Should We Create an Information Operations Command?

MCWAR 1998

Subject Area Topical Issues

SHOULD WE CREATE AN "INFORMATION OPERATIONS COMMAND"?

by
Lieutenant Colonel Arlow A Julian
United States Marine Corps

29 April 1998

Submitted in Partial Fulfillment
of the Requirements for the
Marine Corps War College
Marine Corps University
Marine Corps Combat Development Command
Quantico, VA 22134-5067

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
1998		**00-00-1998 to 00-00-1998**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Should We Create an Information Operations Command?	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Marine Corps War College,Marine Corps University,Marine Corps Combat Development Command,Quantico,VA,22134-5067**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**52**	

ABSTRACT

The purpose of this paper is to propose the creation of an **"Information Operations Command**". The future of success of "Joint Vision 2010" is based on the ability of the United States to obtain "Information Superiority". Smaller forces with enhanced situational awareness, increased speed of command and control, and a thorough understanding throughout the force of the information available will result in a higher degree of performance with less overall military forces.

"Asymmetrical Warfare" is in the news. The National Information Infrastructure (NII) and the Defense Information Infrastructure (DII) are essential for the future security of the United States and systems along with procedures must be developed for their protection. A single point of contact within the Department of Defense is needed to lead the Department's efforts in this new arena.

A 'vision' of the potential of an Information Operations Command is contained in Chapter 1, "Bits and Bytes into the Night — Operation Crystal City". Chapter 2 addresses ongoing initiatives within the Department of Defense by the Joint Staff and the Services to attain Information Superiority. The proposal to create a new Commander-in-Chief will generate tremendous controversy. The potential for a "holistic" approach to Information Operations is high. A wide range of proposed missions/ responsibilities of the Information Operations Command and who might be designated the "Commander-in-Chief" of this new command is examined.

Ultimately, if not a "CINC" some type of "Czar" to get a handle on this crucial aspect of 21st Century warfare will be required.

TABLE OF CONTENTS

Chapter 1

Bits & Bytes, Into the Night
"Operation Crystal City"

What follows is a fictional account of an operation in the future and how an ***Information Operations <u>Command</u>*** might play a critical role. The intent of this piece is to portray the significant impact which could be made by an Information Operations Command during a crisis. Of note here is the attempt to portray the responsiveness and rapidity with which crucial decisions could be made.. A number of the organizations portrayed are the fictional creation of the author. While the overall capabilities represented do not currently exist in any coordinated fashion, bits and pieces are certainly possible today. The year is 2005.

<u>0200 Saturday, European Theater Command Center, Stuttgart, Germany</u>. The Command Duty Officer answers the telephone to find the Defense Attaché from Country Green on the line. Meanwhile, a watchstander has pulled up a flash message from the Embassy in Country Green, action to the Department of State, information only to the Joint and European Command Staffs. Rioting has broken out in the capital city of Country Green. A neighbor, Country Red, has crossed the border, a territorial violation, with the announced purpose of annexing Country Green. The despotic ruler of Country Red has previously shown a propensity to employ chemical weapons and is threatening their use once again should Country Green resist. The quest to escape Country Green has completely shattered the government's control over the population. Anarchy reigns.

<u>1000 Saturday, United States Embassy, Country Green</u>. The democratically

elected president of Country Green has appealed to the United States Ambassador for United States military intervention in order to stabilize the internal security situation and force Country Red military forces to withdraw back to the recognized borders between the two countries.

1025 Saturday, Washington D. C. The United States National Command Authority is informed and agrees to have the United States take a proactive role, triggering a massive United States response. "Operation Crystal City", on the African continent, is in motion.

1122 Saturday, The Pentagon, Washington, D.C. Within minutes of notification, the Joint Staff has issued an Alert Order to the Commander in Chief, United States European Command and various supporting Commander's in Chief around the globe.

1145 Saturday, CONUS and Europe. On both sides of the ocean, the United States military machine swings into action. Orders are transmitted electronically notifying numerous commands of the developing crisis and the responsibilities assigned. In Illinois, the command center for the United States Transportation Command begins the process of notifying the Air Mobility Command, for strategic aviation lift and the associated tanker support required to move troops from multiple locations into the theater of operations. While in Florida, the United States Special Operations Command begins preparation for overseas deployment, expected to be requested by the supported theater commander, of unique specialized skills and units. The United States Atlantic Command generates an alert order to the XVIII Airborne Corps and the II Marine Expeditionary Force notifying both commands of the crisis and their probable future role(s). Unique chemical, biological response units are notified and instructed to be prepared for

immediate deployment.

1230 Saturday. Global Operations Center. United States Information Operations Command. Washington. D. C. The Senior Watch Officer has contacted the Information Command J3 Operations Officer and recommended that the defense posture for the National Information Infrastructure and the Defense Information Infrastructure be upgraded immediately. This requires notification and activation of the "Federal Government Information Infrastructure Defensive Operations Coordinating Group". Key networks such as those operated by the Federal Aviation Administration, the Federal Reserve, Department of Energy and other essential aspects of American life will activate pre-established firewalls and provide significant increases in personnel on duty to detect and counteract hostile intrusions into crucial information networks. The J3 immediately concurred, recalling the catastrophic North Eastern power grid shutdown of 2003 which occurred when another nation, who was not expected to possess an Information Warfare capability, objected to United States military operations.

1315 Saturday, United States European Command, Stuttgart, Germany. The United States European Theater Command Center has been generating orders and instructions to its assigned forces. A Joint Task Force Commander has been designated to be the Commander in Chief's, United States European Command, senior military officer in the area of operations. Forces from Europe and the Continental United States will make up the Joint Task Force.

1330 Saturday, Washington, D. C. The National Command Authority has been extremely clear and specific in issuing guidance…*"Get organized quickly. Use the inherent advantages of United States military forces. Turn the situation around...*

fast...before the entire region is affected"

1500 Saturday, Global Operations Center, Information Operations Command, Washington. D. C. and the Regional Operations Center, Information Operations Command, Stuttgart, Germany. The Joint Task Force Commander is faced with command and control of multiple forces located in various locations. He will be aided in this task by the forces of the newest of the supporting Commander's in Chief, the United States Information Operations Command. Upon receipt of the Joint Staff warning orders, the Global Command Center of the Information Operations Command commenced a series of actions, well rehearsed and orchestrated to enhance one of the key enablers of the Joint Vision 2010. Located in Washington, D. C., the Headquarters of this new command, has the ability to marshal the information resources (systems, networks, and technologies, of both the Federal Government and Industry) of the United States should this action be required.

The Global Operations Center was immediately in contact with its Regional Operations Center in the United States European Command which is located adjacent to the United States European Command aboard Patch Barracks, Stuttgart, Germany, for ease of staff coordination, in facilities previously occupied by the Defense Information Systems Agency Europe. A liaison team was immediately dispatched to coordinate with the Theater Staff.

1600 Saturday, Global Operations Center, Information Operations Command. Washington. D. C. and the Regional Operations Center, Information Operations Command, Stuttgart, Germany. Status checks on long haul communications satellite systems, the Defense Satellite Communications System (DSCS) and the single channel

satellite (manpack-tactical) constellations are conducted. Availability of resources to support the operation is determined. Commercial alternatives are examined. Extensive coordination, via video teleconference, with the United States Space Command is ongoing.

1645 Saturday, Joint Task Force Facility, Kelley Barracks, Stuttgart, Germany. An "Initial Information Support Team" providing limited secure voice (satellite communications and telephone), data, facsimile, and austere video teleconferencing capability arrives. It was dispatched from the Regional Operations Center, Information Operations Command in Stuttgart to link up with and provide support *directly to* the Joint Task Force Commander, for the duration of the operation. This Information Support Team is prepared to operated in any environment chosen by the Joint Task Force Commander, sea, land, or air. This specifically trained team is familiar with the intricacies of operating aboard United States Navy ships, Air Mobility Command strategic transport aircraft, and a variety of land-based situations. This support package is intended for the Commander, not the Joint Task Force Staff.

1800 Saturday, Global Operations Center, Information Operations Command, Washington, D. C. Based upon initial coordination between the Regional Operations Center in Stuttgart, Germany and the Theater Staff, the United States Information Operations Command contacted the United States Transportation Command and requested a strategic lift aircraft to be provided to support the Joint Task Force Commander enroute to the area of operations and to function as an initial temporary command center for the Joint Task Force at a Forward Operating Base or designated Intermediate Support Base should the need arise. The aircraft can fly to any of a number

of locations within CONUS to accept the specially designed aircraft equipment modules designed and maintained by the Information Operations Command. This capability is several orders of magnitude more robust than the package the Initial Information Support Team deployed with.

