REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
05/15/2019

2. REPORT TYPE
Master's of Military Studies

3. DATES COVERED *(From - To)*
SEP 2018 - APR 2019

4. TITLE AND SUBTITLE
Biometrics: A Case Study into how Commanders can Influence Biometrics in a Counterinsurgency Environment

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Porter, Eugene J., MI, 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)

10. SPONSOR/MONITOR'S ACRONYM(S)
Dr. Jonathan Phillips

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

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The Marine Corps must not lose sight of the lessons learned as it shifts focus to a near-peer competitor conflict. Biometrics, a reasonably new technology, emerged as a force multiplier during offensive combat operations in Iraq and Afghanistan. In 2010, when I Marine Expeditionary Force (Forward) deployed to Afghanistan and was re-classified as Regional Command Southwest (RC-SW), biometrics collections became a priority for Commanders at every level. This thesis analyzes the role RC (SW) played in implementing this policy including the challenges and successes it experienced.

15. SUBJECT TERMS
Biometrics, Biometric Automated Toolset (BAT), Handheld Interagency Identity Detection Equipment (HIIDE), Biometric Enrollment and Screening Device (SEEK II), Counterinsurgency

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			USMC Command and Staff College
					19b. TELEPHONE NUMBER *(Include area code)*
Unclass	Unclass	Unclass	UU	42	(703) 784-3330 (Admin Office)

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

TITLE:
Biometrics: A Case Study into how Commanders can Influence Biometrics in a Counterinsurgency Environment

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

AUTHOR:
Major Eugene J. Porter

AY 2018-19

Mentor and Oral Defense Committee Member: Jonathan F. Phillips, Ph.D.
Approved: ______________
Date: 9 May 2019

Oral Defense Committee Member: Mark D. Howard, LtCol
Approved: MDHoward
Date: 15 MAY 2019

Executive Summary

Title: Biometrics: A Case Study into how Commander can Influence Biometrics in a Counterinsurgency Environment

Author: Major Eugene J. Porter, United States Marine Corps

Thesis: This paper will examine the Marine Corps use of biometrics in Iraq and Afghanistan and analyze how, when adequately integrated into combat operations and intelligence cycle, it can serve as a force multiplier for Commanders at any level when operating in a counterinsurgency.

Discussion: The Marine Corps must not lose sight of the lessons learned as it shifts focus to a near-peer competitor conflict. Biometrics, a reasonably new technology, emerged as a force multiplier during offensive combat operations in Iraq and Afghanistan. In 2010, when I Marine Expeditionary Force (Forward) deployed to Afghanistan and was re-classified as Regional Command Southwest (RC-SW), biometrics collections became a priority for Commanders at every level. During this time, the improvised explosive device employed by insurgents was the number one threat to US and Coalition Forces. General Stanley McChrystal, Commander, International Security, and Assistance Force, placed a renewed focus on the prioritization and integration of biometrics collection across a range of military operations. This thesis analyzes the role RC (SW) played in implementing this policy including the challenges and successes it experienced.

Conclusion: As the DOD and Marine Corps begin shifting focus and priorities, the lesson learned from RC (SW), and the intergradation of biometrics into combat operations must not be lost. The commander must prioritize the use of biometrics collection throughout his command to ensure the benefits of its use will a significant impact on the operational and strategic level. Commanders can prioritize biometrics collections through increased training employing the equipment, unity of effort across the staff to include non-organic enablers, and an improved understanding of the long-term impact with biometrics collection.

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 OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

QUOTATION FROM, ABSTRACTION FROM, OR REPRODUCTION OF ALL OR ANY PART OF THIS DOCUMENT IS PERMITTED PROVIDED PROPER ACKNOWLEDGEMENT IS MADE.

Table of Contents

Page

Preface

I decided to research this topic as a result of my experiences in Afghanistan (2010-2011), while a member of the Counter-Improvised Explosive Device Cell, G-3, Regional Command Southwest in Helmand Province. During this deployment, I served as the biometrics Officer-in-Charge for RC-SW.

I want to thank Dean of Academics, Dr. Jonathan Phillips and Military Faculty Advisor, Lieutenant Colonel Mark D. Howard for their mentorship throughout this the entire process. The constructive encouragement provided by these two gentlemen enabled me to focus my research methods. I would be remiss if I did not also thank my family for their assistance over the last few months.

"Biometrics is a critical mission enabler that shall be fully integrated into the conduct of DoD activities to support the full range of military operations."[1]

INTRODUCTION

For almost 20 years the United States (US) military has been involved in combat operations in Iraq and Afghanistan. As conflicts in those two countries begin to draw to an end, the nation and the Marine Corps are shifting its focus and priorities to great powers competition. As this shift occurs, the Marine Corps must not lose sight of the lessons learned during these conflicts specifically those related to technological gains. Biometrics emerged as a technological innovation in response to urgent operational requirements from units operating in this environment.[2] Biometrics technology emerged as a critical enabler for US and Coalition Forces (that national caveats permitted their use) to isolate the local populace from the insurgents. Biometrics collection and verification can be employed across the full range of military operations, both defensively and offensively, and in rural and urban environments. Biometrics employment in itself is very dependent on the collection of biometrics whether it be from an individual or evidence recovered from the battlefield. Although it is beyond the scope of this paper, Marine Corps success achieved through biometric collections has a place in future operations involving a near-peer competitor.

This paper will examine the Marine Corps use of biometrics in Iraq and Afghanistan, and analyze how, when adequately integrated into combat operations and the intelligence cycle, it can serve as a force multiplier for Commanders at any level when operating in a counterinsurgency. Biometrics collections can be integrated along the following lines of operations when operating in counterinsurgency to limit or deter the enemy IED threat: defeating the device, attacking the network, and training the force. The Commander is the key influencer and determines the proper prioritization of biometrics collection, employment, and exploitation.[3] Biometrics has a direct relationship to combat operations and intelligence. This paper is divided into the following sections: counterinsurgency theorist, US strategy, counterinsurgency, training and equipment, improvised explosive device, identity dominance, and doctrine.

