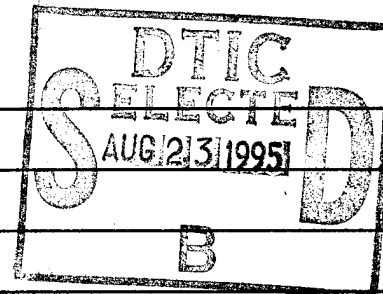


UNCLASSIFIED

Security Classification This Page

## REPORT DOCUMENTATION PAGE



1. Report Security Classification: UNCLASSIFIED			
2. Security Classification Authority:			
3. Declassification/Downgrading Schedule:			
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.			
5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT			
6. Office Symbol: C		7. Address: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, R.I. 02841-1207	
8. Title (Include Security Classification): THE JOINT COMSEC MONITORING ACTIVITY (JCMA): A FOGLIGHT FOR THE OPERATIONAL ARTIST? (U)			
9. Personal Authors: ARTHUR R. THOMPSON			
10. Type of Report: FINAL		11. Date of Report: 16 MAY 1995	
12. Page Count: 33			
13. Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.			
14. Ten key words that relate to your paper: C2-PROTECTION, COMMAND, COMMUNICATIONS, CONTROL, INFORMATION, JCMAT, MONITORING, OPERATIONS, SECURITY, WARFARE			
15. Abstract: The Joint COMSEC Monitoring Activity (JCMA) is a new capability available to joint operations commands. It can be viewed as an instrument of command and control (C2) protection of command and control warfare (C2W). In evaluating its potential contribution to the conduct of operational art, its greatest value appears to be for providing near-real-time input of what the enemy is likely to be perceiving from monitoring friendly unencrypted communications. To the extent possible, this can fill what will almost always be a critical intelligence gap. JCMA's joint composition, forward deployable Joint COMSEC Monitoring and Analysis Teams (JCMATs), and speed of service offer a unique combat multiplier to joint force commanders. JCMA is well into a two-year proof-of-concept period and has performed 17 missions, including both exercise and real-world operations. Supported commands have expressed satisfaction with the results and stated intentions to request JCMA support in the future. It appears JCMA is an effective tool for helping operational leaders see through the "fog" of war.			
16. Distribution / Availability of Abstract:	Unclassified  X	Same As Rpt	DTIC Users
18. Abstract Security Classification: UNCLASSIFIED			
19. Name of Responsible Individual: Chairman, Joint Military Operations Department			
20. Telephone: (401) 841-6457		21. Office Symbol: C	

Security Classification of This Page Unclassified

NAVAL WAR COLLEGE  
Newport, R.I.

THE JOINT COMSEC MONITORING ACTIVITY (JCMA):  
A FOGLIGHT FOR THE OPERATIONAL ARTIST?

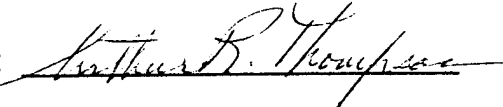
by

Arthur R. Thompson

GG-15, Civilian

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Joint Military Operations Department.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: 

16 June 1995

Paper directed by  
Captain David Watson, USN  
Chairman, Joint Military Operations Department

  
Faculty Advisor

Captain David R. Carrington, USN  
Edwin T. Layton Military Chair of Intelligence  
Professor, Joint Military Operations Department

  
Date

19950822 135

Abstract of

THE JOINT COMSEC MONITORING ACTIVITY (JCMA):  
A FOGLIGHT FOR THE OPERATIONAL ARTIST?

The Joint COMSEC Monitoring Activity (JCMA) is a new capability available to joint operations commands. It can be viewed as an instrument of command and control (C2) protection of command and control warfare (C2W). In evaluating its potential contribution to the conduct of operational art, its greatest value appears to be for providing near-real-time input of what the enemy is likely to be perceiving from monitoring friendly unencrypted communications. To the extent possible, this can fill what will almost always be a critical intelligence gap. JCMA's joint composition, forward deployable Joint COMSEC Monitoring and Analysis Teams (JCMATs), and speed of service offer a unique combat multiplier to joint force commanders. JCMA is well into a two-year proof-of-concept period and has performed 17 missions, including both exercise and real-world operations. Supported commands have expressed satisfaction with the results and stated intentions to request JCMA support in the future. It appears JCMA is an effective tool for helping operational leaders see through the "fog" of war.

Accession For	
NTIS GRA&I	<input checked="checked" type="checkbox"/>
DTIC TAB	<input type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification	
By	
Distribution	
Availability Codes	
Dist	Special
A-1	

FINAL QUALITY INSPECTED 83

## PREFACE

I was assigned to the fledgling Joint COMSEC Monitoring Activity from May 1993 to July 1994. During this period the main activities were: gaining final, formal commitment to JCMA's Concept of Operations and Memorandum of Agreement; gathering resources to get started; and supporting missions with an interim capability to demonstrate the concept. Thus, my knowledge of the background and intent of JCMA that is related throughout this paper stems from this personal experience. The JCMA director and other staff members have been most helpful in providing an update on organizational progress and operations.

