REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
24-04-2015	Master of Military Studies Research Paper	September 2014 - April 2015

4. TITLE AND SUBTITLE

Command and Control Intelligence: The Case for Federation in Modern Operations

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)

Starr, Jeffery L., Major, USMC

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

N/A

14. ABSTRACT

In order to make optimal use of intelligence, commanders must embrace federated intelligence operations. However, selling commanders on the benefits of intelligence federation is easier said than done, and many remain vigilant in the pursuit of intelligence ownership. Intelligence management under unit command is inefficient, as commanders lack the administrative support, procedural understanding, and institutional knowledge essential to effective intelligence operations. Corroboration through multi-intelligence collection is a convoluted process requiring technical expertise and oversight for immediate tasking. Non-intelligence professionals have neither the training nor the time required to support this process. In order to ensure best practices at each level of command across the MAGTF, Coalition, and Joint arenas, administrative, tactical, operational, and technical control measures must be defined and followed in strict adherence. The mission of Marine Corps intelligence is to "provide commanders with seamless, tailored, timely, and mission-essential intelligence, and to ensure its integration into the operational planning process." Commanders are key components of intelligence planning, but do not require ownership of its processes, personnel, or equipment to benefit from its findings.

15. SUBJECT TERMS

Command and Control, MAGTF, MEU, MEB, Low Intensity Conflict, Federated, MCISR-E, FISA, CHD, DNI, IC, OIPR

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
Unclass					Marine Corps University/Command a
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	UU	46	**19b. TELEPHONE NUMBER** *(include area code)*
Unclass	Unclass	Unclass			(703) 784-3330 (Admin Office)

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

Command and Control Intelligence: The Case for Federation in Modern Operations

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

Maj Jeff Starr

AY 14-15

Mentor and Oral Defense Committee Member: Dr. Christopher Stowe
Approved: [signature]
Date: 24 APRIL 2015

Oral Defense Committee Member: Dr Richard DiNardo
Approved: [signature]
Date: 24 April 2015

Hugh Curtright
[signature]
24 Apr 15

Executive Summary

Title: Command and Control Intelligence: The Case for Federation in Modern Operations

Author: Major Jeff Starr, United States Marine Corps

Thesis: In order to make optimal use of intelligence, commanders must embrace federated intelligence operations. However, selling commanders on the benefits of intelligence federation is easier said than done, and many remain vigilant in the pursuit of intelligence ownership. Intelligence management under unit command is inefficient, as commanders lack the administrative support, procedural understanding, and institutional knowledge essential to effective intelligence operations.

Discussion: Marine Corps Fleet Manual 101-5-1 defines command and control as "the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission." Command and control encompasses personnel, equipment, communications, and facilities administered along functional or unit lines. Intelligence is one of six Marine Corps warfighting functions and is often the most difficult to manage due to the technical nature of intelligence analysis and the complex integration of collections platforms. Intelligence collections platforms are best employed in unison, and cross-cuing platforms aids in corroborating information. Platforms are typically allocated to service, joint, and theater levels and require considerable coordination to ensure prioritization of effort and efficient use of high density, low demand assets. Corroboration through multi-intelligence collection is a convoluted process requiring technical expertise and oversight for immediate tasking. Non-intelligence professionals have neither the training nor the time required to support this process. In order to ensure best practices at each level of command across the MAGTF, Coalition, and Joint arenas, administrative, tactical, operational, and technical control measures must be defined and followed in strict adherence.

Conclusion: The mission of Marine Corps intelligence is to "provide commanders with seamless, tailored, timely, and mission-essential intelligence, and to ensure its integration into the operational planning process." Commanders are key components of intelligence planning, but do not require ownership of its processes, personnel, or equipment to benefit from its findings.

Disclaimer

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, THE MARINE CORPS INTELLIGENCE COMMUNITY, OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

Preface

Throughout my commissioned career, I have witnessed several ad-hoc intelligence relationships and operational disconnects in both combat and garrison environments. At the height of OPERATION IRAQI FREEDOM (OEF), Marine Corps intelligence sections, even at the high-command levels, had difficulty synchronizing operations, adopting similar terminology, and sharing information. The all-source analysis and production center in Fallujah was known as the Tactical Fusion Center (TFC), while the Marine Aviation Wing (MAW) titled their section the Intelligence Operation Center (IOC). The two functioned similarly, possessed similar capabilities, were separated by less than 200 miles, but had different names, different procedures, and rarely shared assets or products. The Operational Control and Analysis Center (OCAC), Radio Battalion's headquarters section, was in the same building as the TFC, but hid behind the proverbial "green door" cloaked in a cloud of intrigue. As a Reports Officer (RO) in the Counterintelligence and Human Intelligence Operations Center (CIHOC) in 2005, I liaised consistently with the OCAC to corroborate information in support of enemy targeting operations. Breaching the OCAC door was so difficult that I sometimes questioned my conviction in the very information I sought to corroborate.

As a recent graduate of the Marine Corps' CI/HUMINT course, I could not understand the disconnect between these like units, working for the same institution, and ostensibly with the same objectives: to reduce operational uncertainty and provide force protection to the MAGTF.[1] Intelligence sections had a hard enough time reducing uncertainty among themselves. Even more pervasive was the lack of interoperability between the higher intelligence staffs and the several infantry battalions operating in Anbar Province. Infantry commanders mistrusted the intelligence staffs; to these commanders, intelligence fusion centers were bureaucratic

institutions that existed only to build products for General Officer consumption and defied the laws of gravity. In other words, information went up, but it never came down. Under resourced and starved of actionable intelligence, constructing rudimentary intelligence sections from untrained infantrymen was a common practice for infantry battalions.[2] In a world where the enemy death toll was often the measure of success, insufficient targeting was the fastest way to the bottom of your reporting senior's profile. Unmanned aerial systems (UAS) support was almost impossible to obtain, and was so scarce that collections managers rarely approved them below the regimental level. Infantry battalion commanders were so dissatisfied with the perceived lack of intelligence support that they continually advocated for ownership. Gone were the days of the Surveillance, Reconnaissance, Intelligence Group (SRIG) and attached intelligence sections.[3] We had entered a new era, and it was just a matter of time before the intelligence community resolved the operational divide.

While preparing for my second deployment to Iraq, I thought I was immune to the intelligence-infantry rift. As a young and aspiring HUMINT Exploitation Team (HET) commander in direct Support of an infantry battalion, my responsibilities were twofold: answer the commander's Priority Intelligence Requirements (PIR) and be prepared to expand my mission to include theater-focused collection when necessary.[4] The MEF had operational ownership of my HET, so this seemed like a reasonable proposition. Three months before we deployed, our HET gave a capabilities brief to the supported infantry battalion commander. After the brief, I asked if he had any questions pertaining the team's responsibilities and competencies, to which he replied, "Who writes your fitness report?"[5] He asked about nothing pertaining to our equipment, authorities, products, or processes; he simply wanted to know if he

"owned" us. Two years removed from The Basic School (TBS), I finally learned this valuable lesson: for commanders, ownership trumps all other considerations.

Several years and many conversations after my last Iraq deployment, I learned the lack of intelligence integration was due to several factors: Intelligence and Radio Battalions deploying in mass for the first time, outdated policies, bureaucratic ISR and information-sharing practices, incompatible communications networks, etc.[6] The intelligence community (IC) wanted integrated operations, but it was not yet a position to achieve this goal. The initial framework was underway, but was not yet implementable. Contrary to my initial beliefs, parochialism was no longer the principal problem. However, eight years and three deployments later, I still field questions about intelligence ownership from infantry commanders despite the proven successes of federated intelligence.

Table of Contents

Introduction

> "Intelligence is about people and a study of people. It is not simply a question of studying people on the other side, but studying one's own as well. We have to learn about one another, not just about strangers." –
>
> Maurice Oldfield[7]

In 2008, the Marine Corps introduced a new intelligence concept known as Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise (MCISR-E) to better enable the collaboration and sharing of information and platforms.[8] MCISR-E was born of necessity; it was an effort made to federate Marine Corps intelligence and improve institutional decision making.[9] The unstated or perhaps unconscious objective was to alleviate commanders of a difficult responsibility and provide better intelligence to support their operations. Nonetheless, many commanders still favor broad ownership of intelligence processes, professionals, and equipment in their battlespaces, even at the expense of holistic coordination and without systematic understanding of employment and doctrinal authorities. Single battlespace focus may work in a single command environment, but these insular intelligence methods stovepipe information and hinder the greater intelligence process in multiple-command and joint operations. In order to make optimal use of intelligence, commanders must embrace federated intelligence operations. However, selling commanders on the benefits of intelligence federation is easier said than done, and many remain vigilant in the pursuit of intelligence ownership. Intelligence management along unit lines is inefficient, as commanders lack the administrative support, procedural understanding, and institutional knowledge essential to effective intelligence operations.

Intelligence ownership and management is a consistent topic of debate in the modern Marine Corps. A decade of sustained fighting on the two fronts, Iraq and Afghanistan, led to procedural changes as intelligence units strained to support several commanders in large geographic areas, often without adequate equipment or defined processes to govern operations.