In section one, this paper will define what biometrics is. In section two, this paper looks at how biometrics was employed, available equipment, and the pre-deployment and in-country training provided to Marine Corps units. In section three, this paper will review the strategy for operating in counterinsurgency to establish the foundation of why biometrics collection is essential. In section four, this paper will look at the IED and threat is poised to US and Coalition Forces. In section five, this paper looks at how the use of biometrics and non-organic enablers assigned to the Marine Corps assisted in achieving identity dominance. In section six, looks at the doctrine or lack thereof that was available at that time. Finally, this paper looks at three unique challenges that US and Marine Corps could face as technology and laws conferencing biometrics evolve.

BACKGROUND

Following the September 11, 2001, terrorist attacks then President George W. Bush laid down his mission objectives to the nation in a joint session to Congress on October 7, 2001, in which he stated, “Destroying camps and disrupting communications, we will make it more difficult for the terror network to train recruits and coordinate their evil plans.”[4] In the following years, US and Coalition Forces have been embroiled with conflicts in Iraq and Afghanistan and have faced different tactics and threats from both terrorist and insurgent forces. The employment of the improvised explosive device (IED) was one of those threats. The terrorists and insurgents used the IED as the weapon of choice to disrupt operations and create distrust among the local populace and its government.[5] These asymmetric warfare tactics have resulted in thousands of casualties and deaths of US and Coalition Forces and have cost the US an estimated $5.6 trillion.[6]

Asymmetric warfare is defined as, "something done to military forces to undermine their conventional military strength."[7] In the context of Iraq and Afghanistan operating environment, terrorist and insurgents blended in with the local populace because they were unable to compete militarily. In December 2004, the Defense Science Board released its Summer Study on *Transition to and from Hostilities* to then-Secretary of Defense Donald Rumsfeld. The report stated, "a coherent approach is required in order to develop identification, tagging, tracking, and locating (ID/TTL) capabilities that will give U.S. military forces the same advantage finding targets in asymmetric warfare that it has in conventional warfare."[8] An example of this occurred in Iraq following the battle of Fallujah. In 2004, the Marine Corps effectively used iris identification to control insurgent access and movement following the battle for the city of Fallujah, Iraq.[9] The use of biometrics enabled US forces to isolate the local populace in Fallujah from terrorists and insurgents. The Marine Corps was further able to isolate the local populace through the issuance of an identification card to those individuals that were biometrically enrolled.[10]

BIOMETRICS PROCESS

By 2010, the biometric process consisted of five distinct processes which included: collect, process, analyze, decide, and act.[11] As such, the Multi-Service Tactics, Techniques, and Procedures for Biometrics views this methodology as, "critical to achieving biometrics success and contributes to identity intelligence."[12] The biometric process is defined as, "the process of collecting, matching, storing, analyzing, and sharing biometrics identifiers and associated information of an individual.[13] The Department of Defense (DOD) used biometrics collections as a force protection measure at detention facilities and to screen third-country nationals working aboard forward operating bases.[14] The process step occurs when biometric data is uploaded and transmitted to the authoritative database following collection, which is located in West Virginia. The second process analyze, involves competent authority matching that biometric enrollment to something already in the authoritative database to confirm a match. The third process provides the "so what" for Commanders, which could be as simple as the person had been previously biometrically enrolled or that the person should be detained. The fourth process is to decide, and the Commander must decide on either target that person if they believe he or she is still in their area of operation. This process involves the entire staff providing inputs to ensuring there is a common understanding across the whole of staff. Finally, the last process is to act, and the Commander guides the staff on the course of action taken towards this individual.

Biometrics collections within the DOD involve what is known as a 10-2-1 process, which was also ISAF baseline enrollment standard meaning the collections of ten rolled fingerprints, two iris scan, and one facial photograph as well as biographical contextual data.[15] The ten rolled fingerprints is a physical biometric characteristic, which includes fingerprint data from nail to nail.[16] Fingerprinting is the same process undertaken by local police and federal law enforcement personnel with the only difference that the fingerprints are stored in a biometric device. Iris scan in another way to determine who a person is and due to the difficulties involving with changing the physical characteristic of an iris, it is very reliable for identity confirmation.[17] A full facial photo can be used to produce identification cards, be on lookout reports, and another way to confirm identity. Finally, contextual data (if filled out correctly) provides the five Ws: who, what, when, where, and why behind why that enrollment was collected, along with additional information they deem significant into the contextual data.[18]

BIOMETRIC COLLECTION, EQUIPMENT, AND TRAINING

The average time to complete a biometric enrollment is 20 minutes.[19] The experience and confidence of the person conducting the enrollment can either decrease or increase this time. The collections of biometrics are technology-based and are affected by geography, climate conditions, and ethnic population.[20] The climate condition plays a significant role in the time needed for completing an enrollment since enrollments are not always collected inside buildings. In not ideal conditions biometric enrollments could take up to 30 minutes. The individual, operating environment, and biometric system are all factors, and that must be considered when analyzing collection times. The biometric system, user, or enrollee are factors in the completion time.