# THE JOINT COMSEC MONITORING ACTIVITY (JCMA): A FOGLIGHT FOR THE OPERATIONAL ARTIST?

## TABLE OF CONTENTS

CHAPTER	PAGE
I. INTRODUCTION .....	1
II. BACKGROUND OF JCMA .....	2
Origins .....	2
Concept .....	3
III. USEFULNESS IN OPERATIONAL ART .....	7
Planning .....	7
Preparing .....	9
Conducting .....	11
Sustaining .....	12
IV. JCMA PERFORMANCE--FIRST YEAR .....	13
V. CONCLUSION .....	14
APPENDIX A--JCMA STRUCTURE AND CAPABILITIES .....	17
APPENDIX B--MISSIONS SUPPORTED BY JCMA .....	21
APPENDIX C--JCMA STATUS AND AVAILABILITY .....	23
NOTES .....	25
BIBLIOGRAPHY .....	28

# THE JOINT COMSEC MONITORING ACTIVITY (JCMA): A FOGLIGHT FOR THE OPERATIONAL ARTIST?

## I. INTRODUCTION

Students of military art make ready reference to the "fog of war," an adaptation of a metaphor used by Carl von Clausewitz in describing the use of intelligence information in war as part of "friction." Clausewitz wrote: "War has a way of masking the stage with scenery crudely daubed with fearsome apparitions . . . this is one of the great chasms between planning and execution."<sup>1</sup> The combatant commander cannot expect to fully penetrate this "fog of war," but his intelligence apparatus must try. The enemy is also subject to "fog," and one of the most critical needs of the friendly commander is to know how well the enemy is seeing through his "fog." As interaction takes place during the preparation, conducting and sustaining phases of campaigns and major operations, the practitioner of operational art needs to have the best possible idea of how he is being perceived by the adversary. The Joint COMSEC (communications security) Monitoring Activity provides a new capability that can be a peculiar kind of "foglight," illuminating for combatant commanders and other joint force commanders what the enemy is likely to be perceiving.

This paper is an analysis of the new JCMA concept as an interactive contributor to the execution of campaigns and/or major operations. By emulating adversary communications monitoring and analysis, JCMA can supply timely input to the dynamic operational risk management effort. It will introduce JCMA and assess

its potential and proven usefulness in operational art, a contrast to the traditional role of COMSEC monitoring just for after-the-fact communications protection advice (which is often viewed as having few practical results at the operational level and a nuisance with only punitive connotations). The main focus of this effort is to assess JCMA's potential as a combat multiplier for making unique contributions to the conduct of future joint military operations.

## II. BACKGROUND OF JCMA

### ORIGINS

The Joint COMSEC Monitoring Activity (JCMA) is an outgrowth of lessons learned from Operations Desert Shield and Desert Storm. The perception from these operations was that component service COMSEC monitoring efforts, while usually robust in themselves, have inherent shortcomings for joint operations. Their interest is, appropriately, in supporting their own component; their authority is usually limited to communications of their own component; and their expertise and perspective is centered on their own component, limiting their ability to interpret data and analyze it in the context of what is happening in the entire theater. Because of this inherent narrow focus and fragmentation, assessments of supporting operations and related strategic communications were likely to be overlooked. Reliance on national-level COMSEC monitoring assets to fill this gap still left a lack of unity in both the collection and the analysis efforts and a lack of control of civilian efforts not dedicated to the combatant commanders. JCMA was created to remedy these

shortcomings under the joint sponsorship of the National Security Agency (NSA) and the Joint Staff.

## CONCEPT

A Memorandum of Agreement among the Army, Navy, Marine Corps, Air Force, NSA, and Joint Staff contains JCMA's formal mission statement as follows:

The mission of the JCMA is to conduct COMSEC monitoring (collection, analysis, and reporting) of DoD [Department of Defense] telecommunications and automated information systems (AIS) and monitoring of related noncommunications signals. The purpose is to identify vulnerabilities exploitable by potential adversaries and to recommend countermeasures and corrective actions. Operations will focus primarily on unencrypted DoD systems. JCMA does not perform "traditional telephone monitoring"; this function is performed by the Service Cryptologic Elements (SCEs). JCMA may monitor telephone transmissions when they are accessible in the RF [radio frequency] environment. Priority during real-world operations will be to the supported CINC [Commander in Chief of a Unified Command]. Peacetime priorities will be to support joint exercises, DoD counternarcotics activities, and to conduct DoD systems monitoring.<sup>2</sup>

It is important to recognize in this mission that unencrypted systems are inherently available to an adversary, thus the focus on identifying exploitable vulnerabilities in this case means analyzing the content of signals as well as the significance of their mere presence or other identifying characteristics. This distinguishes JCMA's effort from traditional operational and/or strategic level COMSEC monitoring efforts, which have been directed primarily at discovering vulnerabilities occurring with the use of protection and/or encryption systems.\* These traditional efforts are in support of

---

\* In the vernacular of cryptology, encryption defines a very specific level of security; systems and/or procedures meeting a lesser standard are often referred to as protection. For simplicity's sake in the remainder of this paper, I will refer to encrypted or unencrypted without making the finer distinction.



communications elements and are of concern to the Joint Staff Directorate for Command, Control, Communications, and Computer Systems (J-6).<sup>3</sup> JCMA does produce the traditional advice on communications that ought to be encrypted, or on communications procedures, and this product can be an important contributor to lessons learned. But even with these results, JCMA's concept departs from what has been traditional practice. Ideally, all systems in any way related to joint military operations would be encrypted, but for both practical and cost reasons this will never be the case. Recognizing that encryption will be either impractical or too expensive for many support and tactical applications, JCMA has committed itself to recommending only countermeasures and corrective actions that are practical and inexpensive to implement.<sup>4</sup> Thus, timely reporting can lead to timely correction. But risk management decisions have been, and will continue to be made--one hopes deliberately and after careful analysis as part of the operations security (OPSEC) component of operational protection--to employ a variety of unencrypted communications and automated information systems signals in areas where classified information is not expected to be involved. JCMA's primary focus is on such signals, and its efforts are mainly in support of the operations elements, sponsored by the Joint Staff Directorate for Operations (J-3). It is the picture of friendly forces that JCMA creates from its analysis of unencrypted communications that is unique and becomes of near-real-time use to the combatant commander.

