INTELLIGENCE DISSEMINATION IN THE JOINT LOW-INTENSITY CONFLICT ARENA

Submitted to
Major Tritchler
and Mrs. Cundick
at the Communication Officers School
Quantico, Virginia

Captain B. M. Downs
Captain E. L. Segarra (Editor)
Captain H. W. Vernon
Captain C. L. Levy
Captain V. F. Feliu

United States Marine Corps

April 1, 1991

INTELLIGENCE DISSEMINATION IN THE JOINT LOW-INTENSITY CONFLICT ARENA

OUTLINE

Thesis Statement: When it comes to intelligence support in a low-intensity conflict arena, the problems go beyond the issue of dissemination and into the equally important areas of system and procedure standardization, operator training and tailored operational architecture. To address one of these areas and neglect the others will inevitably lead to a serious degradation in our ability to defeat the enemy in this level of warfare.

I. **Introduction**

II. **Low-Intensity Conflict: The Nature of the Beast**

III. **Current LIC Architecture: The Tower of Babel**

- A. The National Picture
- B. The Front Lines: CINCs and Country Teams
- C. The Marine Corps

IV. **Lessons From Vietnam and Beirut**

V. **Intelligence Dissemination at the Front Lines**

- A. Linking Strategic and Tactical Assets
- B. The Marine Corps Connection
- C. Future Systems: Design and Integration

VI. **Conclusions**

VII. **Bibliography**

"It is the third world, the so-called low intensity arena, where we are most likely to be committed this decade."

A. M. Gray
General, USMC, 1988

INTRODUCTION

Armed conflicts come in all sizes, large and small. The difference between them is primarily one of tactics and scale rather than objectives. However, one undeniable rule of combat still holds true no matter the size of the conflict: knowledge of the enemy leads to success on the battlefield. The acquisition, effective production and dissemination of this knowledge is the task of military intelligence.

The complexity of this task in a low intensity conflict (LIC) environment is significantly greater than in large scale conflicts where the enemy moves in formations over a wide front. Considering the joint aspects of every U.S.-led unconventional warfare effort around the world, and the political nature of LIC, it can be expected that any military initiative in this area will include the gamut of U.S. civilian and military intelligence agencies. Such large number of players will inevitably raise one serious question: in a LIC environment, what kind of joint structure exists, or needs to be created, to ensure the effective

dissemination of processed intelligence to the proper consumer? This paper seeks to find an answer to this question.

LOW INTENSITY CONFLICT: THE NATURE OF THE BEAST

As a form of warfare, low-intensity conflicts appear to have certain unique characteristics setting them apart from other forms of warfare. Chief among these is the political nature of LIC. In these highly politicized conflicts the traditional distinctions between civilians and combatants--and front and rear areas--are extremely blurred, and sometimes do not exist at all. In an attempt to define this form of warfare from a military standpoint, the Joint Chiefs of Staff (JCS) have produced the following definition:

> ...a political-military confrontation between contending states or groups below conventional war and above the routine, peaceful competition among states. It frequently involves protracted struggles of competing principles and ideologies. Low-intensity conflict ranges from subversion to the use of armed force. It is waged by a combination of means employing political, economic, informational, and military instruments. (15:1)

For at least one side, the conflict involves a struggle for a redefinition of the existing political structure within a particular country. The so-called "center of gravity" is the target country's political system. Because of this, the instruments by which this type of conflict is

waged are not purely military, and involve a heavy dose of political solutions. For U.S. military intelligence this translates into the need to fully understand the enemy by having to address a wide range of non-military issues associated with LIC. The military must now venture (in peace as well as in war) into a political-cultural dimension which is not its traditional area of expertise.

Both U.S. military and civilian agencies appear to be ill-equipped and organized for the task. Says one critic:

> Experience has repeatedly shown that unconventional warfare requires a combination of military, economic, political, and psychological tools. Such an interdisciplinary response transcends the organizational boundaries of the U.S. government structure. (23:145)

Perhaps one of the problems in designing this structure can be traced to the many types of conflicts which fall under LIC. In fact, no attempt to define LIC could ever account for this diversity. Thus the problem of definition persists.

But inability to adequately define the concept does not necessarily translate into inability to recognize it. The study of the various LIC-type conflicts allows for some generalizations to be made as to the nature of these conflicts. First, LIC is most likely to occur in the Third World where countries are experiencing significant social and economic changes. Second, while the struggle will be

fought in both rural and urban areas, it will tend to be geographically limited. Third, low intensity does not necessarily equate with low threat or low violence. Fourth, LIC is essentially a political struggle with deep military, economic, social and cultural ramifications.