A biometric system is defined as an automated tool for collecting, measuring, evaluating, transmitting, storing, and analyzing physical or behavioral characteristics or traits for recognition.[21] Throughout the conflicts in Iraq and Afghanistan, Marine Corps units had access to two of the three different types of biometric collection system. The three systems were: biometric automated toolset (BAT), handheld interagency identity detection equipment (HIIDE), and biometric enrollment and screening device (SEEK II).[22]

Within the Department of Defense (DOD) the Army was the first military service to receive and field test the equipment.[23] As the program manager for DOD, the Army is the senior executive agent for all things biometric.[24] The BAT system is the bulkiest of the three systems and was first employed by the Marine Corps in 2003.[25] The BAT is a multimodal biometric system that collects, stores, and shares fingerprints, iris images, and facial photography.[26]

The size and need for a constant power source make the BAT most effective when employed at long-term stationary locations such as entry control points and detention facilities. In "perfect" environmental conditions enrollment of a single individual into the BAT system can take an average of 20 minutes. The BAT system was operationalized in Iraq and used as a force protection measure for base access and detention operation. Eventually, the BAT system was utilized for the enrollment of all Iraqi Security Forces (ISF). This process ensured that all ISF personnel was screened and vetted before working with the Minister of Interior, US, and Coalition Forces.[27]

The second system used for the collection of biometric data was the HIIDE. The HIIDE is a handheld device that weighs approximately 2 pounds and is more mobile than the BAT.[28] It collects and matches fingerprints, iris images, facial photographs, and biographical contextual data of persons of interest against an internally downloaded current biometric database.[29] HIIDE collects and stores multimodal biometric data of personnel encountered during tactical operations and creates tracking reports of biometric encounters for later intelligence analysis.[30]

The last biometric collection device is the SEEK II. It has similar capabilities as the BAT, but the similar physical dimension of the HIIDE. Special Operations Command was the primary users of the SEEK II. The SEEK II is a comprehensive, multimodal identification and enrollment platform that provided forensic-quality fingerprint capture, rapid dual iris scan capability and innovative facial capture technology.[31] The compact, portable solution is designed for rugged field use, making it quick and easy for military, border control, and other U.S. government agencies to identify subjects and verify their identities in the field.[32]

The BAT, HIDDE, and SEEK II were not programs of record for the Marine Corps. These systems were not on hand in a company office, supply unit, or in a logistic section and this prevented Marines from checking out equipment for training. Deploying units had to wait until they were conducting their pre-deployment training to get access to the devices or had the opportunity for a mobile training team to visit their duty station. With the limited number of devices available stateside, individual training was often limited to three to five individuals per platoon instead of the entire platoon. Generalized training was conducted in large group settings and once completed those three to five Marines would receive additional training. To limit the impact of the lack of stateside devices for training the Marine Corps employed civilian contractors as a biometric system administrator (BSA).

The employment of civilian contractors to serve as subject matter experts was a "workaround" to a lack of stateside training provided to deploying units. BSA served as the subject matter expert for the biometrics equipment specifically the BAT and HIDDE devices and was embedded with the battalion, regiment, and MEF levels.[33] Additionally, they provided the first echelon repair for all equipment. Embedded with the battalion S-2, the BSA could travel around the battle space and provide sustainment training and recommendations for system employment to the Commander and his or her staff. Finally, the BSA served as continuity from command to command as units rotated in and out of an area of operations.

Biometric enrollment is complete within the database, once the contextual data and "10, 2, 1" are on an enrollment device. The biometric data must then be transmitted back to the authoritative database. The authoritative database for the storage of biometric data Automated Biometric Identification System (ABIS) and is a subsystem of the Integrated Automated Fingerprint Identification System (IAFIS) located in Clarksburg, WV.[34] The BAT device enrollments can be transmitted directly to ABIS once complete. HIDDE enrollments must be transferred from the HIIDE to BAT device before it can be transmitted to ABIS.[35] The processing time for a file transfer varied greatly from three to four days and as worst as seven to ten days based on the data transfer that following on the network. The BSA played a significant role in ensuring that file transfer was complete. In contrast, the SOCOM architecture provided them the capability to submit and receive notifications within minutes compared to the days it took conventional forces.[36] The biometric file was transferred on the unclassified network, and in Afghanistan, the unclassified network bandwidth was a premium.[37] Thus, most files transfer occurred at night.

The biometric-enabled watchlist (BEWL) is created after the biometrics file was received at ABIS and analyzed by an intelligence professional. The BEWL commonly referred to as "the watch list," is a collection of individuals whose biometrics have been collected and determined by biometrics enabled intelligence analysts to be threats, potential threats, or who merit tracking.[38] A BEWL identifies a person within the database either through the collection of their 10-2-1 profile or through the exploitation of materials and evidence from the battlefield. The BEWL divides into the five-tier categories that included, level 1 (detain), level 2 (question), level 3 (assess), level 4 (disqualify), level 5 (deny).[39] The BEWL contained an additional category named level 6 (track) that was not an actionable level.[40]

US COUNTERINSURGENCY STRATEGY

Biometrics collections served as a force multiplier when its prioritized and integrated into the counterinsurgency strategy. In 2009, following the election of President Barrack Obama and his selection of General Stanley McChrystal as the Commander, International Security and Assistance Force (ISAF) and later General David Petraeus a Counterinsurgency (COIN) strategy was employed in Afghanistan. After being appointed the Commander, ISAF Gen McChrystal took approximately 60 days provided to him by the Secretary of Defense Robert Gates to tour

Afghanistan and obtain a first-hand assessment of the current situation on the ground. Following his appointment and confirmation by the US Senate, General McChrystal instituted his strategy of shape, clear, hold, and build: shape the environment through intelligence and information operations, clear areas affected by insurgent presence, hold the areas cleared to ensure that insurgents will not reassert their authority, and build national and local institutions that improve living standards.[41] The US and Coalition Forces prioritized the identification of Afghanistan civilians to solidify the strong relationship built with the civil affairs team missions.[42]

With a counterinsurgency, the credibility of the government is one of the critical pillars along with economic, military and civic actions that the local populace must have confidence.[43] Afghanistan, unlike Iraq, had no real system in place that enabled the US and Coalition Forces to identify the population. There was no modern form of documentation that the populace could show that prove they were, in fact, an Afghanistan citizen such as a formal birth certificate or citizen registration card. Around the same timeframe of Gen McChrystal assuming control as Commander, ISAF, U.S. Central Command (USCENTCOM), established the Combined Joint Interagency Task Force-435 (CJIATF-435) in Afghanistan to oversee biometric-enabled intelligence (BEI) actions and facilitate the integration of biometrics in mission planning and execution.[44] CJIATF-435 was also the lead agency for all detainee operations. A subset of CJIATF-435 was known as Task Force Biometrics, which had the lead for biometrics operations in Afghanistan for US and Coalition Forces. Additionally, Task Force Biometrics brought additional capabilities that were not organic to Marines Corps units operating in Regional Command Southwest (RC-SW).