In the early years of the wars, analysis was insufficient, collections were too narrowly focused, and actionable intelligence was the exception. Latency was commonplace; commanders requested information to confirm targets, determine threats, and improve atmospherics, but often received answers after events occurred. Many commanders felt they had an understanding of the intelligence picture and were better positioned to make decisions. Frustration led to breakdowns in communication, and these breakdowns led to commanders demanding control of the intelligence personnel supporting their battlespace. Commanders no longer wanted support or advice, they wanted holistic ownership. Intelligence operations improved as the Marine Corps grew its capabilities, but the damage was done. A new generation of commanders emerged from these experiences, and intelligence ownership was their desired end state.

Intelligence is one of six Marine Corps warfighting functions[10] and is often the most difficult to manage due to the technical nature of intelligence collection and analysis, and the complex integration of collections platforms.[11] Intelligence collections platforms are best employed in unison, and cross-cuing platforms to aid corroboration is essential to information credibility and enemy targeting.[12] The Department of Defense (DoD) commonly allocates platforms to the service, joint, and theater levels, requiring considerable coordination to ensure prioritization of effort and efficient use of low density, high demand assets.[13] Corroboration through multi-intelligence collection is a complex process requiring technical expertise and oversight for immediate and appropriate tasking.

Intelligence and the Commander

The relationship between a commander and his intelligence staff is straightforward: the commander directs the intelligence effort, and through a codified process, the intelligence staff manages the effort based on the commander's intent and requirements.[14] The complexities of the intelligence cycle is of little consequence to the commander.[15] His responsibility to the process consists of oversight, direction, and operational integration. A commander requires no comprehensive knowledge of the intelligence process; he needs only the assurance that his staff satisfies his requirements, and an inherent trust in the abilities of his intelligence section. A commander has neither the time nor the inclination to oversee exclusively and direct every aspect of his operation, so he must rely on his staff for sound planning. Prussian soldier and military theorist Carl von Clausewitz eluded to this idea in his book *On War*:

> "War is the realm of uncertainty; three quarters of the factors of which action in war is based are wrapped in a fog of greater or lesser uncertainty…the commander must work in a medium which his eyes cannot see; and with which, because of constant changes, he can rarely become familiar."[16]

Commanders depend on effective staff coordination, and effective intelligence operations depend on a coordinated and harmonious effort. Intelligence confined to one commander's battlespace is advantageous to his operations, but when federated by the IC, supports the collective whole. Former Marine Commandant General David Shoup stated "to lack intelligence is to be in the ring blindfolded," a declaration with which most commanders would agree.[17] Intelligence drives operations through determining enemy capabilities, locations, reactions, and intent.[18] The manner in which intelligence personnel procure information is technical, while coordinating the process and advising commanders is operational and administrative. The technical process is immaterial to battlespace owners; so long as intelligence professionals fill the commander's

information gaps, ownership of processes and intelligence personnel is an unnecessary control measure.

Intelligence is a function of C2, but customarily in terms of feedback and integration.[19] Without feedback on enemy capabilities, intentions, and vulnerabilities, commanders lack the required situational awareness to make sound operational decisions.[20] Without intelligence integration, a unit is blind. Intelligence is a key element of planning, driving the planner's considerations throughout the process.[21] In an operational setting, commanders need intelligence support; they have an obligation to incorporate intelligence tactically into their operations to answer the priority requirements that affect force protection and enemy targeting. However, commanders do not need to own the intelligence process, nor the personnel and equipment supporting the process. Recent innovations make ownership unnecessary, and successful intelligence operations in the latter stages of the two-front war prove the legitimacy for federated intelligence.

Most Marine Corps intelligence professionals understand the importance of defining enemy capabilities and intentions, and virtually all intelligence professionals are versed in practicing their craft in the absence of direction. It is not uncommon for the intelligence cycle to operate in reverse, where synthesized information defines the mission rather than requirements driving the collection, analysis, and dissemination process. Fundamentally, the aforementioned method of intelligence driving operational planning is preferable if not expected; but collecting intelligence solely for collection's sake is an effort made in vain and often results in ineffectual operations. MCISR-E enhances Marine Corps intelligence, narrowing the gap between intelligence and operations, but it does not address the ongoing debate concerning administrative ownership.

Intelligence Administration

Administrative control (ADCON) serves as a doctrinal interpretation of departmental responsibilities outlined in the Federal statute.[22] ADCON traditionally remains with the force's organic unit unless that unit detaches from its organic command and only when assigned to a command of the same service (i.e. a Marine unit detached and assigned to a separate Marine unit). Per MCWP 3-40.7, "the authority vested in a commander is commensurate with the responsibility assigned. Forces, not command relationships, are transferred between commands."[23] This fact is an important distinction, particularly concerning intelligence. When units transfer forces, command relationships must be codified to avoid confusion and to ensure the transferred unit understands the new or revised chain of command. For example, if a tank company detaches from its organic command and attaches to an infantry battalion, all operational and administrative matters are vested in the gaining command. In this scenario, the infantry battalion exercises ADCON, operational control (OPCON), and tactical control (TACON) over the company.[24] Logistical support is the one outlier in this scenario; the Marine infantry battalion does not have the equipment or personnel necessary to logistically support a tank battalion, so logistical support requirements remain with the company's organic higher headquarters.

Much like a tank company, intelligence sections and teams are not easily implementable for the conventional infantry battalion, regiment, or division. A single Counterintelligence and Human Intelligence Detachment (CHD) brings a considerable amount of technical equipment not organic to an infantry battalion, and the infantry battalion lacks the technical maintenance personnel required to account for and repair damaged or inoperable CHD gear.[25] At a minimum, a single CHD carries seven Counterintelligence and Human Intelligence Equipment Program

(CIHEP) suites. Within these suites is a bevy of equipment supporting the research, collection, production, and dissemination of intelligence information. This equipment includes: handheld and vehicle mounted radios, surveillance and countermeasures gear, defense tracking and mapping cameras, defense secret computer mediums, biometric collection platforms, and satellite telephones.[26] Additionally, CHDs are not doctrinally bound to a specific team size (teams are task organized to the environment, size of the element supported, and scope of mission).[27] The amount of equipment multiplies exponentially with larger teams. CHDs are frequently separated from their higher intelligence battalions due to the nature of their mission (the intelligence battalion's primary mission is force providing; i.e. deploying task-organized intelligence sections in support of combat units), so communications experts (MOS 0651, Cyber Network Operators) support the team's technical needs.[28] The infantry battalion intelligence shop (S-2) is comprised almost exclusively of 0231 Intelligence Specialists with no formal training to operate or maintain CHD equipment. Intelligence Specialists analyze and process raw information, but have no formal equipment maintenance training. Moreover, the infantry battalion's communications section (S-6) lacks the special training to maintain intelligence specific gear.

Gear accountability and maintenance is an ADCON function, and one of the many reasons CHDs do not attach to infantry battalions. All Marine intelligence battalions have the essential combat service support (CSS) personnel necessary for administrative support to the CHD, and if support personnel are not sourced to the theater of operations, CHDs send their equipment via mail to one of the three intelligence battalions for maintenance. Similarly, the Marine Radio Battalion's Radio Reconnaissance Team (RRT) and Special Search Team (SST) maintain their own equipment. RRTs and SSTs also support infantry battalions, and much like

the CHD, require organic support for mission integration at the MEF level. Equipment accountability is but one function of ADCON, and usually not separate from other ADCON functions. It would be disingenuous for a commander to request to evaluate the Marines in supporting sections and not also take responsibility for the sections' equipment. If commanders desire tacit ADCON of all non-organic sections supporting his operations, then he must be willing to oversee and support all functions of administration. He must be prepared to address their pay and earnings problems, handle all awards and commendations, support personal issues, and take responsibility for pre and post-deployment training. Many commanders request OPCON and ADCON of intelligence personnel, yet do not want the burdens associated with administrative.

Small-unit leaders in the combat arms occupational fields, primarily at the battalion level and below, prefer ownership of all supporting elements operating in their battlespace. For most commanders, ownership is necessary not only for the essential integration of fire and maneuver, but also to ensure good order and adherence to the commander's mission.[29] If a commander cannot task a section leader, he feels as though he does not own that section, and questions its necessity to his operations. The ownership and management dilemma is not exclusive to the Marine Corps. National intelligence suffered from the same maladies from the beginning of the Cold War era through the September 11, 2001 (9/11) attacks.[30] The national intelligence "need to know" and "need to own" culture crippled inter-organizational relationships and increased U.S. vulnerability to terrorist attacks.[31] Through an unfortunate period of trial and error, national intelligence reforms improved information exchange and agency collaboration.

