive collection and analytic capabilities are needed to provide warning of threats to US national security, give analytical support to the policy and military communities, and provide near real time intelligence while retaining global perspective."[38] Analysts are faced with the awesome task of not only analyzing the large quantities of intelligence data that is currently available to them, but determining situational awareness and enemy intent, based on this material. They are not only expected to find the answers to world problems in this mass of intelligence information, but analysts must then convincingly convey and prove their reasoning to policy and decision makers, reducing the latter's level of uncertainty in dealing with world affairs. This task is expanded by Allies' reliance on US intelligence analysis for reliable information. This tremendous responsibility requires rare skills and the MI analyst provides these skills.

The final capability inherent in the training of a MI officer is integration. Once information has been collected, processed and analyzed, intelligence personnel are responsible for integrating this intelligence into the decisionmaking and planning processes. They may need further clarification, or they may raise new issues. They may need to relate the finished product to a larger picture, or cause the user to consider new operational concepts that require the intelligence to be interpreted in a new context.[39] Integration necessitates a continuous dialogue between the various users of intelligence and the analysts and producers of intelligence.

Additionally, the technological requirements of the military intelligence professional have increased as methods of collection, across all the MI disciplines, have given way to technological advances. Ability to turn a computer on and off is no longer sufficient to perform effectively in the MI arena. In addition to highly technical collection capabilities, there are now new tools for the planner and analyst as well. Additionally, as the multitude of databases increases, the MI officer also has to maintain his/her technical understanding and ability to retrieve, manipulate and disseminate information using this technology.

COMPARISON OF IO AND MI PERSONNEL REQUIREMENTS

> In peacetime, intelligence operations seek to provide the national leadership with the information needed to realize national goals and objectives, while providing military leadership with the information needed to accomplish missions and implement the national security strategy.
>
> —Joint Pub 2-02

Capabilities	MI	IO
Technological: understand capabilities and vulnerabilities of emerging technologies	X	X
Planning: participation in campaign plans, CONPLANS and OPLANS	X	X
Collection: collect information about the battlespace environment and adversary	X	
Processing: convert raw information to forms useful for the analyst	X	
Analysis: analyze data to determine situational awareness and enemy intent, capabilities and vulnerabilities	X	X
Integration: integrate information and activities Targeted at adversary	X	X
Coordination: coordinate the capabilities and activities of various elements into a synergistic plan		X

TABLE 1. COMPARISON OF REQUIRED CAPABILITIES

Table 1 is a chart that illustrates the comparison of IO officer requirements with those of his/her MI officer counterparts. The similarities are readily apparent. As stated earlier, the technological capabilities needed by the IO officer are obvious as a result of emerging technologies. MI officers have already learned to adjust and capitalize on these contemporary capabilities.

Extensive planning among many elements of the joint headquarters, component staffs, and other USG departments and agencies is essential to ensure IO is integral to the whole operational plan.[40] For the IO Officer, planning requires the same capabilities as the MI officer who must do planning. The IO Officer will need to task-organize the various elements of IO to support a single mission objective, for each identified objective. He will be responsible for developing an IO plan—as part of the Campaign Plan, CONPLAN or OPLAN.

> Information Operations require detailed planning and longer lead time for execution. This is necessary to ensure all components of the IO Campaign are functioning during the 'preparation for the objective' phase with non-lethal fires from the IO actors to create the conditions for successful accomplishment of the operation and achieving the commander's desired end-state."[41]

Part of the IO Officer's planning responsibilities will include the issuing of requests to the IO elements needed to support a particular mission. Once the operation is under way, the IO Officer will monitor the effect of the IO conducted. With multiple demands of IO Missions, the IO Officer will be required to prioritize, based on guidance from higher headquarters.

The analytical capabilities required of an IO officer are the same utilized by an MI officer. These are skills that are not only trained, but honed through experience. The analytical capability required of an IO officer is separate and distinct from the analytic functions that the J2 staff will perform in coordination with IO. "Decisionmakers and commanders might be swamped by the quantity of information flowing into a command post."[42] If the volume of information "swamps" the decisionmaking process, the most critical pieces of information may be lost in the volume.[43] An IO officer must develop "a sensitive and discriminating judgment . . . a skilled intelligence to scent out the truth."[44] These are exactly the same analytical capabilities required by an MI analyst. The criticality of analytical capability was manifested in Operation Just Cause:

> Due to the amount of reports generated by the local populace, maneuver elements found that they were quickly overwhelmed by battlefield reporting. From D to D+10, battlefield reports were so numerous that most units were only able to look at each report once. At times, this led to improper evaluations and prioritization of information which may have delayed operations and/or presented a skewed view of the battlefield.[45]

An experienced analyst will have the capability to sort through the information and quickly discern the relevant information. Additionally, an IO officer must have the capability to analyze any given situation or crisis and provide IO options to decision makers. He/she must have the ability to assess the adversary's informational vulnerabilities and exploit them.

