AU/ACSC/063/2000-04

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

FUTURE INFORMATION OPERATIONS (IO) IN THE MILITARY: IS IT TIME FOR AN "IO CINC?"

by

Robert J. Gaines, Commander, U. S. Navy

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Major Mary A. Willmon

Maxwell Air Force Base, Alabama

April 2000

DISTRIBUTION A:

Approved for public release; distribution is unlimited.

Air Command and Staff College
Maxwell AFB, Al 36112

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Preface

I began this research topic driven by a fascination with the incredible growth we are experiencing in information-related technology. Everywhere you turn there is news about how fast the latest microprocessor performs calculations. The technology heavy NASDAQ breaks into record territory almost every week and presidential candidates speak out on the need for Internet access in all schools and in every home. On a typical drive to work, you can see increasing numbers of fellow commuters talking on their cellular phones. You can even receive your GPS location on your wristwatch!

Enter the so-called "Y2K" computer problem. Even though the problem was all fuse and no bang, we became quite aware of our reliance on technology. With widespread dependence comes strategic vulnerability. Therefore, a critical need exists for a strong national defense to protect these vulnerabilities. Conversely, the ability to access this vulnerability in potential adversaries makes the Information "Instrument of Power" a formidable tool for advancing US interests.

The Department of Defense is working diligently on Information Operations on many levels and within each service branch. The goal of this paper is not to criticize these tremendous efforts, but rather to discuss a serious concern about our military's structural ability to manage this dynamic vulnerability.

I wish to give a very special thanks to Major Mary Willmon, my Faculty Research Advisor. Her patience and assistance during the course of this project helped more than she knows.

AU/ACSC/063/2000-04

Abstract

The world is growing. Obviously not in terms of geography, but rather in the "information" dimension. Populations, economies, and individual opportunity are each growing at rates unprecedented in the human experience. With this growth, the worldwide lust for information makes it a most powerful and necessary commodity. The world of Information Operations is where this commodity is produced, guarded, and marketed. If the United States of America is to maintain Superpower status, we must be pre-eminent in our Information Operations capability and readiness. The Department of Defense is funneling significant resources to meet this challenge. The question is: Under what command and control hierarchy are these efforts best shepherded?

The first step in this study was to review existing literature on this topic and glean the present "as is" condition of national Information Operations policy, military vision, private sector concern, law, and ethics. From this foundation, important issues were revealed and analyzed within the contextual framework.

This research indicates our national interest would be best served through establishing an Information Operations Unified Command. Commitment and investment at this level by the National Command Authority and Department of Defense is logical and necessary to shape, respond, and prepare for worldwide Information Operations, potential Information Warfare, and cyber-terrorism.

Part 1

Introduction

Should the National Unified Command Organization expand to include a new "US Information Command?" Currently, formal Department of Defense (DOD) strategic doctrine for Information Operations (IO) details a complex and elaborate "IO Cell" constructed from dispersed resources. Placing the burden for building this cell on a Joint Force Commander (JFC), particularly in time of fast-paced crisis, may not best serve the needs of The National Command Authority or a Unified Commander-in-Chief (CINC).

While most recognize the growing importance of IO, a great deal of public and governmental ambivalence exists concerning the proper legal and ethical role for the military's involvement in this area. What are our military's duties and responsibilities concerning defense of our national critical infrastructures? Should the military engage potential foreign or domestic threats to our national critical infrastructure via IO? What are the legal issues related to potential military offensive/defensive IO activities? The military must successfully operate in this new, potentially hostile environment during a period of transition as national policy and laws evolve. The stakes are high. Private industry, various government agencies, and DOD will spend tens of billions of dollars over the next few years on IO. If we are to maximize proper military involvement in a resource-constrained environment, DOD can ill-afford to proceed in a

disjointed and unfocused manner. Given the magnitude and complexity of IO, perhaps the national interest would be best served by establishing an IO CINC.

