e-Prints

EXECUTIVE SUMMARY

Title: Communications and Intelligence: Why Can't We Get Along?

Author: Major Lisa Tubridy, United States Marine Corps

April 1996:

Thesis: Despite the historical antagonism between the communications and intelligence communities, shrinking budgets, interoperability issues and a requirement to let intelligence drive operations in the information age will force the two professions to call a truce.

Discussion: Intelligence information in national security and on the battlefield has always played a critical role. The unique nature of intelligence information however has created a longtime anathema between it and the communications community. The genesis can be traced to three causes encompassing special handling requirements; vast amounts of data with timely dissemination requirements; and available circuit prioritization. The chasm between the two communities has resulted in stovepipe communications infrastructures supporting unique intelligence requirements. The results of these stovepipes are lack of interoperability and wasted dollars in a declining resource environment. Finally, communicators have born the brunt of the intelligence community's criticism in the area of circuit prioritization when indeed the responsibility lays with the commander. The vogue answer to these problems has been to combine intelligence organizations with communications organizations (e.g. C4I) to ensure adequate support to the intelligence community.

Conclusion(s)or Recommendation(s): Organizational changes providing for the combination of intelligence and communication agencies (e.g. HQMC C4I, ASD/C3I etc.) are not the answer to coordination and support of intelligence communications requirements within the C3 community. Communications requirements, regardless of which function supported (e.g. logistics, C2 etc.), should be consolidated under the technical management of communications agencies or staffs (i.e. DISA, J6/G6/N6). Additionally, although the commander is doctrinally responsible for the prioritization of all communications in support of functional areas, reports in various lessons learned indicate we rarely hold him accountable for same.

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY.

.

List of Works Consulted

Ackerman, Robert K. "Communications Links Vital to Managing Defense Intelligence." Signal, September, 1995, p. 25.

CMC Washington D.C. Message to Joint Staff Washington D.C (J6T). Subject: "Bandwidth Requirements for Standard Tactical Entry Points." 281900Z March 1996.

FleetMarine Force Manual (FMFM) 3-30. " Communications." Washington, D.C.: Department of the Navy, Headquarters, U.S. Marine Corps. 3 April 1989.

Joint Publication 6-0. "Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations. Washington, D.C: Joint Chiefs of Staff. May 1995.

Marine Corps Combat Development Command (MCCDC). "Trojan Spirit Concept of Employment (COE)." Quantico, VA: U.S. Marine Corps MCCDC (C442), 12 February 1996.

Marine Corps Lessons Learned System. On line edition. Under "Communications, Intelligence."

Open Source Intelligence: Selected Readings , Proceedings Volume I. Fourth International Symposium on "Global Security and Global Competitiveness: Open Source solutions." Washington D.C.: 7-9 November, 1995.

Tubridy, Terrence K. Communications Project Leader at Science Applications International Corporation(SAIC). Interview by author, January 1996.

West, Nigel. The SIGINT Secrets. New York: William Morrow and Co., 1986.

Williams, Jason M. Capt. "The Green Door Syndrome." Marine Corps Gazette, April 1995, p. 38.

INTRODUCTION

The Army, Navy, Marine Corps and Air Force have often been accused of blindly defending their individual roles and missions at the expense of overall U.S. military efficiency and, ultimately, the American taxpayer. Indeed, inter-Service antagonism is well documented and has sometimes been a crippling force within the Department of Defense. Just as crippling, but not as well known, is the antagonism that exists between functional areas across the Services.

One would be hard pressed to find the same level of antagonism between functional areas (e.g., administration, logistics, command & control, fire support, etc.) that one finds between communications and intelligence. The chasm between the two is deep and rooted in misunderstandings in doctrine, policy and the unique nature of intelligence information. Most recently, Major General John A. Leide, USA, former director of the Defense Intelligence Agency's (DIA) National Military Intelligence Center, publicly addressed this issue in September 1995. General Leide noted the longtime anathema that has existed between the communications and intelligence communities and the need for a truce between the two.[(1)] This paper will examine the historical differences between the two functional areas, identify some results of this antagonism and offer some solutions to improve operations between the two communities.

