THE JOINT INTELLIGENCE CENTER:

AN EXPLORATORY STUDY OF MILITARY INTELLIGENCE OPERATIONS IN THE MODERN-DAY FIGHT AGAINST AN ASYMMETRIC THREAT

A Thesis

Presented to the

Faculty of the College of Graduate Studies and Research

Angelo State University

In Partial Fulfillment of the

Requirements for the Degree

MASTERS OF SECURITY STUDIES

by

HEATHER MARIE PORT

May 2019

Major: Intelligence, Security Studies, and Analysis

THE JOINT INTELLIGENCE CENTER:

AN EXPLORATORY STUDY OF MILITARY INTELLIGENCE OPERATIONS IN THE MODERN-DAY FIGHT AGAINST AN ASYMMETRIC THREAT

by

HEATHER MARIE PORT

APPROVED:

Dr. Eduardo V. Martinez

Dr. Jeffrey D. Dailey

Dr. Art La Flamme

Dr. Flor L. Madero

April 8, 2019

APPROVED:
Dr. Don R. Topliff
Provost, VPAA, and Interim Dean, College of Graduate Studies and Research

DEDICATION

To my greatest mentor throughout the entirety of my collegiate year, Dr. Han Lheem, many thanks for all of the hours of support and encouragement. Your assistance throughout my college career has been one of motivation and inspiration. I cannot thank you enough for pushing me through this process and always only being “an email away”.

I am also grateful to the remainder of the professors in the Political Science department at Fayetteville State University, especially Dr. Ngozi Kamalu and Dr. Kwame Baokye-Sarpong. You both have motivated me to do so much more with my education than where the “normal path” may take me.

A very special gratitude also goes out to Dr. Eduardo Martinez of Angelo State University for all of his assistance throughout my graduate journey. Your willingness to answer even the simplest of questions and lead me in the right direction has made the world of difference in this accomplishment.

I would also like to thank my husband, Tanner Port, who pushed me to re-engage my education when I had doubts in myself to do so. Your unwavering support and faith in me has meant more to me than I will ever be able to express.

A special mention to my parents- Jimmy and Teresa Amos- and the rest of my family. Your unfailing support and encouragement, as well as your willingness to grant me the time to succeed in my endeavors, has been a huge factor in my ability to complete this journey.

Last, but certainly not least, thank you to the remainder of the educators and staff at Angelo State University. You have only boosted my interest in a field that I already loved. Thank you for that. I cannot wait to see where the next step of my journey takes me.

Thank you for all of the support and encouragement!

ABSTRACT

Reformation efforts in all aspects of intelligence operations have taken place since the inception of the U.S. Intelligence Community yet have been largely based on conventional methods of warfare. This trend continues into the use of intelligence activities in military operations as joint intelligence doctrine and operations also focus on conventional threats rather than taking into account the asymmetric adversary that is commonly faced today. These circumstances, along with previous studies into the subject, have pinpointed the essential need to maximize U.S. national security resources and assets, especially those related to military intelligence operations.

Recent efforts have facilitated better integration and coordination in and among both the Intelligence Community and Military Intelligence entities through the process of reach back intelligence and the use of Joint Intelligence Centers; however, there are further actions to be commenced in the benefit of U.S. national security. This study will employ qualitative measures of exploratory analysis in order to identify areas of weakness in organizational structure and doctrine while advancing efforts of efficiency and success of Joint Intelligence Centers concerning the asymmetric threat.

TABLE OF CONTENTS **Page**

DEFINITIONS

ADMA-	Associate Director of Military Affairs
CCIR-	Commander's Critical Information Requirements
CENTCOM-	U.S. Central Command
CIA-	Central Intelligence Agency
COIC-	Counter-IED Operations Integration Center
COIN-	Counter-Insurgency
CRS-	Congressional Research Service
D3A-	Decide, Detect, Deliver, Assess
DCI-	Director of Central Intelligence
DHS-	Department of Homeland Security
DIA-	Defense Intelligence Agency
DNI-	Director of National Intelligence
DoD-	Department of Defense
DPICM-	Dual-Purpose Improved Conventional Munition
DST-	Defense Support Team
F3EAD-	Find, Fix, Finish, Exploit, Analyze, and Disseminate
IC-	Intelligence Community
IED-	Improvised Explosive Device
IRTPA-	Intelligence Reform and Terrorism Act of 2004
ISE-	Information Sharing Environment
ISR-	Intelligence, Surveillance, Reconnaissance
IT-	Information Technology

JCS- Joint Chiefs of Staff

JEIDDO- Joint Improvised Explosive Device Defeat Organization

JIC- Joint Intelligence Center

JICC- Joint Intelligence Community Council

JICPOA- Joint Intelligence Center Pacific Ocean Areas

JID- Joint Intelligence Division

JIOC- Joint Intelligence Operations Center

JWICS- Joint Worldwide Intelligence Communications System

MLRS- Multiple Rocket Launcher System

MOOTW- Military Operations Other Than War

MTOE- Modified Table of Organization and Equipment

NCPC- National Crime Prevention Council

NCTC- National Counterterrorism Center

NGO- Non-Government Organization

NIC- National Intelligence Council

NJOIC- National Joint Operations Intelligence Center

NSC- National Security Council

ODNI- Office of the Director of National Intelligence

OMA- Office of Military Affairs

PCLOB- Privacy and Civil Liberties Oversight Board

PIR- Priority Information Requirements

RSF- Request for Support

S-2- Battalion-Level Intelligence ‘Shop’

SECDEF- Secretary of Defense

SIGINT- Signals Intelligence

SIPRNET- Secret Internet Protocol Router Network

SME- Subject Matter Expert

TTP- Tactics, Techniques, and Procedures

UAS- Unmanned Aerial System

USDI- Under Secretary of Defense of Intelligence

USSOCOM- U.S. Special Forces Operations Command

WMD- Weapons of Mass Destruction

CHAPTER I

INTRODUCTION

STATEMENT OF TOPIC AREA

In this new age of asymmetric and unconventional warfare, intelligence is commonly considered to be synonymous with national security. The increasingly common threat of terrorist organizations to our direct security, along with the tertiary threat of insurgency toward the U.S. and its foreign allies, have proven to be too disseminated to subdue completely and too fanatical to disband wholly. The most promising opportunity for successful national security is a combined effort of the U.S. Intelligence Community (IC) and military forces through judicious and accessible intelligence provided through the process of reach back intelligence by Joint Intelligence Centers (JICs), not only paired with actionable analyses and provided to those operating at the operational and tactical levels, but also current and comprehensive parameters of such operations as outlined at the strategic level. Use of the IC and its elements by JICs must be organized and detailed by requirements of a mission set rather than that of just a collection mechanism in order to fully exploit its technical and analytic aptitude in contributing to tactical operations. This revelation has brought about not only an apparent need in the operation of the JIC for standard, periodic assessment of procedure, doctrine, and organization in order to more concertedly and effectively assist military forces in addressing current national security needs, but it also highlights the limitations that operating on outdated structure can place on U.S. tactical

operations. It emphasizes the significance of keeping all methods of operations including the process of reach back intelligence current and the consequences of allowing elements of the process to become outdated.

PURPOSE OF STUDY

In order to fully understand the complexities involved in preparing military intelligence entities to support military operations and successfully face the asymmetric threat, one must first analyze and understand the history of the Joint Intelligence Center (JIC), the general practice of the reach back intelligence process, and the joint doctrinal guidelines that directly affect these resources. This exploratory study will highlight the issues that lie in the current usage of these resources and techniques and what difficulties may exist in changing these measures, especially highlighting issues between the integration of the intelligence community, military intelligence, and various military branches.