National Intelligence Accord: The Information Sharing Evolution

> Power tends to corrupt, and absolute power corrupts absolutely. –
>
> Lord Acton[32]

> Another factor is the decision made in 1976, to sharply divide the FBI and the foreign intelligence agencies. The FBI would collect within the United States; the foreign intelligence agencies would collect overseas. –
>
> Admiral Bobby Ray Inman[33]

Mismanagement of and infighting over intelligence ownership is not a new problem. The terrorist attacks on 9/11 heightened earlier concerns over intelligence and law enforcement processes at the state and national levels. Congressionally appointed investigators determined policy barriers stemming from the Cold War era prevented information sharing between intelligence and law enforcement agencies that may have helped construct a complete picture of al Qaeda's intentions.[34] Agencies had the puzzle pieces, but could not put them together due to outdated and restrictive regulations. Several state and federal agencies tracked al Qaeda's activities in the months prior to 9/11, but a Department of Justice (DOJ) effort to delineate the distinction between criminal and foreign intelligence investigations erected a wall that hindered intelligence sharing.[35]

The wall was a visceral response to the enactment of the Foreign Intelligence Surveillance Act of 1978 (FISA).[36] The wall is a set of regulations, both codified and understood, that "limits the ability of law enforcement officials within the federal government to cooperate with intelligence officials involved in FISA investigations."[37] FISA authorizes warrantless electronic surveillance and collection on foreign and domestic intelligence threats in the interest of national security, but often challenges the boundaries of Fourth Amendment rights.[38] FISA's extralegal procedures inhibit the sharing of collected information with law enforcement because they could impede criminal prosecution and concurrently endanger or terminate the collection activity.[39] The wall concept had grave implications on 9/11. Due to

Office of Intelligence Policy and Review (OIPR) restrictions, New York FBI agents could not share known information concerning the hijackers with criminal investigators.[40] Additionally, federal intelligence agencies created special caveats for al Qaeda reporting that precluded the sharing of information without OIPR approval.[41] A combination of FISA restrictions, proprietary tendencies, and federal bureaucracy made possible an avoidable terrorist attack.

The events of 9/11 led to significant reforms in national intelligence to support sharing and address failures in the IC. To better coalesce operations and increase synergy in state and federal agencies, Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) requiring the Director of National Intelligence (DNI) to create a "more collaborative enterprise."[42] Congress also passed the Patriot Act, enhancing domestic security and imposing stiffer penalties for acts of terrorism.[43] Additionally, FISA has since been amended to eliminate impediments to information sharing between both state and federal law enforcement and intelligence communities.[44] National intelligence is now a shared responsibility vice a group of single actors.

Perhaps the most important intelligence innovation since 9/11 was the creation of the Director of National Intelligence (DNI) to manage the seventeen agencies and oversee the National Intelligence Program. DNI advises the President of the United States (POTUS) much like a military intelligence staff officer advises the unit commander. POTUS oversees and defines national intelligence objectives just as a military commander focuses the combat intelligence effort, but DNI manages the intelligence process regardless of geographic location or mission. The Marine Corps should adopt a similar model of intelligence management along functional lines to achieve optimum efficiency and results. The management over ownership approach allows for collective participation and practical integration of collection platforms with

operations. Functional management surpasses single commander ownership in military operations because its vision extends beyond one entity or a single piece of territory. An Armed Forces Communications and Electronic Association (AFCEA) White Paper released in 2007 reinforces this idea, stating "Owners do not always appreciate why information they control could be significant to others. For sharing to be effective, those who have a broader picture may be the best advocate regarding the process."[45] Command and control (C2) is important to military operations, but should be applied more sensibly in terms of intelligence.

Command and Control

> Who is a higher command staff officer to tell me how to employ the personnel working in my area of operations (AO)? He has no idea about the situation in my area. –
>
> Anonymous[46]

> It is not power that corrupts but fear. Fear of losing power corrupts those who yield it and fear of the scourge of power corrupts those who are subject to it. –
>
> *Aung San Suu Ky*[47]

Among the myriad of important planning factors facing military leaders, C2 is unquestionably the most essential to mission success. C2 "encompasses all military functions and operations, giving them meaning and harmonizing them into a meaningful whole."[48] Fleet Manual 101-5-1 defines C2 as "the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission."[49] It encompasses personnel, equipment, communications, and facilities that can be administered along service or functional lines.[50] C2 will not by itself win a decisive battle, directly engage or kill the enemy at a crucial point, or ensure the essential resupply of friendly forces. Furthermore, C2 will not psychologically prepare the fixed-wing fighter pilot for the collateral damage resultant of his close air support mission, nor will it ensure the forward-air-control officer assess the area for non-combatants prior to calling the air strike. However, non-existent or poorly

executed C2 will render the remaining five Marine Corps warfighting functions ineffective and absent of direction and coordination. Without effective C2, warfighting regresses to chaos and synergy of effort decays.

Outlining Marine Corps C2 in a confined, easily discernable environment is a fairly simple task. When a single commander is responsible for directing the only command involved in the operation, everyone understands who is responsible for the final decision. In a single command environment, the commander is ultimately responsible for all things administrative, operational, and tactical. The area of operations (AO) is conclusively defined, the mission is readily apparent to all involved, and in ideal situations, every warfighting function is at the commander's disposal. The commander decides how to move his forces, how to integrate air, sea, and logistics into his scheme of maneuver, where to engage the enemy, and how to integrate his intelligence section.

Single command environments are, however, rare in the post-Goldwater-Nichols era.[51] The four Department of Defense (DoD) services bring unique skills and capabilities to bear, and when working in unison, make for a highly effective organization. Most modern military operations involve multiple services, several commands and non-governmental organizations (NGO), and technical capabilities that, when nested with higher and adjacent units, can convolute decision making. Nevertheless, consistently nesting intelligence requirements across all levels of command supports enemy targeting, enhances collection efforts, increases force protection, and improves information sharing that is beneficial to the MAGTF.[52]

Intelligence is not designed to support a single commander's AO, nor is it feasible to integrate all intelligence processes at the regimental or battalion levels. Commanders must accept that some warfighting functions produce better results when integrated across all levels

of command and managed by technical experts. Decentralized operations are important to technical control measures, and while intelligence is a command function, it is a process more germane to staff oversight.[53] In the best interest of harmonious integration, the Marine Corps needs to find a balance between C2 and staff intelligence operations management. C2 is essential to successful operations, but as management consultant Margaret Wheatley once opined, "in these troubled times, we don't need more command and control; we need better means to engage everyone's intelligence in solving challenges and crises as they arise."[54] Multi-command or joint operational environments are now commonplace. In the joint operations world, functional management is preferable to single service or unit ownership. As stated in the previous section, the failures leading to the 9/11 attacks resulted in the founding of DNI as the functional manager of national intelligence. Similarly, the transition from the single command, Low Intensity Conflict Operations (LIC) of the post-Vietnam War era to modern, joint warfare requires a federated approach to military intelligence.

Single Service Intelligence

> One senior U.S. diplomat remarked that in low-intensity conflict as in real estate, there are only three things that matter. In real estate, these are location, location, location; in low-intensity conflict they are intelligence, intelligence, intelligence. –
>
> General Paul F. Gorman, USA[55]

Intelligence suffered from malaise brought on by a long period of stagnancy after the Vietnam War as the Marine Corps continued steady state operations in the form of low intensity conflicts (LIC). The United States Army Field Manual 100-20 defines LIC as:

> Political-military confrontations between contending states or groups below conventional warfare and above routine, peaceful competitions among states. Low intensity conflicts are often localized, generally in the Third World, but contain regional and global security implications.[56]

From the end of the Vietnam War through 1990, the Marine Corps operated considerably in LIC realms due to a rise in political and ideological dissident groups seeking to depose sitting governments or enforce religious law.[57] Examples of these conflicts include peacekeeping operations in Lebanon (1982-1984), Operation Urgent Fury in Grenada (1983), Noncombatant Evacuation Operations in Liberia and Somalia (1990), and the Iraq-Kuwait war that preceded Operation Desert Shield (1990-91).[58] Marine Expeditionary Units (MEU) were often tasked with these missions due to either geographic proximity to threatened areas, or in keeping with the MAGTF's reputation as a force in readiness with a balanced air-ground component. Very seldom did multiple Marine units deploy in unison to support the large-scale operations that typified previous twentieth-century wars, and individual commanders were largely uninhibited by higher headquarters units in the afflicted areas. Outright ownership of all Marine forces was commonplace, removing the internal discord between like units and higher headquarters elements.

In the LIC environment, Marine Corps intelligence personnel and equipment are routinely attached to the invading force as a supplementary capability. All MEUs have organic intelligence assets, but these assets are numerically insufficient or lacking a required functional area.[59] To address these shortfalls, the MEF routinely augments the MEU with additional personnel derived from either other units within the MEF, or through composing a feasibility of support (FOS) message generated by Headquarters Marine Corps and disseminated across all Marine forces.[60] The MEU commander owns, tasks, and integrates his intelligence personnel across the full spectrum of operations with impunity. The MEU S-2 regularly coordinates with higher or adjacent units to obtain pre-made or "canned" products, but the MEU commander directs all missions.[61] Intelligence C2 is never in question;

however, platforms are limited, and cross-agency integration depends on coordination with Combatant Command (COCOM) intelligence centers. Some commanders prefer this arrangement and often assume the conditions will remain the same in joint or multiple unit environments.

Multiple Service Intelligence

> Tactics is the employment and ordered arrangement of forces in relation to each other. Joint doctrine focuses this term on planning and executing battles, engagements, and activities at the tactical level to achieve military objectives assigned to tactical units or task forces. –
>
> JP 3-0: Joint Operations[62]

Joint operations consist of "activities, operations, and organizations in which elements of two or more military departments participate."[63] Multiple unit and joint military environments differ from single-unit environments in that they require considerably more coordination due to the unique capabilities and procedures of each service. The Department of Defense Reorganization Act of 1986 (Goldwater-Nichols) improved DoD service integration and brought joint operations to the forefront.[64] Joint operations provide Combatant Commanders (CCDR) more flexibility to maximize the benefits and capabilities of each service in a single operating environment.[65] C2 can be challenging in the joint operating arena, but common sense and an understanding of procedural integration alleviates confusion. Joint doctrine provides the commander with several C2 options; the two most commonly employed are service component command and functional command.[66] The MAGTF is an all-inclusive package of air, ground, and sea power, equipped with both operators and maintainers for self-sufficiency.[67] As an expeditionary quick reaction force, it must be ready for immediate tasking to crisis areas.[68] In the joint environment, the MAGTF's constitutional integrity is beneficial, but not imperative to success. One can argue that service C2 is

detrimental to joint operations. Air operations is the best example of the necessity for functional C2.