These many components of LIC require that joint intelligence efforts to be directed to a different operational level than that of conventional warfare. Brigadier General James D. Beans, Director of Intelligence, USMC, recognized this fact when he wrote:

> LIC intelligence requirements necessarily focus at a lower, grass-roots level. Enemy order of battle and data bases usually must be generated to a lower level....Rapid dissemination of highly perishable intelligence will be required to the lowest levels to exploit collection or operational opportunities. (2:29)

It is precisely at the dissemination phase where the greatest challenges and limitations of joint intelligence operations are to be found. Some analysts believe the U.S. experience has been a study in limitations. (23:160) But has it? And if it has, what can be done about it?

CURRENT LIC ARCHITECTURE: THE TOWER OF BABEL

THE NATIONAL PICTURE

At the national level four major agencies are involved in peacetime low-intensity conflict operations: the National Security Council (NSC), the Department of State (DOS), the

Department of Defense (DOD), and the Central Intelligence Agency (CIA). These agencies, while legally and operationally interrelated by virtue of an Executive Order and National Security directives, (22:150) lack any such document defining their interaction for LIC operations in peacetime.

During times of peace, it is the responsibility of the Secretary of State to conduct overt LIC operations. The State Department accomplishes this by means of its country teams, which in turn are headed by the U.S. chief of mission (usually the U.S. Ambassador).

DOD, for its part, has three primary entities involved in LIC operations: the Joint Chiefs of Staff (JCS), the Defense Intelligence Agency (DIA), and the commanders in chief (CINCs) of the various unified commands. Within the JCS, low-intensity conflict is the specialty of the Special Operations Division of the Joint Staff (J-3/SOD). This is an advisory body with no troops at its disposal.

Strategic intelligence is primarily the realm of the CIA. Like the theater CINCs, the CIA possesses limited resources and must constantly prioritize its efforts in accordance with those conflicts likely to have the greatest impact on national security.

The operational relationship between these major players is not a concerted one. In fact, when it comes to LIC operations, the intelligence picture is neither unified

nor well orchestrated. This becomes evident when we look at those who work inside the LIC operational trenches: the CINCs and the country teams.

THE FRONT LINES: THE CINCS AND THE COUNTRY TEAMS

By law, the country teams and the CINCs of regional unified commands are tasked with coordinating and sharing intelligence information related to LIC operations. This is accomplished primarily by an exchange of staff personnel. The country team will normally have a defense attache and possibly a military advisory group attached to it and will be headed by the chief of station (COS); the CINC staff will have a foreign service officer performing similar liaison functions. LIC, however, remains the primary responsibility of the State Department and its country teams--a civilian-led political effort.

This setup places some limitations on the country teams, especially during wartime. For one, the State Department's only organic intelligence agency is the Bureau of Intelligence and Research (INR). This bureau produces intelligence only in support of strategic foreign policy goals. Moreover, DOD personnel attached to the country teams are not only legally barred from collecting their own intelligence, but are also cut off from the military intelligence being generated by the CINC staff. DIA, while providing some support to these teams, does not have a

standing mission to do so, and therefore, the teams can only request information from the agency, but not demand it. From an intelligence dissemination perspective, it becomes readily obvious that information tends to flow in many directions at the same time, but not necessarily to those who need it the most.

The picture is equally complicated within the military unified command structure. By definition, unified commands draw forces from all military services, and generally from a specific region of the world. Each service has its own intelligence component responding to its unique service requirements. However, their peacetime intelligence effort in insurgency-type conflicts are severely limited by law and practice. Under a 1962 Security Action Memorandum signed by President Kennedy, (23:155) overall command for LIC operations in situations short of war was placed under the State Department. Inter-agency coordination would take place at the NSC level. This political approach at the highest levels was found to be severely lacking during the Vietnam conflict.

The picture is further complicated when you look at the CINC intelligence command structure. In the Pacific Command (which covers the Indian Ocean region, parts of Africa, India, Australia, Japan, China, Alaska, parts of Canada and the United States) a significant number of intelligence organizations can be found either directly subordinate to

the command itself or to one of its components. Directly subordinate to the CINC Pacific Command (CINCPACOM) you will find the Director for Intelligence and the Director for Operations. The Director of Intelligence manages four divisions (Planning and Systems, Management, Collection Management, and Special Security), one of which (Management) is responsible for coordination of target intelligence matters with national agencies. However, simplicity ends here, as can be seen by figures 1 and 2.