This study uses open source, unclassified information as a means to consider our current IO posture. However, the very nature of this material, and the inherent security requirements encasing some information on the subject, places significant constraints upon this study. Government agencies, including the DOD, the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), the National Reconnaissance Office (NRO), and the National Security Agency (NSA), each have independent budgets, programs, and policies. This information is unavailable to the author. Additionally, available material on this topic grows and changes with great velocity—a limitation that depreciates the value of some background information. At the same time, the existence of these limitations and complexities may actually help provide an answer to the research question.

Part 2

Background

Defining Information Operations

Information Operations (IO). The very term conjures thoughts ranging from how the news media provides their services to activities and transactions occurring in cyberspace. This wide range can actually contain numerous possible IO issues and situations. So, the initial problem becomes one of properly defining IO. A proper working definition will enable exploration of issues and areas appropriate for military involvement.

We can easily understand that IO evolves very rapidly with the creative application of existing, and the advent of new, technology. Ingenious new uses for existing technology become available each day. "Older" capabilities fold into emergent technology producing dynamic evolutionary changes in information access and management. This happens while an insatiable hunger for new technology both fuels, and is fueled by, tremendous growth in the world's economy. To help understand this rate of change, consider that evolution in information-related technology is sometimes measured in terms of an "Internet-year." One Internet-year currently equals about three calendar months! This means the practical value of what is known about IO today may rapidly depreciate below useful levels. This became evident during research for this paper. While volumes are written on this topic, the shelf life of many reports and papers expired as their ink dried. The dynamics of IO are such that what we know today may not apply next

week and what we know on the topic is greatly exceeded by what we don't know. That said, please keep one thing in mind...this ink is dry.

IO is a very broad topic with implications crosscutting the strategic, operational, and tactical levels of military operations. For example, Information Operations provide a military tactical end-user with data necessary to develop and execute strike packages. At higher levels of decision making, i.e. in the strategic and operational realm, Information Operations provide the basis from which planners designate specific targets. This designation may rest upon facts, predicted political results, or any other information that drives a state to use their military Instrument of Power (IOP).

Information is the germ of a rational decision process. Therefore, an enemy may use IO to support goals that conflict with our own. We must prevent this by achieving Information Superiority. Joint Vision 2010 defines Information Superiority as, "The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[1] Logically, to gain Information Superiority we must conduct Information Operations. Given the definition of the former allows us to define the latter. For purposes of this paper, then, Information Operations is defined as the collection, processing, and dissemination of information.

IO can function using information that might not be factual, accurate, or immutable. It must only be believable, or even simply possible, to drive reaction. A simple example can be seen when a bomb threat causes the evacuation of a building. The bomb may or may not even exist, but the possibility that it *might* still results in an evacuation. This point separates IO from technology. Technology, particularly in the so-called "Information Age," improves collection, processing, and dissemination. This makes technology important to IO. However, it does not

necessarily change how people react to the raw information used in IO. Just as a child can call in the bomb threat in the example given above, false information inserted using very low technology can temporarily paralyze a superpower.

Information Operations do not necessarily occur in purely military channels even if conducted for military leverage. The international media, with its vast reporter network and real-time video relay capabilities, delivers information to decision-makers and the public with colossal impact.

A case in point occurred in Somalia on October 3-4, 1993. Elite US Army Rangers and Delta Force members were ambushed in Mogadishu as they attempted to rescue a downed Black Hawk helicopter crew. What followed was a 17-hour firefight resulting in 18 Americans killed and 84 wounded. The media aired films of the mutilated bodies of US soldiers being dragged through the streets. The US public and congress reacted with immediate revulsion. On October 7, President Clinton ordered all troops withdrawn by March 31, 1994. A short video clip pumped into American households did in three days what Somali warlords could never do by force—quickly getting American military forces out of Somalia.

Could either foreign governments or non-governmental entities use the media in pursuit of their own purpose? We need only look at cases such as Kosovo and various Greenpeace activities to answer this question. Both foreign and domestic forces hostile to US interests will undoubtedly seek to shape future conflict using the collection, processing, and dissemination of information via the media. They will, in fact, engage in Information Operations. Understanding the power this gives presumably weaker adversaries helps to define an important, non-military facet of IO. Enemies of US national interest will undoubtedly exploit worldwide instantaneous media contact via the Internet.