Joint air operations C2 along functional lines exceed the benefits of service lines; the joint forces air component commander (JFACC) allocates assets, serves as the airspace control authority, de-conflicts operations, and generally keeps the airspace safe.[69] A service commander would not consider tasking an aerial platform without first de-conflicting with the JFACC. Sorties are allocated by operational objective, and the JFACC's familiarity with service platforms ensures their efficient use. Additionally, the JFACC safeguards the many pilots and platforms to avoid collisions and inaccurate targeting.[70] Similarly, incorporating MAGTF intelligence sections with geographic COCOM intelligence centers and JTF intelligence staff sections creates a more robust and responsive capability. Federated intelligence supports centralized planning and decentralized execution for better support to commanders throughout the battlespace.[71]

Joint intelligence operations do not present the same dangers associated with joint air operations, but duplicating effort or failure to assimilate each service's capabilities can waste time and cloud the intelligence picture. For example, intelligence collection platforms serve a single purpose regardless of the service employing them; to collect information and feed the intelligence process.[72] However, platforms have different capabilities that, when synchronized in the joint arena, produce corroborated products that increase the collected information's validity. One example is the cross-cueing process; the "passing of detection, geolocation, and targeting information to another sensor or target acquisition system without a human interface."[74] Cross-cueing works best when using collections platforms from all

services, as each one provides unique systems not always available to the others. The following is a generic example of the cross-cueing technique in a joint environment:

> An Air Force Joint Surveillance Target Air Radar System (JSTARS) Common Ground System (CGS) detects enemy ground forces moving towards a friendly location. The JSTARS cues a MAGTF Secondary Imagery Dissemination System (MSIDS) that provides more specific geolocation data on the enemy force. The MSIDS alerts an Army air reconnaissance and surveillance team, which then eliminates the target.

Each service works in unison to collect information, alert friendly forces, and target the enemy. Intelligence analysis works in a similar but less technical manner. Collected intelligence is useless without analysis, production, and utilization, and single service collection provides no benefit to the joint environment if not shared with other services. Joint intelligence centers are now fixtures of every COCOM and functional command.[75] Geographically focused intelligence centers provide continuity through specific focus on each COCOM's AO; information collected by any platform in the AO collates at the intelligence center for production, analysis, and reciprocal support to forces operating within the COCOM's AO.

Federated intelligence at the DoD and joint operating levels improves incrementally with each successful joint operation. Commanders better understand the benefits of integrated intelligence, and are therefore more inclined to accept support from other services and joint intelligence centers. MEU commanders, in particular, are acclimating to federated intelligence because it accelerates the decision-making process; when mass intelligence centers provide canned products on countries of interest in a near real-time fashion, the MEU S-2 can focus on host nation liaison rather than building situational awareness.[76] In short, the MEU skips one step in the planning process. Because the MEU operates in an ever-changing, rapid environment, all opportunities to expedite planning must be exploited.[77] Additionally, U.S. Embassy teams readily understand the threat to inbound forces and can better advise units on foreign points of

contact, training areas, and areas they should avoid during liberty calls. Federated intelligence is well established in the joint world, and MCISR-E seeks to institute the same competencies at the service level.

Marine Corps Intelligence, Surveillance, and Reconnaissance-Enterprise

> Accurate, timely, and relevant intelligence is critical to the planning and conduct of successful operations. Effective intelligence uncovers enemy weaknesses which can be exploited to provide a decisive advantage. Shortfalls in intelligence can lead to confusion, indecision, unnecessary loss of life, mission failure, or even defeat. –
>
> MCDP 2: Intelligence[78]

> The resources at our disposal are not always obvious, can change during the course of a struggle, and usually need to be adapted to suit our needs. Our adversary often refuses to fit our preconceptions of him or to stand still while we erect the apparatus for his destruction. –
>
> MCDP 1-1: Strategy[79]

Marine Corps Intelligence Department developed MCISR-E in response to two enduring problems: inability to fully integrate with the Defense Intelligence Enterprise and the proclivity for reactionary intelligence, surveillance, and reconnaissance (ISR).[80] MCISR-E supports commanders through enlightening the entire operational environment rather than supporting a single commander's battlespace, and its premise is "24/7/365 predictive intelligence that is timely and relevant."[81] Before MCISR-E, MEF and division intelligence sections sporadically supported subordinate commands, and only when requested in times of crisis. The MAGTF operated almost independently, with few ties to national agencies and geographically based intelligence centers. Information was sporadic and often uncorroborated, but operations sometimes succeeded in spite of intelligence shortcomings, leading to a false sense of accomplishment. MCISR-E addresses these historical trends through "synchronizing intelligence programs, units, and personnel at every echelon across the operating forces."[82] Theoretically, synchronization leads to collaboration and information sharing that is beneficial to

the collective. But until commanders embrace MCISR-E tenets and Headquarters Marine Corps (HQMC) codifies the program, it is nothing more than a good idea.

Commanders have yet to adjust to MCISR-E for a myriad of reasons: HQMC has not codified it, there is no management apparatus, many do not know of its existence, and commanders do not own the process.[83] While conducting the research on MCISR-E's origins and current progress, an anonymous HQMC source stated, "It is off the rails," meaning organizations employ it by whichever means they deem appropriate, and often incorrectly.[84] Discussions concerning management are contentious. The intelligence community agrees with MCISR-E's tenets of federation, consistent intelligence support both home and abroad, and community management. Yet, divisions contend it should be managed at the regimental and infantry-battalion levels where units execute combat operations.[85] Above all, there is nothing to prevent commanders from stovepiping collected information if no management section exists. With no management apparatus, information is raw, unevaluated, and useless to other commanders. The puzzle pieces are on the table, but there is no one to put them together.[86]

MCISR-E needs refinement, and HQMC is progressing towards a permanent solution.[87] The MEF Intelligence Cell (MIC) is a MCISR-E success story, and a functional element of all three MEFs.[88] MICs enable units to train as they fight by "providing analytical and intelligence production support from garrison locations to deployed forces," supporting the Commandant's efforts to reinforce forward units.[89] MICs fill several voids: they serve as training opportunities for non-deployed Marines, collate and make sense of collected information, and support commanders' decision making.[90] Prior to the MIC, federated intelligence at the MEF level was a false hope. Commanders focused only on their tasked missions, a reactionary approach to planning.[91] Comprised of several geographically dedicated analytical cells, the MIC focuses

globally, giving commanders insight to threat areas and the ability to train proactively and plan for future threats. The MIC is a proven example of garrison based support, but MCISR-E works equally as well in a deployed environment.

The MEB employed MCISR-E-like processes in the latter stages of Afghanistan with great success. Federated intelligence allowed commanders to focus on operational planning rather than attempting to determine the intelligence picture while lacking crucial information. Alleviating commanders of convoluted intelligence processes was inherently beneficial to decision making.[92] Collection teams across Helmand Province supported areas rather than individual commanders, but simultaneously answered commanders' PIRs. Information collected by a team in one AO was forwarded to the MEF Intelligence Operations Center (IOC), analyzed, and consolidated into products for mass consumption.[93] The enemy does not recognize dotted lines on a map that separates friendly battlespaces; it was not uncommon for enemy personnel to move frequently in order to avoid detection.[94] As such, the MEF-acknowledged information collected in one commander's battlespace may be beneficial to other commanders operating in adjacent AOs. In short, commanders had several teams collecting on their behalves.[95] Additionally, targeting prioritization was a MEF responsibility; the G-2 worked in concert with the G3 Operations Center to reactively target enemy personnel, equipment, and facilities. As enemy personnel moved throughout Helmand Province, intelligence professionals tracked their movements, coordinated with battlespace owners, and supported targeting efforts through the MEF Fires center.[96]

Coordinating ISR in a single command environment is challenging, but in a joint or multiple-command war, it is extremely difficult at best. Commanders consistently clash over use of ISR platforms, as each believes his targets the priority. MCISR-E takes the guesswork out of

ISR allocation by leveraging and sharing platforms in real-time.[97] UASs reallocated or re-missioned based on the senior commander's considerations and the target's value.[98] If a drone is allocated to a pre-determined target, it can be re-directed to a time-sensitive target by the MEF collections manager. Regimental and battalion commanders may be displeased with the decision, but no one can justifiably say the system is inequitable.

MCISR-E is not an infallible concept and there is still work to be done to make it a codified program. However, it meets the requirement for federated intelligence, and further proves that intelligence management at the staff level is more efficient than parochial ownership. Computer systems are now compatible between services and the national intelligence community, units share information in the best interest of the collective effort, and collections teams focus on theater requirements rather than concentrating solely on those threats in a single AO. Production is no longer limited to one area, one service, or one agency. It is available to all, and it better broadens the operational aperture and lessens the impacts of unit dispersion.[99]

Conclusions

The mission of Marine Corps intelligence is to "provide commanders with seamless, tailored, timely, and mission-essential intelligence, and to ensure its integration into the operational planning process."[100] Commanders are key components of intelligence planning, but do not require ownership of its processes, personnel, or equipment to benefit from its findings. The single service and single command environments, while still prevalent, no longer dominate today's battlefields. During the LIC era, holistic ownership of all supporting capabilities was essential to mission accomplishment, as the commander was often the sole operational decision maker and frequently under resourced. From the early 1970s through 9/11 the MEU's linear intelligence processes and the lack of geographic think tanks made self-sufficiency a necessity.