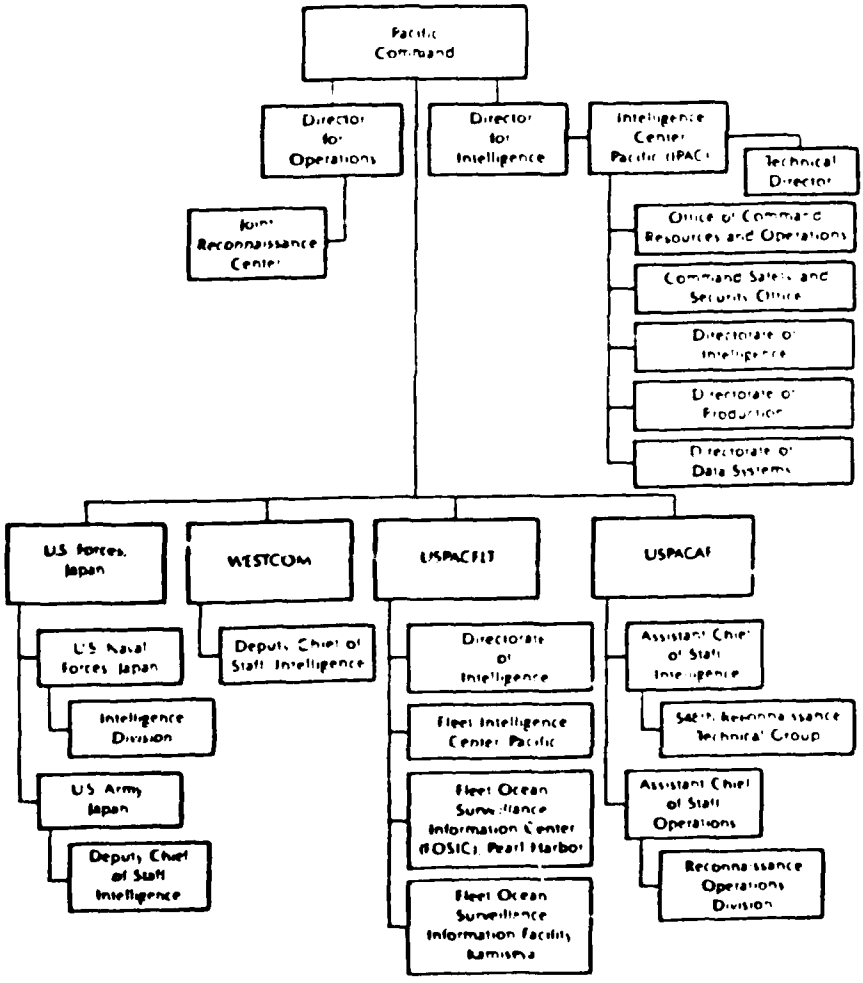

Figure 1.

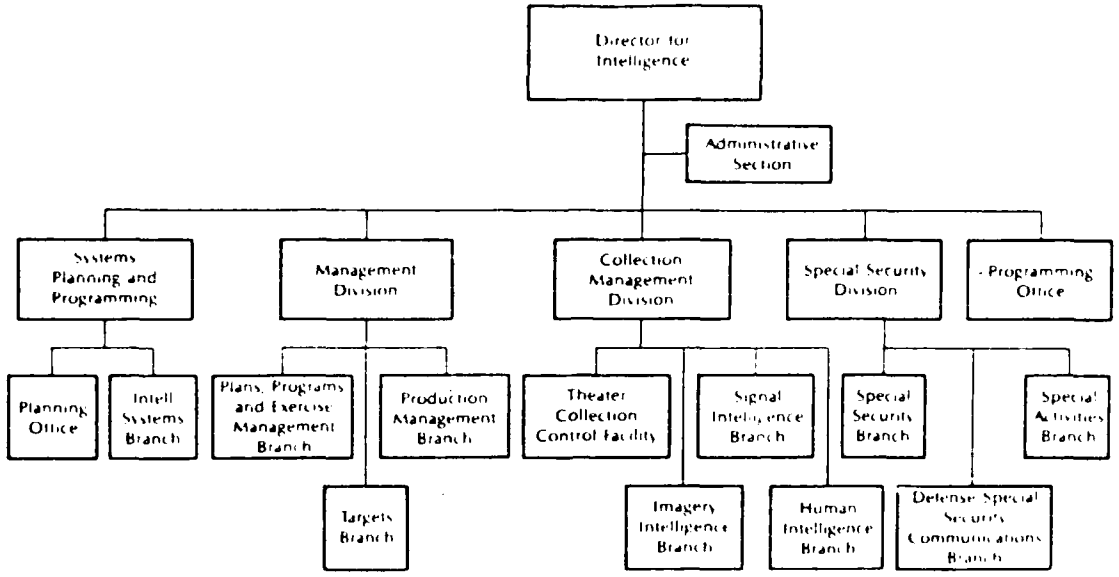

Figure 2.