THE INTELLIGENCE PROBLEM

The intelligence community has become a victim of its veil of secrecy. The genesis of the antagonism between intelligence and communications can be traced to three primary causes: 1) special handling requirements of raw and exploited intelligence information; 2) the vast amount of intelligence data collected and the requirement for timely dissemination; and 3) the prioritization of available communications circuits in support of intelligence requirements.

The sensitivity of intelligence information usually requires special handling by individuals with special clearances; this fact distinguishes intelligence data from most other types of military information. Historically, intelligence data has been a closely held resource. The very fact that a piece of information was known could reveal the source. For example, U.S. and British leaders faced many a dilemma during World War II over the use of intelligence collected via deciphered Purple (Japan) and Enigma (Nazi Germany) messages.[(2)] Too much use of information derived from deciphered messages would have advertised the fact of our codebreaking success. This sensitivity to collection and dissemination of intelligence data led to a closed door approach (known to many as the "Green Door Syndrome")[(3)] to all areas of intelligence. The Green Door Syndrome dictated the secrecy of communications in support of intelligence efforts. With the advent of increasingly sensitive collection methods, the requirement to keep sensitive sources and methods behind the green door became even greater. The fact that certain circuits even existed required and continue to require classification levels far above those held by many mainstream communications providers. This sensitivity to all things intelligence related has lead to the creation of a worldwide communications infrastructure dedicated solely for the use of, and managed by, the intelligence community.

By nature, the intelligence community relies on the collection of vast amounts of information from numerous sources. Sources such as text reports from human intelligence can be large but few sources match the data size of high resolution photography or videotape (i.e., imagery). As noted by General Leide, imagery is an increasingly vital aspect on the battlefield where there is "a constant thirst for imagery tactically as well as strategically."[(4)] Once collected the data must be interpreted, exploited and rapidly disseminated from the intelligence processor to the user (warfighter, other government agencies, etc.). Rapid dissemination often means the transmission of large data files in minutes or seconds. Until recently, DoD communications providers (e.g., the Defense Information Systems Agency - DISA) were unaware of many of the intelligence community's communications needs. Without knowledge of the full scope of the intelligence communications needs, agencies such as DISA were unable to provide sufficient support. A classic "Catch-22" situation exists: DISA is tasked with providing communications support but can not support a requirement it does not know about, hence, the development of separate intelligence communications networks.

For example, the National Security Agency (NSA), the National Reconnaissance Office (NRO) and the Defense Intelligence Agency (DIA) have developed their own unique communications networks. Other "stovepipe" DoD intelligence networks include the Joint Worldwide Intelligence Communications System (JWICS) and the U.S. Army-developed Trojan Special Purpose Integrated Remote Intelligence Terminal (SPIRIT). Unfortunately, the lack of a central communications provider has resulted in disparate and non-interoperable network development across the different agencies. Trojan SPIRIT's highly effective intelligence support during DESERT SHIELD/STORM has convinced the Army, as well as the Joint Staff and the Marine Corps, of its worth to the community, resulting in limited inter-service interoperability. Again, however, Trojan SPIRIT is another "stovepipe" intelligence communications system, which only serves to widen the division between the communications and intelligence communities.

The third point in the intelligence-communications conflict is prioritization of available communications networks. Given the high priority of dissemination of intelligence data, the transmission of large intelligence data files can conceivably saturate existing communications pipes. This is obviously an unacceptable situation for the other functional areas (operations, logistics, etc.). Communications providers are often caught in the middle on deciding how to meet the needs of all customers, not just those from the intelligence community. Unfortunately, the existing general communications architecture is insufficient to support all customer requirements. Once again, this has led the intelligence community to develop a communications infrastructure dedicated to its own needs.

Under the direction of Mr. Emmett Paige, Assistant Secretary of Defense (ASD) for Command, Control, Communications and Intelligence (C3I), there is movement towards transferring management of all communications networks to DISA. However, the intelligence community has been very hesitant to release control of their networks. The "what's mine is mine" and "if I own it, it is responsive to my needs" attitude is prevalent. Although understandable, this "rice bowl" issue hinders improvement of services.

Finally, it should be noted that ignorance of communications requirements and capabilities cuts both ways within the intelligence community. DESERT STORM Lessons Learned and General Leide discuss the failure to use all available communications networks for dissemination of intelligence data. A key factor in this failure was the intelligence community's insulation from the general communications architecture.