With new national intelligence reforms addressing the growing U.S. security threat through encouraging information sharing, IC cooperation and management alleviates commanders of directing convoluted, time consuming intelligence operations.

The intelligence cycle is an iterative process that is more intricate and complicated than it appears. It requires consistent staff interaction and de-confliction, coordination for platform and information sharing, and dissemination across the theater of operations for data basing and metrics development.[101] Intelligence cannot be isolated to a battlespace or concealed from other units that may benefit from its findings. The key to the intelligence process is applying the cycle to the unit commander's intelligence requirements, not providing him ownership of the process. Planning and direction is the commander's foremost responsibility to the cycle. He must focus and support the effort, but once the battlespace is prepped and the direction provided and understood, the larger intelligence apparatus must assume ownership.[102] To best employ intelligence in the joint and multiple-command environments, functional command should be the rule, not the exception. Functional command streamlines operations and federates capabilities to a greater degree than service command.[103] Additionally, functional command is not biased, proprietary, or myopically focused on one portion of the intelligence process. Output is essential to effective operations, but collection, analysis, production, and dissemination are the backbone of the process.

Federated intelligence is the most flexible concept to support MAGTF operations and Marine commanders. The national community learned this important lesson through a series of critical errors that led to the largest attack on U.S. soil since the Japanese attack on Pearl Harbor. As a result of 9/11 and confounding operations in the two-front war, the Marine Corps moved ahead of the power curve with MCISR-E, a practical solution to restructuring the lowest density

occupational field in the service. In the age of DoD downsizing, making efficient use of limited assets is vital to operational success. Commanders must conquer their phobias and accept intelligence federation, and more importantly, must educate themselves on MCISR-E. Until they relent and embrace the process, the organization will not turn the proverbial corner.

Acronyms

ADCON – Administrative Control
AFCEA – Armed Forces Communications and Electronic Association
AO – Area of Operations
C2 – Command and Control
CCDR – Combatant Commander
CCIR – Commander's Critical Information Requirement
CHD – Counterintelligence HUMINT Detachment
CI – Counterintelligence
CIA – Central Intelligence Agency
CIHEP – Counterintelligence and HUMINT Equipment Program
CIHOC – Counterintelligence and Human Intelligence Operations Center
COCOM – Combatant Command
CSS – Combat Service Support
DIA – Defense Intelligence Agency
DNI – Director of National Intelligence
DoD – Department of Defense
DOJ – Department of Justice
FBI – Federal Bureau of Investigation
FISA – Foreign Intelligence Surveillance Act of 1978
FOS – Feasibility of Support
G-2 – Staff Intelligence Officer
G2X – Staff Counterintelligence and Human Intelligence Officer
HET – HUMINT Exploitation Team
HQMC – Headquarters Marine Corps
HUMINT – Human Intelligence
IC – Intelligence Community
IOC – Intelligence Operations Center
J-2 – Joint Staff Intelligence Officer
JFACC – Joint Forces Air Component Commander
JTF – Joint Task Force
LIC – Low Intensity Conflict
MAGTF – Marine Air Ground Task Force
MAW – Marine Air Wing
MCISR-E – Marine Corps Intelligence, Surveillance, Reconnaissance-Enterprise
MEB – Marine Expeditionary Brigade
MEF- Marine Expeditionary Force
MEU – Marine Expeditionary Unity
MIC – MEF Intelligence Cell
MLG – Marine Logistics Group
NGO – Non-governmental Organization
NSA – National Security Agency
OCAC – Operational Control and Analysis Center
OEF – Operation Enduring Freedom
OIF – Operation Iraqi Freedom
OIPR – Office of Intelligence Policy and Review

OPCON – Operational Control
PIR – Priority Intelligence Requirement
POTUS – President of the United States
RO – Reports Officer
RRT – Radio Reconnaissance Team
SRIG – Surveillance, Reconnaissance, Intelligence Group
SST- Signals Intelligence Support Team
TACON – Tactical Control
TBS – The Basic School
TECHCON – Technical Control
TFC – Tactical Fusion Center
UAS – Unmanned Aerial System
UAV – Unmanned Aerial Vehicle

Glossary

All-Source Intelligence - Intelligence products and/or organizations and activities that incorporate all sources of information, most frequently including human resources intelligence, geospatial intelligence, measurement and signature intelligence, signals intelligence and open source data in the production of finished intelligence. (USMC ISR Roadmap)

Counterintelligence - Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments of elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (JP 1-02)

Corroboration – A process by which national intelligence and military organizations use multiple forms of intelligence to validate sources of information, i.e., human intelligence and signals intelligence.

Cross-Cuing – A method used to obtain different types of intelligence such as current activity; location; use of radio or radar emitters; or movement, direction, and speed on a given enemy element. Three factors affect the sensor selection process: sensor availability, current knowledge, and type of additional knowledge required to support the desired action. (fas.org)

Foreign Intelligence Surveillance Act – A United States federal law which prescribes procedures for the physical and electronic surveillance and collection of "foreign intelligence information" between "foreign powers" and "agents of foreign powers" (which may include American citizens and permanent residents suspected of espionage or terrorism). (50 USC §1801.B)

Force Protection - Security program designed to protect soldiers, civilian employees, family members, facilities, and equipment, in all locations and situations, accomplished through planned and integrated application of combatting terrorism, physical security, operations security, personal protective services, and supported by intelligence, counterintelligence, and other security programs. (Army) — one of the four primary elements that combine to create combat power. It conserves the fighting potential of a force. The four components of force protection are: operational security and deception operations; the soldier's health and morale; safety; and the avoidance of fratricide. (JP 1-02)

Geospatial Intelligence - The exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict features and geographically referenced activities on the earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information. (USMC ISR Roadmap)

Human Intelligence - A category of intelligence derived from information collected and provided by human sources. (FM 101-5-1)

Imagery Intelligence - Intelligence derived from the exploitation of collection by visual photography, infrared sensors, lasers, electro-optics, and radar sensors such as synthetic aperture radar wherein images of objects are reproduced optically or electronically on film, electronic display devices, or other media. (FM 101-5-1)

Intelligence - Intelligence derived from the exploitation of collection by visual photography, infrared sensors, lasers, electro-optics, and radar sensors, such as synthetic aperture radar

wherein images of objects are reproduced optically or electronically on film, electronic display devices, or other media. (FM 101-5-1)

Intelligence Cycle - The steps by which information is converted into intelligence and made available to users. There are five steps in the cycle: a. planning and direction — Determination of intelligence requirements, preparation of a collection plan, issuance of orders and requests to information collection agencies, and a continuous check on the productivity of collection agencies. b. collection — Acquisition of information and the provision of this information to processing and/or production elements. c. processing — Conversion of collected information into a form suitable to the production of intelligence. d. production — Conversion of information into intelligence through the integration, analysis, evaluation, and interpretation of all source data and the preparation of intelligence products in support of known or anticipated user requirements. e. dissemination — Conveyance of intelligence to users in a suitable form. (JP 1-02)

Intelligence Federation - Enables CCMDs to form support relationships with other theater JIOCs, Service intelligence centers, JRICs, or other DoD intelligence organizations to assist with the accomplishment of the joint force's mission. These support relationships, called federated partnerships, are preplanned agreements (formalized in OPLANs, national intelligence support plans (NISPs), or memorandums of agreement) intended to provide a rapid, flexible, surge capability enabling personnel from throughout the IC to assist the CCMD while remaining at their normal duty stations. Federated support can be provided in specific functional areas directly related to the crisis, or by assuming temporary responsibility for non-crisis-related areas within the GCCs' AORs, thereby freeing the supported command's organic assets to refocus on crisis support. (JP 2-0)

Intelligence Preparation of the Battlespace - A systematic approach to analyzing the enemy, weather, and terrain in a specific geographic area. It integrates enemy doctrine with the weather and terrain as they relate to the mission and the specific battlefield environment. This is done to determine and evaluate enemy capabilities, vulnerabilities, and probable courses of action. (FM 101-5-1)

Intelligence Operations Center - An interdependent, operational intelligence organization at the Department of Defense, combatant command, or joint task force (if established) level, that is integrated with national intelligence centers, and capable of accessing all sources of intelligence impacting military operations planning, execution, and assessment. Also known as Tactical Fusion Center and All Source Analysis Center (JP 2-0)

Intelligence Requirement - Any subject, general or specific, upon which there is a need for the collection of information or the production of intelligence. (FM 101-5-1)

Intelligence Surveillance and Reconnaissance - An activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function. (JP 2-01)

Marine Corps Intelligence, Surveillance, and Reconnaissance-Enterprise – A Marine Corps intelligence plan that articulates and implements the Director of Intelligence's vision for designing and developing the MCISR-E. As the Annex B to the Marine Corps Service Campaign Plan (MCSCP), it describes how the MCISR-E plans and executes the intelligence warfighting

function across all echelons of the Service, the Intelligence Community, and the Joint Force. It provides the framework and Service-level direction for continued development of an all-source Intelligence, Surveillance, and Reconnaissance Enterprise to meet the specified and implied tasks identified in the Marine Corps Service Campaign Plan and the subordinate Campaign Support Plan. (MCISR-E 2015-2020)

Signals Intelligence - A category of intelligence comprising either individually or in combination all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted. 2. Intelligence derived from communications, electronics, and foreign instrumentation signals. (JP 1-02)

Targeting - The process of selecting targets and matching the appropriate response to them, taking account of operational requirements and capabilities. 2. The analysis of enemy situations relative to the commander's mission, objectives, and capabilities at the commander's disposal, to identify and nominate specific vulnerabilities that, if exploited, will accomplish the commander's purpose through delaying, disrupting, disabling, or destroying enemy forces or resources critical to the enemy. (FM 101-5-1)

The Wall - A separation of intelligence investigators from contact with criminal prosecutors, and evolved to include a separation of FBI investigators working on intelligence investigations from investigators working on criminal investigations. The wall concept was cited as the primary inhibitor to preventing the September 11 attacks. (justice.gov)

Endnotes

[1]Headquarters U.S. Marine Corps, *Intelligence Operations*, MCWP 2-1 (Washington, D.C.: U.S. Marine Corps, September 10, 2003), 1-5.