Thus, JCMA support can be viewed as a risk management tool for command and control warfare (C2W):

By taking an adversarial signals intelligence (SIGINT) perspective, JCMA can collect, analyze and report on friendly signals in the RF spectrum and provide a means to gauge success of C2-protection operations. JCMA can also recommend, from a risk management perspective, appropriate countermeasures or corrections to shore-up U.S. communications weaknesses. This information will assist a commander in accurately assessing the actual threat to a theater of operations and support his C2-attack efforts.<sup>5</sup>

The JCMA product of "assessing the actual threat to a theater of operations" is the most valuable to the operational artist. In March 1995, the Director, Joint Staff moved primary responsibility for JCMA matters to the J-3 from the J-6, surely in recognition of this more vital role as a combat multiplier.<sup>6</sup> An example of the application of this concept is in the U.S. Marine Corps publication Warfighting: "By studying our enemy we will attempt to appreciate his perceptions." These will change as interaction takes place, and a major cause will be information we reveal, so this philosophy requires anticipating how the enemy will change from what he learns. "We must try to see ourselves through our enemy's eyes in order to identify our own vulnerabilities which he may attack."<sup>7</sup> To integrate JCMA capabilities into C2W plans, preparations, and operations; JCMA has developed a close relationship with the Joint C2W Center (JC2WC) for involvement in C2W operation plan (OPLAN) development and joint exercise scripting.<sup>8</sup> This is consistent with NSA's responsibilities under the Chairman, Joint Chiefs of Staff (CJCS) Memorandum of Policy No. 30, Command and Control Warfare to "Assess US C2 vulnerability to, and evidence of actual exploitation by, adversary SIGINT. . . . Provide Information

Security (INFOSEC) [sic]\* measures and advice to help protect against hostile SIGINT and C2W efforts. . . . [and] Plan for, approve as authorized, and employ C2-protection in support of agency operations."<sup>9</sup>

In emulating an adversary monitoring and analysis effort, JCMA's concept is to use analysts from all of the services so that component expertise will be brought to bear. The JCMA analysts are not expected to use classified or "insider" information, but rather they prepare for and conduct their missions by using only information that is readily available to anyone dedicated to gathering and analyzing it. Thus, JCMA analytical conclusions can reasonably be attributed to any adversary who cares to seek them. JCMA's conclusions normally are to be provided without specific attribution so that they cannot be used for punitive purposes.<sup>10</sup> JCMA's joint military composition is also an important aspect of its concept; it is readily deployable and sustainable wherever needed.

When appropriate, and in coordination with the supported command, JCMA will deploy a Joint COMSEC Monitoring and Analysis Team (JCMAT) to the supported command's main or forward headquarters or to the headquarters of the joint task force (JTF). JCMAT personnel will come primarily from JCMA. The JCMAT will act as the forward HQ JCMA. The JCMAT will coordinate all COMSEC monitoring and analysis support for the supported command or JTF, perform initial analysis, and provide reports to the supported combatant commander.<sup>11</sup>

The JCMAT is the heart of JCMA's contribution to operational art. Its mission is: "To provide direct, deployable joint COMSEC monitoring support to combatant commanders during real world operations and joint exercises." Its composition is

---

\* The correct expansion of the acronym INFOSEC is information systems security.

tailored to meet the needs of the supported command. "If directed by the combatant commander, the JCMAT team leader will coordinate the efforts of all supporting COMSEC monitoring resources to include service component elements."<sup>12</sup> The latter point is an important adjunct to the overall JCMA mission because it brings into the JCMA analytical effort "traditional telephone monitoring" and any other component monitoring by individual service efforts. The JCMAT's most useful product to operational art is the Tactical Advisory (TACAD). It reports "tactically significant, time-sensitive intelligence information derived from COMSEC monitoring. . . . an intelligence loss that could provide opposing forces with some tactical advantage. It also provides a means to evaluate force posture and to change tactics as required based on the estimate of intelligence lost."<sup>13</sup> (Appendix A describes JCMA's organizational structure and capabilities).

### III. USEFULNESS IN OPERATIONAL ART

#### PLANNING

The risk management and combat multiplier advantages of JCMA support appear to be called for already in both the Deliberate Planning Process (DPP) and Crisis Action Planning (CAP). What JCMA can provide is specifically relevant to development of the Commander's Estimate of the Situation (CES) and the staff estimates which are its foundation.<sup>14</sup> (In the CJCS guidance, NSA is included among the supporting agencies that "should be considered early in the planning process."<sup>15</sup>)

In the DPP, the phase "Considerations Affecting the Possible Courses of Action (COA)" includes assessing "relative combat power." Elements to be

considered for each side in this assessment include OPSEC, deception, surprise, and knowledge of enemy intentions.