As it stands, the CINC's intelligence architecture may be too cumbersome to support LIC-type operations. This architecture responds primarily to agency function rather than operational task, and because of this, it is not designed to fuse and disseminate intelligence product at the lowest levels where insurgency and unconventional warfare are dealt with. But is the picture really that bad? A look at intelligence dissemination within the Marine Corps may provide a clue.

THE U.S. MARINE CORPS

Currently, the Marine Corps utilizes the so-called "top-down" intelligence dissemination system. Under this system, primary responsibility for intelligence matters is placed at the MAGTF G-2 section, which in turn accomplishes

its tasks through the employment of a task-organized SRIG detachment.

In the joint LIC arena, this MAGTF G-2 section will be the link between the deployed MAGTF and any external participating agencies. This relationship was well depicted in a series of studies conducted by Captain W. Philbin of the Marine Corps Warfighting Center, Quantico, Virginia. (21:1) According to these studies, the MEF G-2 (or its lower-echelon MAGTF equivalent) has cognizance over intelligence information input from national and theater collection and analysis assets. Intelligence from local country teams and the operating National Military Intelligence Support Teams (NMIST) will also come to the G-2 section prior to dissemination to lower echelons. Conversely, intelligence gathered by MAGTF elements will be routed via the G-2 section prior to dissemination to external agencies.

Central to the MAGTF intelligence structure is the SRIG concept. As pointed out by Lieutenant Colonel D. R. Fry, Senior Intelligence Instructor on the MAGTF Integration Team, (10:-) prior to the formation of the SRIG, all Marine Corps intelligence assets were independent of each other and often operated without the expected amount of cooperation and coordination which brings about mission enhancement.

The intelligence fragmentation which existed in the Marine Corps prior to the formation of the SRIG was

representative of a greater problem confronting the joint intelligence community: the lack of unity of command. In his extensive analysis of the role of this community in LIC operations, Michael H. Schoelwer, a long time military analyst, observed that some of the problems within the community were rooted on the lack of acceptance of a seemingly simple concept: that proper intelligence flow is a function of the existing command structure. Schoelwer stated that, "If the chain of command lacks unity, coherence, and clarity, intelligence cannot be efficiently used." (23:160)

The current top-down dissemination system significantly clears up the fragmentary system which existed in the past, but at a price. By somewhat forcing centralization of the dissemination process, the system may have planted the seed of delay in the exchange of critical time-sensitive intelligence between echelons. These delays could be critical, especially in a LIC environment dominated by counterinsurgency operations.

Also apparently lacking in this system (and in the joint arena as well) are established procedures for skip-echelon reporting. This form of reporting would allow--when the mission requires it--both intelligence and critical combat information to be disseminated throughout the different levels of command without the constraints and

time-consuming limitations associated with the top-down system.

LESSONS FROM VIETNAM AND BEIRUT

Vietnam proved to be the classical case of intelligence fragmentation and parochialism. The war had caught the U.S. intelligence community by surprise, specially as it related to unconventional warfare. Without an existing structure with which to address unconventional warfare and its politico-military aspects, both military and civilian agencies attempted to deal with this type of warfare from a conventional and parochial standpoint. At least during the first part of the conflict the results were extremely disappointing. William Colby, then a senior CIA operative in Vietnam, alluded to this parochialism:

> The predominance of the American military during the mid-1960's produced the problem that intelligence concentrated on the military aspects of the enemy....Their focus, therefore, was the Communist military enemy rather than the "civilian" activist who inhabited the rural communities or visited them to conduct the basic elements of the people's war strategy--proselytizing, taxing, conscripting. (7:218)

The problem, however, was deeper than parochialism--it was systemic in character. On the U.S. side the divide between civilian and military agencies was particularly significant. The American CINC in Vietnam, General Westmoreland, who was responsible for all U.S. military

intelligence in the country, answered to U.S. CINCPAC, Hawaii, the theater commander. General Westmoreland only controlled U.S. forces within the country, and without the title of Supreme Allied Commander, was forced to deal as a military equal to his South Vietnamese counterpart.