0400 Sunday, Regional Operations Center, Information Operations Command, Stuttgart, Germany. The Regional Operations Center, in coordination with the European Theater Staff, the ever-growing Joint Task Force Staff, and its own Global Operations Center, has made input(s) into the "Time Phased Force Deployment Data" in support of the Joint Task Force Main and Forward Headquarters requirements for information operations systems support. This includes a full Ground Mobile Forces (GMF) satellite capability providing robust secure telephones, facsimile, data, video teleconferencing, switchboards, servers, desktop computers, and all the necessary ancillary devices (generators, telephone instruments, etc) to support deployed staffs. Personnel to setup, maintain and operate specific unique items are included. These are the technical experts intended to support the "operators" of the Joint Task Force. A significant single channel secure satellite capability, with operators, has been provided for the Joint Task Force, Joint Operations Center(s) (JOC). No "user owned, user operated" here. This is a "turn key" operation which the Joint Task Force personnel will fall in on.

The Commander, European Regional Operations Center has chosen Team Alpha, who has recently concluded an Emergency Deployment Readiness Exercise (EDRE) at a U.S. Army training facility in Germany, coincidentally training with the officer who has just been designated the Commander of the Joint Task Force. The Team Alpha Executive Officer and the Assistant Operations Officer, both well known to the newly designated

Task Force Commander, link up with the growing Joint Task Force Staff, at the Joint Task Force Facility, Kelley Barracks, Stuttgart, Germany in order to receive guidance, get updates, and to inform the staff of capabilities which can be made available. This two man liaison team from Team Alpha will remain with the staff throughout the deployment. It is separate from the Initial Information Support Team, provided to the Commander, sent by the Regional Operations Center.

1140 Sunday, United States Embassy, Country Green. The crisis in Country Green continues to intensify. The Ambassador has requested a military Information Support Team to provide linkage between the Country Team, Department of State, the European Theater Command Center, and the assembling Joint Task Force. The Joint Staff and the Department of State have concurred with this request and passed the requirement to the Information Operations Command (info to the European Theater Command Center). Fortunately, just such a team was exercising in Egypt under the cognizance of the United States Central Command. Coordination between the European Command and Central Command resulted in the removal of the team from the Egyptian exercise and its subsequent redeployment into Country Green. Within minutes of arrival at the United States Embassy in Country Green, a limited capability was established. Within hours, the United States Embassy was fully in the network, sending and receiving information by the most modern means available.

1300 Sunday, Various Locations Throughout the World. The Command Centers of the Joint Staff, European Command, Atlantic Command, Central Command, Special Operations Command, Transportation Command, Space Command, and the Information Operations Command are alive with activity. Electronic Mail, supported by extensive

graphical representations of plans, timelines, intelligence information, and all manner of pieces of information required to make an operation successful were flowing seamlessly between all locations with a speed that only today's technology could provide. Multiple video teleconferences were occurring. On average, each command was participating in 4 video teleconferences: policy and force structure, deployment, logistics support, and information systems. Players moved seamlessly between conferences. Secure telephones buzzed with the hum of activity as staff officers conducted the business of military operations in support of a crisis.

1500 Sunday, Joint Task Force Facility, Kelley Barracks, Stuttgart, Germany. The Joint Task Force Commander has requested that a civilian team with specialized skills in chemical warfare, resident at a major university with ties to Department of Defense chemical response forces, be provided an Information Support Team to link their expertise with deployed chemical response teams and the Joint Task Force Headquarters. The request is approved by the Joint Staff and the tasking goes out to the Information Operations Command. A U.S. Army Reserve Information Support Team receives the task of providing the initial response. This unit is less than 3 hours driving time away from the university in question and will arrive on scene by nightfall.

1500 Sunday, Global Operations Center, "Black Operations Cell", Information Operations Command, Washington D. C. A crisis response team has activated to determine what recommendations to make to both the Joint Task Force Commander and the National Command Authority regarding Offensive Information Warfare operations against Country Red. Potential targets include the power distribution system, internal communications networks (telephone and data - both civilian and military), and the

banking system. Operations of this nature are highly sensitive and require National Command Authority approval.

1515 Sunday, Joint Task Force Facility, Kelley Barracks, Stuttgart, Germany. An Information Support Team for the Ministry of Defense, Country Green has been requested by the Joint Task Force Commander. After coordination with the United States Embassy Country Green, the Department of State, the Joint Staff and the Commander in Chief, United States European Command approval for this mission is granted. The European Theater Command Center passes the requirement on to the Regional Operations Center. An Information Support Team is dispatched to Country Green.

0015 Monday, Stuttgart Army Airfield, Stuttgart, Germany. The strategic airlift aircraft, previously requested by the Global Operations Center, Information Operations Command arrives. The "Information Support Modules" have been installed and were thoroughly tested enroute from CONUS to Europe. It is assigned to the Joint Task Force.

1500 Monday, Various Locations Throughout Africa. Intermediate Support along with Forward Operating Bases begin building up. At each location, information systems fully compatible with the Information Operations Command's global standards are installed. All manner of information begins flowing into and throughout the Joint Task Force.

1800 Monday, Primary Intermediate Support Base, Africa. The Joint Task Force Commander and his Battle Staff arrive on the specially modified strategic aircraft from Stuttgart, Germany and assume control of deployed forces using the internal aircraft information support modules as their Headquarters.

2230 Monday, Primary Intermediate Support Base, Africa. Team Alpha lands and

begins establishing the necessary infrastructure to support the Main Headquarters for Joint Task Force Crystal City. The Main Headquarters is currently operating out of the Joint Task Force Facility, Kelley Barracks, Stuttgart, Germany and will time their deployment so as to arrive approximately 18 hours after Team Alpha.

0600 Tuesday, Various Locations Throughout Africa. As combat forces arrive and assemble for future operations they are provided with the latest information available from intelligence, logistics, operations, and the myriad of other functional areas required to maintain forces which have been forward deployed in a crisis. A full exchange of information is occurring, every unit knows what is expected and what role the unit will play during the crisis.

0800 Tuesday, Primary Intermediate Support Base, Africa. Although the deployment of forces continues, the leverage obtained by the seamless information operations infrastructure has created a situation where the Joint Task Force Commander is ready to conduct operations. Fewer forces, with better "battlefield awareness" can begin to make a difference.

Chapter 2

The Requirement for Information Superiority

> The rapid evolution of technology has altered warfare. Forces on land, at sea, and in the air now reinforce and complement each other more than ever. The speed of communications and pace of events in the modem world have accelerated. Joint teams must be trained and ready prior to conflict.[1]

The Joint Task Force of the future will likely have elements spread over large geographical areas. Intermediate Staging and Forward Operating Bases will, in many instances, be located in areas surrounding the principle area of operations. The locations of ports, airfields, and the availability of fuel and rations are often determining factors in locating these facilities. The Commander must consider the following:

> The importance of an efficient joint force command structure cannot be overstated. Command, control, and communications should be reliable, survivable, flexible, interoperable, timely, and secure.[2]

The ability to effectively command under these conditions is essential for a Commander to accomplish all the assigned tasks/missions.

The following definitions are germane to understanding the challenges facing the Commander who is faced with the responsibility of exercising command.

> **Command and Control—(DOD)** The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. Also called C2.[3]

---

[1]Joint Publication 1, Joint Warfare of the Armed Forces of the United States, (Washington, D.C.: Joint Staff, May 1995), 2.

[2]Joint Publication 1, Joint Warfare of the Armed Forces of the United States, (Washington, D.C.: Joint Staff, May 1995), 4.

[3]Joint Publication 1-02, Approved Dictionary, (Washington D.C.,: Joint Staff, 23 March 1994 updated through April 1997), 111.

> **Command and Control System—(DOD) The** facilities, equipment, communications, procedures, and personnel essential to a commander for planning, directing, and controlling operations of assigned forces pursuant to the missions assigned.[4]
>
> **Command, Control, Communications, and Computer Systems—(DOD)** Integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander's exercise of command and control across the range of military operations. Also called C4 systems[5]

All the definitions of "Command and Control", "Command and Control System", and "Command, Control, Communications, and Computer Systems" imply that some type of structure(s) is provided to aid the Commander. In today's world that will generally be accomplished by “jury rigging" capabilities and units together to provide support to the Commander. "Work arounds" will be developed in order to resolve differences in compatibility between multiple locations/commands throughout the globe. The advent of the Global Command and Control System (GCCS) is a step in the direction towards a common operating environment. GCCS works best today in a fixed installation environment but far less effective with deployed forces primarily due to the communications architecture limitations.