Following the resignation of Gen McChrystal, President Obama nominated Gen Petraeus to be the next Commander, ISAF. General Petraeus had previously served as the Commander, USCENTCOM in Tampa, Florida, and had experience and knowledge of the threat facing US and Coalition Forces. General Petraeus had gained notoriety from outside of the military while he was overseeing the Iraq surge while serving as the Commander, Multi-National Force–Iraq under President Bush in 2007. The operational use of biometrics expanded rapidly as toward a population central counterinsurgency strategy in Iraq and was a critical tool during the "surge" period as one of the primary means of separating insurgents from the larger population.[45] In December 2006, Petraeus co-author *Field Manual 3-24, Counterinsurgency*.[46] FM 3-24 was heavily influenced by the writings of David Galula as noted by one of the co-authors who stated, "Galula laid down a general principle that is recognized as the core of a successful counterinsurgency strategy: "The population becomes the objective for the counterinsurgent as it was for his enemy."[47]

David Galula and his fellow Frenchman Roger Trinquier are two of the 21st-century leading counterinsurgency theorists. They were both highly distinguished military officers in the French Army and possessed immense combat experiences from the Algerian War.

In 1960, David Galula wrote, *Counterinsurgency Warfare* based on the strategy of fighting in a counterinsurgency.[48] He identified how the grassroots nature of an insurgency makes it challenging to defeat. Galula stated that a counterinsurgent force would struggle to keep an area clean so that they are free to operate elsewhere.[49] The counterinsurgent force must have a plan to isolate the insurgent from the local populace to ensure they can keep the area secure without leveraging a lot of additional resources in the area. In contrast to Galula, in 1964, Roger Trinquier wrote *Modern Warfare: A French View of Counterinsurgency*.[50] Trinquier argued that the number one priority of both the insurgent and counterinsurgent should be control of the population by stating, "Control of the masses through a tight organization, often through several parallel organizations, is the master weapon of modern warfare."[51] Trinquier recommended the implementation of a census program in which the local populace would be issued a photo identification card once vetted.[52] The photograph identification card ensured that the counterinsurgent force could quickly identify the enemy and also isolate them from the local populace.

Meanwhile, insurgent activity in Afghanistan was the highest it has ever been and in 2010 US and Coalition Forces took more causalities in 2010, than in any other year of the war.[53] Insurgent was employing a strategy that included interrupting road access, capturing territory, and economic sabotage. This focus on alienating the local populace from the government was very successful, and in some areas, insurgents were also killing government officials in those areas to create an environment of fear.[54]

The number of US and Coalition Forces causalities were at a record high compared to other years, and Commanders placed a renewed focus on biometric collections: to include operations, employment, and best practices throughout Afghanistan.[55] Commanders at all levels were required to ensure that a biometrics collection plan was included in all combat operations. Specifically, in 2010 Regional Command Southwest (RC-SW) released a fragmentary order that made the mandatory planning and use of biometric collections in all combat operations.[56] Major General Richard Mills, Commander, RC-SW approved this order, which was the first of its kind for Marine Corps units. The battlespace owners, which included the 1st Marine Division, Marine Logistic Group, and MEF Headquarters Group (now, MEF Information Group), were the units that facilitated collections.

Within the RC-SW construct, the Marine Corps struggled with the organizational placement of the Biometrics program. Initially, the MEF G-2 had oversight of the biometrics program. However, in 2010 a shift was made to place oversight of all biometrics operations to the G-3, Counter-Improvised Explosive Device Cell. The leadership with the MEF determine that C-IED cell was much better suited to integrate all capabilities of biometrics along with the additional enablers that C-IED already possessed. This decision aligned RC-SW biometrics programs with other RC within Afghanistan.

INSURGENT WEAPON OF CHOICE - IMPROVISED EXPLOSIVE DEVICE

In the Global War on Terrorism, Iraq was the first theater of operations that insurgents deployed the IED against US and Coalition Forces. First employed in 2004, the insurgents used the improvised weapons to exploit gaps in military tactics, techniques, and procedures. From the use of homemade explosives, artillery, or pressure plates they were more lethal than conventional weapons; and built at a fraction of the cost. Additionally, because of their improvised nature, the IED could be easily modified from its original form to cause even greater damage. The IED gained increased public perception about their lethality once recorded videos from insurgents were published online. Internet posting provided insurgents a platform to recruit additional personnel and provide a visual for all nations worldwide to discredit US and Coalition Forces.

By 2010, the IED was the number one contributor of US and Coalition Forces casualties.[57] The IED and how to counter the threat it posed to US forces was the main reason the Department of Defense created the Joint Improvised Explosive Device Organization (JIEDDO, currently known as Joint Improvised-Threat Defeat Organization). Created in 2004, JIEDDO was intended to serve as a joint solution for DOD and the central focal point of all DOD actions against the IED threat. The creation of JIEDDO brought a lot of additional capabilities to the strategic, operational, and tactical level. Units across the DOD started forming what was known as counter-improvised explosive device (C-IED) cells. The structure of the C-IED cells varied from unit to unit and service to service. The basic structure consisted of explosive ordnance platoon, force protection officer, targeting officer, and weapon tactics instructor. With the additional force structure and equipment, this provided Commanders with the capabilities to counter the IED threat with assets that were not organic to their table of organization and equipment.

> JIEDDO's actions and activities fall under three lines of operation: (1) "Defeat the Device," (2) "Attack the Network," and (3) "Train the Force." The primary focus of the Defeat the Device effort is on neutralizing the IED after it is emplaced. This includes funding the development of technical and non-technical countermeasures and the ability to rapidly field new equipment. Attack the Network activities aim to find and eliminate bomb makers and their supporters before they can assemble and emplace IEDs.[58]

JIEDDO facilitated the purchasing of additional capabilities to Combatant Commanders typically not found in a military organization. For example, these additional enablers were in most cases assigned in direct support or general support to the Commander: Joint Expeditionary Team (JET), Combined Explosive Exploitation Cell (CEXC), Joint Expeditionary Forensic Facility (JEFF), and Law Enforcement Personnel (LEP).