The Cyber-Dimension

2010: Computers are the new Superpowers. Those who control them control the world.

—Tom Clancy

A particularly interesting aspect of IO resides in the cyber-dimension. Each day, consumer services, e-commerce, and data are added to the World Wide Web at geometrically increasing rates. Every hour of every day sees hundreds of thousands of visitors to the Web. While most of these visitors engage in benign activities, there are some that seek to vandalize or do harm to others. These interlopers range from individual "hackers" to foreign government sponsored cyber-terrorists. With ever increasing Web utilization and dependency comes a corresponding increase in avenues for potential incursion. Both commercial enterprises and government agencies recognize this situation and expend tremendous amounts of time and resource countering this threat. For example, each year brings the release of thousands of new computer "viruses." So many that a multi-million dollar industry exists around the development and sale of fixes and "immunizations" against these threats.

Worldwide concern over the so-called "Y2K bug" provides us insight on the extent computers have become part of our daily lives. Just the possibility of computer problems when the calendar rolled-over on January 1, 2000, caused some people to cancel their flights, hoard cash, and stockpile survival materials. Worries over an accidental Inter-continental Ballistic Missile launch, or the false indication of a launch, prompted the US and Russian governments to exchange missile officers to monitor and report on any unusual activities. With such effort expended to counter and prepare for Y2K, we can see that the information trafficked via computer is critical to our way of life. Both offensive and defensive Information Operations can therefore flourish in the cyber-dimension. Understanding this helps define the cyber facet of IO.

IO, as an Act of War

With such global reliance on information functions, it is easy to understand *defensive* IO. Passive defensive IO measures taken to protect from situations and threats, like those described above, seem intuitively acceptable and within the bounds of privacy and sovereignty. This contrasts sharply with *offensive* IO. Active offensive IO actions taken to leverage some advantage, or cause harm, may not be "acceptable" behavior. Offensive IO can be segregated into two principle levels based upon the actor(s) government/state-based affiliation. Individual(s) or a non-governmental group engaged in offensive IO might be dealt with by local, national, or international law enforcement authorities. A state sponsored or directed offensive IO activity, on the other hand, can only be dealt with through the action of other states. Offended states may pursue remedy using any or all of the IOP's at their disposal. At some currently undetermined level of perceived aggression, an offended state may consider offensive IO an *Act of War*. Any government engaging in Information Operations must therefore exercise great care.

Considering IO as a "Place"

As shown above, Information Operations raise issues, concerns, and opportunities relevant to the way the United States defends itself. What, then, are the areas appropriate for the US Department of Defense's involvement in IO? Considering IO to exist in a "place," as some suggest, may help to answer this question. Obviously not a place in the traditional sense of the term because information, and therefore IO, is not geographically constrained. Consider, instead, IO as a place more analogous to cyber-space. We might even call it "Information-space" or "info-space" for short. Envisioning IO in this manner allows us to specify a portion of info-space as a "battlespace" where DOD can conduct offensive and defensive actions to support more traditional, geographic battlespace(s) or Area(s) of Operation (AO).

Literature Review

The US government demonstrates a great deal of concern over the protection of cyber-based information systems and certain critical infrastructures. In May 1998, President Clinton signed Presidential Decision Directive 63 (PDD 63), entitled "The Clinton Administration's Policy on Critical Infrastructure Protection." This directive states:

> Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failures, human error, weather and other natural causes, and physical and cyber-attacks. Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security.[2]

The President established a national goal that by May 2003, the US will achieve and maintain the protection of critical infrastructures from intentional acts. PDD 63 cites three specific critical functional areas for protection. First, the Federal Government must be capable of performing essential national security missions and ensure the general public health and safety. Second, state and local governments must be able to maintain order and deliver minimum essential public services. Lastly, the private sector must have the ability to ensure orderly functioning of the economy and deliver telecommunication, energy, financial, and transportation services.

PDD 63 establishes a structure and directs specific Lead Agencies for "Sector Liaison" and "Special Functions." A Sector refers to a critical infrastructure area that could be a target for significant cyber or physical attack. Sector Liaisons bridge between public and private

counterparts within a sector. Special Functions refer to the critical infrastructure areas that must be chiefly performed by the Federal Government. PDD 63 designates twelve government agencies with Lead Agency responsibilities. DOD is the Special Function Lead Agency for the very broad Special Functions area of National Defense.