The National Military Strategy (1997), Joint Vision 2010, Expanding Joint Vision 2010, and the Quadrennial Defense Review all look toward the future state of the Armed Forces of the United States. These future forces will be lighter, more mobile, more lethal, and operating under a wide range of conditions, i.e. environmental (NBC, weather extremes,

---

[4]Joint Publication 1-02, Approved Dictionary, (Washington D.C.,: Joint Staff, 23 March 1994 updated through April 1997), 111.

[5]Joint Publication 1-02, Approved Dictionary, (Washington D.C.,: Joint Staff, 23 March 1994 updated through April 1997); 112.

natural disasters, coalition, and unilateral). A common theme in all these documents is the requirement for the Armed Forces to possess an unchallenged edge in the ***Information Superiority*** arena. For instance:

> The *unqualified importance* (emphasis added) of information will not change in 2010. What will differ is the increased access to information and improvements in the speed and accuracy of prioritizing and transferring data brought about by advances in technology. ... Sustaining the responsive, high quality data processing and information needed for joint military operations will require more than just an edge over an adversary. We must have information superiority: the capability to collect; process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. Information superiority will require both offensive and defensive information warfare (IW)[6]

The "Emerging Operational Concepts" - Dominant Maneuver, Precision Engagement, Focused Logistics, and Full-Dimensional Protection are the cornerstone of the future of the United States Armed Forces.

"The basis for this framework is found in the improved command, control, and

[6]Joint Vision 2010, (Washington D.C., Chairman of the Joint Chiefs of Staff, 1997), 16.
[7]Joint Vision 2010, (Washington D.C., Chairman of the Joint Chiefs of Stan 1997), 19.

intelligence which can be assured by information superiority."[8]

> Information superiority...is *the key enabler* (emphasis added) for the C2 function. Optimum C2 in the 2010 environment will depend on seamless communications, all-weather real-time sensors, current and accurate data bases, and the resulting near-real-time situational awareness for the JFC and the entire chain of command. Joint information systems that produce seamless interoperability between services could well reside within a single national information architecture that is defined by national policy and focuses national efforts on the same 2010 goals. The complexity of this effort will require that the acquisition of information systems be coordinated at the joint level, ensuring that future systems are "born joint".[9]

Section III of the Quadrennial Defense Review, "Defense Strategy", identified the elements of information superiority (under the topic of "global communications"), as a *critical enabler* for the future Armed Forces of the United States. Both Joint Vision 2010 and the Concept for Future Joint Operations refer to information superiority as a *key enabler.* The expanded discussions of the "Emerging Operational Concepts" contained in the Concept for Future Joint Operations illustrate the importance of information superiority in achieving the new concepts. The Joint Warfighting Capability Objectives list information superiority as the only objective which receives "strong support", as determined by the Office of the Secretary of Defense, across all four Joint Vision 2010 Operational Concepts.[10]

The December 1997 Report of the National Defense Panel, "Transforming Defense - National Security in the $_{21}$st Century echoed the importance of information superiority, although here it is presented as Information Operations. The comments and emphasis remain the same.

---

[8] Joint Vision 2010, (Washington D.C., Chairman of the Joint Chiefs of Staff, 1997), 19.

[9]Concept for Future Joint Operations, Expanding Joint Vision 2010, (Fort Monroe, VA, Joint Warfighting Center, May 1997), 66.

[10]Conoept for Future Joint Operations, Expanding Joint Vision 2010, (Fort Monroe, VA, Joint Warfighting

The importance of maintaining America's lead in information systems - commercial and military — cannot be overstated. Our nation's economy will depend on secure and assured information infrastructure. These systems are also instrumental to the success of military operations ... information operations are likely to be crucial to the course of future conflict, challenging us, and our allies, in both offensive and defensive ways.... The entity that has greater access to, and can more readily apply, meaningful information will have the advantage in both diplomacy and defense.

Effective use of information superiority demands that we move rapidly to the next level of “jointness" among the uniformed services: full commonality of U.S. military information systems. This commonality must be interoperable with the information systems of our allies as well, if we are to reap the advantages of coalition operations.

Given the importance of information — in the conduct of warfare and as a central force in every aspect of society — the competition to secure an information advantage will be a high-stakes contest, one that will directly affect the continued preeminence of U.S. power.[11]

Information Superiority is not only the processing of information. There exists a requirement for protection of information (Defensive Information Warfare), the Defense Information Infrastructure (DII) and the National Information Infrastructure (NII).

> The domestic infrastructure *(aka the National Information Infrastructure)* which underpins the economic life of our society increasingly depends on electronic networks for the flow of information. In sectors such as transportation, finance, energy, and telecommunications, computer networks have become indispensable in providing essential services that we take for granted. Air traffic data for the safe conduct of thousands of flights per day, financial transactions worth many millions of dollars daily, and control signals for operation of power distribution grids, railroads, pipelines, and the telephone system itself, all travel over electronic networks. Electronic networks have truly become the "nerves" of our infrastructure in yet another manifestation of the proliferation of information technology that characterizes the world today.[12]

The National Information Infrastructure has a direct impact on the deployment abilities and

---

Center, May 1997), 32-33.

[11]Report of the National Defense Panel, Transforming Defense - National Security in the 21st Century, (Washington, D.C., National Defense Panel, Dec 1997), 13-14.

[12]John H. Gibbons, A Technical Primer on Risks arid Reliability, CYBERNATION: The American Infrastructure in the Information Age, (Washington D.C., Executive Office of the President, Office of Science and Technology, April 97), "abstract letter" (no page number).

overall operation of the Department of Defense and on the holistic operation of the nation while engaged in crisis resolution. Every agency, department, or organization, civilian or federal, is thoroughly dependent on services provided by the information age and will be even more so in the future. The United States must be prepared to respond to an asymmetric attack on the National Information Infrastructure. The ability to detect and defend against such attacks should be coordinated across and throughout all levels of our federal and civilian sectors; the Department of Defense must "sit at the table" as a major player.

A significant "force multiplier" in the future will be influencing (Offensive Information Warfare) an opponent's ability to attain Information Superiority against the United States. Future opponents will be as dependent on an electronic infrastructure as the United States. Our ability to conduct asymmetric attacks might result in shorter conflicts and fewer friendly casualties as future opponents become unable to prosecute operations while their country is driven into chaos.

The responsibility and capability for Offensive Information Warfare should remain within the Department of Defense, but due to the potential global impacts of these type of operations, all such actions should be carefully orchestrated and evaluated by an Interagency Group which has the knowledge and expertise to evaluate the effectiveness and potential impacts of such activities. It is important to recognize that Information Warfare encompasses much more than simply direct attacks on an opponents electronic infrastructure. Psychological operations, public affairs, and other disciplines are all incorporated.

If the templates for the future of the Armed Forces are contained in Joint Vision 2010 and its companion document the Concept for Future Joint Operations, the Quadrennial Defense Review, and studies such as the White House Office of Science and Technology

"Technical Primer on Risks and Reliability, CYBERNATION: The American Infrastructure in the Information Age, then the role of Information Superiority is well established for the future. Still, questions need to be answered. How will this transformation take place? Who will direct the effort? Where will the Department of Defense fit in?

Chapter 3

Current Initiatives

The Joint Staff J6 Directorate, Command, Control, Communications, and Computer Systems, has since 1992, embarked upon a program designated "C4I for the Warrior" (C4I = Command, Control, Communications, Computers, and Intelligence). Today this program, agreed to by all the services, is the principle effort for coordinating Department of Defense efforts to attain Information Superiority. The basis of C4I for the Warrior is the coordination of individual efforts of each of the services into systems, architectures, and technologies which will either be compatible or complement each other. Joint Standards (protocols) have been established and published in the Chairman, Joint Chiefs of Staff (CJCS) 6231 publication series. The Defense Information Systems Agency has been a participant throughout this process. The individual services have taken "lead" for various program initiatives.

The C4I for the Warrior strategy is the foundation on which the movement toward ***Network Centric Warfare*** is based. Network Centric Warfare is the currently identified solution for Information Superiority in the 2010 timeframe.

Network Centric Warfare:

- Changes the dynamics of competition in warfare
- Enables increased speed of command
- .Rapidly "locks out" adversary's courses of action
- Provides decisive competitive edge in warfare[13]

Network Centric Warfare is currently thought of as being built around three distinct grids:

[13]Dr R.T. Gooden, Information Superiority Integrated Product Team Briefing, (Washington, D.C., Joint Staff J6 Directorate, IS IPT Brief Jul 30, 1997), slide 10.

Information, Sensor, and Engagement Grids'[4] Network Centric Warfare is the long term goal. Each service is pursuing that goal in a different fashion.