The IO Officer must also be adept at integration. Just as the MI officer must disseminate and integrate intelligence into an increasing number of operations in which the US is involved with NATO and UN forces, so the IO officer will be required to integrate all the capabilities mentioned above into a well thought out and orchestrated operation. He will be required to integrate IO within the joint force staff and with higher echelon, adjacent, subordinate, and multinational staffs and NGOs.

The two MI capabilities that have not been identified as an IO competency (collection and processing) are nonetheless capabilities that will be useful to the IO officer in exploiting an adversary's information systems. Moreover, the coordination competency of IO is an inherent capability of the intelligence professional, though not specifically delineated. The IO officer is required to coordinate requirements of the CINC with the all source capabilities, much as the MI officer is required to coordinate the operations of all collection sources and other CI activities

with law enforcement and security activities.[46] Both must coordinate and deconflict activities and operations with all levels in the civilian, joint and combined forces.

FINDINGS

> It is not enough, of course, simply to collect information. Thoughtful analysis is vital to sound decision making.
>
> —Ronald Reagan

Although it is very probable that there are officers available in all the specialties that could effectively perform the planning, coordinating and integrating functions of the IO officer, as a rule the MI officer is the only one specifically trained and experienced to perform the functions of IO, to include the critical analytical functions. MI capabilities and responsibilities directly align with IO officer requirements. This indicates, as a minimum that MI is a viable option to lead and manage IO.

Additionally, the preponderance of technical specialties within the reserve components' MI force is an attractive option for filling the personnel needs which IO is going to engender. These part-time soldiers bring a wealth of expertise and experience that is not available in military schooling, and which could readily be applied to IO. The following specialties are available among reserve component MI personnel: corporate information technology (IT) executives; Microsoft certified systems engineers (MCSE); defense messaging system (DMS) specialists; corporate software developers; computer network defense (CND) experts; corporate and government computer security professionals; system/network administrators; and soldiers with advanced computer science degrees.[47] These service members could easily fill the technological requirements of IO, and have already been trained in the other relevant MI competencies.

It is also obvious, however, that the demands of IO are tremendous and management of IO would place an additional burden on the MI community. Currently there are concomitant demands on intelligence. Previously, with the Cold War, the MI could focus intelligence resources and methods, and maximize their effectiveness. Now, there are nearly 30 more countries than there were when the cold war ended with more in prospect.[48] The intelligence community's effort is being spread across a vast array of threats and missions. The increasing demands placed on military intelligence speaks well of dependence on MI products and the

capability of MI to perform and deliver. Despite new and varied threats and expanded missions, the intelligence community continues to provide the same level of in-depth information and intelligence, and strives to "satisfy, in quality and quantity, the illusory and insatiable demands of its customers."[49]

CONCLUSION

> War plans cover every aspect of a war, and weave them all into a single operation that must have a single, ultimate objective in which all particular aims are reconciled.
>
> —Carl von Clausewitz, On War

It is obvious that intelligence has the training and expertise necessary to fulfill the demanding functions of IO, a fact acknowledged by leaders in all the services, since it is from the pool of MI personnel that many IO personnel are being selected. Additionally, MI continues to meet the needs and expectations of the warfighter, despite the diminished resources of the contemporary military. These demonstrated capabilities make MI the only logical and expedient choice to fill the IO officer's role and to manage IO. The reasons for the choice of MI are:

- The relationship between intelligence and information already exists.
- MI personnel are already trained and competently functioning in the planning, coordination and integration skills needed to perform in IO.
- The skills needed by IO align with core competencies of the MI professional, especially the analytical capabilities, which are vital to successful IO operations.
- Shortage of personnel could be offset by the availability of technical expertise within the Reserve Components.
- C2 relationships between J2/Intelligence and J3/Operations are already established and functional. This avoids adding another layer to C2.

All information is potential intelligence. The manipulation of information as a military tool requires a creative mind, as well as knowledge of the enemy. MI officers are trained and capable to be effective IO officers. MI competencies mirror stated requirements for IO officers, and already have an established command and control structure. MI personnel provide the optimum solution for managing and leading information operations.

WORD COUNT = 5191

ENDNOTES

[1] Department of the Air Force, Aerospace Weather Operations, Air Force Doctrine Document 2-5 (5 August 1998):[database on-line]; available from http://afpubs.hq.af.mil/pubsforms/pubs/af/dd/d0205000/d0205000.pdf.

[2] Carl Von Clausewitz, On War (Princeton, N.J.: Princeton University Press, 1976), 117.