Weaknesses in one force's operations security procedures must be assessed in terms of the other force's ability to exploit the weakness. There are significant differences in intelligence collection capabilities between opposing forces; therefore it is important that the mirror image approach be avoided. A detailed analysis must be made to learn how the enemy "sees" the battlefield. Once this is determined, our own operations security vulnerabilities can be investigated.<sup>16</sup>

In the next step of the estimate process, "Development of Enemy Capabilities," it is important to consider enemy SIGINT capabilities and analytical paradigms in evaluating all possible enemy capabilities, intentions, and strategies. JCMA's reliance on such assessments for realistic emulation cause it to be closely connected to all sources of information on INFOSEC threat. Thus, JCMA should come to the table prepared to contribute a carefully considered view of what to expect. Friendly weaknesses and vulnerabilities are also to be considered during this step, and JCMA can bring a unique perspective and a breadth of experience in this area also.\*

In developing actual COAs, each needs to include essential elements of friendly information (EEFI)--the elements for the COA that need to be hidden from enemy view. Tests for suitability of the COA need to couple the EEFI with the knowledge of enemy capabilities--evaluation of whether or not the COA will achieve the military objective can only be accurate with a good knowledge of how the enemy

---

\* JCMA is required in its formal concept of operations (p. 4) to produce an annual report: "A general summary of the trends, common problems, and lessons learned observed by JCMA during the previous year."

will perceive the action. The same holds true for tests of feasibility. The ability of available forces to accomplish the mission is likely to depend on some element of deception and/or surprise, so this test needs to include evaluation of the abilities to protect EEFI and to adjust the plan if intentions appear to be compromised as interaction takes place. Tests for acceptability also need input of an assessment of how the enemy will be perceiving the COA--the cost-benefit calculation may vary greatly depending on the degree of surprise achieved for specific tactical actions within the major operation. Thus, it seems clear that the concept of operations for each retained COA needs to be developed with a full understanding of the EEFI that will be involved, and the OPSEC, C2-protection, and monitoring efforts that will best support the COA. The true relative importance of EEFI are likely to be revealed during the "Analysis of Opposing Courses of Action" phase of estimate development as the results of interactions between individual friendly and enemy COAs are assessed.

CAP will benefit from JCMA support plans that are generated as part of the DPP. JCMA's perspective will be available (and will have less chance of being overlooked) when deliberately generated plans are looked at for adaptation to CAP.<sup>17</sup>

#### PREPARING

"Know the enemy, know yourself; your victory will never be endangered."<sup>18</sup> This admonition from Sun Tzu is easy to accept but extremely difficult to accomplish. When preparing a theater of war or theater of operations, knowing the enemy is part of operational reconnaissance and intelligence and knowing yourself is part of operational protection. But both of these are dynamic as opposed to static

assessments because of the interactive nature of military activity. Knowing yourself includes, perhaps more importantly than any other element, the image of your arms, forces, strategy, and tactics that is perceived by the enemy. The adversary has made its own assessment and will use its intelligence capabilities to the fullest. Thus, OPSEC has become, at least in theory, an essential and integral part of military operations from their inception. JCMA support needs to be included in such plans and implemented at the start of the preparation phase along with other OPSEC procedures.

The supported commander's Letter of Instruction (LOI) that starts "Phase III-- Plan Development" of the Joint Operation Planning and Execution System (JOPES) process "should contain the supported commander's . . . OPSEC planning guidance." It follows that the resulting operation plan (OPLAN) and/or concept plan (CONPLAN) should include a COMSEC monitoring plan, best done by arranging for a JCMAT and providing for the combatant commander's operations staff to react to TACADs and other results of the monitoring effort. Supporting plans should include a JCMA support plan as provided for in JCMA's formal concept of operations.<sup>19</sup>

It is particularly important that EEFI be carefully determined and communicated to supporting commands early and with great emphasis because the EEFI will not be as readily apparent to those not directly anticipating combat and because supporting organizations are more likely to be using unencrypted communications. For example, the Vietnam-era "Purple Dragon" investigation (which was the genesis of today's OPSEC program) determined that bomber flight and refueling information passed in unencrypted communications revealed details of

aircraft destinations, routes, and schedules that was monitored and exploited by the North Vietnamese--certainly a key to the operation's questionable effectiveness.<sup>20</sup>

## CONDUCTING

In describing an estimate, the "Doctrine for Joint Operations" states: "the central focus for strategic, operational, and tactical analysis" includes "what has changed?"<sup>21</sup> JCMA's potential as a combat multiplier derives from its ability to supply to the friendly command and control process near-real-time assessments of EEFI that have become available to the adversary.

As the forces execute . . . the commander monitors the situation and makes adjustments to increase the effectiveness and efficiency of the operation. . . . The timely reduction of uncertainty, and hence reduction in the risk, of making decisions is one of the fundamental objectives of the command and control process. The ambiguity, fog, and friction of war, and the fact that combat is two-sided with commanders at all levels on both sides making decisions make the elimination of uncertainty and risk virtually impossible. However, the more efficient the command and control process, the greater the probability that the commander will make and execute the correct decisions in a more timely manner than the opposition, thus operating inside the decision cycle of the opposition and using friendly forces to their fullest and most effective capability.<sup>22</sup>

JCMA's unique contribution to plan execution can come from its multi-service composition, making it "component smart" across the spectrum of a joint environment; and from its ability to forward deploy and operate in near-real-time. The dynamics of this can be synergistic, and should be incorporated in training. In exercises actually involving opposing players, JCMA could play a dual role, serving "blue" forces in its normal role, and "red" forces as a SIGINT element. Allowance for such interaction seems to be embodied already, for example, in Air Force doctrine--exercises "must include 'free-play' scenarios . . . ." <sup>23</sup>