> The Army's ***Enterprise Sfrategy*** supports digitization efforts and focuses on the information needs of the Army as a whole. ... The Enterprise Strategy is the synchronization of Army programs with the Joint Staff's C4I for the Warrior concept, sound business practices,, and the Defense Information Infrastructure Master Plan.[15]

The digitization efforts ongoing in the Army "Force XXI" are the most noticeable efforts to date.

> The Navy and Marine Corps ***Copernicus*** vision takes on added significance in meeting the challenges of C4IFTW. This common vision enables the Navy and Marine Corps to adapt, evolve, and fully integrate their Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) capabilities and resources and conduct successful joint Naval Expeditionary Force operations..[16]

The Navy "Cooperative Engagement Capability" (CEC) and the Marine Corps "Operational Maneuver From The Sea" (OMFTS) are directly supported by this effort.

> The Air Force has fully embraced the concept of expanding the battlespace beyond the conventional view of land, sea, air, and space into the flflh dimension of the infosphere. ***Horizon*** provides the vision leading the Air Force to fully integrated information operations as a full partner in all activities across the spectrum of conflict.[17]

The Air Force has committed significant resources, in many areas, to insure the success of Horizon. An example is the progress being made to provide accurate and timely information to aircraft during the conduct of a mission.

Each of the service programs strive to complement the "end state" provided in Joint Vision 2010. Each of these programs is highly dependent on the communications

---

[14]Dr R.T. Gooden, Information Superiority Integrated Product Team Briefing, (Washington, D.C., Joint Staff' J6 Directorate, IS IPT Brief Jul 30, 1997), slide 10.
[15]J6 Directorate, Joint Staff C4I for the Warrior, (Washington, D.C., 1997 update), 2.
[16]J6 Directorate, Joint Staff; C4I for the Warrior, (Washington, D.C., 1997 update), 3.
[17]J6 Directorate, Joint Staff, C4I for the Warrior, (Washington, D.C., 1997 update), 3.

infrastructure provided by the Defense Information Systems Agency (DISA). The ***Defense Information System Network,*** known as "DISN", is integral to every aspect of the service initiatives Defense Switched Network (DSN)

> The DISN is a critical piece of the Defense Information Infrastructure providing the integrated network that meets the needs of DoD for voice video, and data communications. DISN expands the common-user capacity of the network and provides value added services. The DISN establishes a high speed, common-user backbone which bundles individual circuits into a managed high capacity system. Through these high speed, common-user circuits, the DISN provides the backbone on which the warfighter's global, wide-area network will reside. The six essential DISN elements are:
>
> - Defense Red Switched Network (DRSN)
> - Unclassified but Sensitive Internet Protocol Router Network (NIPRNET)
> - Secret Internet Protocol Router Network (SIPRNET)
> - Joint Worldwide Intelligence Communications System (JWICS)
> - Video Teleconferencing (VTC)[18]

In order to provide DISN directly to the Warfighter, the Defense Information Systems Agency has created the ***Standardized Tactical Entry Points (STEP)*** program. This program is designed to provide predesignated entry points for Warfighters to enter the DISN. This will reduce the time required to activate a variety of services by deployed forces.[19]

The ***Joint Warrior Interoperability Demonstrations (JWID)*** is an annual series of exercises, conducted to evaluate potential solutions to warfighter C4I interoperability requirements in a low risk environment. Oversight of this program resides with the Joint Staff J6 Directorate. Each year a different Commander in Chief (CINC) sponsors the exercise with the lead for execution rotating among the services. This provides the opportunity to have many different agendas or points of view looked at in depth.

Battle Laboratories have been established by the Army, Navy, and Air Force to

[18] J6 Directorate, Joint Staff; C4I for the Warrior, (Washington, D.C., 1997 update), 17.
[19] J6 Directorate, Joint Staff; C4I for the Warrior, (Washington, D.C., 1997 update), 18.

provide in depth analysis of proposed C4ISR solutions. The Marine Corps Warfighting Laboratory serves a similar purpose. These labs exchange information, albeit informally, which inturn facilitates the Joint Warrior Interoperability Demonstration exercises.

The Joint Staff and the Services are aggressively pursuing the quest for Information Superiority. The effort is one of mutual coordination with no recognized authoritative single point of contact. As long as the personalities work, mutual cooperation may well be effective. The ability to participate with the Federal and Civilian sectors in a coordinated and organized fashion is suspect however. Who is the 'voice' for the Department of Defense?

Within the last decade there are two examples where a "community" was brought together under a single entity in order to maximize resources and bring a higher degree of efficiency. These are the United States Transportation Command and the United States Special Operations Command. Both of these commands have specialized charters and forces from the various services assigned to them.

The time has come to consider the creation of an independent command oriented toward ***Information Operations.***

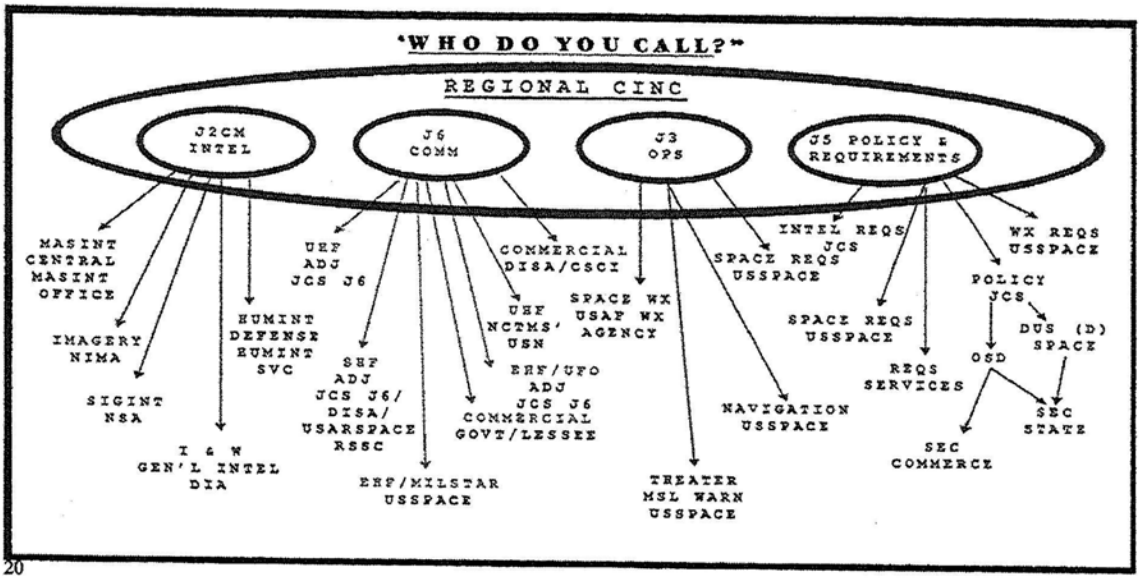
Chapter 4

Current Operational Relationships for Crisis Response

Providing support to today's Warfighter during contingency operations can be a complex task. Key players are the Joint Task Force Staff, various elements of the Theater Staff (Commander in Chief level), the Joint Staff J6Z (CINC Operations Division) and J3 (with minimal input from other Joint Staff directorates), the Defense Information Systems Agency, and the Headquarters and components (i.e. USARSPACE Regional Space Support Centers) of United States Space Command.. The following discussion is limited to supporting a *deployed Warfighter who is removed from the traditional sustaining base environment.*

During the initial stand-up of a Joint Task Force the Theater Staff will act on behalf of a Joint Task Force. The initial issues facing a Joint Task Force revolve around support for intelligence, communications, navigation, and theater missile defense-all elements of the Joint Task Force Commander's overall command and control capability. The demand for information is tremendous and continues to grow in each of these functional areas. When attempting to determine where to turn for support, today's environment provides endless opportunities for disaster, either in timeliness or the ability to actually receive needed support.

The following illustrates (from a CINC's perspective) the complexity of the coordination required between CINC staff functions and external agencies if a Warfighter is to get support in the areas depicted. Policies and the process for obtaining support widely vary between responsible organizations/agencies. This environment is much too complex for a Joint Task Force to contend with while at the same time attempting to get its "arms around" a crisis.



The Joint Communications Support Element, located aboard MacDill AFB, is the single unit officially designated (by mission, equipment, personnel, and funding) to provide support to a Joint Task Force Headquarters and has the lead for establishing the connectivity and linking all active workstations to the systems identified in the picture above.