The study of intelligence operations, along with military intelligence operations, is critical in refining the policies, tactics, and procedures for future intelligence activity. It is through the study and reassessment of current policies and activities revolving around the use of reach back intelligence and the engagement of asymmetric enemies, that we can look toward the future and determine the best course of action involving subsequent recommendations of change. It is the goal of this paper to expand on previous efforts of joint intelligence as it related to the use of JICs and reach back intelligence and redirect focus to a higher strategic level to better integrate the IC into the military realm and do so in a manner that benefits modern national security realities of the asymmetric threat. This should be done using methods that lay groundwork for the entirety of the U.S. military force to conduct

intelligence-based operations in a manner that coincides with, but is not based solely on, Special Operations Forces (SOF). This action should assist in placing intelligence and national security defense assets, including that of both at-home agencies and military forces, to better use through an enhanced and more efficient process of reach back intelligence provided by JICs.

CHAPTER II

BACKGROUND / LITERARY REVIEW

THE ASYMMETRIC THREAT DEFINED

Although the official term 'asymmetric threat' is quite new, the ideas that the term encompasses are as 'old as warfare itself'.[1] Many strategic theorists have touched on the topic within their writings throughout the course of history. Sun Tzu is perhaps one of the most notable proponents of asymmetric attack and stated that: *"All warfare is based on deception. When confronted with an enemy, one should offer the enemy a bait to lure him; feign disorder and strike him. When he concentrates, prepare against him; where he is strong, avoid him".* [2] Strategic theorists from B.H Liddle Hart to Edward Luttwak have generalized rules of warfare based on the idea of exploiting an adversary's weaknesses in unconventional manners. In operational history, historical military leaders from Genghis Khan to Joan of Arc have exhibited measures of asymmetric strategy within their tactical military strategy.[3]

The first official mention of the term "asymmetric warfare" was in a publication of Joint Doctrine in 1995 as it defined asymmetric engagements as those between dissimilar forces, specifically in instances of air versus land, sea versus land, etc.[4] As such, the concept

---

[1] Steven Metz and Douglas Johnson II, *Asymmetry And U.S. Military Strategy: Definition, Background, And Strategic Concepts*, eBook (repr., Carlisle, PA: Strategic Army War College, 2001), http://ssi.armywarcollege.edu/pdffiles/PUB223.pdf.
[2] Bin Sun, Ken Langdon and Karen McCreadie, *Sun Tzu's The Art Of War* (Oxford: Infinite Ideas, 2008).
[3] Steven Metz and Douglas Johnson II, *Asymmetry And U.S. Military Strategy: Definition, Background, And Strategic Concepts*, eBook (repr., Carlisle, PA: Strategic Army War College, 2001), http://ssi.armywarcollege.edu/pdffiles/PUB223.pdf.
[4] Dan Daley, *Asymmetric Warfare: The Only Thing New Is The Tactics*, eBook (Washington D.C.: National War College, 2000), http://www.dtic.mil/dtic/tr/fulltext/u2/a433588.pdf.

of asymmetry was presented in an incredibly narrow sense until the 1995 National Military Strategy broadened the definition listing other means of threat as asymmetric threat including that of terrorism, weapons of mass destruction (WMD), and information warfare.[5] Once acknowledged officially by military entities, it was not long before the entirety of the IC and other agencies involved in foreign affairs began to approach the concept of asymmetric warfare as a topic of utmost importance. The concept of asymmetry began to appear in official strategy documents across intelligence, military, and policy community agencies in order to address the issue and begin study and development of strategy and doctrine in order to help prevent attack from an asymmetric front as well as launch offensives using our own asymmetric capabilities.

In 1999, the Joint Strategy Review provided what was, to-date, the broadest official conceptualization of asymmetric adversary stating: "*Asymmetric approaches are the attempts to circumvent or undermine U.S. strengths while exploiting U.S. weaknesses using methods that differ significantly from the United States' expected method of operations. [Asymmetric approaches] generally seek a major psychological impact, such as shock or confusion that affects an opponent's initiative, freedom of action, or will. Asymmetric methods require an appreciation of an opponent's vulnerabilities. Asymmetric approaches often employ innovative, nontraditional tactics, weapons, or technologies, and can be applied at all levels of warfare- strategic, operational, and tactical- and across the spectrum of military operations.*".[6]

[5] Steven Metz and Douglas Johnson II, *Asymmetry And U.S. Military Strategy: Definition, Background, And Strategic Concepts*, eBook (repr., Carlisle, PA: Strategic Army War College, 2001), http://ssi.armywarcollege.edu/pdffiles/PUB223.pdf.
[6] Rod Thornton, *Asymmetric Warfare* (Cambridge: Polity Press, 2008).

While this definition expanded on the concept of asymmetric adversary, it has been pointed out that it has two glaring shortcomings. First of all, it remains specific to the strategic environment and national security scenario of the time of its inception. Secondly, it only seems to deal with what is referred to as negative asymmetry. Negative symmetry is the understanding and acknowledgement of what action an adversary may take against the U.S. but does not take into account the asymmetric action that the U.S. may employ against its adversaries.[7]

The CIA defines asymmetric warfare as "The use of innovative strategies, tactics, and technologies by a 'weaker' state or sub-state adversary that are intended to avoid the strengths and exploit the potential vulnerabilities of larger and technologically superior opponents. This includes:

- The selective use of weapons or military resources by a state or sub-state group to counter, deter, or possibly defeat a numerically or technologically superior force.
- The use of diplomatic and other non-military resources or tactics by a state or sub-state group to discourage or constrain military operations by a superior force."[8]

The DoD defines asymmetric warfare in simpler terms. In the DoD definition which was formulated by the Joint Chiefs of Staff (JCS), asymmetric warfare should be considered "attempts to circumvent or undermine an opponent's strengths while exploiting his weaknesses using methods that differ significantly from the opponent's usual mode of

[7] Steven Metz and Douglas Johnson II, *Asymmetry And U.S. Military Strategy: Definition, Background, And Strategic Concepts*, eBook (repr., Carlisle, PA: Strategicd Army War College, 2001), http://ssi.armywarcollege.edu/pdffiles/PUB223.pdf.
[8] Ashton B. Carter and William J. Perry, *Countering Asymmetric Threats*, eBook (Washington D.C.: The Brookings Institution, 1999), https://www.belfercenter.org/sites/default/files/legacy/files/kte_ch5.pdf.

operations".[9] The U.S. Army War College even further simplifies this definition as it refers to asymmetric warfare as strategic asymmetry, or "the use of some sort of difference to gain an advantage over an enemy".[10]

Perhaps the most detailed conceptualization of asymmetric warfare was defined by Steven Metz and Douglas Johnson in a report for the Army War College as it describes strategic asymmetry in the following manner: "*In the realm of military affairs and national security, asymmetry is acting, organizing, and thinking differently than opponents in order to maximize one's own advantages, exploit an opponent's weaknesses, attain the initiative, or gain greater freedom of action. It can be political-strategic, military-strategic, operational, or a combination of these. It can entail different methods, technologies, values, organizations, time perspectives, or some combination of these. It can be short-term or long-term. It can be deliberate or by default. It can be discrete or pursued in conjunction with symmetric approaches. It can have both psychological and physical dimensions."* [11]

Regardless of the official definition provided by a particular agency or branch representative, all definitions of the term asymmetric warfare include the same primary factors-

- The use of unconventional and inventive methods of attack and/or defense
- Disproportionate effect in military or financial investment

---

[9] Ashton B. Carter and William J. Perry, *Countering Asymmetric Threats*, eBook (Washington D.C.: The Brookings Institution, 1999), https://www.belfercenter.org/sites/default/files/legacy/files/kte_ch5.pdf.
[10] Steven Metz and Douglas Johnson II, *Asymmetry And U.S. Military Strategy: Definition, Background, And Strategic Concepts*, eBook (repr., Carlisle, PA: Strategic Army War College, 2001), http://ssi.armywarcollege.edu/pdffiles/PUB223.pdf.
[11] Steven Metz and Douglas Johnson II, *Asymmetry And U.S. Military Strategy: Definition, Background, And Strategic Concepts*, eBook (repr., Carlisle, PA: Strategic Army War College, 2001), http://ssi.armywarcollege.edu/pdffiles/PUB223.pdf.