Two primary warning and information centers, the National Infrastructure Protection Center (NIPC) and the Information Sharing and Analysis Center (ISAC), maintain the critical infrastructure protection directed by PDD 63. NIPC is responsible for conducting critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response functions for the Federal Government. All executive departments and agencies support NIPC. Depending upon the decision of the President during special situations, NIPC may be placed in a direct support role to DOD or the Intelligence Community. ISAC is designed by private sector representatives and serves as a mechanism to facilitate, but not interfere with, the movement of information within the government-industry partnership. ISAC possesses a high degree of technical focus and expertise necessary to be a clearinghouse for information between and among sectors.

As discussed earlier, DOD is the Special Function Lead Agency for the broad area of National Defense. DOD's typical role is to assist federal agencies and the private sector to develop security-related best practice standards. The magnitude and complexity of this role is unpredictable, but we can expect demands on DOD resources to increase proportionately to national cyber-dependency. Working with NIPC, ISAC, plus eleven other Federal agencies presents great challenges to DOD leadership and should be managed from the highest Joint levels—hence this is one significant reason to establish an IO CINC.

By 2002, the world could have 500 million personal computers and 19 million individuals with skills in cyber-attack.[3] During Operation Allied Force in the spring of 1999, hackers with Internet addresses resolved to China launched coordinated cyber-attacks against the US. Chinese government involvement is unknown, but attacks came after US forces accidentally bombed the Chinese Embassy in Belgrade and China's government maintains very tight control over Internet access.[4] In January and March 1999, a sustained and coordinated intrusion into DOD networks may have originated in Russia.[5] Again, no released evidence implicates the Russian government. In fact, cyber-attacks on DOD were up over 300 percent from 1998 to 1999 according to General David Kelley, Director of the Defense Information Systems Agency (DISA). Nearly every day brings news of another cyber or IO related attack on DOD or commerce. It is easy to understand why our military is greatly concerned about IO. The Navy alone plans to spend $10 billion on IO over the next five years.[6] President Clinton's Fiscal Year 2001 Budget proposal contains $1.5 billion designated for critical infrastructure defense.[7] Government IO spending and investment on this scale shows commitment but is dwarfed by the billions that will be spent by the private sector. This spending disparity is inevitable but likely means most governmental critical infrastructure defense initiatives will remain reactive in nature.

The Military's Role

Federal Government dollars alone will not protect critical infrastructures. A coherent, forward-looking strategy must give direction for IO in support of national defense. To accomplish this, the National Security Strategy (NSS), National Military Strategy (NMS), Joint Chiefs of Staff's Joint Vision 2010 (JV 2010), Joint doctrine, and service doctrine each recognize the importance of IO to our present and future defense. The NSS places protection of critical national infrastructures next to managing consequences of Weapons of Mass Destruction

(WMD) incidents. Both are considered "Emerging Threats at Home." The NMS also puts WMD and Information Warfare together as "Asymmetric Challenges." It states Information Superiority, like air superiority, must be achieved in the battlespace through both offensive and defensive operations. JV 2010 envisions not just the unqualified importance of IO but raises the ante by flatly stating we must have Information Superiority over an adversary. Joint and service doctrine all take their cues from the NSS, NMS, and Joint Vision statements to provide the military direction on how to proceed with IO.

IO in the Private Sector

Our government is not the only party very concerned with IO and critical infrastructure defense. Private sector industry, groups, and individuals have Information Operations of their own that rely upon shared critical infrastructures. Increased use of a shared infrastructure, such as the Internet, translates into increased reliance upon continuity and viability of that information system. In a world where foreknowledge of a company's quarterly profits can translate into millions of dollars on the stock market, the quest for that information may become fierce and unscrupulous.