[2]Several infantry battalions in Iraq trained young infantry Marines to run human source operations and interrogations. Formally trained CI/HUMINT Marines were restricted by theater and COCOM policies on the conduct of CI/HUMINT operations. HETs were not always staffed to support battalions conducting distributed operations.

[3]The SRIG was an intelligence unit providing surveillance, reconnaissance, intelligence, and counterintelligence in support of the MAGTF. The SRIG was subordinate to the MEF, and deployed as a complete intelligence package in support of deploying units. It existed from 1988-1997 and was eventually replaced by the Intelligence, Radio, and Reconnaissance Battalions. Thomas E. Leard, "Marine Corps Intelligence For War As It Really Is," (master's thesis, Naval Postgraduate School, 1991), 52-57.

[4]A PIR is an intelligence requirement (IR) associated with a decision that will critically affect the overall success of the command's mission. PIRs are a subset of commander's critical information requirements (CCIR) and are focused on the environment and the threat. Headquarters U.S. Marine Corps, *Intelligence Operations*, MCWP 2-1 (Washington, D.C.: U.S. Marine Corps, September 10, 2003), 1-5.

[5]A Marine Corps Fitness Report is system provides the official evaluation and record of a Marines performance.
Shannon Phillips and Adam Clemons, "The Fitness Report System for Marine Officers: Prior Research," *Center for Analysis and Solution*, (2011). 1-2.
https://www.cna.org/research/2011/fitness-report-system-marine-officers.

[6]Based on my firsthand experience as a Reports Officer, HET Officer in Charge, and CI/HUMINT Company Operations Officer while a member of 2nd Intelligence Battalion in Camp Lejeune, North Carolina. The data was acquired through several discussions with various intelligence officers between 2006-2009.

[7]Nick Van Der Bijl, *Sharing the Secret: The History of the Intelligence Corps 1940-2010* (South Yorkshire: CPI Group, 2013), 76.

[8]Headquarters U.S. Marine Corps, *Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise (MCISR-E)*, 2014, Marine Corps Concepts and Programs, https://marinecorpsconceptsandprograms.com/programs/intelligence-surveillance-and-reconnaissance/marine-corps-intelligence-surveillance-and.

[9]"Intelligence, Surveillance, & Reconnaissance Enterprise Plan," 2015, Headquarters, United States Marine Corps, Intelligence Department, Washington D.C.

[10]Headquarters U.S. Marine Corps, *Marine Corps Operations*, MCDP 1-0 (Washington D.C.: Marine Corps, August 9, 2011), 1-3.

[11]Headquarters U.S. Marine Corps, *MAGTF Intelligence Collection*, MCDP 2-2 (Washington D.C.: Marine Corps, July 30, 2004), 2-4.

[12]Ibid., 1-5.

[13]U.S. Department of Defense, *Joint Intelligence,* JP 2-0 (Washington, D.C.: Department of Defense, October 22, 2013), I-11.

[14]Headquarters U.S. Marine Corps, *Intelligence Operations*, MCWP 2-1 (Washington, D.C.: U.S. Marine Corps, September 10, 2003), 1-8.

[15]The intelligence cycle consists of a sequence of related activities that translate requirements for various types of information into intelligence that is furnished to the commander for use in the decision making cycle.
Headquarters U.S. Marine Corps, Intelligence Operations, MCWP 2-1 (Washington, D.C.: U.S. Marine Corps, September 10, 2003), 3-1.

[16]Carl von Clausewitz, *On War*, ed. Michael Howard and Peter Paret, trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1984), 101.

[17]U.S. Department of Defense, *Military Intelligence Handbook,* Vol 1 (Washington D.C.: Department of Defense, 2009), 226.

[18]Headquarters U.S. Marine Corps, *Intelligence Operations*, MCWP 2-1 (Washington, D.C.: U.S. Marine Corps, September 10, 2003), 1-2.

[19]Headquarters U.S. Marine Corps, *Command and Control*, MCDP 6 (Washington, D.C.: U.S. Marine Corps, October 4, 1996), 40.

[20]Headquarters U.S. Marine Corps, *Intelligence Operations*, MCWP 2-1 (Washington, D.C.: U.S. Marine Corps, September 10, 2003), 1-4.

[21]Headquarters U.S. Marine Corps, *Marine Corps Planning Process*, MCWP 5-1 (Washington, D.C.: U.S. Marine Corps, August 24, 2010), 2-7.

[22]Army Logistician: Professional Bulletin of United States Army Logistics, Volume 39, Issue 6 *COCOM, ADCON, OPCON, TACON, Do You Know the Difference?* (Washington D.C: Army Logistics, 2007), http://www.almc.army.mil/alog/issues/NovDec07/cmmd_relat_difference.html.

[23]Headquarters U.S. Marine Corps, *Joint Force Land Component Commander Handbook,* MCWP 3-40.7 (Washington, D.C.: U.S. Marine Corps, June 8, 2012), 1-4.

[24]Ibid., II-14.

[25]Headquarters U.S. Marine Corps, *Counterintelligence*, MCWP 2-6 (Washington, D.C.: U.S. Marine Corps, July 13, 2004), 3-14.

[26]Ibid., 5-11.

[27]The MEU is the accepted standard for the size of a CHD. MEU CHDs consist of six team members; one officer in charge and five enlisted collectors. However, there is no doctrinally accepted team size. The area of operations, size of the unit supported, mission requirements, and capability requirements will determined the size of a CHD.

[28]Cyber Network Operators are responsible for the installation, configuring and management of cyber network systems in both stand alone and client-server environments including Microsoft based curriculum and MS Exchange/Server, CISCO Certified Network Associate (CCNA) Modules 1, 2 and 3, as well as other authorized cyber network systems. They install, configure and maintain cyber services, both hardware and software. They also plan and execute the integration of multiple information systems to include Data Distribution System-Replacement/Modular (DDS-R/M), in a network environment, evaluate and resolve customer information system problems and effect hardware upgrades and repair to maintain mission capability. Skill progression for Sergeants and Corporals is the Cyber Network Supervisor Course. Marine Corps Credentialing Opportunities On-line, *MOS 0651 Cyber Network Operator*, accessed 19 February, 2015. https://www.cool.navy.mil/usmc/enlisted/0651.htm.

[29]Headquarters U.S. Marine Corps, *Command and Control*, MCDP 6 (Washington, D.C.: U.S. Marine Corps, October 4, 1996), 44-47.

[30]Counterterrorism Intelligence Capabilities and Performance Prior to 9-11," July 2002, Headquarters, U.S. House of Representatives, Subcommittee on Terrorism and Homeland Security, Washington D.C.

[31]Richard A. Best Jr, *Intelligence Information: Need to Know vs. Need to Share*, CRS Report for Congress R41848, (Washington, DC: Congressional Research Service, June 6, 2011).

[32]Lord John Dalberg-Acton, Letter received by Mandell Creighton, April 5, 1887, Hanover College History Department.

[33]Bobby Ray Inman interviewed by Ann Louise Bardach, 2004, Slate Website, accessed 13 January, 2015, http://www.slate.com/articles/news_and_politics/interrogation/2004/12/listen_to_the_admiral.html.

[34]National Commission of Terrorist Attacks, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States (Authorized Edition)*, (New York: W.W. Norton), 221-225.

[35]Ibid., 71-82.

[36]Neil A, Lewis, “THREATS AND RESPONSES: INTELLIGENCE SHARING; Rule Created Legal 'Wall' To Sharing Information,” *nytimes.com,* April 14, 2004. http://www.nytimes.com/2004/04/14/us/threats-responses-intelligence-sharing-rule-created-legal-wall-sharing.html.

[37]Cedric Logan, “The FISA Wall and Federal Investigations,” New York University Journal of Law & Liberty, 2009.

[38]Fletcher N. Baldwin, Jr. and Robert B. Shaw, “Down to the Wire: Assessing the Constitutionality of the National Security Agency’s Warrantless Wiretapping Program: Exit the Rule of Law,” *University of Florida Law Scholarship Repository* (2006): 429-435.