IDENTITY DOMINANCE

Not only were US and Coalition Forces able to counter the IED threat, but through the use of biometrics collection, they were also able to achieve identity dominance over the insurgents. The US military must make maximum use of biometrics information and the technologies that collect, process, store, and search data, to achieve identity dominance. One capability that came with the biometric equipment was the ability to produce identification cards. In summer 2010, at the direction of President Hamid Karzai, all US and Coalition Forces were no longer allowed to issue biometric enrollment cards.[59] This decision also coincided with the push for a national identification card by President Karzai.[60] Before this, the government of Afghanistan had no identification card, and there was no formal record system within the country. Afghanistan citizens were not provided birth certificates or formal documentation upon birth.[61] The issuance of a national identification card is one way the government attempted to isolate the insurgent from the local populace further.

An additional way to isolate insurgents from the local populace is by linking the intelligence products with operations. As previously stated, the BEWL had to be downloaded from the server into the BAT system and then transferred into the HIIDE system. A limiting factor with the HIIDE was its storage capacity. The Commanders were forced to decide on the type of downloaded watchlist because of the limited storage capacity. The standard operating procedures for this varied from unit to unit, but it should be done at least three to four times a week. Additionally, as noted by 1stLt Agamir of RC (SW)'s C-6 Operations section, "...the downside of the HIIDE system... [is that] without the capability to communicate to the outside world, there is no ability to do first encounter matches."[62] US and Coalition Forces would have the most updated information for combat operations, which provided high levels of risks but one that otherwise could not be mitigated due to the device storage capacity.

From an operations perspective, it requires unity of effort by multiple different entities when materials are collected from the battlefield by the explosive ordnance device technician (EOD). An EOD technician plays a vital role in the collection of materials and evidence once they have rendered an area safe for exploitation. Rendering an area safe can occur pre-blast or post-blast and once complete must be transmitted back for further exploitation and analysis once their report is complete.

A weapons technical intelligence (WTI) is another enabler in the exploitation of material and evidence. WTI combined technical and forensic IED exploitation techniques to link persons, places, things, and events.[63] WTI enabled operations personnel to have better information when conducting planning. WTI outcomes are used to target insurgents, develop force protection measures, formulate counter-IED TTP, design countermeasures, provide indications and warnings of IED attacks, interdict supplies, and precursors, and support prosecution by the host nation.[64] A WTI is not an organic capability that is resident within the Marine Corps. In Afghanistan, the Marines Corps relied heavily upon contractors to fill this support role.

Finally, the Combined Explosives Exploitation Cell (CECX) is another non-organic Marine Corps capability. CECX provides expert-level technical and forensic exploitation and analysis of IEDs and associated components, improvised weapons, and other weapons systems in order to determine enemy tactics, identify IED trends, bomb makers, and assist in the development of defensive and offensive C-IED measures.[65] In Iraq and Afghanistan, the Navy provided augmented personnel to support these cells.

Biometrics collections were not only facilitated by the integration of JIEDDO enablers, but also by the employment across all three lanes of JIEDDO lines of operations for C-IED operations. While this was being accomplished, the overall recidivism rates (same person committing crimes across the country) within Afghanistan remained at reality low levels. Biometrics collections and detainee operations were integrated since the very beginning of combat operations. U.S. forces use biometrics to identify and classify possible recidivist-detainees. During an interview with the Pentagon press corps Vice Admiral Robert Harward, the detention operations chief, said, “as of January 2010, 3000 Afghans have been detained by U.S. forces in eight years, and the U.S. could document a total of 17 ex-detainees who had returned to the fight, less than half of one percent."[66] This is not to say that biometrics enrollment was the main reason for the low rate of recidivism; however; it cannot be discounted either.

Biometric collections do not have to be defensive to prevent recidivism. Biometrics collections can be offensive in terms of working closely with tribes and provincial leaders. Tribal and provincial leaders must be made aware of those persons that biometrically enrolled from their region and with the help of those leader targeted operations can be conducted if they are supporting individuals that are a direct threat to the US.

DOCTRINE

Biometrics collections used in offensive operations was a reasonably new concept that lacked the appropriate doctrine to guide the force. In a 2011 interview, Vice Admiral Robert S. Harward stated, "There is no formal doctrine; universally accepted tactics, techniques, and procedures; or institutionalized training programs across the Department of Defense. To help bridge that gap, the Center for Army Lessons Learned produced this handbook to help guide commanders' employment of biometric capabilities in Afghanistan."[67] The commander at all levels relied heavily on this and other documents to provide a baseline to build their situational awareness the appropriate employment and integration of biometrics. A lack of doctrine also made it difficult to build confidence in a commander on its effectiveness. Commanders understood the importance but if they were unable to see immediate results from enrollments or the exploitation of munitions and devices.

The lack of biometrics doctrine served as a limiting factor with a commanders ability to influence their operating areas by using the full potential. Biometrics operations can either be offensive or defensive. Defensive operations consist of personnel screening, base access, and checkpoint screening. Offensive operations that could be utilized to increase enrollments and population control consist of medical, dental, and cordon operations. Within RC-SW the use of the female engagement team that coordinated with civil affairs teams to conduct humanitarian symposiums was missed opportunities for collections. Also, medical civic assistance program and dental civic assistance programs were completed throughout the area of operations, and these would have been perfect opportunities if planned accordingly to conduct targeted based biometric enrollments. Also, the female engagement teams and civil affairs groups leading efforts mentioned above can be a force multiplier to commander's biometrics collection operations.