[3] U.S. Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Publication 3-13, (Washington, D.C,: U.S. Government Printing Office, October 9, 1998), I-9.

[4]U.S. Joint Chiefs of Staff, Doctrine for Intelligence Support to Joint Operations, Joint Publication 2-0, (Washington, D.C,: U.S. Government Printing Office, March 9, 2000), GL-5.

[5] Henry H. Shelton, Joint Vision 2020, (Washington D.C.:US Government Printing Office, June 2000), 10.

[6] Kevin R. Cunningham, Bounded Rationality and Complex Process Coupling: Challenges for Intelligence Support to Information Warfare, Strategic Research Project (Carlisle Barracks: U.S. Army War College,), SRP, 1.

[7] AFDD 2-5.

[8] JP 3-13, I-1.

[9] This information was extracted from a briefing provided by a Land Information Warfare Activity (LIWA), in Beltsville, Maryland, to visiting personnel, 26 Jan 01.

[10] JP 3-13, GL-7.

[11] There are some exceptions to this. The Navy considers, when out of port, to be operating in a crisis mode. For this reason, IO at sea is regarded as Information Warfare. The Air Force breaks IW down into Defensive and Offensive IW, allowing defensive IW in peace or war. The Marines apply IO across the full spectrum of civil-military operations—from peace to crisis to conflict.

[12] Mary Sue Winneke, ed., Information Operations, (Fort Leavenworth, KS.: Center For Army Lessons Learned, Jan 1999), 1.

[13] Ibid.

[14] AFDD 2-5.

[15] Martin C. Libicki, What is Information Warfare? (Washington D.C.: US Government printing Office, June 2000), 39.

[16] Michael L. Warsocki, "Seizing the High Ground: Land Operations and Information Operations," in The Information Revolution and National Security , ed. Thomas E. Copeland, (Carlisle Barracks: Strategic Studies Institute, August 2000), 130.

[17] Libicki, 50.

[18] William J. Clinton, "The President's Commission on Critical Infrastructure Protection," Implementing National Military Strategy IV, (Carlisle Barracks, 2000), 25-29.

[19] Sam Cox, Ron Stimeare, Tim Dean, Brad Ashley, "Information Assurance—the Achilles' Heel of Joint Vision 2010?" Implementing National Military Strategy IV, (Carlisle Barracks, 2000), 25-70.

[20] Alan D. Campen, "Intelligence is the Long Pole in the Information Operations Tent," Signal 54, (MAR 00): [database on-line]; available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 294399055.

[21] Warsocki, 130.

[22] Cox et al, 25-69.

[23] Winneke, 1.

[24] Charles Ayala, "New Approaches to Information Warfare," in The Information Revolution and National Security, (Carlisle Barracks: Strategic Studies Institute, August 2000), 129.

[25] IBID, 132.

[26] Warsocki, 134.

[27] Robert K. Ackerman, "Military Intelligence Looks Within" Signal, (October 2000),4.

[28] JP 3-13, IV-3.

[29] JP 3-13, IV-4.

[30] JP 3-13, taken from Figure IV-1.

[31] Ayala, 129.

[32] Winneke, 1.

[33] JP 2-02, I-1.

[34] Clinton, 5.

[35] Alan E. Goodman, "The Future of US Intelligence," Intelligence and National Security 11, (OCT 96), 652.

[36] JP 2-02,.II-7.

[37] Cunningham, 2.

[38] Clinton, 5.

[39] JP 2-0, II-13.

[40] JP 3-13, IV-1.

[41] Winneke, 69.

[42] Cunningham, 6.

[43] David S. Alberts, "The Unintended consequences of Information Age Technologies, Avoiding the Pitfalls, Seizing the Initiative," (Washington D.C.: Institute for National Strategic Studies, National Defense University: 1996),4.

[44] Clausewitz, 101

[45] "Operation Just Cause Lessons Learned," Bulletin, No. 90-9,(Fort Leavenworth: Center for Army Lessons Learned, Oct 90), III-5.

[46] JP 2-0, II-2.

[47] COL Steve Pedigo, LIWA Commander, US Army Research Center, Interview by author, 26 Jan 01, Beltsville, MD.

[48] Goodman, 652.

[49] Campen, 3.

BIBLIOGRAPHY

Ackerman, Robert K. "Military Intelligence Looks Within." Signal. October 2000.

Alberts, David S., "The Unintended Consequences of Information Age Technologies, Avoiding the Pitfalls, Seizing the Initiative." Washington, D.C.: Institute for National Strategic Studies, National Defense University, 1996.

Ayala, Charles, "New Approaches to Information Warfare," in The Information Revolution and National Security. ed. Thomas E. Copeland, 134-141. Carlisle Barracks: Strategic Studies Institute, August 2000.