THE COMMUNICATIONS PROBLEM

The communications community cannot be held responsible for its alleged failure to support past needs of the intelligence community. As outlined above, the wall of secrecy surrounding intelligence operations essentially prevented communicators from providing meaningful support. Existing support was limited to simple tactical voice traffic (e.g., MEF/MAGTF CE/DIV/REGT Intel Nets) and the common user Automated Digital Information Network (General Service message traffic).

However, post-DESERT SHIELD/STORM requirements for joint interoperable communications, combined with the drastically declining DoD budget and compelling top down direction from ASD C3I, are forcing communicators to support the majority of the intelligence community's communications requirements. Obstacles to providing this service include ignorance of intelligence needs, competing requirements from other functional areas, a lack of resources, and a lack of command involvement.

On the one hand, communicators have been tasked with supporting intelligence communications without being given the requisite background information, or familiarization, on intelligence requirements. The intelligence community's numerous communications architectures only serve to add to the confusion. Without a central provider, communicators are forced to track down each individual user's needs. On the other hand, communicators originally failed to aggressively address these problems. Fortunately, Mr. Paige stepped in and directed, in very clear terms, the transfer of intelligence communications support to the DISA. Currently headed by LTGEN Edmonds, USAF, DISA has begun an earnest effort to assume responsibility for supporting the intelligence community. Training communicators to better understand and anticipate intelligence communications requirements is a first step towards meeting that responsibility. However, that first step is expensive and must occur during a severely restricted fiscal period.

The problem of meeting intelligence communications requirements is two-fold: the Information Age and a Commander's prioritization. As discussed earlier, the intelligence community is reluctant to release control of its communications systems. This reluctance is based on a fear of a loss of responsiveness and is quite understandable. The larger problem facing communicators however, is the revolution of the Information Age and its affect on available resources.

Suddenly, all functional areas within DoD have information requirements far surpassing current communications capabilities to support them. Users are no longer satisfied with textual or even voice communications. In today's environment of multimedia data presentations, the communicator is forever pressed to deliver more data with fewer resources. Information requirements now include graphical displays (e.g., situational map displays of unit locations), high resolution still pictures (e.g., imagery or X-rays) and real time video (e.g., video teleconferencing). Current trends in information technology and on-going programs such as the Global Command and Control System (GCCS) will soon make the current bandwidth requirements obsolete. Programs like INTELINK, INTELINK-S, Split Basing, Reachback, Data Archival Search Tools, Common Operational Picture, Telemedicine and other new technologies are going to place even greater demands on common user networks. The amount of military and commercial bandwidth per soldier in Bosnia as compared to that of Desert Storm just six years ago is indicative of this trend.(5)

Unfortunately, the information explosion can not be fully supported within today's climate of fiscal downsizing. DISA and other communications agencies do not have the budget resources to increase the manpower and equipment required to support current customer needs. To alleviate this, service providers must become more efficient in the design, installation and management of communications networks. However, intelligence users must understand that their requirements are not the only ones left unmet.

The prioritization of communications support, in other words who gets what and when, is probably one of the most misunderstood aspects of military communications. For example, in a recent professional military journal, a Marine Corps intelligence officer admonished the communications community and proposed they redefine intelligence circuit priorities within the communication doctrinal publication (FMFM 3-30). However, the FMFM 3-30 does not prioritize any communications circuit, intelligence or otherwise. Because communicators, as the service provider, establish communications links, supported users are under the impression that priority of service is determined by the communicator. In fact, it is the commander who is responsible for setting priorities. As with all facets of any organization and operation, the commander is responsible for providing guidance regarding his priorities for information flow.(6) Too often however, the commander is more concerned with his own direct communications and leaves the communicator to guess the commander's priorities for indirect communications links (e.g., intelligence, logistics, etc.). In turn, communicators tend to support those functional areas with which they are familiar, leaving intelligence priorities near the bottom.

The Marine Corps provides ample illustrations of this problem. Desert Shield/Storm, Valiant Blitz 91 and Kernel Raider 93 Lessons Learned are replete with examples where low priority was given to intelligence dissemination. "Intelligence is sometimes not on the same level of priority as the other sections...we must have an appreciation for intel."(7) "Lack of a dedicated intelligence net for continuous flow of data...S-2 was required to jump to another net to pass/receive data."(8) "The Division failed to assign the necessary priority to intelligence dissemination...dissemination was sketchy at best and often left the Division's subordinate units without critical information."(9) "Most intelligence was being relayed via an overloaded Tactical Air Command (TAC) net since the intelligence net was eliminated in order to reduce communications links...place intelligence as a priority on the command net.(10) These are just several examples of dozens. Many times doctrinal S-2/G-2 nets are not established at all and intelligence is forced to be relayed over already overloaded tactical command or logistics nets. In a service which prides itself on the adage intelligence drives operations, the aforementioned lessons learned would argue otherwise.