However, the Joint Communications Support Element is not large enough to support all global requirements. Therefore each Theater CINC has addressed this shortfall and has the ability to support a Joint Task Force Headquarters within existing Theater resources, if required. For the most part the "solution" is to employ a "component lead" for a Joint Task Force and let that service component become responsible for providing the required support. Still, services do not provide "purple" forces, even though a they may be a "component lead" and "theater requirement" exists. This results in adhoc organizations, work-arounds and the use of off-the-shelf solutions not recognized, funded or supported

[20]C0L Partridge, USA, United States Space Command 33 Briefing, Feb 97.

by the services. However, forces which can be prepared to assume a Joint Communications Support Element like mission exist within the force structure today.

See Annex A "UHF/SHF Satellite and Direct Support Capabilities for a Joint Task Force" for a more comprehensive description of the relationships which come into play when supporting a deployed Joint Task Force headquarters.

In order to obtain Information Superiority in the next century, changes to unit missions, capabilities, and responsibilities must be made. Too many organizations are involved today, primarily because no one organization has been tasked with responsibility to insure successful information operations. The result-unnecessary confusion, delays in decision-making, and great deal of operator frustration in the ability to acquire required support in a timely fashion without having bureaucratic hurdles placed in the way. The decision making process must be streamlined and involve skilled, knowledgeable personnel capable of "seeing" the requirements and acting upon them.

Our information management must be a structured process and not one which we struggle through. The forces tasked to represent the United States deserve no less. A single organization, an ***Information Operations Command,*** is required with responsibility for delivering and protecting information for the Department of Defense with an emphasis on deployed (out of sustaining base) forces. This organization should be equipped with the best resources of all the services and should possess a global mission as a functional command. This organization should be chartered with responsibility for developing direct action attacks on electronic infrastructures (an element of Offensive Information Warfare). The development of a superior "defense" means complete understanding of potential offensive operations which might be used in

an asymmetric attack against the United States. With this in mind, what organization would be better suited for an offensive role as well?

Chapter *5*

The Role of the Information Operations Command

This new command would be the responsible authority for developing and coordinating the Department of Defense's Information Superiority campaign to achieve the goals of Joint Vision 2010. This new headquarters would be responsible for the Defense Information Infrastructure and would represent the Department of Defense on interagency functional issues which affect the National Information Infrastructure and its impact on Federal Departments and Agencies, particularly as it relates to Defensive and Offensive Information Warfare.

The Information Operations Command would be directly responsible for:

- Developing and coordinating the Defensive Information Warfare operations of the Department of Defense.
- Coordinating Defensive Information Warfare operations with other elements of both the Federal and Civilian sectors.
- Developing and establishing interoperability standards, protocols, and architecture design within the Department of Defense. Services would be designated "Executive Agent" for specific programs. This includes the supporting establishment as well as tactical forces, from radios to high speed data networks.
- Coordinating and reviewing the development of all systems being acquired or procured which will use any portion of the National or Military Infrastructures. This is a significant role which would ensure the "health" of the common operating environment crucial to the success of Information Superiority. The United States Army has taken the position that "the pace of development is so great that it renders our current materiel management and acquisition system inadequate".[21]

[21] TRADOC Pamphlet 525-5, Force XXI Operations - A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Early Twenty-First Century, (Fort Monroe, VA, United States Army Training and Doctrine Command, 1 Aug 1994), p 1-5.

- Coordinating with Federal and Civilian sectors to ensure that the Department of Defense is capable of seamlessly operating with external organizations as necessary in pursuit of national goals and objectives.

- Assuming control of the Defense Information Systems Agency (DISA) and provide for continued installation, operation, and maintenance of the existing Defense Information Infrastructure as accomplished today by the Defense Information Systems Agency (DISA), or the potential oversight of "outsourcing" as appropriate. This would include commercial leasing, terrestrial and space resources, as is currently done today.

- Providing deployable tactical forces capable of providing a full range of services to the Joint Forces/Joint Task Force Commander. These forces will provide a "turn key" operation which fully integrates the Commander into the National Infrastructure and permits the attainment of Information Superiority and be capable of operating on land, in the air, and at sea. Coalition operation support would be available as well.

- Managing the day-to-day operations of the single channel UHF satellite constellation, the EHF (Extra High Frequency) constellation (equipment is just beginning to be delivered to operating forces), and the Defense Satellite Communications System (DSCS, aka X band,, SHF, or GMF) with guidance from the Joint Staff (J3 especially). Note that this set of responsibilities requires extensive, continuing coordination with the "operators" on the Joint Staff.

- Developing and operating the United States Offensive Information Warfare capability to include assuming control of the Defensive and Offensive Information Warfare operations of the National Security Agency (NSA)

    - This will likely require elements currently assigned to the National Security Agency.

    - The NSA intelligence collection gathering mission might gravitate to the DIA or remain autonomous as it exists today.

- Working with industry to develop the most effective, fiscally responsible solutions to Information Superiority requirements. The Department of Defense does not need to duplicate what has or is being done. An Industry/Department of Defense Council should be established under the purview of the ***Information Operations Command.*** This council would provide current state-of-the-art concepts and thinking within industry to the ***Information Operations Command.***

The ***Information Operations Command*** would operate in much the same fashion as both the United States Transportation Command and the United States Special Operations

Command. The United States Transportation Command moves people and things. The ***Information Operations Command*** would move bits and bytes. For "force structure" the United States Special Operations Command model is applicable. Department of Defense agency and service forces would be earmarked for service with the ***Information Operations Command.*** Examples of such units might be:

- The Defense Information Systems Agency, to include the Joint Interoperability Testing Center

- The National Security Agency (NSA) for its role in both Defensive and Offensive Warfare operations. Due to the involvement by the National Security Agency in the development of cryptographic support (both encoding and decoding) there is an obvious connection to Offensive and Defensive Information Warfare.

- The Joint Communications Support Element with a robust tie-in to United States Army Reserve, Air National Guard, and individual State National Guard organizations. Ideally each state would possess a capability, which would provide a significant capability for disaster and crisis response support locally as well as providing a superior capability for wartime expansion.

- United States Army Echelon Above Corps (EAC), Signal units are well suited for operations at forward locations away from established airfields and where mobility is an issue. They might also be used in a port environment where reception, staging, onward movement, and integration (RSOI) of heavy forces being brought in by sea is occurring, such as with a United States Marine Corps Maritime Prepositioning Force (MPF) or the United States Army Prepositioned Stocks (APS).

- United States Air Force Combat Communications Squadrons are particularly well suited for employment at Intermediate and Forward Support Bases, both of which are usually based at airfields. These locations have generally taken on a distinct "joint" flavor as opposed to a single service (Air Force) orientation. Operation Assured Response (Liberia - 1996) and Guardian Assurance (Eastern Zaire - 1996) and other contingency planning by the United States European Command have developed and proven the suitability of a Combat Communications Squadron for this type of mission.

- United States Navy "MICFAC"s could be assigned as appropriate. Navy resources might not only be employed in the immediate vicinity of a port, but due to their nature are extremely light and transportable and might well be suited for "first in" temporary command posts. This was proven by the deployment of

a Navy MICFAC to Freetown, Sierra Leone to support the Joint Task Force Headquarters during Operation Assured Response in Liberia during 1996.

- Marine Corps contributions would generally be limited to the single Communications Battalion located within the United States Marine Corps Reserve and to the "JTF Enabler" packages being forward deployed with Marine Expeditionary Units.

There is no question, that the creation of another "Commander in Chief' with the responsibility and authority to "pull" forces would be a source of concern with the Services. The old ways of doing business need to be changed if the "future", as depicted in Joint Vision 2010, is to be attained. Information Superiority is going to require trained and equipped personnel who know what they are doing and why they are doing it in order to provide the Joint Forces/Joint Task Force Commander with the tools needed to accomplish assigned missions. The "territory" (for deployment of actual units) of this new ***Information Operations Command*** stops before it reaches the component level in an organization. Someone needs to be "in charge" of Department of Defense "Information Operations" and be held accountable for its effectiveness. Due to the potential Offensive and Defensive Information Warfare role(s) and the ability to project force(s) into a theater of operation, much as the United States Special Operations and Transportation Commands do today, this organization needs to "sit at the table" recognized as another supporting command (like the United States Transportation and Special Operations Commands).

Chapter 6

Options for Designating a Commander in Chief, Information Operations Command

This chapter will address three options for designating the ***Commander in Chief information Operations Command (CINCIOC).*** These options are: Commander-in-Chief, United States Space Command; the Director, Defense Information Systems Agency; and the Director, Joint Staff J6.

The ability to interface with the Joint Staff, which has an enormous role to play in establishing priorities over limited resources, is essential. If the desire is for a "turn-key" operation, as described in Chapter 1 (Operation Crystal City) whereby designated forces arrive with the personnel, equipment, procedures, and training to support Joint Task Force headquarters or other deployed headquarters, the role and composition of the entire organization is affected. This "ownership" of deployable forces is a significant departure from the emphasis of cooperation between the services under the "C4I for the Warrior" concept previously discussed. Having deployable forces under an Information Operations Command with the responsibility to operate down to the Joint Task Force level would not eliminate the requirement for the services to continue the initiatives begun under the "C4I for the Warrior" framework and tested under the Joint Warfighter Interoperability Demonstrations (JWID).