Bay, Austin. "Tossing, Turning Over Intelligence." San Antonio Express-News, 24 January 2001, p.15(A).

Campen, Alan D. "Intelligence is the Long Pole in the Information Operations Tent." Signal (March 2000)54: 35-36. Database on-line. Available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 294399055.

Clausewitz, Carl Von. On War. Princeton, N.J.:Princeton University Press, 1976.

Clinton, William J. A National Security Strategy for a New Century. Washington, D.C.: The White House, October 1998.

Clinton, William J. "The President's Commission on Critical Infrastructure Protection." Implementing National Military Strategy IV. Carlisle Barracks: 2000.

Cox, Sam, Ron Stimeare, Tim Dean, and Brad Ashley, "Information Assurance—the Achilles' Heel of Joint Vision 2010?" Implementing National Military Strategy IV. Carlisle Barracks, 2000.

Cunningham, Kevin R. "Bounded Rationality and Complex Process Coupling: Challenges for Intelligence Support to Information Warfare." Strategy Research Project. Carlisle Barracks: U.S. Army War College,

"DCI Annual Report for the US Intelligence Community." 1998. Available from <http://www.odci.gov/cia/publications/fy98intellrpt/intro.html>. Internet. Accessed 5 October 2000.

Denning, Dorothy E. "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy." Available from http://www.cs.georgetown.edu/~denning/infosec/nautilus.html. Internet. Accessed 11 September 2000.

DiCenso, David J. "Information Operations: An Act of War?" 31 July 2000; Available from http://www.airpower.maxwell.af.mil/airchronicles/cc/dicenso!.html. Internet; accessed 27 March 2001.

Everett III, James R. "NATOs New Strategic Concept: Kosovo and the Implications for Intelligence." US Army War College Selected Readings. Carlisle Barracks, 2000.

Goodman, Allan E. "The Future of US Intelligence." Intelligence and National Security, 14. October 1996.

Lawson, Jay E. "Peace Operations from an Intelligence perspective." Strategy Research Project. Carlisle Barracks: U.S. Army War College,

Kuehl, Dan. "Educating the DOD about Information Warfare: Is the Glass Half Full, or Half Empty?" Available from <http://www.ndu.edu/irmc/publications/educ_the_dod.htm> Internet. Accessed 23 January 2001.

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

Metz, Steven. Armed Conflict in the 21st Century: The information Revolution and Post-Modern Warfare. Carlisle Barracks: Strategic Studies Institute, April 2000.

"Operation Just Cause Lessons Learned." Bulletin No. 90-9. Fort Leavenworth: Center for Army Lessons Learned, Oct 90.

Shalikashvili, John M. National Military Strategy of the USA. Washington D.C.: US Government Printing Office, June 2000.

Shanahan, Stephen W. and Beavers, Garry J. "Information Operations in Bosnia." Nov/Dec 1997. Available from <http://www-cgsc.army.mil/milrev/english/novdec97/shanahan.htm> Internet. Accessed 23 January 2001.

Shelton, Henry H. Joint Vision 2020. Washington D.C.: U.S. government Printing Office, June 2000.

Taylor, Francis X. "Dangerous Liaisons on the New Landscape of Information Operations," The Inspector General Brief 51. (Nov/Dec 1999): 8-9/ Database pm-line. Available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 294401126.

Tenet, George. "DCI Annual Report for the US Intelligence Community." 1998. Available from <http://www.odci.gov/cia/publications/fy98intellrpt/intro.html> Internet. Accessed 5 October 2000.

U. S. Department of the Airforce, Aerospace Weather Operations, Air Force Doctrine Document 2-5.(5 August 1998):[database on-line]; available from http://afpubs.hq.af.mil/pubsforms/pubs/af/dd/d0205000/d0205000.pdf.

U.S. Joint Chiefs of Staff Doctrine for Intelligence Support to Joint Operations, Joint Publication 2-0, Washington, D.C,: U.S. Government Printing Office, March 9, 2000.

U.S. Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Publication 3-13, Washington, D.C,: U.S. Government Printing Office, October 9, 1998.

U.S. Joint Chiefs of Staff, National Intelligence Support to Joint Operations, Joint Publication 2-02. Washington, D.C,: U.S. Government Printing Office, September 28, 1998.

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

Warsocki, Michael L. "Seizing the High Ground: Land Operations and Information Operations," in The Information Revolution and National Security. ed. Thomas E. Copeland. Carlisle Barracks: Strategic Studies Institute, August 2000.

Wentz, Larry K. "Information Operations: The IFOR Experience." Available from http://www.dodccrp.org/bo_infoop1.html. Internet. Accessed 23 January 2001.

Winneke, Mary Sue, ed., Information Operations. Fort Leavenworth, KS: Center For Army Lessons Learned, Jan 1999.