- Use of exhibited strengths against the organizational weaknesses of one's enemies[12]

THE JOINT-INTELLIGENCE CENTER: A BRIEF HISTORY

While the concept of a joint intelligence center had been thinly addressed for some time, the official initiative of a joint intelligence center did not arise until somewhat recently. In 1942, in response to the probability of active operations in the Pacific arena, an U.S. Marine Corps commandant made an official proposal for such an organization highlighting the need for integrated intelligence efforts amongst military branches.[13] This proposal was acknowledged yet did not provoke any implementation until several months later, with the creation of an intelligence center at Pearl Harbor. This facility would eventually become the first veritable JIC- the Joint Intelligence Center/Pacific Ocean Area (JICPOA).[14]

The primary dynamic leading to the Pearl Harbor Intelligence Center's transition to the JICPOA was the tragic event of Pearl Harbor itself and the causal intelligence failures that led to the tragedy. Other factors played key roles in the evolution of the JIC at this point as well. World War II had once again forced U.S. military operations to transition from fundamentally defensive operational tactics to offensive operations and helped to demonstrate an essential need for integration and inter-service cooperation amongst the different military branches, as well as a reliance on intelligence products derived from IC

[12] Military Intelligence, Intelligence Studies, Intelligence Operations, National Intelligence, Intelligence Analysis, Gateway to Intelligence. 1. accessed February 2019. https://www.au.af.mil/au/awc/awcgate/awc-ntel.htm
[13] Military Intelligence, Intelligence Studies, Intelligence Operations, National Intelligence, Intelligence Analysis, Gateway to Intelligence. 1. accessed February 2019. https://www.au.af.mil/au/awc/awcgate/awc-ntel.htm
[14] Military Intelligence, Intelligence Studies, Intelligence Operations, National Intelligence, Intelligence Analysis, Gateway to Intelligence. 1. accessed February 2019. https://www.au.af.mil/au/awc/awcgate/awc-ntel.htm

agencies domestically.[15] The resulting shift in emphasis from smaller-scale, special operations to that of large-scale joint operations throughout the Pacific further underscored the need for collaborative intelligence efforts.

Another major contributing factor to the projected need of joint intelligence operations was the increase in availability of new intelligence sources. The increase in military operations throughout the Pacific naturally increased the volume of intelligence-based sources including seized documents, prisoners used in interrogation procedures, and other forms of raw data.[16] The compartmentalized system of intelligence operations that existed up to this point could not effectively or efficiently handle this influx of intelligence, as its framework would lead to further duplication of effort, intra-service competition, issues in resource allocation, errors in dissemination, and inconsistent analysis and assessment.[17]

With the end of the war came the inevitable organizational downsizing that takes place after the dissolution of any largescale conflict. Intelligence organizations such as the JICPOA and other joint intelligence operational units were trimmed from the budget and eliminated. The next forty years of JIC progression was interwoven with efforts synergize DOD and the U.S. IC.[18] This led to in-battling between military branches as some military-related organizations (i.e. the War Department) supports the expansion and centralization of the JIC as associated with the JCS, while others (i.e. Secretary of Naval Command) opposed

[15] *Report of Intelligence Activities in the Pacific Ocean Areas*, report, Archives, Joint Forces Staff College, US Pacific and Pacific Ocean Areas.
[16] *Report of Intelligence Activities in the Pacific Ocean Areas*, report, Archives, Joint Forces Staff College, US Pacific and Pacific Ocean Areas.
[17] Military Intelligence, Intelligence Studies, Intelligence Operations, National Intelligence, Intelligence Analysis, Gateway to Intelligence. 1. accessed February 2019. https://www.au.af.mil/au/awc/awcgate/awc-ntel.htm
[18] Andrew Rathmell, "Towards Postmodern Intelligence," *Intelligence and National Security* 17, no. 3 (2002): , doi:10.1080/02684520412331306560.

these efforts, further intensifying interservice and cross-branch issues of command and control of resources.[19]

As a compromise, Joint Intelligence Divisions (JID) were created to direct focus on the standardization of procedural methods and to assist in the prevention of effort duplication among the services. The overall goal of the JID was to emphasize support and cohesiveness among the various intelligence factions of the military branches while leaving the core of the intelligence cycle procedures to the service components of the individual branches.[20] A full revival of the JIC, while acknowledged in discussion of organizational change as a replacement and better alternative to the JID, would not appear for several decades.

Over this period of time there were other changes and progressions taking place in the realm of defense intelligence as well. Focus of defense intelligence (to be noted, this does not refer to intelligence operations as a whole, but that which is labeled specifically defense intelligence) was steered away from overall military planning and beginning to focus more on the support of operational forces.[21] Further adjustments were being followed through as a more thorough result of the Goldwater-Nichols Act leading to a refinement of the Defense Intelligence Agency's (DIA) role as a military intelligence organization in better response of declining funding and the rapidly changing nature of the global threat.[22]

---

[19] Edward M. Coffman, Allan R. Millett, and Peter Maslowski, "For the Common Defense: A Military History of the United States of America.," *Military Affairs* 50, no. 1 (1986): , doi:10.2307/1988538.
[20] Coffman, Edward M., Allan R. Millett, and Peter Maslowski. "For the Common Defense: A Military History of the United States of America." *Military Affairs*50, no. 1 (1986): 51. doi:10.2307/1988538.
[21] McDonnell, Janet A. *Adapting to a Changing Environment: Defense Intelligence Agency in the 1990s*. DIA Historical Research Division. Defense Intelligence Historical Perspectives. 2013. http://www.dia.mil/Portals/27/Documents/About/History/HistoricalPerspectiveVol3_Web.pdf.
[22] McDonnell, Janet A. *Adapting to a Changing Environment: Defense Intelligence Agency in the 1990s*. DIA Historical Research Division. Defense Intelligence Historical Perspectives. 2013. http://www.dia.mil/Portals/27/Documents/About/History/HistoricalPerspectiveVol3_Web.pdf.

OPERATION DESERT STORM AND THE RE-EMERGENCE OF THE JOINT INTELLIGENCE CENTER

The DIA, in order to improve management of military intelligence resources, as to help consolidate multiple efforts, went through a period of restructure during the Gulf War. As such, Operation Desert Storm marked a resurgence in the use of the JIC concept. The use of JICs had been a long-suggested method for intelligence operations; yet oddly, regardless of the realization of its importance, the use of JICs was not a widely accepted practice to use these centers until after the Gulf War. This is not to say that the idea was completely disregarded prior to this point. During World War II, JICs were used in several theaters of operation; however, their use was not recorded in detail until the period of the Gulf War, causing most scholarly study that has been performed in the area to be conducted from this point forward and leaving its years of infancy largely unexamined.

The factors associated with the Gulf War at both the geopolitical and social levels were designed in such a way to further facilitate the re-emergence of JICs into the military intelligence theater. As Hussein's military structure presented itself much like a "miniature version of the Soviet Army in equipment, doctrine, and tactics", the threat presented itself in conventional terms, with the exposition of a symmetric military force. Therefore, the U.S. was able to use its expertise in the area of Air-Land Battle Doctrine, a tactic U.S. forces had actively been training for since the 1970s, in order to quickly and efficiently contain and minimize the threat in the Gulf.[23] Considering this was the type of warfare that we had focused resources and training in since the IC's inception, Operation Desert Storm as it was

[23] C. Jones, *Intelligence Reform: The Logic Of Information Sharing*, eBook (University of Maryland, 2016), http://gvpt.umd.edu/sites/gvpt.umd.edu/files/pubs/Jones_IntellReform.pdf.

called, was quickly successful and U.S. and coalition forces were victorious in minimizing the threat of Hussein's regime for the time being. While Operation Desert Storm was a battlefield success, it also served as a reminder of the dominance of U.S. military forces in conventional terms, encouraging other regimes and sub-state forces to begin to contemplate an increase in the use of unconventional and asymmetric tactics in engaging and attacking the security of the U.S.