Parallel to the military effort, the political battle for Vietnam was being spearheaded by the office of the U.S. Ambassador, Vietnam, and his country team. The Ambassador and the country team where in a totally different chain of command from that of the military, and for that matter, that of the CIA. Fragmentation and parochialism reigned supreme. Wartime studies (i.e., assessment) produced during this early period were the product of individual agencies and did not reflect the analyses of the intelligence community as a whole.

Another dimension of this complex intelligence picture was the relationship between American intelligence agencies and their South Vietnamese counterparts. This relationship was based on a 1965 agreement establishing cooperation at two main levels: the Joint General Staff (JGS) and the operational division levels. At the highest JGS level coordination was conducted via four Combined Intelligence Centers, Vietnam (CICV); at the division level coordination was conducted via the division G-2 staff.

The structure, however, had its problems. In a highly revealing book, former Army Captain Bruce E. Jones described

at length his experiences as an Army intelligence analyst within I Corps' CICV. (15:-) In his memoirs he speaks of constant duplication of effort, of perpetual service rivalries limiting information exchange, and of the lack of effective interaction with the South Vietnamese analysts at the Center. When it came to the South Vietnamese, the "us versus them" mentality appeared to be all-pervasive, but it was certainly not as big a problem as the Vietnamese intelligence morass. William Colby described the proliferation of intelligence agencies, both Vietnamese and American:

> Each acted as a separate fiefdom, however, so that information known to one was zealously guarded and used for its own purposes and only rarely shared with others....When one added...the existence and separate interest of the many American equivalents, each serving its separate commander, the result was a tangle of reports, a limitation of perspective, and a confusion of conclusions. (7:218)

This complex reality relegated lateral intelligence dissemination to secondary importance, and in the absence of combined procedural agreements governing such dissemination, the whole process became voluntary and ineffective.

The lessons from the Vietnamese experience are many. In a monograph by South Vietnamese Colonel Hoang Ngoc Lung, written for the U.S. Army Center for Military History, (13:-) the Vietnam war intelligence situation was addressed in great detail. Among Colonel Hoang's findings were the

following: that there were too many intelligence agencies, civilian, military and paramilitary; that existing agencies were in different command channels and reported to different authorities; that there were great redundancies in tasks and objectives which lead to dilution of effort and unhealthy competition; and that no one really wanted an all-powerful intelligence authority, and everyone wanted to maintain his own assets and capabilities. (13:232) Without a doubt, these shortfalls have been repeated many times since the Vietnam war.

One of those times occurred in Beirut in 1983. The Marine Amphibious Unit (MAU) which deployed to Beirut was designated Landing Force, 6th Fleet (LF6F), and was subordinate to the Commander In Chief, Europe (CINCEUR), while in the area.

The Long commission, appointed to investigate the bombing of the Marine barracks in October of that year, found that intelligence support and direction had not improved over the years, or after three consecutive Marine deployments to the area. In conclusions reminiscent of the Vietnam-era problems, the commission reported as follows:

> The Commission concludes that although the USMNF Commander received a large volume of intelligence warnings concerning potential terrorist threats prior to 23 October 1983, he was not provided with the timely intelligence, tailored to his specific operational

> needs, that was necessary to defend against the broad spectrum of threats he faced. (23:159)

To these problems were added those brought about by the lack of unity of command. While terrorism expertise was available from the European Command (EUCOM) in the form of the Office of the Special Assistant for Security Matters (OSASM), the benefits of this expertise did not reach everyone in Beirut. There OSASM was able to advise the country teams and their attached military assistance group on matters relating to their security, but the advice was not available to the MAU because OSASM representatives were not in the MAU's chain of command. Once again the lack of a central authority for intelligence and a common chain of command was to degrade American ability to deal with unconventional warfare and its unpredictable manifestations. But what is to be done? And where should the reform work start? Perhaps the answer lies in our military establishment.

INTELLIGENCE DISSEMINATION AT THE FRONT LINES

LINKING STRATEGIC AND TACTICAL ASSETS

The intelligence requirements of military units involved in low-intensity conflict are many and varied. These include information on everything from political affiliations, economics, tactics and sociology, to the more exact sciences of geography, hydrography, and weather. Very

seldom will the intelligence users have local experts which can provide them with a comprehensive view of the enemy whenever they need it. This valuable intelligence must come from agencies external to the operational units, and must be accessible to these units at those critical times when it can be of greatest use for the accomplishment of the mission.