The last phase of the military planning process, "Supervision of Planned Action," is depicted by a decision block for the question "Is [the] mission being accomplished?" If the answer is "no," it may be the result of EEFI losses; but in any case JCMA results can contribute to changes in the plan. Even if the answer is "yes," it is still wise to consider whether or not there may be a more "acceptable" (cost-effective) way in view of any EEFI losses and/or inadvertently-created opportunities for deception. Indeed, use of such information seems to be the key for achieving "agility," defined in the CJCS policy on Command and Control Warfare as "thinking, planning, communicating, and acting faster than the enemy can effectively react"--attacking enemy C2 "while simultaneously protecting friendly C2."<sup>24</sup>

#### SUSTAINING

OPSEC, by definition, aims at "measures that eliminate or reduce to an acceptable level" risks to our EEFI.<sup>25</sup> Thus, the key to effective risk management is the determination of what constitutes an acceptable level of risk; to a great extent a function of the combatant commander's intuition, artistry, and experience. But Clausewitz pointed out that when faced with the reality of battle, commanders tend to be pessimistic: "As a rule most men would rather believe bad news than good, and rather tend to exaggerate the bad news."<sup>26</sup> An example of this overcautious tendency became one of the lessons learned from Operation Eagle Claw, the 1980 attempt to rescue U.S. hostages in Iran: "there needs to be a balance between the emphasis on operational security (OPSEC) and effective communications . . . Security considerations should not so completely stifle effective communications that the mission being created is doomed to failure before it begins--because of

overprotection."<sup>27</sup> Joint Doctrine for Intelligence Support to Operations states the central principle of joint intelligence is "know the adversary." This specifically includes "Understanding how an adversary will conceptualize the situation. . . . How will the adversary likely perceive this action . . . ?"<sup>28</sup> Emulating at least minimal capabilities of the adversary can give a much improved basis for risk management of communications rather than simply precluding them.

The principles of warfare include security and surprise; and security "includes prudent risk management. . . . The purpose of security is to never permit the enemy to acquire unexpected advantage."<sup>29</sup> Surprise is the other side of this point, acquiring an advantage that the enemy does not expect. Each of these relies on the combatant commander knowing what to expect. The compromise of an EEFI is dangerous, but far more perilous is to have compromised an EEFI and not be aware of it. JCMA support can be a combat multiplier for sustaining operations by protecting assets and saving lives. This enhancement not only can preserve forces, but it also can sustain the critical element of U.S. public support by helping to keep casualties as low as possible.<sup>30</sup> Awareness can turn an EEFI loss into an opportunity for deception. Ignorance is not always bliss!

#### IV. JCMA PERFORMANCE--FIRST YEAR

Since May 1993, JCMA has supported 17 missions, mostly joint exercises. Appendix B is a list of the missions, each associated with the supported command.<sup>31</sup> Although the specific results of these efforts are required to stay under the proprietary control of the supported command, the Director of JCMA reports that in

every case the customer has expressed satisfaction with JCMA results and an intent to request JCMA support in the future.<sup>32</sup> The major real-world mission in this period was Vigilant Warrior, the U.S. reaction to the Iraqi build-up of forces in southern Iraq in October 1994. The CINC, United States Central Command (USCENTCOM), formally described JCMA support as "excellent" and added: "Future USCENTCOM operations and exercises will include plans for JCMA support, which I regard as key in helping identify and pursue objectives for C2 Protect."<sup>33</sup> In addition to direct support to these missions, JCMA produced a report of "generic" highlights and trends which has been distributed to a wide community that includes the Unified Commands and service COMSEC elements. "During its short life-span, JCMA has routinely monitored communications that revealed information on real-world operations, missions and future plans. These communications provided COMSEC analysts (and potentially, adversary SIGINT analysts) with sensitive information on real-world operations in the USACOM [U.S. Atlantic Command], EUCOM [U.S. European Command] and CENTCOM areas of responsibility."<sup>34</sup> JCMA customer service representatives also have assisted in seeking practical countermeasures for identified vulnerabilities, attempting to stick with each customer need from "cradle to grave."<sup>35</sup> (Appendix C describes JCMA's status and availability.)

## V. CONCLUSION

MG John F. Stewart, Jr., Commandant of the U.S. Army Intelligence School, sees the need for the fullest picture of C2-protection as critical for the electronic innovations that comprise the "digitized battlefield":

We must develop solutions across DOTLMS [doctrine, organizations, training, leaders, material and soldiers] that give us the capability to identify when our information systems are being attacked and allow us to respond to these attacks. . . . As the digital battlefield becomes a fundamental element of the commander's knowledge base, requirements to use and protect this capability will become critical to the success of military operations.<sup>36</sup>

An adversary's actual conclusions from monitoring friendly unencrypted communications and noncommunications signals virtually always will be an intelligence gap. JCMA support can give a basis for risk management--both for modifying plans because of conclusions discernable by JCMA, and for proceeding with some confidence that the risk is reasonable because EEFI have not been discernable by JCMA. The latter, a "negative-positive," would be, of course, only one of many inputs available to the commander. While JCMA by charter seeks to emulate the adversary, it will never be able to duplicate an adversary possessing extensive and robust intelligence capabilities. Thus, in the face of the tendency noted by Clausewitz and cited earlier in this paper for commanders to be overly-pessimistic, JCMA results can be considered to be conservative by their nature because of JCMA's very modest resources in contrast to almost any adversary's intelligence apparatus. An additional contribution that JCMA can make from its assessment of actual adversary capabilities is recommendations of targets for destruction to "deafen" and "blind" the adversary at the outset of hostilities.<sup>7</sup>

Reassessing and changing plans based on changes in the situation is one of the basic functions of operational leadership. A dynamic, joint COMSEC monitoring program can make the principles of security and surprise much more likely to be achieved. The operational design needs to be flexible so that the operational idea

can be altered based on interaction on the battlefield. JCMA results can indicate which branch to take, alterations in sequencing of tactical actions, or when to start the next phase of the operational scheme, for example.