A commander must bear responsibility for the lack of priority given to intelligence dissemination circuits. This prioritization fight results in intelligence producers resorting to non-standard commercial communications and/or unique communication assets provided by DoD or outside intelligence agencies (stovepipes). These assets are usually unfamiliar to the general communicator and, consequently, not supported by them. In addition, the extra communications afforded some units by outside intelligence agencies, particularly for exercises only, give a commander a sense that sufficient tactical communications are available to support his requirements when indeed, during real operations they would be insufficient. Unfortunately, a real world contingency is the wrong time to learn about a communications, or any other, deficiency.

THE SOLUTION

Solving the problem of communications support of intelligence will require a significant change in institutional mindsets. This mindset change must involve not only the shifting of management responsibilities but also the shifting of resource allocation. The solution, or end state, should be the reconciliation of all DoD communications services under a single agency - DISA.

To achieve this end state however, it must be clearly stated what the responsibilities of a single service provider will be.

A current approach to solving the problems between the intelligence and communications communities has been to combine the two into a single staff agency. Specifically, this approach has been adopted by ASD C3I and the Marine Corps (HQMC C4I). Other approaches include reorganization of intelligence communications support agencies as general communications support agencies. For example, within ASD C3I the Intelligence Communications Architecture group and the Intelligence Programs Support Group have been combined to form the C4I Integration Support Activity. These actions are intended to ensure closer coordination and support of intelligence communications requirements within the C3 community.

However, the fallacy inherent in these approaches is that the intelligence and communications communities must be combined to ensure proper support for intelligence. If this were true, then all other functional areas would also have to be merged into the communications community as well. In other words, the tail begins to wag the dog. Imagine if you will, an organization called C4ILAAFS... (Command, Control, Communications, Computers, Intelligence, Logistics, Aviation, Administration, Fire Support,...).

The changes listed above are merely headline service given to meaningless organizational name changes. These changes amount to little more than form over substance. The two communities do not need to be combined. The other functional areas, which are equally important, have not required merging with the

C4 community to have their needs met. The DoD communications community is a service community analogous to AT&T. Its mission is to support the customer, be it the intelligence community or any other community.

Regardless of the security level or type of communications required, a single agency, DISA, should be tasked with providing the necessary support. The goal is to consolidate resources under a single agency. Although not a panacea, this approach would serve to reduce duplication of networks, duplicate management organizations, and network interoperability problems. A single service provider would be aware of the total information architecture and would be much more likely to take advantage of existing infrastructures to minimize costs. This approach does not necessarily mean the elimination of dedicated intelligence communications networks. In fact, it is doubtful that dissemination of information such as imagery can be effectively supported via non-dedicated means. Security classification will also continue to be an issue. The intelligence community may be using open-source material on an increasing basis(11), but many sources will continue to require special handling. Given the proper security clearances, a single service provider should be capable of supporting both dedicated and general service networks.

More importantly, it should be recognized that current and new intelligence communications needs can be supported through a sharing of resources. As the responsibility for communications support shifts from the intelligence community to DISA, so must the resources shift. In other words, the people, equipment, and budget currently involved in supporting intelligence communications networks must also be moved to DISA. Future needs could be supported through the transfer of money from the intelligence community or through a shift in agency program funding. The intelligence community would be responsible for identifying their functional requirements and DISA would be responsible for developing the technical means to support them.

On a tactical level, this general support concept has already taken hold. The Marine Corps, through three years of debate, has decided to place the Trojan Spirit communications system within the Communications Battalion (vice the Radio Battalions which provides Signals Intelligence (SIGINT) support to the Marine Air Ground Task Force (MAGTF) commander) in general support of the Marine Expeditionary Force (MEF) with a priority towards intelligence.(12) This places the onus on the commander to give the priority to intelligence, exactly where it should be.