Despite the success of strategic and tactical operations during Operation Desert Storm, the IC caught its share of criticism on an operational level once again. During a post-operational testimony before Congress, General Normal Schwarzkopf criticized the efforts of the IC during the operation, highlighting a "breakdown in the integration of national intelligence and military forces".[24] He attributed this breakdown to fragmented preparation, poor communication activity, and a deficiency in knowledge and understanding of the operational environment that the mission set contained.[25] Also contributing to the return of the JIC was the implementation of the 1986 Goldwater-Nichols Act.[26] By increasing the power of the Chairman to the JCS as a principal military adviser, and granting combatant commanders more autonomy and authority, the Goldwater-Nichols Act successfully generated an organizational structure requirement best met by JIC development.[27]

[24] David Oakley, "Adapting To Change: Strategic Turning Points And The CIA/Dod Relationship", *Interagency Journal* 5, no. 1 (2014), http://thesimonscenter.org/wp-content/uploads/2014/03/IAJ-5-1Winter-2014-3-11.pdf.
[25] David Oakley, "Adapting To Change: Strategic Turning Points And The CIA/Dod Relationship", *Interagency Journal* 5, no. 1 (2014), http://thesimonscenter.org/wp-content/uploads/2014/03/IAJ-5-1Winter-2014-3-11.pdf.
[26] "The Evolution And Relevance Of Joint Intelligence Centers — Central Intelligence Agency", *Cia.Gov*, 2018, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol49no1/html_files/the_evolution_6.html.
[27] "The Evolution And Relevance Of Joint Intelligence Centers — Central Intelligence Agency", *Cia.Gov*, 2018, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol49no1/html_files/the_evolution_6.html.

During the Gulf War, JICs were successfully implemented at both the national and theater levels. The DoD Joint Intelligence Center (later renamed the National Military Joint Intelligence Center) was established in August 1990 in order to provide a "single, integrated DoD intelligence position to national decision-makers and the theater commander".[28] Providing a much-needed bridge between the military intelligence and IC agency communities, the use of JICs was further implemented amongst CENTCOM units and established at each of the theater commands. This requisite, along with the aforementioned Goldwater-Nichols Act, created a state of affairs that ensured that the use of JICs would not fade away as in previous implementations, but would rather become an integral part of military intelligence and IC operations.

The successful implantation of JICs during the Gulf War did not mean that the use of such entities was without its own share of challenges. Several studies into the use of JICs at this time, as well as noted statements from key players in the conflict, point to several dilemmas within its operations. Perhaps the most mentioned problem of the use of the JIC during Operation Desert Storm was in its developmental operational procedures. As the use of JICs was only implemented as an effort to streamline analysis and dissemination during the planning phase of Desert Storm, it was done so quickly and inefficiently, leaving its organizational nature "loose and largely informal", limiting its efficiency and effectiveness and creating strain in the military community and IC relationship.[29] Tensions between the military community and the IC were further exacerbated by the use of JICs in the analysis of

[28] "The Evolution And Relevance Of Joint Intelligence Centers — Central Intelligence Agency", *Cia.Gov*, 2018, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol49no1/html_files/the_evolution_6.html.
[29] David Oakley, "Adapting To Change: Strategic Turning Points And The CIA/Dod Relationship", *Interagency Journal* 5, no. 1 (2014), http://thesimonscenter.org/wp-content/uploads/2014/03/IAJ-5-1Winter-2014-3-11.pdf.

battle damage assessments, as the two groups disagreed upon the nature of these reports and the IC was perceived as supporting the military operations poorly.[30] Poor intelligence support was an issue commonly referenced in other discussion and critiques of Operation Desert Storm as well. Other Congressional reports panned the CIA specifically as exhibiting inadequacy in its support role towards the JIC. The CIA was denunciated as demonstrating a "hands-off approach" that failed to unify an adequate intelligence picture of the scenario exhibited in the mission set.[31]

In response to the criticisms of the functionality of the JICs during Desert Storm, the DoD established permanent JICs at the Combatant-Command level.[32] To parallel this improvement, the IC, in turn, established non-permanent national support teams, groups of subject matter experts and IC analysts that would come together in periods of need in order to support joint task forces during operations.[33] The CIA also extended effort to improve intelligence support operations by developing crisis operation liaison teams to better provide military commanders access to CIA realm products and to better integrate CIA and DoD operations.[34]

Demonstrating an alacrity to go beyond the role of support to the policymaker that the IC is required to hold, the CIA went a step further to help bridge the gap between IC and

[30] David Oakley, "Adapting To Change: Strategic Turning Points And The CIA/Dod Relationship", *Interagency Journal* 5, no. 1 (2014), http://thesimonscenter.org/wp-content/uploads/2014/03/IAJ-5-1Winter-2014-3-11.pdf.
[31] David Oakley, "Adapting To Change: Strategic Turning Points And The CIA/Dod Relationship", *Interagency Journal* 5, no. 1 (2014), http://thesimonscenter.org/wp-content/uploads/2014/03/IAJ-5-1Winter-2014-3-11.pdf.
[32] "The Evolution And Relevance Of Joint Intelligence Centers — Central Intelligence Agency", *Cia.Gov*, 2018, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol49no1/html_files/the_evolution_6.html.
[33] David Oakley, "Adapting To Change: Strategic Turning Points And The CIA/Dod Relationship", *Interagency Journal* 5, no. 1 (2014), http://thesimonscenter.org/wp-content/uploads/2014/03/IAJ-5-1Winter-2014-3-11.pdf.
[34] David Oakley, "Adapting To Change: Strategic Turning Points And The CIA/Dod Relationship", *Interagency Journal* 5, no. 1 (2014), http://thesimonscenter.org/wp-content/uploads/2014/03/IAJ-5-1Winter-2014-3-11.pdf.

DoD activity at this time through its establishment of the Office of Military Affairs (OMA). This office was created in an effort to "enhance information flow and increase cooperation" amongst the military community and the IC. This increased the mission of the IC to provide support to military operations when the need arises, identifying military agencies as another 'customer' to the products that the IC disseminates.[35] This office, along with the CIA Associate Director of Central Intelligence for Military Support were consolidated into the Office of the Associate Director of Military Affairs (ADMA) after the events of 9/11.[36]

POST 9/11 CHANGES

"*I am not opposed to intelligence reform on its face, but any changes should reflect the current context*".[37] These words, uttered by Ted Stevens during the proceedings and debates of the second session of the 108th Congress, reflects an opinion shared by a large part of Western society in a post-9/11 world.[38] Prior to 9/11, our nation's intelligence agencies remained poised for a single, traditional enemy. There was an intrinsic need to adapt to a post-Cold War threat environment.[39] The 9/11 attacks accelerated efforts to "transform the orientation of intelligence services from rivalry, both domestic and international, to cooperation against the new threats".[40] This was an unprecedented situation for intelligence

[35] M. Lowenthal, *Intelligence: From Secrets To Policy* (Washington, DC: CQ Press, 2000).
[36] David Oakley, "Adapting To Change: Strategic Turning Points And The CIA/Dod Relationship", *Interagency Journal* 5, no. 1 (2014), http://thesimonscenter.org/wp-content/uploads/2014/03/IAJ-5-1Winter-2014-3-11.pdf.
[37] "Congressional Record", *Congress.Gov*, 2004, https://www.congress.gov/crec/2004/09/29/CREC-2004-09-29/pdf.
[38] "Congressional Record", *Congress.Gov*, 2004, https://www.congress.gov/crec/2004/09/29/CREC-2004-09-29/pdf.
[39] Eric Rosenbach and A. J. Peritz, "Intelligence Reform | Belfer Center For Science And International Affairs", *Belfercenter.Ksg.Harvard.Edu*, 2009, http://belfercenter.ksg.harvard.edu/publication/19154/intelligence_reform.html.
[40] Larry Watts, "Intelligence Reform In Europe's Emerging Democracies", *Cia.Gov*, 2007, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no1/article02.html.

services, domestic, military, and overseas alike, where considerations of secrecy, trust, and national security made them the strongest bulwark of sovereignty. The events of 9/11 not only brought the CIA and DoD relationship back to the forefront of consideration, but also the entire IC into the spotlight of critique and review. It exacerbated the fact that while our IC remained prepared for conventional/symmetric adversary, its organizational structure and procedural doctrine was lacking in response to that of an unconventional/asymmetric threat.