For the strategic intelligence producer the task of making this intelligence available is enormous, but not impossible. Lieutenant General Leonard H. Perroots (USAF), former DIA director, defined the challenge facing the intelligence producers as follows:

> Putting timely, useful intelligence in the hands of a myriad of consumers where and when they need it is the raison d'etre of military intelligence. The failure to provide that link at the critical moment may mean the difference between success and failure in a future operation. (20:31)

For DIA the answer to the intelligence connectivity problem lies in its Theater Intelligence Architecture Program (TIAP). Through this program, geographic CINCs will be able to capitalize on existing communication and data processing technologies under a program of regional management of intelligence information.

The communications component of the TIAP is known as the INCA Project. Under this program, and with the aim of resolving standardization problems, issues affecting

intelligence processing and availability for tactical commanders (communications, hardware shortfalls, procedures, policies, and organization) are constantly addressed and resolved.

The transfer of intelligence data under TIAP is accomplished by the DOD Intelligence Information System (DODIIS). This system, which is gradually expanding to unified and specified commands, substantially increases the interoperability between national and tactical automated data processing equipment. It accomplishes this by coordinating the interoperability of more than fifty separate DOD computer types and providing standard intelligence system architectures, common software and training. Working in tandem with the INCA project, connectivity of the DODIIS information sources to tactical units is accomplished by means of the Defense Data Network (DDN) satellite communications system.

However, connectivity is not the only obstacle standing between intelligence users and producers. Once connectivity is achieved, the data elements used by different systems must also be standardized. DOD's attempt at intelligence data element standardization is known as the Military Intelligence Integrated Data System (MIIDS). This system is geared primarily towards operational intelligence, and addresses intelligence requirements at the strategic, operational and tactical levels. Support to user commands

is accomplished via MIIDS's Integrated Data Base (IDB). This data base provides information on the type of enemy units, their locations, facilities, and equipment characteristics. Moreover, by using IDB capabilities, different command levels can exchange information among themselves.

The overall goal of the MIIDS architecture is the creation of IDB subsets maintained at regional tactical intelligence centers. These regional IDBs would be part of DOD's Joint Tactical Fusion Program (JTFP), which in turn aims at tailoring multiple-source intelligence information for use by the lowest tactical command levels needing it. During times of peace, IDB update would be accomplished by national and theater intelligence producing organizations; during times of war, tactical organization input would also contribute to IDB update.

Unified and specified commanders also receive intelligence support from DIA via the attachment of National Military Intelligence Support Teams (NMIST) to their commands, if they so request. These teams provide the supported CINCs with critical, tailored, all-source intelligence in response to his stated requirements. Communications connectivity between the teams and DIA is accomplished via secured UHF communications utilizing the MILSATCOM system. NMIST is also gradually expanding its mission for the incorporation of NSA's Scalable

Transportable Intelligence Communications System (STICS) to allow for the transfer of imagery information to remote units. With this support the teams continue to narrow the gap between intelligence producers and consumers at all levels, but challenges still remain.

One major challenge has nothing to do with hardware or software, but with policy. In its simplest form, it involves a decision on what intelligence information to share, and with whom. The issue is one of classification and access (the old "need to know" test). Classification authorities, by virtue of labeling some information at a particular classification level, virtually impose a form of censorship over what could be critical combat-related information. These stop-gap measures are more critical in the area of special compartmented information (SCI), where fears of revealing intelligence sources lead to suppression of vital information from tactical commanders. Said Lieutenant General Perroots, former head of DIA: "My analysis shows that more than 90 percent of intelligence necessary to prosecute a war can be passed system low." (20:34) The intelligence community should should note this.

THE MARINE CORPS CONNECTION

The communications infrastructure which connects the Marine Air Ground Task Force (MAGTF) with the external world

is quite significant, but less predictable than its internal structure. The Marine All-Source Fusion Center (MAFC) is currently the critical intelligence node linking the various MAGTF elements with supporting external agencies. During amphibious operations, the MAFC's principal external connectivity will be to the Joint Intelligence Center (JIC) aboard ship, via single channel radio.

Once the MAGTF has established operations ashore, the connectivity picture changes somewhat. At this stage, the landing force will begin to move larger and more capable communications systems into secure areas. These systems will be utilized to improve connectivity with the Commander Amphibious Task Force (CATF) and to establish independent connectivity with external agencies without going through ship-based terminals.