Industrial espionage is a fact of everyday life in commerce as competitors seek to lever any advantage. One avenue for this is via industrial cyber-attack. Extreme and expensive measures are often taken to protect against this threat. Reports of an information defense, particularly a cyber-defense, compromise often translates into stock price drops and the loss of large amounts of hard-earned customer faith. Preventing information compromise is therefore a high priority. While exact amounts of private sector spending on offensive or defensive IO are unavailable, undoubtedly figures exceed multiple millions of dollars annually.

Industry is often reluctant to partner with government on IO. This not necessarily borne of distrust but may result from desire to remain proprietary. Partnering with government agencies means sharing information. Reluctance to share this information is reasonable from the private sector point of view. Take, for example, a corporation that discovers an internal IO vulnerability and seeks help from ISAC to correct their problem. If knowledge about this vulnerability becomes available to the market, stock prices and consumer confidence may suffer. PDD 63 recognizes issues concerning private partnering and seeks to encourage IO evolution to prevent vulnerabilities from becoming critical infrastructure failures. DOD's role as a Special Function Lead Agency is vital to the success of this effort since the military typically enjoys public confidence ratings significantly higher than other Federal agencies.

Notes

[1] CJCS. *Joint Vision 2010.* Washington, DC
[2] PDD 63. *The Clinton Administration's Policy on Critical Infrastructure Protection.* Washington, DC, May 1998.
[3] Correll, John T. "War in Cyberspace." *Air Force Magazine* 81, no. 1 (January 1998), 32-36.
[4] Brewin, Bob. "Cyberattacks Against NATO Traced to China." *IDG* (September 2, 1999).
[5] Vernon, Danuel. (Cyberattacks Against DOD Up 300 Percent This Year." *CNN* (November 5, 1999)
[6] Abel, David. "Navy Slates $10 Billion For Information Operations." *Defense Week,* (February 8, 1999).
[7] Budget of the United States Government, Fiscal Year 2001

Part 3

Issues and Analysis

Information Operations span space, time, economies, borders, and people. While this has always been true, IO themselves are critical activities in today's "Information Age." This results from our insatiable thirst for increases in information exchange velocity, accuracy, and quantity. Information thirst drives technological evolution, which causes even greater thirst. As this snowballing cycle gains mass and velocity, the direction it takes may depend on how people of the United States, through their political leadership, decide to engage in IO. The issue at hand for DOD centers upon establishing a command structure that best supports future national defense tasking. Consideration of current national policy, critical infrastructure defense, legal issues, and expected military uses of IO helps address this important issue.

National Policy

Our national policies help "set the table" for both public and private concerns to gather and prepare against expected threats. Growing potential vulnerabilities resulting from Information Age developments help bring diverse guests to this table. DOD has a permanent seat here and must be able to interact with private sector companies and other government agencies. This seat must be occupied and supported by the proper military organization because ability to interact appropriately is vital to national defense and future military IO. Without these abilities, DOD may fail for two reasons. First, DOD could not effectively fulfill its PDD 63 mandated role of

assisting federal agencies and the private sector with implementation of best practice standards. Second, in times of crisis DOD will be supported by other agencies. The military representative must be capable of determining, and coordinating, resource and action requirements. Effective response to crisis demands the shortest appropriate decision cycle to achieve Information Superiority over an opponent. Military representation not empowered to make decisions, allocate resources, or demand National Security Council direct attention undermines DOD's ability to fulfill this critical responsibility.

Critical Infrastructure Defense

National critical infrastructures are both physical and cyber-based systems essential to minimum operations of the economy and government. Defense of these infrastructures requires both physical and cyber-based attention. While issues such as Y2K increase awareness of the cyber aspect, thus far the US has fortunately avoided physical attack. Many of the critical infrastructures are privately held. For example, various companies and co-ops own much of the nation's power grid. Do these private concerns have adequate physical security to protect the grid? If not, can cyber control of the entire grid be gained through an unprotected remote node? Defense of a critical infrastructure may be only as strong as its weakest link. DOD has arguably the strongest skill set available for assisting with the establishment and maintenance of viable physical and cyber-based security for publicly or privately held national critical infrastructures.[1] The ability to develop and draw these skills together in peace or conflict requires DOD to invest adequate power and authority in IO command and control. This IO command and control, along with the critical need to prepare both deliberate and crisis response plans are compelling reasons to establish an IO CINC.