Perhaps the most widespread and well-known instance of reformation stemming from 9/11 affecting military intelligence operations was the passage of the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004. This reformation act is highly considered to be a "decade's effort to coordinate the work of military and intelligence agencies that used to compete". [41] The passage of the IRTPA forced intelligence agencies to share information amongst one another, finally centralizing the process to some degree and allowing a further level of integration among agencies within the IC, further benefitting military intelligence activities that derive part of their data from these arenas. The National Counterterrorism Center (NCTC) was created with the IRTPA, setting up a joint command structure across the entirety of the intelligence agencies and establishing guidelines for new information sharing measures benefitting the JICs in avenues of collection.[42] The new emphasis on information sharing and the reorganizational measures that resulted also led to a significant application of resources.[43] Other important provisions of the IRTPA included: the National Crime

[41] Patrick Neary, "Intelligence Reform, 2001-2009: Requiescat In Pace?", *Studies In Intelligence* 54, no. 1 (2010), https://nsarchive2.gwu.edu//NSAEBB/NSAEBB370/docs/Document%207.pdf.
[42] James Burch, "The Domestic Intelligence Gap: Progress Since 9/11? - HOMELAND SECURITY AFFAIRS", *HOMELAND SECURITY AFFAIRS*, 2008, https://www.hsaj.org/articles/129.
[43] James Burch, "The Domestic Intelligence Gap: Progress Since 9/11? - HOMELAND SECURITY AFFAIRS", *HOMELAND SECURITY AFFAIRS*, 2008, https://www.hsaj.org/articles/129.

Prevention Council (NCPC), and the Joint Intelligence Community Council (JICC); establishment of an "information sharing environment", creating a Privacy and Civil Liberties Oversight Board, and mandating that service be required in multiple agencies of the IC as a condition of promotion to specific positions.[44]

As it stands in its modern-day construct, the JIC operates as the principal organization in each Combatant Command as a Joint Intelligence Operations Center (JIOC). JIOCs were established in 2006, based much on the model of the JIC, as DIA organizations conducting all avenues of intelligence planning, collection, analysis, and dissemination procedures under the control and authority of their respective Combatant Commanders.[45] Resource allocation and oversight is provided to JIOCs through the Office of the Under Secretary of Defense for Intelligence [USD(I)], offering the JIOC a set of stipulated assignments to be performed by task-organized teams of specialists.[46] These specialists are comprised from various intelligence disciplines with the specific constituents of each team being adapted as needs change.

THE REACH BACK INTELLIGENCE PROCESS AND JOINT INTELLIGENCE DOCTRINE

Overall, joint doctrine defines intelligence as a "product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information

---

[44] J. Tama, *Intelligence Reform: Progress, Remaining Deficiencies, And Next Steps*, eBook (Princeton University, 2005), https://www.princeton.edu/~ppns/papers/intel_reform.pdf.
[45] DeMattei, Lou Anne. "Knowledge Management in Joint Intelligence Operations Centers." *American Intelligence Journal*31, no. 2 (2013). https://www-jstor-org.easydb.angelo.edu/stable/26202080?read-now=1#page_s.
[46] DeMattei, Lou Anne. "Knowledge Management in Joint Intelligence Operations Centers." *American Intelligence Journal*31, no. 2 (2013). https://www-jstor-org.easydb.angelo.edu/stable/26202080?read-now=1#page_s.

concerning foreign countries or areas".[47] As it stands, joint intelligence doctrine focuses primarily on combat operations and getting Joint Force Commanders (JFCs) intelligence products concerning the battlespace and adversary in question in times of war and in Military Operations Other Than War (MOOTW).[48] It is used in combat situations to support operations and in MOOTW to determine when and where conflict may arise that may require U.S. military intervention. The Joint Intelligence Preparation of the Battlespace doctrine in JP 2-01.3 highlights the focus that most doctrinal requirements maintain on the conventional battlefield, as it is directed towards the "preparatory intelligence analysis for operations level force-on-force confrontations" in the conventional sense, rather than the asymmetric adversary our military forces face more commonly today.[49]

This is important in our research as it is known that in both circumstances of when joint intelligence doctrine is used, it is often used in a process known as "reach back intelligence". It is when furthering study on reach back intelligence that the underlying conventional conditions on which joint intelligence doctrine is based on becomes a matter of importance.

The Joint Publication 3-30 defines reach back intelligence as the "process of obtaining products, services, and applications, or forces, or equipment, or material from organizations that are not forward deployed".[50] This process allows those in tactical and

[47] Joint Chiefs of Staff, Joint Publication 1-02 DOD Dictionary Of Military And Associated Terms (Washington, DC: 12 April 2001)
[48] Lt. Commander John P. Coles, USN, *Cultural Intelligence & Joint Intelligence Doctrine*, report, Graduate Studies. USAF Air University (USAF AU).
[49] Joint Chiefs of Staff, Joint Publication 2-01.3, Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace (Washington, DC: The Joint Staff, May 24, 2000), i.
[50] *Joint Publication 3-30 | Command And Control Of Joint Air Operations*, eBook (Washington D.C.: Office of the Chairman of the Joint Chiefs of Staff, 2014), https://fas.org/irp/doddir/dod/jp3_30.pdf.

operations fronts to ‘reach back’ to those on back end missions or in undeployed standing to assist in operations.[51] This may involve assistance from both military intelligence entities and agencies within the IC. This process encourages the use of resources that are otherwise unavailable onsite in support and integration of advise and assist missions, as well as in operations of assessment.[52]

The process of reach back intelligence support can be explained simply as it relies on a system of questions and answers. Within the reach back process, once a tactical unit identifies an area in which they could use supplementary intelligence to their own analytical information, they pose the question to a reach back support agency in order to seek assistance in the matter. This agency provides a team of analysts who address the problem through analysis of stored and collected intelligence data, creating a product that can be quickly and efficiently disseminated back to the unit in forward deployment.[53]

It is not difficult to understand why the use of reach back support and intelligence efforts are necessary in today’s operational environment. Prior to the emergence of official reach back procedures, it was the sole responsibility of company commanders to progress the ground situation through efforts such as patrol reports, atmospherics, and general situational awareness.[54] Battalion level intelligence shops (i.e. S-2) took the initiative in the tracking and identification of patterns within adversarial groups in an effort to help drive targeting

[51] John Pike, "FM 3-11.22 Appendix G, Reach-Back Capability And Federal Response Assets", *Globalsecurity.Org*, 2018, https://www.globalsecurity.org/security/library/policy/army/fm/3-11-22/appg.htm.
[52] John Pike, "FM 3-11.22 Appendix G, Reach-Back Capability And Federal Response Assets", *Globalsecurity.Org*, 2018, https://www.globalsecurity.org/security/library/policy/army/fm/3-11-22/appg.htm.
[53] Phillip Radzikowski, *'Reach Back'- A New Approach To Asymmetrical Warfare Intelligence*, eBook (ARMY, 2008), https://www.ausa.org/sites/default/files/FC_Radzikowski_1208.pdf.
[54] Phillip Radzikowski, *'Reach Back'- A New Approach To Asymmetrical Warfare Intelligence*, eBook (ARMY, 2008), https://www.ausa.org/sites/default/files/FC_Radzikowski_1208.pdf.

operations, those of which are executed at the company level. A broader network analysis is then created in order to assist in the amalgamation of bringing a larger portion of the IC's assets into use.