CHALLENGES

As the focus shifts towards near-peer competitors, it will be more important for senior military leaders or legal advisors to have some basic understanding of biometric collection laws. For example, in 2005, Pakistan instituted laws that require all citizens that purchase or own a cell phone must be enrolled in a national biometric database that maintains there iris scans, fingerprints (both hands), a photograph, and other contextual data.[68] Pakistan is a nation that has over 136 million cell phones users, which is a tremendous endeavor to undertake, but one that the national leadership felt was needed to deter and limit the use of terrorist activities. Biometrics enrollments do not only apply to the cellular industry but the banking industry as well for its citizens. The law also applies to the banking industry as well. If futures conflicts do involve near-peer competitors and they have laws similar to Pakistan that mandates biometric collection gaining access to that national database can lead to a range of military operations open to supporting lethal and non-lethal targeting.

Another challenge the Marine Corps will need to address is the bandwidth infrastructure for biometrics. In 2010, the biometric data was transferred over the network internet protocol.

The Marine Corps should procure a very small aperture terminal (VSAT) to every battle space owner for the specific use of biometrics. In an audit conducted by the GAO it stated, "Special Operations Command (SOCOM) employs a Very Small Aperture Terminal (VSAT) satellite system which enables them to connect directly with ABIS and send and receive biometrics data in approximately 22 minutes"; and "…match/no match responses are provided to the warfighter via the portal within two to seven minutes."[69] VSAT will facilitate the data transfer via a network internet protocol. Biometrics data files would flow through its own separate and distinct network, which would decrease the latency. The process flows decrease the time and space required for data to transfer from the ground unit to an authoritative database and vice versa.

Another challenge facing the US and Coalition Forces in future counterinsurgency conflict involves recidivism. The Afghan government approved the Afghanistan Peace and Reintegration Program in 2010, to "encourage Taliban fighters and leaders, previously sided with the armed opposition and extremist groups, to renounce violence and join a constructive process of reintegration to benefit from a chance at peace and sustained governance and economic development."[70] The integration of the rule of law with biometrics operations is required to account for those individuals who rejoin the insurgency. Additionally, biometrics technologies have offered one of the few effective means of tracking recidivism.[71] The 2013 National Defense Authorization Act established reporting requirements relating to recidivism by former detainees in Afghanistan. Specifically, it required a report to be filed within 120 days describing the "estimated recidivism rates and the factors that appear to contribute to the recidivism of individuals…who were transferred or released, including the estimated total number of individuals who have been recaptured on one or more occasion.[72] US forces should expect that future conflicts will require mandatory tracking of recidivism.

Finally, the Marine Corps faces challenges at the operational and tactical level. Currently, the Marine Corps distributes biometrics equipment issued to Law Enforcement Battalions (LE BN), Marine Information Group within the Continental United States. The equipment facilities LE BN defensive operations and their mission essential tasks of detainee operations, but that creates a gap when viewed through the lens of offensive operations. Biometric equipment that is procured by the Marine Corps should be issued to the infantry battalion and added to the table of equipment, which will mitigate a deficiency with CONUS based equipment shortages and training sustainability identified in the Biometrics Efforts in the Afghanistan report published by Marine Corps Center For Lessons Learned.

CONCLUSION

Combat operations in both Iraq and Afghanistan are coming to a close. As the DOD and Marine Corps begin shifting focus and priorities, the lesson learned from RC (SW), and the intergradation of biometrics into combat operations must not be lost. As history has shown, the Marine Corps may once again find itself fighting in a counterinsurgency. As technological advances continue the use of biometrics will need to remain at the forefront. The Marine Corps has already taken the initial step a settled on a biometric device to become a program of record. Biometrics has proven to be vital in separating the insurgent from the local populace through the use of iris scans or identification issuance. Identity dominance requires the proper integration of biometric-enabled intelligence with a command intelligence section, operation section, and additional enablers assigned to support the unit. Biometric-enabled intelligence integrated into the targeting cycle degrades the insurgent ability to hide among the local population.[73] However, most importantly the Commander must prioritize the use of biometrics collection throughout his command in order to ensure the benefits of its use will have an impact at the operational and strategic level. Commanders should prioritize biometrics collections through increased training employing the equipment. Commander can achieve unity of effort across the staff to include non-organic enablers and improved understanding of the long term impact with biometric collections. Finally, biometrics that can be exploited from the battlefield can facilitate other lethal and non-lethal operations for Commanders. Removing the ability of insurgents to operate in anonymity can help ensure the safety of the local populace.

Endnotes

[1] DoD Directive 8521.01E, approved October 15, 2018.

[2] The United States Marine Corps Biometrics Concept of Operations, Jun 7, 2018

[3] Commander's Guide to Biometrics in Afghanistan, Center for Army Lessons Learned (CALL), April 2011

[4] http://www.washingtonpost.com/wp-srv/nation/specials/attacked/transcripts/bushaddress_100801.htm?noredirect=on, assessed on January 5, 2019.

[5] FMI 3-07.22, Counterinsurgency Operations, October 2004, page D-2

[6] Neta C. Crawford, United States Budgetary Costs of Post----9/11 Wars Through FY2018, page 1

[7] Joint Strategy Review 1999, Washington, DC: The Joint Staff, 1999, p. 2

[8] Defense Science Board 2004 Summer Study on Transition to and from Hostilities, Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics, January 2005.