Legal and Ethical Issues

IO is awash with legal and ethical issues. Not surprising in a society that properly holds individual rights and privacy as sacred tenets. Existing law, however, often lacks applicability in the IO realm. New law will germinate as IO-related ethical issues evolve.

Any government agency engaged in gathering information on people or their private activities may soon find civil or criminal lawsuits and testimony to Congress dominating their agenda. DOD must avoid this entanglement, particularly given law enforcement limits imposed by the *Posse Comitatus Act.* Under the interpretations of this act, the military may only assist US civilian law enforcement authorities. Despite this, future situations may develop where the President directs DOD to be the "supported agency" during time of crisis to national critical infrastructures. Then DOD may have to direct law enforcement activities against US citizens. DOD awareness of potential IO legal issues is essential to establishing Information Superiority. Pre-planning at the strategic level can prevent inadvertent legal or ethical violations.

IO as an Instrument of Power

IO concerning other governments or non-state agents is another issue of growing concern. Information is considered an Instrument of Power (IOP). Information Operations embody how states use this IOP. The great Chinese philosopher Sun Tzu some 2,500 years ago recognized the importance and power of IO in his stratagem of using the "Sheathed Sword" to triumph without fighting. He considered this the highest form of "generalship." We can draw two inferences from Sun Tzu's wisdom. First, IO as an IOP can allow a military to prevail during conflict. Second, the military should develop skills necessary to effectively wield this IOP. China recognizes this as evidenced by Chang Mengxiong's paper that first appeared in *China Military*

Science (Spring 1995). He serves on the Committee of Science, Technology and Industry of the System Engineering Institute in China. He writes:

> Numerous facts show that we are in the midst of a new revolution in military technology in which electronic information technology is the central technology. This technology provides unprecedented applications for the development of new weaponry. Information acquisition will be the main distinction of 21st-century military forces. Military battles during the 21st century will unfold around the use of information for military and political goals.

Realizing states could consider certain IO as "acts of war," particularly if aimed against any of their critical infrastructure, highlights the need for very cautious, and well considered, use of this IOP.

Since IO can come in both offensive and defensive forms, selective use and application of IO becomes an issue. Just as we expect air superiority to result from superior aircraft, skilled pilots, and sound aerospace doctrine, Information Superiority demands state-of-the-art technology, skilled technicians, and sound IO doctrine. DOD invests heavily in all three of these areas. Sound IO doctrine is the linchpin needed for success of the other two. Development and maintenance of Joint IO doctrine is crucial to how the military selects and applies offensive and defensive IO. Responsibility for this doctrine should be vested in an IO CINC.

Few would argue a state's right to defend itself using any tool, including IO. Offensive operations, however, always seem to be under the glare of skeptical public opinion. Offensive IO is no exception. This is one example of the value in considering info-space. Envisioning IO occurring in an information battlespace dimension of its own may help focus military actions while helping the public to understand and support these actions. Military activities relating to an enemy's threat "*info*structure" may help frame doctrine and debate. Hesitation in supportive public opinion can end a military operation faster than an enemy's guns. Remember Somalia?

IO in the Unified Command Structure

> *Unity of effort* ***requires coordination among government departments and agencies*** *within the executive branch, between the executive and legislative branches, nongovernmental organizations, and among nations in any alliance or coalition.*
>
> — Joint Publication 0-2

Unity of effort is not only the most logical approach to national defense, it is also the law. The Goldwater-Nichols Department of Defense Reorganization Act of 1986, consistent with the congressional declaration of policy in section 2 of the National Security Act of 1947 (50 U.S.C. 401) seeks to "increase attention to the formulation of strategy and to contingency planning," and "to provide for more efficient use of defense resources." The Unified Command structure provides the roles, missions, and functions needed to fulfill this legal requirement.