While this method of intelligence procedure works in conflict with the conventional threat, it becomes less efficient within a fight involving insurgency or asymmetric adversaries. This is largely due to the speed at which the operational environment in which asymmetric conflict takes place begins to evolve; the decentralized structure of the insurgent organization as well as the consistent transformation of tactics, techniques, and procedures (TTP) involved help to contribute to this problem. This creates an even more difficult environment in which the various levels of military operations can sustain activity, requiring a more expedient and efficient method for the gathering and usage of intelligence assets.[55]

The use of reach back intelligence support has increased substantially in recent years with the evolution of adversarial threats into asymmetric conflicts; therefore, a general understanding of the reach-back intelligence process is necessitated when analyzing any portion of military intelligence operations.

Reach back intelligence is achieved through a common Request for Support (RFS). When the operational unit experiences a gap in intelligence, the S-2 must provide a RFS in order to initiate the reach back process; this request is provided to a geographically assigned Division Support Team (DST) located within the JIC or other reach back support agency [i.e. Joint Improvised Explosive Device Defeat Organization (JIEDDO), Joint Fusion and Analysis Center (JFAC), Counter-IED Operations Integration Center (COIC), etc.] through a

[55] Phillip Radzikowski, *'Reach Back'- A New Approach To Asymmetrical Warfare Intelligence*, eBook (ARMY, 2008), https://www.ausa.org/sites/default/files/FC_Radzikowski_1208.pdf.

secure and approved communications system such as the Secret Internet Protocol Router Network (SIPRNET). The DST take the request and begin to look through databases of previously collected data and intelligence analysis reports in order to see if the information is readily available for dissemination.[56] Relevant information is then gathered and integrated into a product for dissemination and use in the specific operation from which it was requested. It is important to note there is no specific timeline for how long the reach back process is to take in response to the RFS; however, the goal of this action is to be as efficient and effective as possible to allow for tactical and operational activities on the ground to continue toward success.

[56] C. Jones, *Intelligence Reform: The Logic Of Information Sharing*, eBook (University of Maryland, 2016), http://gvpt.umd.edu/sites/gvpt.umd.edu/files/pubs/Jones_IntellReform.pdf.

CHAPTER III

RESEARCH DESIGN

METHODOLOGY

Driven by the question "how could the joint intelligence center better support military intelligence operations, especially in the process of reach back intelligence", this study must first answer several sub-questions. First, this study must establish what the current policy deficiencies are in relation to both IC and military intelligence operations against the asymmetric adversary, what organizational deficiencies are negatively affecting intelligence operations in both of these realms, and what corrections should be made in order to remedy these problems. Understanding the nature of the problem and necessary solutions are necessary prerequisites in the development and dissemination of recommendations regarding better organizational structure and processes in the realm of national security, military operations, and the asymmetric threat, specifically in the areas of the Joint Intelligence Center and its impact on reach back intelligence activities.

The methodology conducted in this study is a qualitative study based on retrospective historical exploratory analysis. Previously conducted reports and studies involving U.S. military intelligence activities have resulted in scholarly analyses to determine the impact of certain circumstances on military intelligence measures and reform. The current study is considered to be 'retrospective' in nature, as the effects have already been studied in previous works and are known; therefore, the researcher must look back in order to determine the

relation of previous events to the causes of the current standing of the JIC and its need for improvement.

By focusing study in this manner, a timeline for organizational efforts can be established based on the issues addressed in background and literary review in order to demonstrate the need for periodic assessment and adjustment within the JIC or the reach back intelligence process in order to more concertedly and efficiently address national security needs. Once the scope of previous reformation efforts is considered, this study can then begin to identify any other doctrinal reform and recommendations that must take place in order for the new strategy to achieve desired outcomes.

It is at this point that the study transitions to a prospective approach as its aim changes to predict the effects of a change to the current situation in order to properly suggest recommendations in support of a better codification of policy against the asymmetric threat. To better provide such, the study must weigh the influence of such action against the limitations of current procedure. It is important to again note that this study is qualitative in nature and is therefore based on an open-ended and considered more subjective in nature than a quantitative approach to such a study would be. This type of research design best suits this type of qualitative study, as the issues that exist within the structure and integration of the JIC and military intelligence agencies are observable, but the underlying causes and future effects of action and/or inaction are both debatable in current context.

SIGNIFICANCE, RATIONALE, AND PURPOSE

It is important to understand that while national-security challenges grow, and budgets decrease, the key to addressing these changes and remaining relevant within such an

open society is building a more efficient military intelligence operations structure while supporting it with proper guidelines backed by joint intelligence doctrine. It is proposed that the best course of action within intelligence reform and the fight against modern-day asymmetric threats lies directly in integration based on mission set, not only among the various agencies within the IC, but also amongst other prominent and associated groups and agencies, including DoD and tactical groups, that can directly impact national security measures. It is also proposed that current doctrinal support to tactical operations be revised in order to meet the needs of the current mission set.

It is noted in preliminary findings that most policy and doctrine related to the asymmetric threat is dependent solely on SOF operations in a conventional warfare situation, yet today it is the entirety of our military and national security forces that faces the asymmetric threat. This study is intended to expand on previous efforts in this realm and redirect focus to the organizational and strategic level, bringing mission directives and authorizations into current context. The purpose of this study is to offer suggestions on how to better codify doctrine and practices through revision of current doctrine using methods that benefit and coincide with, but are not based solely on, Special Operation Forces; this is to be conducted through recommendations to the JIC structure and joint intelligence doctrinal guidelines related to reach back intelligence and asymmetric adversaries in effort to put intelligence and national security defense assets to better use, rather than formulate a suggested change in policy and overall tactical measures.

CHAPTER IV

RESEARCH FINDINGS / DISCUSSION

SUMMARY OF FINDINGS

The qualitative review of previously conducted reports and studies involving various aspects of intelligence and military operations has led to a better recognition and deeper understanding of the issues involved in various realms of the intelligence and military relationship. These issues must be addressed individually in order to make a better effort in the suggested recommendations towards policy revision and reformation regarding intelligence and military intelligence operations as they relate to U.S. national security and the fight against the asymmetric threat. It is hopeful that a more in-depth acknowledgement of the issues and weaknesses that exist in the current state of the intelligence – military relationship will also lead to suggestions for future research in the area and a recognition of more specific topics and questions that should be addressed and corrected in the future.

This study was successful in identifying that there are definitive weaknesses and flaws in current intelligence and military intelligence operations that must be addressed in order to make more efficient and effective use of resources and assets associated with these operations. This study was also successful in identifying a small number specific areas of weakness and making suggested recommendations in order to increase the odds of success in operations against asymmetric threats. The reasons for the limited amount of findings based on this study will be addressed in the later section of this paper.

THE FUTURE OPERATIONAL ENVIRONMENT

The National Intelligence Council (NIC) has recently published works that help to project and estimate probable trends exhibited in today's operational environment that will help to shape such in the future, providing world scenarios based on those prognostications. Within its work *Global Trends 2030*, it details four 'megatrends' that will impact the global operational theater greatly- individual empowerment, diffusion of power, demographic patterns, and the food, water, energy nexus.[57]

Based on its projections, individual empowerment will hasten through the use of widening means of communication and technology. This will help lead to the diffusion of power as power shifts in a multipolar world to networks and coalitions versus that of the previously prominent hegemonic authority. Both of these megatrends will contribute to the operation of asymmetric warfare mechanisms as it will allow the means to inflict damage that was only previously accessible by state actors while also increasing competition amongst nation-states who will turn to those activities in order to better shape outcomes to their favor.[58] In order to best achieve viable solutions to long-standing issues, the possibilities that the asymmetric threat will continue to evolve and increase in scope, specifically within the multi-domain , must be considered. This will help to best keep any aspects of intelligence reform current and applicable to contemporary asymmetric operational scenarios.