Option 1- <u>Commander-in-Chief. United States Space Command</u>

The Commander-in-Chief, United States Space Command could be assigned as the focal point for Department of Defense efforts to manage Information Operations. The Defense Information Systems Agency would be assigned as a sub-unified command per

the suggestion of the National Defense Panel.

> Space Command would expand the use of space and information to implement a vision of global awareness, integrated space operations, and information superiority. CINCSPACE would be responsible for providing global infrastructures for the geographic commands. *The Defense Information Systems Agency would be transferred to Space Command and become one of its subordinate commands.* (emphasis added) Space Command would be responsible for managing information infrastructure on a global scale and providing support and immediate access by combat commanders.[22]

Pros

- United States Space Command has unique knowledge and experience with space-based resources. These resources are integral to achieving the Information Superiority established in JV-2010.
- The Headquarters organization for a CINC-level organization is already in place.
- Several components, some with deployable resources, exist within United States Space Command providing an experience base upon which to draw when discussing oversight of the deployment and employment of "Information Operations Task Forces
- With the Defense Information Systems Agency as a sub-unified command, United States Space Command gains some critical required expertise.
- United States Space Command understands the interfaces with the Joint Staff and the Theater CINCs.

Cons

- United States Space Command has a full range of responsibilities which continues to expand.
- The scope of a global Information Superiority responsibilities will be significant.

---

[22] National Defense Panel, Transforming Defense - National Security in the 21st Century, (Washington D.C., Dec 1997), 72.

Issues within the Federal and Civilian sectors will have significant potential impact on the National Information Infrastructure and the Defense Information Infrastructure.

- Initiatives currently underway by United States Space Command create a spectrum of responsibilities too vast for a single organization.

- While space support is a big player in combat operations and intelligence collections, it is only one element when the entire information infrastructure is examined. Supporting establishments, fixed command posts, theater headquarters all rely more heavily on traditional forms of support vice space.

- Issues such as interoperability, tactical systems ability to interface, protocols, etc. are not arenas unique to the United States Space Command.

- The scope of testing, training, and oversight of that necessary to accomplish the JV-2010 Information Superiority will be significant.

Option 2- <u>Director, Defense Information Systems Agency</u>

Historically the Defense Information Systems Agency has had a relatively limited view of operations based upon their missions.

<u>Pros</u>

- Extensive experience in the development of interoperability standards of various devices, especially as it pertains to communications, transmission systems, and data networks.

- Experienced in developing training programs.

- Manages the Joint Interoperability Testing Center.

- Manages all the interconnectivity and long haul transmission paths which interconnect Department of Defense sites.

- Plays the most significant a role in the management of the utilization of the Defense Information Infrastructure.
- Manages the Defense Satellite Communications Systems (DSCS) under oversight of the Joint Staff J6.
- Location in Washington. D. C. provides easy accessibility to the Federal and Civilian sectors.

Cons

- Will require significant reorganization to evolve into a CINC-level organization.
- Historically, possesses an institutionally narrow viewpoint on operations.
- Possesses no deployable forces. No institutional knowledge base for deployment and employment of an "Information Operations Task Force".
- Does not routinely interface with the Joint and Theater staffs (beyond the J6 and limited J3 interface).

Option 3- Director. Joint Staff J6

Designate the Director, Joint Staff J6 Directorate as the Commander in Chief, Information Operations Command. The Joint Staff J6 would then be "dual-hatted" as the ***Joint Staff J6*** and the ***Commander in Chief, Information Operations Command.*** This would be similar to the Joint Staff J2/Defense Intelligence Agency model which exists today, recognizing the significant differences between an agency and a CINC-level organization.

Pros

- The J6 staff is well tied into the requirements of the Joint Staff J3 and other decision makers.

- Relationship(s) with the individual Commander-in-Chief staffs is well established.
- Relationships with United States Space Command, the National Security Agency (NSA), and the Defense Information Systems Agency (DISA) are well established.
- Manages the "C4I For the Warrior" program.
- Currently functioning as the lead proponent for coordinating service efforts toward achieving Information Superiority as envisioned by JV-2010.
- Manages the "Joint Warrior Interoperability Demonstration" (JWID) program.
- Apportions and provides oversight of the UHF satellite constellation, considered by many to be the critical tactical resource employed during crisis response operations.
- Extensive experience in deployment and employment, coupled with a thorough understanding of the capabilities and limitations of the Joint Communications Support Element.
- Possesses experience base familiar with requirements necessary to manage Information Operations and attain Information Superiority.
- Conflict between the Joint Staff J6 and the Information Operations Command is eliminated.
- Might provide a model for reorganizing the Theater J6s in order to streamline the processes required today to obtain support.

--Location in Washington, D. C. provides easy accessibility to the Federal and Civilian sectors.

Cons

- Significant reorganization required in order to become a CINC-level organization
- A limited Joint Staff J6 presence would be required to be maintained in the Joint

Staff.

- Two General Officer Deputies, one for the Joint Staff and one for the Information Operations Command functions, required.
- While detailed analysis is yet to be accomplished, this option might well provide for the highest initial "start up" costs due to the extensive reorganization required.

Any of the three previously discussed options will work. In all cases what is required is a new way of addressing the issue(s) surrounding Information Operations and the attainment of Information Superiority. Someone must be in charge and held accountable for the Department of Defense effort. An agency-level solution will not sit "at the table" with the other Commander's-in-Chiefs as a co-equal. A "CINC" is needed.

RECOMMENDATION: Option 3 is preferred, notwithstanding the significant reorganization which would be required.. Many of the existing relationships already exist including the significant "tie in" to the Joint Staff when determining allocations of scarce resources and the coordinating effort(s) for the "C4I for the Warrior" program. A streamlined operating environment for decisions and responsiveness is obtained. Using this model, it might follow that each theater J6 could be "dual-hatted" as well, both as the theater J6 and the "Commander, Regional Operations Center, Information Operations Command" within their respective theaters. This would result in a completely new construct of staff responsibilities and provide significant relief to the difficulties experienced today.

Chapter 7

Summary

Does the United States really need an ***Information Operations Command?*** Absolutely. The future of warfare and military operations will rely significantly upon information operations. "Information technology is expected to make a thousandfold advance over the next 20 years"[23] The growth of specialists within this arena will be noticeable. Skills which in the past, under attrition warfare, were often viewed with distain by the Warrior community will become essential. It is likely that some of the future Warriors will be those with specialized skills.

"Information Task Forces", similar to the Special Operations Task Forces of today, may even prove useful in future conflicts. An ***Information Operations Command*** is appropriate for the development and maintenance of forces for this mission. Deployed Joint Force/Task Force Commanders deserve much better support than what they receive today. Using today's technologies, tremendous improvements are possible.

The fictional piece at the beginning of this paper, ("Bits & Bytes Into the Night, Operation Crystal City") portrays an organization dedicated to mission support. Joint Task Force Commanders should not have to be concerned with where the support comes from, how it is configured, deployment and employment of information superiority resources in direct support of the Joint Task Force Headquarters, and whether it will meet the needs of the Joint Task Force. The speed of today's operations, from the moment the

---

[23]TRADOC Pamphlet *525-5*, Force XXI Operations - A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Early Twenty-First Century, (Fort Monroe, VA, United States Army Training and Doctrine Command, 1 Aug 1994), p 1-5.

National Command Authority decides to execute a given mission to the time a Commander is expected to begin influencing the operation is tremendously accelerated - far more from just a few years ago. Time is critical.

Critics of this proposal will object to the National Security Agency (NSA) being included under the ***Information Operations Command,*** the assignment of Offensive Information Warfare responsibility, and the ability to task service units as the Special Operations Command does today. The intent of this paper was not to specifically develop the organization, but to develop the requirement for an ***Information Operations Command.*** Much work would be required to bring this command into being.

Others will argue that space is preeminent and therefore the United States Space Command should be given the mission. The case presented here is that of a command with responsibilities far beyond what proponents of the United States Space Command have envisioned. Space Operations and Information Operations are enormous areas of future growth for the Department of Defense. Each represents a valuable tool in the nation's arsenal. Individually, the scope of each area is virtually unlimited and complementary to the other.

It must be noted that Information Superiority (obtained through Information Operations) must be viewed on a global basis. There should be no risk entailed in moving and operating forces from one theater to another. The world, in so far as the Department of Defense is concerned, should reflect one common environment, accessible by any force, anytime, anywhere.