JCMA support clearly has the potential to be a "foglight" for the operational artist. And, according to Michael Howard's commentary on Clausewitz, those who have found a way "to discern through the fog of war what was happening" often are attributed with military genius.<sup>38</sup>

APPENDIX A

JCMA STRUCTURE AND CAPABILITIES

## JCMA STRUCTURE AND CAPABILITIES

JCMA is a joint service organization "under the operational control of NSA." Its headquarters is located at NSA and is closely aligned with NSA's Office of COMSEC Monitoring and Analysis (OCMA). An organizational chart is enclosed. JCMA's Director, currently a military O-6,\* is dual-hatted as the chief of that NSA office, which is responsible for the national-level COMSEC monitoring and analysis effort. Thus, resources can be used flexibly, and unity of effort is assured through the control of this individual. JCMA's seven officer positions are staffed by NSA and four are joint duty assignment (JDA) rotational billets; its 44 enlisted positions are allocated and staffed by the individual services. NSA also has contributed 12 civilians, mainly for headquarters management, technical expertise, and coordination roles.<sup>39</sup>

JCMA describes its signals monitoring capabilities, as listed on the enclosed chart, as follows:

To accomplish its mission, JCMA has four Regional COMSEC Monitoring Centers (RCMCs) throughout the world, a vast array of deployable monitoring equipment and access to Service COMSEC monitoring assets. The four RCMCs . . . have a collective capability of monitoring voice, data, facsimile and modem communications from VLF to SHF. The majority of support is with HF, UHF/VHF Tactical Satellite (FLTSAT, LEASAT, AFSAT, etc.) and other satellite communications. JCMA's array of deployable equipment includes a mobile RCMC, collection vans, S-250 shelters and fly-away equipment to support theater-based long-haul and line-of-site [sic] monitoring requirements. Service assets are used to conduct telephone monitoring and support tactical commander line-of-site [sic] communications security needs.<sup>40</sup>

In addition to its arrangements with the services for complementary use of component assets and with NSA for use of national assets, JCMA has arrangements with component reserves to use individual augmentees. In supporting joint exercises, JCMA has demonstrated that a string of individual reservists--each performing two weeks of active duty--can be managed effectively to succeed each other in filling a single position, providing a low-cost source of augmentation.

---

\* The military officer grade O-6 is Colonel in the Army, Marines, and Air Force; and Captain in the Navy.



# ORGANIZATION

**Manning**  
**Officer 8**  
**Enlisted 47**  
**Civilian 60**

**C5**  
**OCMA/JCMA**

**C51**  
**Plans, Programs and**  
**Technical Support**

**C511**  
**Rqmnts & Tasking**

**C512**  
**Technical Support**

**C513**  
**Mission Support**

**Regional COMSEC**  
**Monitoring Centers**

**PISCES**

**WATERCUP**

**FIREBACK**

**SPRINKLER**

**C52**  
**Operations**

**C521**  
**Collection Mgmt**

**C522**  
**Technical Analysis**

**C523**  
**Analysis & Rptg**

JCMA/OCMA INTEGRATED ORGANIZATIONAL CHART<sup>41</sup>





# CAPABILITIES

## COVERAGE

FREQUENCIES: VLF, LF, HF, VHF, UHF, SHF  
SYSTEMS: SATCOM, INMARSAT, RADIO  
MODE: VOICE, FAX, MODEM

## SYSTEMS

### RCMCs

ALL FREQUENCIES, ALL SYSTEMS, ALL MODES

### FLYAWAY PACKAGES (SPLASHDOWN)

COMPREHENSIVE PORTABLE COLLECTION, ANALYSIS, AND  
COMMUNICATIONS/REPORTING CAPABILITY  
ALL FREQUENCIES, ALL SYSTEMS, ALL MODES

### MOBILE SYSTEMS

FULLY CONFIGURED COMSEC VAN  
MOBILE SELF-CONTAINED COLLECTION, ANALYSIS,  
REPORTING AND COMMUNICATIONS TRAILER  
ALL FREQUENCIES, ALL SYSTEMS, ALL MODES

### SCE AUGMENTATIONS

MISSION DEPENDENT  
CONVENTIONAL WIRELINE TELEPHONE, LINE OF SIGHT  
(HF, VHF, UHF)

APPENDIX B

MISSIONS SUPPORTED BY JCMA



## Unit Supported

## Mission

USACOM

OCEAN VENTURE 93  
AGILE PROVIDER 94  
JTF-4

USSTRATCOM

BULWARK BRONZE 94

USCENTCOM

RESTORE HOPE 94  
INTRINSIC ACTION 94  
VIGILANT WARRIOR 95

USEUCOM

EAM ASSESSMENT  
USAFE AIR OPERATIONS  
ABLE SENTRY PREPARATIONS  
COMSIXTHFLT

USPACOM

LIGHTNING THRUST 94  
TEMPO BRAVE 94  
TANDEM THRUST 95

USFK

FOAL EAGLE 95  
ULCHI FOCUS LENS 94

US COAST GUARD

CARIBBEAN OPERATIONS

MISSIONS SUPPORTED BY JCMA<sup>43</sup>

APPENDIX C

JCMA STATUS AND AVAILABILITY

## JCMA STATUS AND AVAILABILITY

JCMA began operating in May 1993 as the formal concept of operations was being finalized, initially borrowing resources from the services and NSA. All of the billets now have been allocated and staffing is increasing steadily. A multi-year equipment procurement program started in fiscal year 1994, adding additional monitoring equipment for JCMA at each of the RCMCs and acquiring equipment suitable for deployment with a JCMAT. A two-year proof-of-concept period started with the conclusion of the Memorandum of Agreement in September 1994.<sup>44</sup>