The projected operational environment is one that crosses several domains and therefore there are several factors that must be taken into account when conducting this level

[57] NATIONAL INTELLIGENCE COUNCIL., *GLOBAL TRENDS 2030* ([S.l.]: U S GOVT PRINTING OFFICE, 2013).
[58] NATIONAL INTELLIGENCE COUNCIL., *GLOBAL TRENDS 2030* ([S.l.]: U S GOVT PRINTING OFFICE, 2013).

of exploratory analysis to maintain a context for doctrine and organizational structure recommendations. The Department of Defense has focused efforts on developing doctrine that tackles the problem set that presents itself when adversaries are able to contest the joint force in all multiple domains.[59]

The forecasted operational environment, by nature, will be contested across all five domains (air, land, maritime, space, and cyberspace) and will require a comprehensive and joint response from the intelligence community. Examples of this multi-domain operational environment can be gleaned from current conflicts around the globe. Specifically, the conflict in the Donbass region of the Ukraine provides a glimpse of what near-peer multi-domain conflict will look like and the devastating effects it can have. Russia has used a variety of techniques and tactics in each domain and is consistently innovating new ways to use the domains to gain an advantage.

This multi-domain initiative was put on display July 11, 2014 outside the village of Zelenopillya, A brigade of armored Ukrainian forces were consolidating gains after a successful offensive operation against separatists in the area. The Ukrainian armored units were preparing to begin an enforcement operation along the Ukrainian/Russian border that aimed to cut the separatists off from their Russian support areas. Utilizing unmanned aerial systems (UAS), the separatists were able to identify and relay the location of several columns of Ukrainian armor to Russian artillery and rocket units.[60] Russia's prosecution of the Ukrainian armor forces was devastatingly lethal, essentially neutralizing an entire Ukrainian

[59] Fox, MAJ Amos C. *Hybrid Warfare: The 21st Century Russian Way of Warfare*. Master's thesis, School of Advanced Military Studies, 2017. United States Army Command and General Staff College.
[60] Fox, MAJ Amos C. *Hybrid Warfare: The 21st Century Russian Way of Warfare*. Master's thesis, School of Advanced Military Studies, 2017. United States Army Command and General Staff College.

Armored Brigade in under three minutes. Estimated by analysts to have taken less than 15 minutes from the time the separatists passed the target locations using off-the-shelf drones to the time that conventional uniformed Russian forces fired their multi-launch rocket system (MLRS) with dual-purpose improved conventional munition (DPICM), anti-tank submunitions, and thermobaric explosives.[61] The ability of the separatists to use readily accessible technology to assist the Russians in mass destruction seems rudimentary, yet in practice is an extremely sophisticated and deliberate operation. It is important to note that in this particular instance, the Russian-backed targeting process took place across three domains; air, land, and cyber.

The attack at Zelenopillya, along with subsequent Russian attacks, has shown that this event was not an anomaly. In fact, it is proving to a be a continuation in a trend upward of multi-domain warfare. The ability for adversaries to coordinate attacks across all five domains is a constant threat in the current operational environment.

Another specific example drawn from the Ukrainian conflict is the ability of Russian supported separatists to leverage their advantage in four of the five domains to engage the Ukrainian military. In a particularly diabolical method, the separatists used the cyber/electronic domain to send text messages to the Ukrainian military that they had been surrounded. Subsequently, they sent messages to the families of Ukrainian units that they were targeting; these messages stated that the families' loved ones had died and were remitted with the intent of either party generating phone traffic with the other. Russians then leveraged their assets that can collect on the cyber and electronic domain to gauge the spike

[61] Fox, MAJ Amos C. *Hybrid Warfare: The 21st Century Russian Way of Warfare*. Master's thesis, School of Advanced Military Studies, 2017. United States Army Command and General Staff College.

in electrometric signature in the suspected Ukrainian unit locations.[62] Using UAS, the Russian's engaged the Ukrainians with an artillery strike. This effort of targeting mirrors the U.S. Army's targeting process Decide, Detect, Delivery, and Assess (D3A) and shows a sophistication and willingness to leverage asymmetric tactics and techniques to engage targets.[63] This multi-domain operational environment provides almost unlimited combinations for adversaries to gain advantages. Therefore, it becomes critical that the joint intelligence community develop methods and institutions that can process data collected from each of the five domains.

MILITARY INTELLIGENCE OPERATIONS AND JOINT INTELLIGENCE CENTERS IN THE FIGHT AGAINST THE ASYMMETRIC ADVERSARY

The process of reach back intelligence and the increased use of the JIC in support of reach back activities are a fairly new approach to today's unconventional threats. The ability of intelligence entities within the military, specifically that of S-2, to meet the expectations of battalion commanders has become increasingly difficult with the increasing decentralization of our adversaries. Reach back intelligence support helps to bridge this gap by providing operational military forces another prospect for gathering and use of national IC assets. This information can be used to assess and assist in current situations within tactical intelligence operations, specifically as it relates to military intelligence activity.[64]

---

[62] Fox, MAJ Amos C. *Hybrid Warfare: The 21st Century Russian Way of Warfare*. Master's thesis, School of Advanced Military Studies, 2017. United States Army Command and General Staff College.
[63] Targeting, Headquarters, Department of the Army § ATP 3-60 (FM 3-60) (2015). https://fas.org/irp/doddir/army/atp3-60.pdf
[64] Phillip Radzikowski, *'Reach Back'- A New Approach To Asymmetrical Warfare Intelligence*, eBook (ARMY, 2008), https://www.ausa.org/sites/default/files/FC_Radzikowski_1208.pdf.

In a recent qualitative report of the success of reach back intelligence operations, the Joint Improvised Explosive Device Defeat Organization (JIEDDO) and the later-conceived Counter-IED operations Integration Center (COIC) were studied to see how the use of reach-back support effected operations directly related to Improvised Explosive Devices (IEDs). This report took a closer look at the process as it related to JIEDDO and COIC operations and identified how RFS and intelligence products may vary according to immediate need; this type of research is useful when examining the influence of reach-back support on the fight against the asymmetric threat, as IEDs contribute to the TTP and operational environment provided by insurgency and asymmetric adversaries. JIEDDO was created in 2003 by the DoD in an effort to "defeat the IED as a weapon of strategic influence".[65] The creation of JIEDDO only led to further evolution of the TTP of use of the IED as an insurgency weapon; therefore in 2006, JIEDDO created the COIC in order to add a realm of intelligence support to the tactical activity that it already provided. COIC operates much like a JIC in its use of RFS and its process for analysis and dissemination of collected data in support of forward deployed operations. Intelligence data is used in this process in an effort to establish patterns and trends of insurgencies to those on the front lines for use in tactical operations.

The report determined that RFS to COIC would most likely vary according to a multitude of factors involved in a particular hostile situation. A unit who is has left its "traditional area of responsibility" will request this type of support in order to gain a better understanding of the new operational environment; this typically means that the type of RFS

[65] Phillip Radzikowski, *'Reach Back'- A New Approach To Asymmetrical Warfare Intelligence*, eBook (ARMY, 2008), https://www.ausa.org/sites/default/files/FC_Radzikowski_1208.pdf.

from neoteric tactical units will differ from RFS that come from established and matured units, who in turn have helped to provide much needed atmospherics to COIC for future support activity.[66] The longer standing units' requests differ in that they are not usually sent as an appeal for initial battlefield preparation, but rather are necessitated as a way to bridge gaps in their own intelligence data.[67]

The report also points to RSF that are in response to immediate need based on significant happenings that may arise on the battlefield. RSF of this nature are designed to acquire immediate intelligence data in relation to the area and circumstances surrounding the attack itself. For example, an attack on U.S. forces by an insurgency group (i.e. U.S. casualty due to IED attack) may require intelligence on ingress/egress routes from the attack. This results in what is known as a 'surge' of intelligence by the COIC to turn stored data and information into immediately actionable intelligence.[68] The report also reflects on the ease in which the COIC can be used in its support of military forces on the ground. The SIPRNET is used for the majority of its RSF through various and useful apparatus that are available through agency-ran secure sites.