The paradigm of today will not permit the United States to attain the goals of Joint Vision 2010. Dramatic changes - new ways of thinking, different methods of conducting

operations, a different force structure, new ways of looking at old problems - will be required. The United States cannot afford to stand still.

ANNEX A

CRISIS CONTINGENCY SUPPORT: UHF/SHF SATELLITE AND DIRECT SUPPORT CAPABILITIES FOR A JOINT TASK FORCE

During the initial stand-up of a Joint Task Force the Theater J6 Staff will act on behalf of a Joint Task Force. The initial issues facing a Joint Task Force are generally:

- Single Channel UHF (Ultra high Frequency) Tactical Satellite support. A critical aspect of initiating operations this support is used with Embassy Liaison Teams, reconnaissance forces, special operations, and more frequently in place of traditional VHF FM (Very High Frequency - Frequency Modulated) radios employed by conventional forces.. Voice and some low rate data exchanges are used in this medium

- Multichannel SHF (Super High Frequency) X-Band DSCS (Defense Satellite Communications System) support. Known as Ground Mobile Forces (GMF) when referring to the systems employed by conventional forces, this support provides staff and command post locations, with long haul, high throughput voice and data services transmission path. DSN, DRSN, NIPRNET, SLPRNET, JWICS, and VTC are normally provided over this medium. End user equipment is a user responsibility. This support provides the "staying power" for a Joint Task Force.

- Commercial leased services. This category encompasses a wide range of services. Some of the most frequently asked questions in the initial stages of a contingency operation are:

    - What is the availability of cellular telephones?

    - What kind of commercial satellite services can operate within the area? Are vendors available who can provide "bigger pipes" with accompanying data support, especially high capacity routers?

    - Can local and international commercial telephone service be provided where Headquarters (of varying sizes) are located? If so, in what quantity? What are the restrictions?

    - How fast can additional unique service requirements be activated and brought online at the Standardized Tactical Entry Point (STEP) site

> designated to support the Joint Task Force. (The complexity of this answer is directly related to whether one service component has the "lead" for establishing the Joint Task Force Headquarters-Army led Task Forces are generally heavy in Army systems, Marine in Marine systems, etc.)

This all appears pretty straightforward but a closer look sheds insight into the mechanics of providing this support.

Single Channel UHF Tactical Satellite channels are in constant demand so there is no such thing as an "unassigned or free" channel. The Joint Staff J6Z in concert with the Joint Staff J3 prioritizes and apportions a certain number of channels to each Theater. Each Theater J6 has a different mechanism for managing UHF apportionment. At the outset of a crisis, a Theater J6 will reexamine current satellite utilization and make adjustments to internal allocations to components or existing contingency forces. If Theater requirements cannot be met within existing apportionment, the Theater J6 will ask the Joint Staff J6Z for additional channels to support the crisis

The Joint Staff J6Z has no "hip pocket" channels available to it. To provide additional channels to a Theater, the Joint Staff J6Z reapportions channels of another CINC. A good example of this is the support provided for Bosnia. United States Atlantic Command, Central Command, and the Southern Command have all "lost" channels to the United States European Command and Bosnia operations. It is interesting to note that while components of United States Space Command fly and operate the spacecraft, the United States Space Command has no role whatsoever in channel allocation.

Multichannel SHF X-band (GMF) support is provided in the following manner. Bandwidth requirements are determined by the Theater J6. The local Regional Space Support Center (RSSC), an element of the United States Army Space Command

(USARSPACE), a component of the United States Space Command, performs the mathematical analysis to determine the impact of the request, potential satellite assignment, etc. (The Regional Space Support Center will often coordinate concurrently with the local Defense Information Systems Agency office which has cognizance over Defense Satellite Communications System (DSCS) support.) The local Defense Information Systems Agency office will contact the Defense Information Systems Agency Headquarters (Office: DOT) in Washington, D. C. for approval. The Washington DOT office will frequently run its own set of computations which may or may not provide the same "answers" developed within the theater. At this point, three separate groups have done "computations/supportability analysis" to some degree.

The Theater J6 looks for feedback from the local Regional Space Support Center and the local Defense Information Systems Agency office. Once feedback is received, the Theater J6 contacts the Joint Staff J6Z and requests approval for the support. It is not uncommon for the Defense Information Systems Agency Headquarters in Washington, D. C. and the Joint Staff J6Z to come to two separate and distinct conclusions as to supportability of an operation. These must be resolved. Once all pertinent issues are resolved and approval is received by the Theater J6, contingency forces can begin detailed planning for employment of this extremely critical resource.

Multichannel SHF DSCS support is in such demand that it would not be unusual to "bump" someone from a satellite in order to provide the required bandwidth. Much like the Single Channel UHF Tactical Satellite, components of United States Space Command only fly and maintain the spacecraft - the command has no authority to prioritize or assign channel bandwidth. This responsibility is reserved by the Joint Staff

J6, in coordination with the Defense Information Systems Agency (DISA), so that this critical and limited resource is managed based upon the requirements of the Warfighters.

The demands for commercial support increase exponentially depending on the size and expected duration of the operation. Tactical resources held by the services are currently incapable of providing the high bandwidth requirements estimated to be required by a medium to large deployed Joint Task Force Headquarters. Within the Department of Defense the Defense Information Systems Agency is the principle contractor and procurer of commercial services. The Defense Information Systems Agency is involved with connectivity between installations including deployed locations, but not aboard the installations themselves. In field environments internal networks and systems of service forces are service provided. (e.g., the U.S. Army's Mobile Subscriber Equipment (MSE) The Theater J6 will contact the local Defense Information Systems Agency office and levy the "requirements". The Defense Information Systems Agency does not possess funds to support contingency operations so along with the requirements comes information regarding funds responsibility and transfer. (In order to provide timely support, reimbursement is frequently made to the Defense Information Systems Agency after agency funds have been redirected temporarily while the various fund managers work out the details.)

As one can see, the Theater J6 and Joint Staff J6Z play significant roles in providing initial contingency support to an operation. Once the operation gets underway, commercial services provided through the Defense Information Systems Agency take on increased emphasis as the size and scope of an operation increases. Significantly, the United States Space Command performs a supporting role, not a decision making one.

But what of the support provided to the Joint Task Force itself?

There are as many options as there are units which might be tasked to provide support to a Joint Task Force. The premier unit within the Department of Defense is the Joint Communications Support Element (JCSE) located aboard MacDill Air Force Base in Florida. The Joint Communications Support Element organized into squadrons after the Air Force model for the Combat Communications Squadrons, is equipped with the latest state-of-the-art equipment and specially manned from all services. It is "purple". This unit's mission is "to provide unified commands with worldwide, rapidly deployable telecommunications support for *two* JTFs and *two* Joint Special Operations Task Forces (JSOTFs) [emphasis added]. These major deployments would be directed by the Chairman of the Joint Chiefs of Staff"[24] The Joint Communications Support Element unit is operationally controlled by the Joint Staff J6Z, administratively controlled by the Central Command. This unit is expected to come under the control of the U.S. Atlantic Command in the near future.

It is not unusual for a Theater J6 to attempt to establish conditions whereby a Joint Task Force might be supported by in-theater assets vice requesting the Joint Communications Support Element. There are a variety of techniques used to accomplish this. The most frequent is attempting to create an environment where an element of a component is trained and capable of performing such a mission. This is especially true if the theater uses a "component lead" technique for establishing a Joint Task Force. Most Theater CINCs today employ the concept of "component lead such as is portrayed in the United States European Command Directive for Joint Task Force Headquarters Policies,

[24] Joint Communications Support Element, C4 Planners Guide, (Ma~Di1l AFB, 1996),1-4.

Procedures, and Organization.[25] Commanders prefer "going to war" with an organization with which they have trained.