Each February, JCMA is to solicit mission requirements for the upcoming fiscal year and prepare a prioritized Mission Requirements List which is then submitted to the Joint Staff for validation. Requests that are received later will be worked into the schedule as possible. Real-world operations will always take priority.<sup>45</sup> Basic funding for JCMA and real-world deployments is arranged through NSA. Funding for participation in exercises is expected to be allocated as part of exercise costs, but this is negotiated during planning for each exercise.<sup>46</sup>

Legal constraints are imposed on all COMSEC monitoring by National Telecommunications and Information Systems Security Directive 600, federal statutes and implementing regulations, Executive Orders, and Department of Defense directives and regulations. JCMA will always obtain a prior legal review of monitoring missions; customer commands and participating component service COMSEC elements must fulfill legal notification requirements and submit certification for this review.<sup>47</sup> To ensure this process can be carried out expeditiously, JCMA is pursuing and encouraging combatant commands to pursue standing certification, renewed as frequently as the law requires.

To assist in all phases of COMSEC monitoring support, JCMA has assigned a customer service representative for each Unified Command. JCMA can be reached by phone at DSN 644-0111, Extension 6184; or commercial (410) 859-6184.<sup>48</sup>

## NOTES

1. Carl von Clausewitz, On War (Princeton: Princeton University Press, 1984), pp. 117-118.
2. U.S. Joint Staff, "Support of the Joint COMSEC Monitoring Activity (JCMA)," Memorandum of Agreement (Washington: 27 September 1994), p. 2.
3. Armed Forces Staff College, The Joint Staff Officer's Guide 1993, AFSC Pub 1 (Norfolk, VA: 1993), p. 2-16.
4. Telephone conversation with Colonel Raleigh H. Macklin, USAF, Director, Joint COMSEC Monitoring Activity, Ft. Meade, MD, 17 March 1995.
5. Helena E. Reeder, "JCMA...Support to the Warfighter," Unpublished Organizational Description, Joint COMSEC Monitoring Activity, Ft. Meade, MD: 1995, p. 2.
6. U.S. Joint Staff, "Joint COMSEC Monitoring Activity," Memorandum (Washington: 2 March 1995).
7. U.S. Marine Corps, Warfighting, FMFM 1 (Washington: 1989), pp. 61 & 66.
8. Telephone conversation with Director, JCMA.
9. U.S. Chairman of the Joint Chiefs of Staff, Command and Control Warfare, Memorandum of Policy No. 30 (Washington: 8 March 1993), p. 26.
10. Joint COMSEC Monitoring Activity, Joint COMSEC Monitoring Activity Concept of Operations (Ft. Meade, MD: 18 June 1993), p. 2.
11. Ibid.
12. Ibid., pp. B-1 & B-2.
13. Ibid., p. C-1.
14. U.S. Joint Chiefs of Staff, Joint Operation Planning and Execution System, Volume I (Planning Policies and Procedures), Joint Pub 5-03.1 (Washington: 1993), p. III-9.
15. Ibid., pp. V-5 & V-6.
16. Ralph G. Rosenberg, "Relative Combat Power," Military Review, March 1978; reprint ed., NWC 4088, Newport, RI: U.S. Naval War College, n.d., pp. 61-63 & 66.
17. U.S. Joint Chiefs of Staff, Joint Operations Planning and Execution System, p. V-1.

18. Samuel B. Griffith, trans., Sun Tzu, The Art of War, (London: Oxford University Press, 1963) p. 129.
19. U.S. Joint Chiefs of Staff, Joint Operations Planning and Execution System, pp. III-9, III-10 & III-26; Joint COMSEC Monitoring Activity, Concept of Operations, p. 2.
20. Reeder, p. 3.
21. U.S. Joint Chiefs of Staff, Doctrine for Joint Operations, Joint Pub 3-0, (Washington: 1993), p. I-10.
22. E. K. Nielsen, Command and Control, NWC 3152 (Newport, RI: U.S. Naval War College, n.d.), p. 3.
23. U.S. Air Force, Basic Aerospace Doctrine of the United States, Air Force Manual 1-1, v. 1 (Washington: 1992; reprint ed., NWC 3111, Newport, RI: U.S. Naval War College, 1992), p. 18.
24. U.S. Chairman of the Joint Chiefs of Staff, Command and Control Warfare, p. 4.
25. Ibid., p. A-1.
26. Clausewitz, p. 117.
27. Stephen E. Anno and William E. Einspahr, Command and Control and Communications Lessons Learned: Iranian Rescue, Falklands Conflict, Grenada Invasion, Libya Raid, Air War College Research Report, No. AU-AWC-88-043 (Maxwell Air Force Base, AL: U.S. Air Force, Air University, n.d.; reprint ed., NWC 3231, Newport, RI: U.S. Naval War College, n.d.), pp. 3-18.
28. U.S. Joint Chiefs of Staff, Joint Doctrine for Intelligence Support to Operations, Joint Pub 2-0 (Washington: 12 October 1993), pp. IV-1 & IV-2.
29. U.S. Joint Chiefs of Staff, Doctrine for Joint Operations, p. I-10.
30. Telephone conversation with Lieutenant Commander Helena E. Reeder, USN, Chief, Requirements and Tasking Branch, Joint COMSEC Monitoring Activity, Ft. Meade, MD, 12 May 1995.
31. Joint COMSEC Monitoring Activity, "JCMA/OCMA Organizational Briefing," Unpublished Briefing Charts, Ft. Meade, MD: March 1995, p. 8.
32. Telephone conversation with Director, JCMA.
33. Letter from Commander in Chief, United States Central Command, to Director, JCMA, 13 December 1994.