The current Unified Command organization consists of five Unified Commands with responsibilities based on geographic area. There are also four Unified Commands with responsibilities based on function. Each is headed by a four star (O-10) Commander-in-Chief (CINC) that has a direct line to the National Command Authority (NCA). The basis for this current organizational structure can be found in Joint Publication 0-2's discussion of the Military Component of National Security Strategy:

> As the national leadership generates national objectives and a national security strategy to pursue them, the leadership will also devise--or modify--the **military instrument of national power** as a component of national security strategy. This strategy takes the form of objectives for the development of **broad military capabilities**, their **worldwide posture**, and their **functional and geographic orientation**. In the event of armed conflict, this strategy will take the form of military objectives for the establishment of military conditions essential to support national security objectives and terminate the conflict on terms favorable to US interests. These objectives need to be coordinated with associated diplomatic, economic, and informational objectives.

Joint Publication 0-2 states each CINC has the Combatant Command (COCOM) authority necessary to, "ensure that the authority of the commanders of the unified and specified combatant commands is fully commensurate with the responsibility of those commanders for the accomplishment of missions assigned to their commands." This gives them several powers including Planning, Programming, Budget System (PPBS) input, assignment of subordinate commanders, and relations with DOD agencies. Joint Publication 0-2 also states, "The combatant commanders are responsible for the development and production of joint operation plans. During peacetime, they act to deter war and prepare for war by planning for the transition to war and military operations other than war. During war, they plan and conduct campaigns and major operations to accomplish assigned missions." These powers align well with responsibilities placed upon DOD by PDD 63.

When needed, a Joint Task Force (JTF), headed by a Joint Force Commander (JFC), is established and is subordinate to a CINC. Per Joint Pub 13-3, each JFC should establish a fully functional IO cell that is, "sufficiently flexible to accommodate a variety of planning and operational circumstances." This cell is elaborate and built from dispersed resources. Placing burden for constructing this cell on the JFC, particularly during a fast-paced crisis, may not be prudent. Given the recognized importance of IO, and the need to rapidly gain Information Superiority in crisis, the national interest may best be served by establishing an IO CINC capable of simultaneously supporting several JFCs around the world. A JFC established by an IO CINC could also be the most effective means of managing crises occurring in info-space.

Notes

[1] Harreld, Heather & Busse, Torsten. "Reno Unveils Plan to Protect Infrastructure." Federal Computer Week, (March 2, 1998).

Part 4

Conclusions

When the president asks whether the United States is under Information Warfare attack--and, if so, by whom--and whether the U.S. military plan and strategy is vulnerable, a foot-shuffling "we don't know" will not be an acceptable answer.

—Roger C. Molander, Andrew S. Riddile, Peter A. Wilson,
Rand Corporation

Summary of Findings

Individual, corporate, US, and international dependence on information and its supporting technology continues to grow at amazing rates. With this dependence comes the danger from hackers, terrorists, some non-governmental organizations, and hostile foreign states. Each of these understands the asymmetric power available through application of IO. In fact, many have used IO effectively with dramatic results. We can fully expect others to follow suit and launch IO campaigns within the information "battlespace."

The President, through PDD 63, recognizes the need for protecting those national critical infrastructures needed to support activities in the Information Age. DOD has a very important role outlined in PDD 63. Fulfilling this critical national defense role requires attention, cooperation, and support at the very highest levels of military leadership. To this end, DOD must train, prepare, and be available to ensure critical infrastructure protection is achieved and maintained.

IO is a very broad topic with implications across all levels of military operations. Achieving Information Superiority requires state-of-the-art technology, skilled technicians, and sound IO doctrine. Fortunately, each military branch recognizes IO as a key feature in future national defense and billions of DOD dollars over the next few years will pursue IO skills and technology. This spending, and most Joint doctrine, currently focuses principally on the operational and tactical end of the IO spectrum. Greater strategic vision in the form of strategic doctrine would serve the nation better as IO implications unfold over time. Responsibility for this doctrine can only reside at strategic, Unified levels of command.