Perhaps the first direct access to national and theater level intelligence will come through the communications assets organic to special intelligence teams provided by DIA, NSA, and CIA. These teams usually carry easily transportable UHF SATCOM radios allowing them to transmit and receive secure voice, data, and imagery intelligence.

A critical link for Marine Corps intelligence connectivity will be provided by the AN/TSC-96 satellite communications terminal. This MEB-level terminal will provide the MAGTF command element with general service (GENSER) traffic through the CUDIX system. Moreover, it

will also process special compartmented information (SCI), provided it has the correct terminal device (MSC-63A) and the corresponding crypto protection.

A critical communications path for the Marine Corps is expected to appear in FY-93 with the procurement of the AN/TRC-170 system. This digital multichannel terminal will replace existing SHF analog systems and will allow for massive unit-to-unit communications capabilities. Moreover, it will provide enhanced access to the Defense Data Network (DDN) via one of the Defense Satellite Communications System (DSCS) Gateways, as well as full compatibility with Army, Navy and Air Force digital systems. This "digital backbone" was extensively used during the war in Southwest Asia for the exchange of secure voice, data, and imagery, and is growingly seen as the staple communications path for the joint intelligence community. Lack of operator training, however, affected dissemination speed during this recent engagement.

However, in the advent of the tactical digital communications era, several weaknesses have been identified in the Marine Corps. First, the AN/TRC-170 has not yet been fielded, and in the current budgetary atmosphere, its timely appearance in the field appears to be threatened. Second, computer hardware and software compatibility allowing for the unimpeded exchange of intelligence information is still a thing of the future. Third, current systems are not

designed specifically for a LIC environment, and thus tend to be heavy, relatively stationary, and better suited for conventional warfare operations. Fourth, that in the absence of effective checks and balances and adequately trained operators, the systems could overwhelm users with excessive amounts of intelligence information which no one has the time to analyze. These obstacles are not unique to the Marine Corps and seem to apply to the national intelligence community as a whole.

FUTURE SYSTEMS: DESIGN AND INTEGRATION

The future of intelligence dissemination in LIC operations is inextricably tied to the compatibility and integration of emerging technologies. Because of this, communications hardware and software must be flexible enough to allow for the transmission and receipt of all forms of intelligence (data, voice, and imagery) in the encrypted mode. Moreover, with the continuous growth and availability of communications paths, software packages must be designed to allow for the active search of the best and most direct path to the user (a capability similar to that found in the PLRS system).

Future reporting systems should also have compatible formats allowing for automated retransmission of messages by the push of a button. With the existence of common intelligence data bases and the introduction of fully

automated filtering and retransmission technology, the ability of small or remote units to receive first class information on a timely basis would be further enhanced. Full automation, however, will not do away with the need to have competent and well trained operators who can utilize alternate transmission paths when the need requires it.

Another critical feature of these future systems would be the establishment of procedures for skip-echelon reporting. By not restricting reporting channels to fixed paths, dissemination channels could also be tailored for the particular operation at hand and the whole process of intelligence transfer could be expedited. This is particularly useful to small support units operating independently from a larger command. The ability of small units involved in LIC to tap the intelligence resources of joint, theater, and national data bases, and find information tailored to their specific needs, will be one of the critical components of our future involvement in LIC.

CONCLUSIONS

It becomes readily apparent from this discussion that the problem of intelligence dissemination in a joint LIC environment is a multidimensional and multidiscipline one. Because of the political nature of LIC and its heavy dosage of unconventional and insurgency operations, any U.S. effort

in this area will inevitably involve both civilian and military assets.

Because of its unique capabilities, the nation's military is bound to play a key role in this form of conflict. As in the recent past, military involvement in LIC will continue to include resources from all four branches of the service. This grouping of resources is both a solution and a problem. At once it brings all available military assets to bear on a conflict, but in doing so it must integrate different--and sometimes conflicting--chains of command, procedures, equipment and operational doctrine.

From a dissemination point of view, joint intelligence efforts at the unconventional war level have not enjoyed the same success rate as in larger strategic conflicts. The reasons for this limited success are rooted in problems of complexity and scale. Small, unconventional conflicts generally need tailored, unconventional solutions. The sheer size and complexity of the U.S. intelligence community (with its civilian and military components) makes it more "institutionally comfortable" to deal with larger, conventional warfare than with counterinsurgency operations.