Within the United States European Command two units have been assigned support to a Theater Joint Task Force as a potential mission. The 1st Combat Communications Squadron (1ST CCSQ) of the United States Air Forces Europe (USAFE) and the 7th Signal Brigade (7th SIGBDE) of the 5th Signal Command (5th SIGCMD), United States Army Europe (USAREUR) are considered by the Theater J6 as the units of first choice to support a theater generated Joint Task Force. The Air Force and the Army however have not assigned either of these units this mission nor have the two units been manned, equipped or trained to accomplish this theater generated requirement. (technically the services provide forces through the components, i.e. Army Forces, not "Joint Forces). The services are not required to train and equip to a "Joint" requirement. This means virtually everything comes out of hide and adhoc to support a Joint Task Force Headquarters. The Air Force 1st Combat Communications Squadron tends to be more flexible in providing support to a Joint Task Force Headquarters since its mission of supporting an expeditionary airfield is similar, in many ways, to the type of support a Joint Task Force Headquarters requires. The 7th Signal Brigade is designated as an Echelon Above Corps (EAC) unit and has significant limitations in its ability to support a Joint Task Force Headquarters. For example, radio operators/maintainers can be provided for the Joint Operations Center (JOC) when the 1st Combat Communications Squadron provides the support. If the 7th Signal Brigade is assigned the mission, these

[25] United States European Command Directive 55-11, Joint Task Force Headquarters Policies, Procedures, and Organization, (Stuttgart, Germany, United States European Command, 29 May 1997), p I-1 throught I-3

same radio operators, if provided at all, must be brought together in an ad-hoc fashion since the 7th, as an EAC unit, does not possess this capability and United States Army doctrine designates the employment of this type of resource as "user owned and user operated". If an Army led Joint Task Force Headquarters is established operators will then be provided on an individual vice a unit basis. Additionally it is significant to point out that no unit in either the Army or the Air Force has the mission or responsibility to provide data services directly to the user in a deployed environment. The Air Force officially provides the Combat Communications Squadrons with a router for deployed forces but it is up to the deployed forces to provide the server, necessary cable, and installation if the deployed forces wish to establish a local area network (LAN), which is virtually an essential element of a Joint Task Force Headquarters. Within the Army, no unit is tasked to provide even the router, let alone the server. That's not to say that it isn't being accomplished today, however the basis is informal and beyond the scope for which the units are manned, equipped, trained, and funded.

The Standardized Tactical Entry Point (STEP) program operated by the Defense Information Systems Agency is a good program. However, it doesn't go far enough. Large books with volumes of superfluous detail do not tell a tactical system operator what switch to set on the equipment or who is in charge of what aspect of establishing a circuit between the STEP site and a deployed location. The United States European Command J6 has created its own Technical Interface Guide (TIG) to provide practical information to operators on connecting to the STEP site located at Landstuhl, Germany. This guide is an authoritative directive, United States European Command 55-10[26], and is

[26] United States European Command Directive 55-10, Landstuhl Technical Interface Guide, (Stuttgart,

complementary document to United States European Command Directive 55-11, Joint Task Force Headquarters Policies, Procedures, and Organization.

Specific circuits, unique to the components within the United States European Command, and services not addressed by the STEP program, such as long local telephone circuits which permit the effective operation of STU IIIs (secure telephones) in the secure mode have been established and in many cases paid for either through CINC Initiative Funds (CIF) or the Command and Control Improvement Program (C2IP) both managed by the Joint Staff. The European Command Technical Interface Guide has been published on the United States European Command J6 SIPRNET webpage and is available to all forces coming into or operating within the theater. A series of exercises with the 1st Combat Communications Squadron, the 7th Signal Brigade, and deploying Marine Expeditionary Units (MEU) equipped with a "JTF Enabler" package validated the document's effectiveness using virtually every conceivable equipment permutation, based upon bandwidth and circuits, likely to be provided to a Joint Task Force within the European Theater during the initial stages of an operation. This Technical Interface Guide has been extremely well received by the Joint Staff, the Defense Information Systems Agency, and is being reviewed by other Theater J6 staffs for applicability within their AOR. It is important to recognize and remember that what theater units are capable of and what the Joint Communications Support Element is capable of are two completely different issues. The Joint Communications Support Element is better equipped, manned, trained, and funded than are organic theater units.

Germany, United States European Command, 1 Jul 1997, pp i and 1-1.

Bibliography

Air University. Spacecast 2020 Into the Future (a study). Air University Study Group. Maxwell, AFB: 22 Jun 1994.

Chairman of the Joint Chiefs. Joint Vision 2010. Washington, D. C.: Chairman of the Joint Chiefs of Staff, 1997.

Department of the Army. C4I Technical Architecture Version 3.1 (31 Mar 95). Department of the Army Unclassified Internet Web Site. (Publication location/date unknown - retrieved Oct 97).

Department of the Army. Army Enterprise Strategy (20 Jul 93). Department of the Army Unclassified Internet Web Site. (Publication location/date unknown - retrieved Oct 97).

Department of the Army. Army Digitization Master Plan '96. Department of the Army Unclassified Internet Web Site. (Publication location/date unknown - retrieved Oct 97).

Department of the Army. Army Regulation 25-1 - Information Management. Headquarters, Department of the Army. Washington, D. C.: 25 Mar 1997.

Department of the Army. Army Vision 2010. Department of the Army Unclassified Internet Web Site. (Publication location/date unknown - retrieved Oct 97).

Defense Information Systems Agency Unclassified Internet Web Site (DISA CORE MISSION AREAS-GCCS, DISN, DMS, GCSS, & DII COE). Washington, D. C.: Oct 1997.

Donahue, Maj Brian J, USA. J6T Analysis on STEP CONOPS and Current Direction of the Program Briefing. Joint Staff J6T Directorate. Washington, D. C.: Oct 97.

Gooden, Dr R. T. Information Superiority Integrated Product Team Briefing. Washington, D. C.: Joint Staff J6 Directorate, July 1997.

Joint Communications Support Element. C4 Planners Guide. MacDill, AFB: Systems Integration and Research, Inc, 1996.

Joint Staff. Joint Publication 1, Joint Warfare of the Armed Forces of the United States. Washington., D. C.: Joint Staff May 1995.

Joint Staff. Joint Publication 1-02, Approved Dictionary. Washington, D. C.: April 1997

Joint Staff Unclassified Internet Web Site. (J1, J2, J3, J4, J5, J6 and J7 Sections).

Washington, D. C.: Oct 1997

Joint Staff J6 Directorate. C4I for the Warrior. Washington, D. C.: Joint Staff J6 Directorate, 1997 update.

Joint Staff J6 Directorate. Information Warfare - Legal, Regulatory, Policy and Organizational Considerations for Assurance (Research Report). Joint Staff J6 Directorate. Washington, D.C.:Sep 97.

Joint Warfighting Center. Concept for Future Joint Operations, Expanding Joint Vision 2010. Fort Monroe, VA: Joint Warfighting Center, May 1997.

Marsh, Robert T. "Securing, Protecting Critical U.S. Infrastructures". Chairman, President's Commission on Critical Infrastructure Protection. Speech presented to the 20th National Information Systems Security Conference. Baltimore, MD: Oct 7, 1997.

National Defense Panel. Transforming Defense - National Security in the 21st Century. Washington, D. C., National Defense Panel, December 1997.

Naval Information Systems Management Center. Information Resources Strategic Plan 1995-2010 FY 95 (version). Department of the Navy Unclassified Internet Web Site. (Publication location/date unknown - retrieved Oct 97)..

Roman, Lt Col Gregory A, USA. The Command or Control Dilemma: When Technology and Organizational Orientation Collide. Air University. Maxwell, MB: Apr 96.

Roper, CDR Ben USN. Global Broadcast Service Briefing. Washington, D. C.: Joint Staff J6 Directorate, Spring 97.

Stein, COL Fred P., USA. The Emerging Joint Strategy for Information Superiority Briefing. Washington, D. C.: Joint Staff J63 Directorate, Spring 97.

The Commission on America's National Interests. America's National Interests. The Commission on America's National Interests. Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University. Jul 96.

United States Air Force. Horizon '95 - A Vision of the Future. United States Air Force Unclassified Internet Web Site. (Publication location/date unknown - retrieved Oct 97)..

United States Air Force Scientific Advisory Board. Vision of Aerospace Command and Control For the 21st Century 26 Nov 96. United States Air Force. (Publication location unknown - retrieved from United States Air Force Unclassified Internet Web Site, Oct 97).

United States Army Training and Doctrine Command. TRADOC Pamphlet 525-5, Force XXI Operations - A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Early Twenty-First Century. Fort Monroe, VA,: United States Army Training and Doctrine Command, 1 Aug 1994.

United States European Command Directive 55-10. Landstuhl Technical Interface Guide. Stuttgart, Germany: United States European Command, 1 July 1997.

United States European Command Directive 55-11. Joint Task Force Headquarters Policies, Procedures, and Organization. Stuttgart, Germany: United States European Command, 29 May 1997.

United States Navy. From The Sea - Preparing the Naval Service for the 21st Century. United States Navy. Sep 92.

United States Navy. Forward From the Sea (94 version?). United States Navy Unclassified Internet Web Site. (Publication location/date unknown - retrieved Oct 97)..

White House Office of Science and Technology Policy. CYBERNATION: The American Infrastructure in the Information Age - A Technical Primer on Risks and Reliability. White House Office of Science and Technology. Washington, D. C.: 1997.