[39]Daniel J. Solove, *Nothing to Hide: The False Tradeoff Between Privacy and Security*, (Hartford: Yale University Press, 2011), 76-78.

[40]Senate Committee Proceedings, Congressional Record, 108th Cong., 2004, Committee Print 20389-20400.

[41]Office of the Inspector General, “A Review of the FBI's Handling of Intelligence Information Prior to the September 11 Attacks,” Ch 2 (November 2004), http://www.justice.gov/oig/special/0506/chapter2.htm.

[42]Gerhard Peters and John T. Woolley, "George W. Bush: "Statement on Signing the Intelligence Reform and Terrorism Prevention Act of 2004," December 17, 2004. *The American Presidency Project*.

[43]Lisa Mascaro, “Patriot Act provisions extended just in time,” *latimes.com,* May 27, 2011. http://articles.latimes.com/2011/may/27/nation/la-na-patriot-act-20110527.

[44]U.S. Federal Bureau of Investigation. *Testimony by FBI Director Robert S. Mueller and U.S. Attorney General Alberto R. Gonzalez to the Select Committee on Intelligence United States Senate*, Washington D.C., (April 27, 2005).

[45]“The Need to Know: The U.S. Intelligence Community and Law Enforcement,” *Armed Forces Communications and Electronic Association*, White Paper, (April 2007), 9.

[46]Interview with a Marine Corps Officer during a combat mission after action discussion in Al Anbar Province, Iraq, 2006.

[47]Justin Wintle, ed, *New Makers of Modern Culture: Volume I, A-K* (New York: Routledge, 2007), 66-67.

[48]Headquarters U.S. Marine Corps, *Command and Control*, MCDP 6 (Washington, D.C.: U.S. Marine Corps, October 4, 1996), 36.

[49]Headquarters U.S. Marine Corps, *Operational Terms and Graphics*, FM 101-5-1 (Washington, D.C.: U.S. Marine Corps, December 30, 1997), 1-33.

[50]U.S. Department of Defense, *Doctrine for the Armed Forces of the United States*, JP 1 (Washington, D.C.: Department of Defense, October 22, 2013), IV 12-IV 17.

[51]*Goldwater-Nichols Department of Defense Reorganization Act of 1986*, HR 3622, 99th Cong., Congressional Record 131, no. 132, daily ed. (1 October 1986).

[52]Headquarters U.S. Marine Corps, *Intelligence Operations*, MCWP 2-1 (Washington, D.C.: U.S. Marine Corps, September 10, 2003), 1-7.

[53]Ibid., 2-1.

[54]Margaret J. Wheatley, *Finding Our Way: Leadership for an Uncertain Time* (San Francisco: Barret-Kohler, 2005), 77.

[55]C. Christine Fair, *Fighting to the End: The Pakistan Army's Way of War*, (Oxford: Oxford University Press, 2014), 219.

[56]Headquarters U.S. Army, *Military Operations in Low Intensity Conflict*, FM 100-20 (Washington, D.C.: U.S. Army, 5 December, 1990), 1-1.

[57]William Weir, *Guerrilla Warfare: Irregular Warfare in the Twentieth Century* (Mechanicsburg: Stackpole Books, 2008) 204-216.

[58]Claude C. Sturgill, *Low-Intensity Conflict in American History* (Portsmouth: Preager, 1993).

[59]The MEU Commander has several intelligence capabilities at his disposal, including: all source, geographic, imagery, signals, communications, ground sensors, counterintelligence, and human intelligence. The MEU S-2 is comprised of approximately 20-25 intelligence professionals, and are capable of collections, analysis, and fusion operations.

[60]Feasibility of support messages are common for low-density, high demand units, or for unites supporting multiple contingencies. Based on the MEU's mission requirements, MEU commanders may request additional personnel or equipment to augment their operations abroad or during training exercises. Most augmenting personnel derive from the Intelligence, Radio, or Reconnaissance Battalions, and in extreme cases, from higher-level staffs such as the MEF, MAW, MLG, or Division.

[61]Canned briefs are pre-made briefs developed by intelligence analysts and collectors who with either the placement and access or information, or reside in proximity of the area of operations. Each Component and Functional command has a Joint Analysis/Intelligence Center dedicated to answering commander's requirements. These centers provide direct intelligence support for all assigned forces supporting the command on either a permanent or temporary basis. The National Security Strategy describes the Joint Intelligence Center as "the principle element for ensuring effective intelligence support for combatant commanders in chiefs and theater forces." MEU S-2 sections regularly request briefs from JICs when preparing for combat, military engagement, humanitarian and disaster relief, etc, operations.

[62]U.S. Department of Defense, *Joint Operations,* JP 3-0 (Washington, DC: Department of Defense, September 10, 2001), vii.

[63]U.S. Department of Defense, *Doctrine for the Armed Forces of the United States,* JP 1 (Washington, D.C.: Department of Defense, March 25, 2013), GL-8.

[64]*Goldwater-Nichols Department of Defense Reorganization Act of 1986,* HR 3622, 99th Cong., Congressional Record 131, no. 132, daily ed. (1 October 1986).

[65]U.S. Department of Defense, *Doctrine for the Armed Forces of the United States,* JP 1 (Washington, DC: Department of Defense, March 25, 2013), V-17.

[66]U.S. Department of Defense, *Joint Operations,* JP 3-0 (Washington, DC: Department of Defense, September 10, 2001), x-xi.

[67]Headquarters U.S. Marine Corps, *Marine Corps Operations*, MCDP 1-0 (Washington D.C.: Marine Corps, August 9, 2011), 1-6.

[68]Ibid., 1-12.

[69]U.S. Department of Defense, *Joint Operations,* JP 3-0 (Washington, DC: Department of Defense, September 10, 2001), II-16 – II-18.

[70]Ibid., II-16 – II-18.

[71] Ibid., II-19.

[72]Headquarters U.S. Marine Corps, *Intelligence Operations*, MCWP 2-1 (Washington, D.C.: U.S. Marine Corps, September 10, 2003), 3-2 – 3-10.

[73]Ibid., 4-9.

[74]Steven M. Bargman, "The Utility of Hyperspectral Data in Detecting and Discriminating Actual and Decoy Target Vehicles." Master's thesis, U.S. Naval Postgraduate School, 1996.

[75]U.S. Department of Defense, *Joint Intelligence,* JP 2-0 (Washington, D.C.: Department of Defense, October 22, 2013), V-5.

[76]Ibid., II-11.

[77]Headquarters U.S. Marine Corps, *Marine Corps Operations*, MCDP 1-0 (Washington D.C.: Marine Corps, August 9, 2011), 1-16.

[78]Headquarters U.S. Marine Corps, *Intelligence*, MCDP 2 (Washington D.C.: Marine Corps, June 7, 1997), 28-29.

[79]Headquarters U.S. Marine Corps, *Strategy,* MCDP 1-1 (Washington D.C.: Marine Corps, November 12, 1997), 9-15.

[80]Headquarters U.S. Marine Corps, *Marine Corps Intelligence, Surveillance, & Reconnaissance Plan,* (Washington D.C.: Marine Corps, May 5, 2010), 2.

[81]Headquarters U.S. Marine Corps, *Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise (MCISR-E),* 2014, Marine Corps Concepts and Programs,

https://marinecorpsconceptsandprograms.com/programs/intelligence-surveillance-and-reconnaissance/marine-corps-intelligence-surveillance-and.

[82]Ibid.

[83]Ibid.

[83]Interview with a HQMC staff officer, December 28, 2014.

[84]Ibid.

[85]Ibid.

[86]Ibid.

[87]Ibid.

[88]The MEF Intelligence Cell is the primary MEF intelligence node responsible for leveraging the MEF intelligence enterprise. It ensures the MEF's collective intelligence effort remains aligned with the CG's objectives and priorities through the development of PIRs and CIPPs as published in the MEF Intelligence Campaign Plan; assists G-2 Plans by coordinating with HHQ Marine Forces (MARFORs) and Marine Corps Intelligence Activity (MCIA) to identify and validate intelligence requirements associated with Operations Plan (OPLAN), CONPLAN, and Top Secret (TS) Clearance responsibilities; and publishes a weekly report providing regionally focused estimative assessments, conducts temporal analyses, coordinates intelligence preparation of the battle space (IPB) support, and manages standing collection and production requirements, and intelligence training and readiness evaluations. Commandant of the Marine Corps, I Marine Expeditionary Force Order P5000.3, June 6, 2011.

[89]Headquarters U.S. Marine Corps, *Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise (MCISR-E)*, 2014, Marine Corps Concepts and Programs, https://marinecorpsconceptsandprograms.com/programs/intelligence-surveillance-and-reconnaissance/marine-corps-intelligence-surveillance-and.

[90]Interview with a I MEF staff officer, November 16, 2014.

[91]Ibid.

[92]Based on firsthand experience while serving as the 1st Intelligence Battalion Operations Officer in Helmand Province, Afghanistan from November 2011 – June 2012. Many infantry battalion commands cited initial concerns with the latency in collection, analysis, and production. However, streamlining the dissemination process through lateral, higher, and subordinate level product distribution ensured commanders received timely and accurate information for operational planning. Additionally, the MEB Intelligence Operations Center augmented infantry battalions with intelligence liaisons, collectors, and equipment to support their operations. This process created great symbiosis and ensured theater wide understanding of enemy activities, plans, and tactics, which led an increase in enemy targeting and friendly force protection.