Another example is changes occurring at U.S. Transportation Command (USTRANSCOM) at Scott AFB IL. Currently, the USTRANSCOM SCI local area network is managed by the J2. However, the J2 and the J6 have begun working on consolidating all network management under the J6.(13)

CONCLUSION

Mr Paige's mandate to change the way the intelligence community's communications needs are supported has created much turmoil and consternation. In light of over 40 years of "tradition," this is understandable. However, the atmosphere of distrust between the intelligence and communications communities can no longer be tolerated. Individual intelligence and communications efforts have created redundant communications management organizations, redundant research and development organizations and redundant means for providing alternate means of communications.

From a resource management perspective, none is probably more wasteful than two redundant communications architectures. Redundancy in this case applies to the creation of a multitude of backup circuits that remain in standby until a primary circuit fails. These backup circuits are the legitimate result of the requirements for flexible, responsive, survivable and sustainable communications. However, the existence of two backup communications architectures places too much capability in standby, particularly during a time when communications bandwidth is at a premium.

Ultimately, the current approach fails to take advantage of consolidated "bulk shopping." In other words, the creation of separate small communications pipes is far more expensive than having a single manager create large communications pipes in support of several users. This concept of discount bulk shopping can be seen in the Wal-Mart stores created by market pioneer Sam Walton. The same principles can be applied towards communications service within DoD.

Fiscal constraints and DESERT STORM Lessons Learned clearly indicate the need for consolidation of communications providers. Advocacy of this course of action should not be confused with any advocacy of a single "Purple" military service. Instead, this course of action should be seen as beneficial to the taxpayer in terms of cost savings and as beneficial to the warfighter in terms of efficient, timely and, possibly, lifesaving information flow.

Finally, despite all the rhetoric on the criticality of intelligence to any operation, countless lessons learned highlight the disparity between the importance of intelligence and the lack of importance given to dissemination of same. Commanders, from the Chairman of the Joint Staff on down to the platoon level, are the only ones who can truly solve this problem.

---

1. Robert K. Ackerman, "Communications Links Vital to Managing Defense Intelligence," Signal, September 1995, p. 25.

2. Nigel West, The SIGINT Secrets (New York: William Morrow & Co., 1986).

3. Capt. Jason M. Williams, "The "Green Door Syndrome," Marine Corps Gazette, April 1995, p. 38.

4. Ackerman, p. 25.

5. CMC Washington D.C. message to Joint Staff Washington D.C (J6T), subject: "Bandwidth Requirements for Standard Tactical Entry Points,"281900Z March 1996.

6. Joint Publication 6-0, "Doctrine for Command, Control, Communications, and Computer (C4) Systems

Support to Joint Operations (Washington, D.C: Joint Chiefs of Staff, May 1995), p. III-9. FleetMarine Force Manual (FMFM) 3-30, " Communications" (Washington, D.C.: Department of the Navy, Headquarters, U.S. Marine Corps, 3 April 1989).

7. Marine Corps Lessons Learned System, On line edition, Under "Communications, Intelligence," Number 00668-68268 (00578), submitted by G-2 Systems Officer Capt Nolan, Phibex Kernel Raider 93.

8. Marine Corps Lessons Learned System, On line edition, Under "Communications, Intelligence," Number 11603-91064 (01832) submitted by 3d Bn, 7th Mar, Maj.Washabaugh, Phibex Valiant Blitz 91.

9. Marine Corps Lessons Learned System, On line edition, Under "Communications, Intelligence," Number 30941-23487 (04513) submitted by 6th Marines S-2, Major R.S. Moore, Operation Desert Storm 1991.

10. Marine Corps Lessons Learned System, On line edition, Under "Communications, Intelligence," Number 11174-69153 (01820) submitted by 1st AA BN S-2 Phibex Valiant Blitz 91.

11. Open Source Intelligence: Selected Readings, Proceedings Volume I, Fourth International Symposium on "Global Security and Global Competetiveness: Open Source Solutions, "Washington D.C., 7-9 November, 1995.

12. Marine Corps Combat Development Command (MCCDC), "Trojan Spirit Concept of Employment (COE)" (Quantico, VA: U.S. Marine Corps MCCDC (C442), 12 February 1996).

13. Terrence K. Tubridy, Communications Project Leader, Science Applications International Corporation (SAIC), interview by author, January 1996.