This is also the case at the joint military level. However, the military's ability to promptly focus its resources on any conflict around the world imparts it with some capabilities unmatched by its civilian counterparts. It is precisely in the area of quick response where timely

intelligence dissemination, specifically tailored for the situation at hand, becomes crucial. A dissemination system which does not include joint architectures, common procedures, compatible technologies, and skip-echelon reporting, is bound to fail the timeliness/adequacy test which governs success and failure in a LIC environment. Fortunately, when it comes to LIC, the U.S. intelligence community appears to be moving in the direction of reform and innovation, but the road is treacherous and unpredictable.

BIBLIOGRAPHY

1. Colby, Williams, and James McCargar. Lost Victory. Chicago: Contemporary Books, Inc., 1989.

2. Beans, James D. "Marine Corps Intelligence in Low Intensity Conflict." Signal, Mar 1989: 27-30.

3. Berkowitz, Bruce D., and Allan E. Goodman. Strategic Intelligence for American National Security. Princeton: Princeton University Press, 1989.

4. Betts, Richard K. Analysis, War, and Decision: Why Intelligence Failures are Innevitable. Washington, D.C.: The Brookins Institution, 1978.

5. Bowen, D. G., and Benjamin V. Cox. "Tactical Communications to Support Intelligence." Signal, Jun 1988: 185-189.

6. Burchett, Wilfred G. Vietnam: Inside Story of the Guerilla War. New York: International Publishers, 1965.

7. Colby, Williams, and James McCargar. Lost Victory, Chicago: Contemporary Books, Inc., 1989.

8. Early, T.M., Colonel, USMC. Personal Interview, Quantico, VA. 22 Oct 1990.

9. Elliot, Ronald D. "Intelligence Communications in Nonconventional Warfare." Signal, Nov 1989, 57-63.

10. Fry, D.R., Lieutenant Colonel, USMC. Personal Interview, Quantico, VA. 10 Oct 1990.

11. Godson, Roy. Intelligence Requirements for the 1980's: Elements of Intelligence. Washington, D.C.: National Strategy Information Center, Inc., 1979.

12. Hoadley, Erwin T. "Special Operations C3I Requirements." Signal, Sep 1989: 59-61.

13. Hoang, Ngoc Lung. "Intelligence." Monograph for the U.S. Army Center of Military History, 1982.

14. Hopple, Gerald W., and Bruce Watson, eds. The Military Intelligence Community. Colorado: Westview Press, 1986.

15. Joint Chiefs of Staff. Low-Intensity Conflict, JCS 1-02, Draft Document, 1989.

16. Jones, Bruce E. War Without Windows. New York: Vanguard Press, Inc., 1987.

17. Lake, Julian S. "Interservice C3I--A Department of Defense Concern For Over Two Decades." Defense Science and Electronics, Nov 1987: 59-60.

18. Livingston, R. W.. "Low Intensity Conflict Intelligence: Lessons From Vietnam." Unpublished study, 1990.

19. Motley, James B. "Intelligence Requirements--A Contrast in the Conventional Battlefield and the Low-Intensity Conflict Environment." Journal of Defense and Diplomacy, Apr 1988: 50-52.

20. Perroots, Leonard H. "New Approaches to C3 Interoperability in the Intelligence Community." Signal, Sep 1988: 31-34.

21. Philbin, W. "MAGTF Intelligence Information Exchange Architecture." Unpublished study, 1990.

22. Richelson, Jeffrey. The U.S. Intelligence Community. Cambridge: Ballinger Publishing Company, 1989.

23. Schoelwer, Michael H. "The Failure of the U.S. Intelligence Community in Low-Intensity Conflict." Low-Intensity Conflict. Ed. Loren B. Thompson. Massachusetts: Lexington Books, 1989.

24. Sarkesian, Sam C. "Low-Intensity Conflict: Concepts, Principle, and Policy Guidelines." Symposium on the role of Special Operations on U.S. strategy for the 1980's, National Defense University, 1983.

25. Stewart, John F. "Military Intelligence Operations in Low-Intensity Conflict." Military Review, Jan 1988: 17-27.

26. Thomas, Stafford T. "Intelligence Production and Consumption: A Framework of Analysis." Intelligence Policy and Process. Eds. Alfred C. Maurer, Marion D. Tunstall, and James M. Keagle. Boulder: Westview Press, 1985.

27. United States Marine Corps. Small Arms Manual, SWM 1-1, 1939.