[9] Biometrics in Support of Identity Dominance, Newsletter NO 09-35, May 2009, 33

[10] Ibid 29

[11] Capstone Concept of Operations For DOD Biometrics in Support of Identity Superiority, approved November 2006, 5

[12] Biometrics, Multi-Service Tactics, Techniques, And Procedures for Tactical Employment of Biometrics in Support Of Operations, MCRP 3-33.1J, Aug 2014, 2

[13] Ibid 8

[14] United States Marine Corps Biometrics Concept Of Operations, June 7, 2018, page 23

[15] Biometrics Efforts in Afghanistan, Marine Corps Center for Lessons Learned, September 10, 2012, page 21

[16] Biometrics in Support of Identity Dominance, Newsletter NO 09-35, May 2009, 87

[17] Ibid 22

[18] Ibid 87

[19] Biometrics Efforts in Afghanistan, Marine Corps Center for Lessons Learned, September 10, 2012, page 21

[20] Paul C. Clark, Heather S. Gregg, Biometric Challenges for Future Deployments A Study of the Impact of Geography, Climate, Culture, and Social Conditions on the Effective Collection of Biometrics, Naval Postgraduate School, page i

[21] DOD Capstone Concept of Operations for Employing Biometrics in Military Operations approved 10 Jun 2012

[22] Biometrics Efforts in Afghanistan, Marine Corps Center for Lessons Learned, September 10, 2012, page 3

[23] Biometrics in Support of Identity Dominance, Newsletter NO 09-35, May 2009, 29

[24] Biometrics Efforts in Afghanistan, Marine Corps Center for Lessons Learned, September 10, 2012, page 10

[25] Ibid 13

[26] United States Marine Corps Biometrics Concept Of Operations, June 7, 2018, page A-6

[27] II MEF Biometrics Townhall Conference, Camp Lejeune, NC, April 2, 2008, page 2

[28] Technical Inquiry Use of Biometrics in Afghanistan and Iraq: The Sharing of Biometric Devices or Systems between NATO or ISAF, HDIAC, publication date unknown.

[29] Biometrics Efforts in Afghanistan, Marine Corps Center for Lessons Learned, September 10, 2012, page 13

[30] Ibid 13

[31] Ibid 3

[32] Ibid 15

[33] Ibid 4

[34] Ibid 9

[35] Ibid 15

[36] “Government Accountability Office Report to Congressional Requesters on Defense Biometrics,” April 2012, page 23

[37] Biometrics Efforts in Afghanistan, Marine Corps Center for Lessons Learned, September 10, 2012, page 19

[38] Commander's Guide to Biometrics in Afghanistan, Center for Army Lessons Learned (CALL), April 2011, page 8

[39] Biometrics Efforts in Afghanistan, Marine Corps Center for Lessons Learned, September 10, 2012, page 23

[40] Ibid 23

[41] Stanley McChrystal, “COMISAF Initial Assessment,” August 30, 2009, available at; Bill Gertz, “Inside the Ring,” The Washington Times, August 20, 2009.

[42] https://civiliansinconflict.org/press-releases/civilian-protection-prioritized-in-syria-iraq-operations/, accessed on May 1, 2019

[43] Counterinsurgency for U.S. Government Policy Makers, United States Government Interagency Counterinsurgency Iniative, Unite States Department of State, October 2007.

[44] Biometrics Efforts in Afghanistan, Marine Corps Center for Lessons Learned, September 10, 2012, page 3

[45] Voelz, Glenn J. Report. Strategic Studies Institute, US Army War College, 2015. http://www.jstor.org.lomc.idm.oclc.org/stable/resrep11804, page 28

[46] United States. Department of the Army. The U.S. Army/Marine Corps Counterinsurgency Field Manual : U.S. Army Field Manual No. 3-24 : Marine Corps Warfighting Publication No. 3-33.5. Chicago :University of Chicago Press, 2007. page i

[47] https://www.cnn.com/2012/11/10/opinion/bergen-petraeus-legacy/index.html

[48] Galula, David, Counterinsurgency warfare, Westport, CT: Praeger Security International, 2006, page i

[49] Ibid page 52

[50] Roger Trinquier, *Modern Warfare*, page i

[51] https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/Modern-Warfare.pdf. Page 30

[52] Roger Trinquier, *Modern Warfare*, page 60-63

[53] iCasualties: Operation Iraqi Freedom and Operation Enduring Freedom Casualties, http://icasualties.org/oef/ (accessed September 02, 2010).

[54] https://tnsr.org/2018/05/unbeatable-social-resources-military-adaptation-and-the-afghan-taliban/, accessed on April 30, 2019

[55] http://archive.boston.com/news/world/asia/articles/2010/07/31/us_casualties_in_afghanistan_reach_record_high, accessed on January 3, 2019.

[56] Captain Eugene J. Porter, served as the action officer for this FRAGO in 2010.

[57] https://fas.org/sgp/crs/natsec/R41084.pdf, accessed on January 3, 2019

[58] https://armedservices.house.gov/_cache/files/c/f/cfddccb2-fc15-4a3d-b7e3-50fe3ea68eca/D09F0BEF55D1B39D2CC196408918781D.jieddo-report-11-08-vf.pdf, accessed on January 3, 2019

[59] Presdent Karza forbid ISAFpersonnel from issuing biometric enrollment cards to Afghanistan citizens. He communicated this order to Commder, ISAF during a sync in 2010. Commander ISAF approved the release of a fragmentary order at codified this policy in writing. Major Eugene Porter

[60] https://www.reuters.com/article/us-afghanistan-identification-cards/afghanistan-plans-national-electronic-id-cards-idUSTRE6BB0P720101212, access on March 26, 2019.

[61] https://www.reuters.com/article/us-afghanistan-identification-cards/afghanistan-plans-national-electronic-id-cards-idUSTRE6BB0P720101212, accessed n March 26, 2019.

[62] Biometrics Efforts in Afghanistan, Marine Corps Center for Lessons Learned, September 10, 2012, page 14

[63] https://apps.dtic.mil/dtic/tr/fulltext/u2/a622235.pdf, accessed on January 3, 2019

[64] Ibid 125

[65] https://www.bits.de/NRANEU/others/jp-doctrine/JP3-15.1%2812%29.pdf, accessed on January 7, 2019

[66] Spencer Ackerman, U.S. Detentions Chief in Afghanistan Says Recidivism Is Very Low, Wash. Indep., (Jan. 27, 2010, 11:03 am), available at http://washingtonindependent.com/74901/u-s-detentions-chief-in-afghanistan-says-recidivism-is-very-low.