[93]Ibid.

[94]Ibid.

[95]Ibid.

[96]Ibid.

[97]Headquarters U.S. Marine Corps, *Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise (MCISR-E),* 2014, Marine Corps Concepts and Programs, https://marinecorpsconceptsandprograms.com/programs/intelligence-surveillance-and-reconnaissance/marine-corps-intelligence-surveillance-and.

[98]U.S. Department of Defense, *Joint Operations,* JP 3-0 (Washington, DC: Department of Defense, September 10, 2001), I-5 – I-12.

[99]Headquarters U.S. Marine Corps, *Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise (MCISR-E),* 2014, Marine Corps Concepts and Programs, https://marinecorpsconceptsandprograms.com/programs/intelligence-surveillance-and-reconnaissance/marine-corps-intelligence-surveillance-and.

[100]Headquarters U.S. Marine Corps, *Intelligence Department,* Mission Statement. http://www.hqmc.marines.mil/intelligence/UnitHome.aspx.

[101]Headquarters U.S. Marine Corps, Intelligence Operations, MCWP 2-1 (Washington, D.C.: U.S. Marine Corps, September 10, 2003), 3-1.

[102]Ibid. 1-8.

[103]U.S. Department of Defense, *Joint Operations,* JP 3-0 (Washington, DC: Department of Defense, September 10, 2001).

Bibliography

[1]Army Logistician: Professional Bulletin of United States Army Logistics. *COCOM, ADCON, OPCON, TACON, Do You Know the Difference?* Volume 39, Issue 6. Washington D: Army Logistics, 2007. http://www.almc.army.mil/alog/issues/NovDec07/cmmd_relat_difference.html.

[2]Baldwin, Fletcher N. Jr. and Robert B. Shaw. "Down to the Wire: Assessing the Constitutionality of the National Security Agency's Warrantless Wiretapping Program: Exit the Rule of Law." *University of Florida Law Scholarship Repository*, 2006.

[3]Bargman, Steven M. "The Utility of Hyperspectral Data in Detecting and Discriminating Actual and Decoy Target Vehicles." Master's thesis, U.S. Naval Postgraduate School, 1996.

[4]Best, Richard A. Jr, *Intelligence Information: Need to Know vs. Need to Share*. CRS Report for Congress R41848. Washington, DC: Congressional Research Service, June 6, 2011.

[5]Clausewitz, Carl von. *On War*. Edited by Michael Howard and Peter Paret, Translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1984.

[6]Commandant of the Marine Corps. I Marine Expeditionary Force Order P5000.3. June 6, 2011.

[7]Dalberg-Acton, Lord John. Letter Received by Mandell Creighton Hanover College Department, April 5, 1887.

[8]Fair, C. Christine. *Fighting to the End: The Pakistan Army's Way of War*. Oxford: Oxford University Press, 2014.

[9]Headquarters U.S. Army. *Military Operations in Low Intensity Conflict*. FM 100-20. Washington, DC: U.S. Army, 5 December, 1990.

[10]Headquarters U.S. Marine Corps. *Marine Corps Operations*. MCDP 1-0. Washington DC: U.S. Marine Corps, August 9, 2011.

[11]Headquarters U.S. Marine Corps. *Strategy*. MCDP 1-1. Washington DC: U.S. Marine Corps, November 12, 1997.

[12]Headquarters U.S. Marine Corps. *Intelligence*. MCDP 2. Washington DC: U.S. Marine Corps, June 7, 1997.

[13]Headquarters U.S. Marine Corps. *MAGTF Intelligence Collection*. MCDP 2-2. Washington DC: U.S. Marine Corps, July 30, 2004.

[14]Headquarters U.S. Marine Corps. *Command and Control*. MCDP 6. Washington, DC: U.S. Marine Corps, October 4, 1996.

[15]Headquarters U.S. Marine Corps. *Intelligence Operations*. MCWP 2-1. Washington, DC: U.S. Marine Corps, September 10, 2003.

[16]Headquarters U.S. Marine Corps. *Counterintelligence*. MCWP 2-6. Washington, DC: U.S. Marine Corps, July 13, 2004.

[17]Headquarters U.S. Marine Corps. *Marine Corps Planning Process*. MCWP 5-1. Washington, DC: U.S. Marine Corps, August 24, 2010.

[18]Headquarters U.S. Marine Corps. *Joint Force Land Component Commander Handbook*. MCWP 3-40.7. Washington, DC: U.S. Marine Corps, June 8, 2012.

[19]Headquarters U.S. Marine Corps. *Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise (MCISR-E),* Washington, DC: Marine Corps Concepts and Programs, 2014. https://marinecorpsconceptsandprograms.com/programs/intelligence-surveillance-and-reconnaissance/marine-corps-intelligence-surveillance-and.

[20]Headquarters U.S. Marine Corps. *Marine Corps Intelligence, Surveillance, & Reconnaissance Plan.* Washington DC: Marine Corps, May 5, 2010.

[21]Headquarters U.S. Marine Corps. *MOS 0651 Cyber Network Operator.* Marine Corps Credentialing Opportunities On-line. Accessed 19 February, 2015. https://www.cool.navy.mil/usmc/enlisted/0651.htm.

[22]Headquarters U.S. Marine Corps. *Operational Terms and Graphics*. FM 101-5-1. Washington, DC: U.S. Marine Corps, December 30, 1997.

[23]Headquarters, U.S. Marine Corps Intelligence Department. "Intelligence, Surveillance, & Reconnaissance Enterprise Plan." Washington DC: 2015.

[24]Lear, Thomas E. "Marine Corps Intelligence For War As It Really Is." Master's thesis, Naval Postgraduate School, 1991.

[25]Lewis, Neil A. "THREATS AND RESPONSES: INTELLIGENCE SHARING; Rule Created Legal 'Wall' To Sharing Information," *nytimes.com*, April 14, 2004. http://www.nytimes.com/2004/04/14/us/threats-responses-intelligence-sharing-rule-created-legal-wall-sharing.html.

[26]Logan, Cedric Logan. "The FISA Wall and Federal Investigations." New York University Journal of Law & Liberty, 2009.

[27]Mascaro, Lisa. "Patriot Act provisions extended just in time." *latimes.com*, May 27, 2011. http://articles.latimes.com/2011/may/27/nation/la-na-patriot-act-20110527.

[28]Peters, Gerhard and John T. Woolley. "George W. Bush: "Statement on Signing the Intelligence Reform and Terrorism Prevention Act of 2004." *The American Presidency Project*, December 17, 2004.

[29]Philips, Shannon, and Adam Clemons. "The Fitness Report System for Marine Officers: Prior Research." *Center for Analysis and Solution*, November 2011.

[30]Solove, Daniel J. *Nothing to Hide: The False Tradeoff Between Privacy and Security*. Hartford: Yale University Press, 2011.

[31]Sturgill, Claude C. *Low-Intensity Conflict in American History.* Portsmouth: Preager, 1993.

[32]U.S. Congress. House. *Goldwater-Nichols Department of Defense Reorganization Act of 1986*. HR 3622. 99th Cong., Congressional Record 131, no. 132, daily ed. (1 October 1986).

[33]U.S. Congress. Senate. Congressional Record. 108th Cong., 2004. Committee Print 20389-20400.

[34]U.S. Department of Defense. *Doctrine for the Armed Forces of the United States.* JP 1. Washington, DC: U.S. Department of Defense, October 22, 2013.

[35]U.S. Department of Defense. *Joint Intelligence.* JP 2-0. Washington, DC: U.S. Department of Defense, October 22, 2013.

[36]U.S. Department of Defense. *Joint Operations.* JP 3-0. Washington, DC: U.S. Department of Defense, September 10, 2001.

[37]U.S. Department of Defense. *Military Intelligence Handbook*. Volume 1. Washington DC: U.S. Department of Defense, 2009.

[38]U.S. Federal Bureau of Investigation. *Testimony by FBI Director Robert S. Mueller and U.S. Attorney General Alberto R. Gonzalez to the Select Committee on Intelligence United States Senate*, Washington D.C: April 27, 2005.

[39]U.S. Government Accountability Office. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States (Authorized Edition)*, New York: W.W. Norton.

[40]U.S. House of Representatives. "Counterterrorism Intelligence Capabilities and Performance Prior to 9-11." Washington, DC: Subcommittee on Terrorism and Homeland Security. July 2002.

[41]U.S. Office of the Inspector General. "A Review of the FBI's Handling of Intelligence Information Prior to the September 11 Attacks." Ch 2, November 2004. http://www.justice.gov/oig/special/0506/chapter2.htm.

[42]Van Der Bijl, Nick. *Sharing the Secret: The History of the Intelligence Corps 1940-2010*. SouthYorkshire: CPI Group, 2013.

[43]Weir, William. Guerrilla Warfare: Irregular Warfare in the Twentieth Century. Mechanicsburg: Stackpole Books, 2008.

[44]Wheatley, Margaret J. *Finding Our Way: Leadership for an Uncertain Time*. San Francisco: Barret-Kohler, 2005.

[45]White Paper. "The Need to Know: The U.S. Intelligence Community and Law Enforcement." *Armed Forces Communications and Electronic Association*, April 2007.
Wintle, Justin ed, *New Makers of Modern Culture: Volume I, A-K.* New York: Routledge, 2007.