Principle Conclusions and Recommendation

Information itself is virtually a Center of Gravity (COG) in the military sense of the term. Is it time for an "IO CINC?" If DOD is to shape, respond, and prepare for future IO at home, abroad, and in "info-space," the answer is a resounding "YES." Only a Unified Command responsible for Information Operations could provide the vision, span of control, and resource horsepower our nation deserves for the defense of critical infrastructures, and for the development of IO doctrine to focus DOD resources. Only an IO CINC can provide regional CINCs the rapid response capability needed for modern crisis response operations. Finally, only an IO CINC could adequately manage future threats residing only in "info-space" or cyber-space. Gaining Information Superiority against such a threat will not involve drawing lines on a map or most other traditional warfare constraints. Our nation demands the military be capable of full spectrum defense. Doing this day in and day out requires an IO superstructure well above the JFC "cell" level.

Adding IO responsibilities to an existing CINC, such as US Space Command, may seem an attractive alternative to establishment of a totally new Unified Command. While this option may

yield savings in infrastructure and manpower, it fails to recognize the truly unique focus and skill-sets needed to conduct IO. US Space Command, for example, may indeed be able to support and conduct many present-day Information Operations. However, US Space Command's focus is, appropriately, space. Fitting IO into this structure could restrict DOD's ability to conduct successful offensive and defensive Information Operations in the future. We cannot afford this restriction given the asymmetric threat potential inherent in IO.

Implications

Expanding the Unified Command structure to include an IO CINC has many implications. The most restrictive of these is, of course, dollars. Constructing such an IO superstructure would be very expensive. However, we can be certain that potential adversaries are currently making this very investment. To quote Sun Tzu, "Hostile armies may face each other for years, striving for the victory that is decided in a single day. This being so, to remain in ignorance of the enemy's condition, simply because one grudges the outlay of a hundred ounces of silver in honors and emoluents, is the height of inhumanity." The ancient philosopher is talking about investing in information. While Information Operations have changed over the last 2500 years, the wisdom of this philosophy has not.

Bibliography

Abel, David. "Navy Slates $10 Billion For Information Operations." *Defense Week*, (February 8, 1999).

AFSC Pub 1. *The Joint Staff Officer's Guide.* Washington, DC, 1997.

Becker, Elizabeth. "Pentagon Set Up New Center For Waging Cyberwarfare." *The New York Times News Service* (August 10, 1999).
Brewin, Bob. "Cyberattacks Against NATO Traced to China." *IDG* (September 2, 1999).
Bridis, Ted. "High-Tech Crime-Fighting Lab Unveiled." *AP* (September 25, 1999).

CJCS Instruction (CJCSI) 3210.01.
CJCS. *Joint Vision 2010.* Washington, DC
CJCS. *National Military Strategy of the United States of America.* Washington, DC, 1997.
Clancy, Tom. *Net Force.* Berkley, 1999.
Correll, John T. "War in Cyberspace." *Air Force Magazine* 81, no. 1 (January 1998), 32-36.
Critical Infrastructure Assurance Office. *Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructures.* Washington, DC. July 1998.

Department of Defense press release. *Joint Task Force on Computer Network Defense Now Operational* (December 12, 1998).

Gansler, Jacques S. *Achieving Dominant Battlespace Awareness Through Advanced Information Technology.* Remarks to the Armed Forces Communications and Electronics Association (AFCEA) at the J W Marriot Hotel, Washington, DC (September 29, 1999).

Harreld, Heather & Busse, Torsten. "Reno Unveils Plan to Protect Infrastructure." *Federal Computer Week*, (March 2, 1998).

Joint Chiefs of Staff. *Information Warfare: a strategy for peace...The decisive edge in War.* Washington, DC, 1996.
Joint Pub 3-13.1. *Joint Doctrine for Command and Control Warfare (C2W)* (date).

PDD 62. *Combating Terrorism.* Washington, DC, May 1998.
PDD 63. *The Clinton Administration's Policy on Critical Infrastructure Protection.* Washington, DC, May 1998.

President of the United States. *A National Security Strategy for a New Century.* Washington, DC, 1998.

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

Stanton, John J. "White House Plans Cyber Homeland Defense Effort." *National Defense* 83, no. 540 (September 1998), 24-25.

Stanton, John J. "Dilemmas Abound in Crafting National Information Policy." *National Defense* 82, no. 529 (July-August 1997), 52.

Van Cleave, John. (LCDR, USN). *Critical Factors in Cyberspace.* Naval War College Report (Newport, RI, 1997).