[67] Commander's Guide to Biometrics in Afghanistan, Center for Army Lessons Learned (CALL), April 2011

[68] https://www.washingtonpost.com/world/asia_pacific/pakistanis-face-a-deadline-surrender-fingerprints-or-give-up-cellphone/2015/02/23/de995a88b93211e4bc30a4e75503948a_story.html?noredirect=on&utm_term=.3b04c9ae4a57, accessed on April 22, 2019

[69] Government Accountability Office, Defense Biometrics Additional Training for Leaders and More Timely Transmission of Data Could Enhance the Use of Biometrics in Afghanistan, (Washington, DC: Government Accountability Office, 2012), page 21

[70] Memorandum from General Stanley McChrystal, Subject: Initial Guidance on Reintegration, R:\1800-FRIC\Initial Guidance, HQ ISAF/USFOR-A, October 25, 2009

[71] Voelz, Glenn J. Report. Strategic Studies Institute, US Army War College, 2015. http://www.jstor.org.lomc.idm.oclc.org/stable/resrep11804, page 31

[72] Section 1042 of the House-passed version would have required an assessment of “recidivism rates and the factors that cause or contribute to the recidivism of individuals formerly detained at the Detention Facility at Parwan, Afghanistan, who are transferred or released, with particular emphasis on individuals transferred or released in connection with reconciliation efforts or peace negotiations”; and “a general rationale of the Commander, International Security Assistance Force, as to why such individuals were released.”

[73] Voelz, Glenn J. Report. Strategic Studies Institute, US Army War College, 2015. http://www.jstor.org.lomc.idm.oclc.org/stable/resrep11804, page 30

Bibliography

Army Reveals Afghan Biometric ID Plan; Millions Scanned, Carded by May, 29 Sep 10, http://www.wired.com/2010/09/afghan-biometric-dragnet-could-snag-millions/ (accessed January 9, 2016).

Center for Army Lessons Learned (CALL). *Biometrics in Support of Identity Dominance,* Newsletter No 09-35, May 2009.

Center for Army Lessons Learned (CALL). *Commander's Guide to Biometrics in Afghanistan,* Newsletter No 11-25, April 2011.

Deputy Commandant, Combat Development and Integration (DC, CD&I). MCRP 3-33.1J, Publication, *Biometrics: Multi-Service Tactics, Techniques, and Procedures for Tactical Employment of Biometrics in Support of Operations,* April 1 2014.

Deputy Commandant, Combat Development and Integration (DC, CD&I). Marine Corps Warfighting Publication (MCWP) 3-33.5, Publication, *Insurgencies and Countering Insurgencies,* May 13, 2014.

United States Army**,** Capstone Concept of Operations for Employing Biometrics in Military Operations, June 10, 2012.

Hays, Major Michael G., Master of Military Studies Research Paper, *Regimental Combat Team One in Afghanistan: A Case Study into the Organization and Operation of a Tactical Level C-IED Cell,* April 26, 2012.

Headquarters, Supreme Allied Commander Transformation, Commanders' and Staff Handbook for Countering Improvised Explosive Devices, August 10, 2011.

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

Homeland Defense and Security Information Analysis Center. Technical Inquiry. *Use of Biometrics in Afghanistan and Iraq: The Sharing of Biometric Devices or Systems between NATO or ISAF*, July 31, 2015.

Integrated Automated Fingerprint Identification System, https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis, (accessed January 9, 2016).

Joint Strategy Review 1999, Washington, DC: The Joint Staff, 1999.

Marine Corps Center for Lessons Learned (MCCLL). *Biometric Efforts in Afghanistan,* September 2012

Marine Corps Center for Lessons Learned (MCCLL). Gunnery Sergeant Jason R. Hart, *Weapons*

Intelligence Team After Action Report for Counter IED Operations in Support of Regimental Combat Teams 2 And 8 from December 2010 To May 2011

Marine Corps Center for Lessons Learned (MCCLL). *Marine Expeditionary Brigade – Afghanistan (MEB-A) Operations: Summary of 2d MEB and MEB-A Observations from Planning and Operations in Support of International Security Assistance Force*, May 21, 2010

Marine Corps Interim Publication (MCIP) 3-17.02, *MAGTF Counter-Improvised Explosive Device Operations*, Washington, DC: Headquarters U.S. Marine Corps, January 24, 2011

Marine Corps Warfighting Laboratory (MCWL), *Counter – Improvised Explosive Device (C-IED) C-IED Smart Book*, February 2013

Regimental Combat Team 5, After Action Report for Operation Enduring Freedom 11.2-12.2, July 30, 2012

U.S. Department of Defense. *Joint Publication 3-15.1. Counter-Improvised Explosive Device Operations*, Washington, DC: Department of Defense, January 9, 2012

U.S. Department of Defense. *Joint Publication 3-0. Joint Operations*, Washington, DC: Department of Defense, February 13, 2008

U.S. Government Accountability Office. Defense Biometrics: Additional Training for Leaders and More Timely Transmission of Data Could Enhance the Use of Biometrics in Afghanistan. Washington, DC: Government Accountability Office, April 2012.

U.S. Government Accountability Office. Defense Biometrics: DoD Can Better Conform to Standards and Share Biometric Information with Federal. Washington, DC: Government Accountability Office, March 2011.

U.S. Government Accountability Office. Defense Management: DOD Needs to Establish Clear Goals and Objectives, Guidance, and a Designated Budget to Manage Its Biometrics Activities. Washington, DC: Government Accountability Office, September 2008

U.S. Joint Forces Command. Commander's Handbook for Attack the Network Joint Warfighting Center, Joint Doctrine Support Division. May 20, 2011

Vickers, Melana Z. *"Going on a Manhunt: Do We Have the Technology to Win?"* <http://cryptome.quintessenz.org/mirror/dsb101504.txt>, 15 October 2004, (accessed January 9, 2016).

Woodward Jr., John D. *Using Biometrics to Achieve Identity Dominance in the Global War on Terrorism, Military Review* September-October 2005