- 34. Reeder, p. 7.
- 35. Telephone conversation with Director, JCMA.
- 36. John F. Stewart, "Command and Control Warfare and Intelligence on the Future Digital Battlefield," Army Research, Development and Acquisition Bulletin, November-December 1994; reprint ed., NWC 3169, Newport, RI: U.S. Naval War College, n.d., pp. 14-15.
- 37. Reeder, p. 5.
- 38. Michael Howard, Clausewitz (Oxford: Oxford University Press, 1983), p. 27.
- 39. Joint COMSEC Monitoring Activity, Concept of Operations, pp. A-1 & A-3.
- 40. Reeder, pp. 5-6.
- 41. Joint COMSEC Monitoring Activity, "JCMA/OCMA Organizational Briefing," p. 9.
- 42. Ibid., p. 11.
- 43. Ibid., p. 8.
- 44. Telephone conversation with Director, JCMA.
- 45. Joint COMSEC Monitoring Activity, Concept of Operations, p. 3.
- 46. Telephone conversation with Director, JCMA.
- 47. Joint COMSEC Monitoring Activity, Concept of Operations, p. 5.
- 48. Telephone conversation with Reeder.



## BIBLIOGRAPHY

- Anno, Stephen E. and William E. Einspahr. Command and Control and Communications Lessons Learned: Iranian Rescue, Falklands Conflict, Grenada Invasion, Libya Raid. Air War College Research Report, No. AU-AWC-88-043. Maxwell Air Force Base, AL: U.S. Air Force, Air University, n.d.; reprint ed., NWC 3231. Newport, RI: U.S. Naval War College, n.d.
- Armed Forces Staff College. The Joint Staff Officer's Guide 1993. AFSC Pub 1. Norfolk, VA: 1993.
- Clausewitz, Carl von. On War. Princeton: Princeton University Press, 1984.
- Griffith, Samuel B., trans. Sun Tzu, The Art of War. London: Oxford University Press, 1963.
- Howard, Michael. Clausewitz. Oxford: Oxford University Press, 1983.
- Joint COMSEC Monitoring Activity. "JCMA/OCMA Organizational Briefing." Unpublished Briefing Charts, Ft. Meade, MD: March 1995.
- \_\_\_\_\_. Joint COMSEC Monitoring Activity Concept of Operations. Ft. Meade, MD: 18 June 1993.
- Letter from Commander in Chief, United States Central Command, to Director, JCMA, 13 December 1994.
- Nielsen, E. K. Command and Control. NWC 3152. Newport, RI: U.S. Naval War College, n.d.
- Reeder, Helena E. "JCMA...Support to the Warfighter." Unpublished Organizational Description, Joint COMSEC Monitoring Activity, Ft. Meade, MD: 1995.
- Rosenberg, Ralph G. "Relative Combat Power." Military Review, March 1978; reprint ed., NWC 4088. Newport, RI: U.S. Naval War College, n.d., pp. 56-67.
- Stewart, John F. "Command and Control Warfare and Intelligence on the Future Digital Battlefield." Army Research, Development and Acquisition Bulletin, November-December 1994; reprint ed., NWC 3169. Newport, RI: U.S. Naval War College, n.d., pp. 14-15.
- Telephone conversation with Colonel Raleigh H. Macklin, USAF, Director, Joint COMSEC Monitoring Activity, Ft. Meade, MD. 17 March 1995.

Telephone conversation with Lieutenant Commander Helena E. Reeder, USN, Chief, Requirements and Tasking Branch, Joint COMSEC Monitoring Activity, Ft. Meade, MD. 12 May 1995.

U.S. Air Force. Basic Aerospace Doctrine of the United States. Air Force Manual 1-1, v. 1. Washington: 1992; reprint ed., NWC 3111. Newport, RI: U.S. Naval War College, 1992.

U.S. Chairman of the Joint Chiefs of Staff. Command and Control Warfare. Memorandum of Policy No. 30. Washington: 8 March 1993.

U.S. Joint Chiefs of Staff. Doctrine for Joint Operations. Joint Pub 3-0. Washington: 1993.

\_\_\_\_\_. Joint Doctrine for Intelligence Support to Operations. Joint Pub 2-0. Washington: 12 October 1993.

\_\_\_\_\_. Joint Operation Planning and Execution System, Volume I (Planning Policies and Procedures). Joint Pub 5-03.1. Washington: 1993.

U.S. Joint Staff. "Joint COMSEC Monitoring Activity." Memorandum. Washington: 2 March 1995.

\_\_\_\_\_. "Support of the Joint COMSEC Monitoring Activity (JCMA)." Memorandum of Agreement. Washington: 27 September 1994.

U.S. Marine Corps. Warfighting. FMFM 1. Washington: 1989.