Modern day joint intelligence operations and its role in military operations is currently outlined in JP-2_01. This doctrine outlines the objective of such operations in its support of military operations to provide an understanding of the operational environment

[66] Phillip Radzikowski, *'Reach Back'- A New Approach To Asymmetrical Warfare Intelligence*, eBook (ARMY, 2008), https://www.ausa.org/sites/default/files/FC_Radzikowski_1208.pdf.
[67] Phillip Radzikowski, *'Reach Back'- A New Approach To Asymmetrical Warfare Intelligence*, eBook (ARMY, 2008), https://www.ausa.org/sites/default/files/FC_Radzikowski_1208.pdf.
[68] Phillip Radzikowski, *'Reach Back'- A New Approach To Asymmetrical Warfare Intelligence*, eBook (ARMY, 2008), https://www.ausa.org/sites/default/files/FC_Radzikowski_1208.pdf.

through the timely provision of accurate intelligence to commanders.[69] Current joint intelligence operations not only focus on support of forward deployed units, but also maintain intelligence activities in informational operations, cyberspace operations, and in further examination of a multitude of factors that affect operational environments. This enables it to serve as "the single focal point for crisis intelligence support to national and theater decision makers, along with managing the worldwide defense warning system".[70] The use of JICs help to integrate the various "INTs" involved in intelligence operations as many agencies are utilized in support of particular "INT" operations rather than as a collective source of support. Currently, Joint Intelligence Centers (and Joint Operations Intelligence Centers- JOICs) are available at the COCOM level up to the National Joint Operations and Intelligence Center (NJOIC) with the COCOM JOICs integrating all DoD intelligence from external IC sources and defense organizations, non-governmental organizations (NGOs), and other Law Enforcement Agencies in order to best incorporate all assets in order to best provide intelligence support. Operational-level JOICs are implemented in situations in which a sustained operation is being conducted.[71] If this level of JOIC is necessitated, it may be required that subject matter experts (SMEs) be deployed in ground-level support of operations. Furthermore, the DIA, as the largest military-based intelligence analytical organization and acting as the head of the JICs, has made significant advancements in helping to reduce duplicity and redundancy in intelligence analysis and product

[69] *Joint Publication 2-01 | Joint And National Intelligence Support To Military Operations*, eBook (Washington, D.C: Office of the Joint Chiefs of Staff, 2017), https://fas.org/irp/doddir/dod/jp2_01.pdf.
[70] *Joint Publication 2-01 | Joint And National Intelligence Support To Military Operations*, eBook (Washington, D.C: Office of the Joint Chiefs of Staff, 2017), https://fas.org/irp/doddir/dod/jp2_01.pdf.
[71] *Joint Publication 2-01 | Joint And National Intelligence Support To Military Operations*, eBook (Washington, D.C: Office of the Joint Chiefs of Staff, 2017), https://fas.org/irp/doddir/dod/jp2_01.pdf.

dissemination within the military intelligence world.[72] The development of the Joint Military Intelligence Program (JMIP), is designed to address the needs of defense-wide intelligence operations rather than the needs of one military branch or service.[73] Large issues remain however, as "*dividing lines between the DIA's analytical responsibilities and those of the military departments remain blurred despite the agreed-on production process".*[74]

In an American Intelligence Journal study by Lou Anne DeMattei, key challenges that directly effect a JIOC's operation were addressed. While the original study acknowledges and examines both individual and organizational issues within the JIOC, for the purposes of this study, focus will be on the organizational factors addressed. The primary challenge that was discovered within the JIOC is enveloped in the organizational management processes and their ability to quickly assemble task-oriented teams efficiently. As DeMattei points out, this aspect of intelligence operations is similar in nature to management functions, and the inability to "*identify, apply, and develop individual skills and talents directly affects continuous knowledge creation… at the organizational level."*[75]

This in itself leads to issues that reduce the efficiency of the JIOC. Task-oriented teams in operational settings are, by nature, geographically dispersed, yet they must coordinate and collaborate on a regular and continuous basis. In order to achieve this, virtual

[72] Brown, Harold, and A. Aspin. "Aspin Brown Report on the Intelligence Community." *The Commission on the Roles and Capabilities of the US Intelligence Community*. https://www.govinfo.gov/content/pkg/GPO-INTELLIGENCE/html/int014.html.
[73] *Commission of the Roles and Capabilities of the Defense Intelligence Agency a*. Report no. 011. Archives, USAF Air University. USAF AU.
[74] Brown, Harold, and A. Aspin. "Aspin Brown Report on the Intelligence Community." *The Commission on the Roles and Capabilities of the US Intelligence Community*. https://www.govinfo.gov/content/pkg/GPO-INTELLIGENCE/html/int014.html.
[75] DeMattei, Lou Anne. "Knowledge Management in Joint Intelligence Operations Centers." *American Intelligence Journal*31, no. 2 (2013): 96-102. doi:10.1016/j.intman.2013.03.009.

teaming approaches and technologies are used, yet require significant administrative overhead for coordination and scheduling. Often this must be coordinated through multiple military branches in order to offer the best data for the operational environment.[76] The issue lies in the efficiency of the process and the lack of timeliness it contributes. This method does not enable on-the-spot and continuous contact and cannot be independently initiated; therefore, it severely limits the ability to denote the collective understanding of the team in its entirety. De Mattei explains the issue best, as she explains "*Because JIOC operations rely heavily on structured, scheduled, and continuous interaction…it constrains JIOC potential to optimize knowledge and intelligence dissimenation, and can engender a fragmented and chaotic rather than integrated knowledge creation environment",* negatively affecting the reach back intelligence process.[77]

OTHER ISSUES WITH REACH BACK INTELLIGENCE & THE USE OF JOINT INTELLIGENCE CENTERS

Intelligence analysis conducted at the strategic, operational, and tactical levels (i.e. military intel) will, by nature, receive the burden of carrying a bad reputation for operations gone wrong. Ultimately, it is the Commander, not the intel officers, who are held responsible for the decisions and orders they make. "Bad intel" is often blamed for skewing the Commander's decision; however, a couple of variables need to be kept in perspective. Operational decisions will often lead to second and third order effects that can be hard to

[76] DeMattei, Lou Anne. "Knowledge Management in Joint Intelligence Operations Centers." *American Intelligence Journal*31, no. 2 (2013): 96-102. doi:10.1016/j.intman.2013.03.009.
[77] DeMattei, Lou Anne. "Knowledge Management in Joint Intelligence Operations Centers." *American Intelligence Journal* 31, no. 2 (2013): 96-102. doi:10.1016/j.intman.2013.03.009.

anticipate, especially in the realm of asymmetric threat. As General Mattis reminds us, the enemy always has a vote.[78]

When operations go wrong, intelligence agencies, including those involved in military intelligence activities, becomes the perceived "catch-all" excuse to the public for what is really a widespread ignorance on how intelligence feeds a commander's decision-making process. Military intel in operations begins with the "running estimate" consisting of "effects of key terrain and weather, impact of civil considerations on operations, significant cultural factors, threat intent, threat courses of actions, etc.…[79] Running estimates are developed by the intelligence analysts on staff and are used to help develop the battlefield. The intelligence preparation of the battlefield (IPB) will then be used by all other war-fighting functions to drive their respective planning processes. A flawed IPB can doom an operation; yet, it is important to note that the IPB is 'interpreted' by operational planners for its effects on their war-fighting functions.

A specific example of this would be the establishment of a Commander's Critical Information Requirements (CCIR) and how they drive priority information requirements (PIR).[80] At the tactical level, intel analysts must focus on supporting the commander and are responsible for developing priority information requirements that assist in answering questions that will drive the commander's decision-making process. In essence, if a

[78] Tim Ball, "Replaced? Security Force Assistance Brigades Vs. Special Forces", *Texas National Security Network*, 2017, https://warontherocks.com/2017/02/replaced-security-force-assistance-brigades-vs-special-forces/.
[79] *Joint Publication 2-01 | Joint And National Intelligence Support To Military Operations*, eBook (Washington, D.C: Office of the Joint Chiefs of Staff, 2017), https://fas.org/irp/doddir/dod/jp2_01.pdf.
[80] *Joint Publication 2-01 | Joint And National Intelligence Support To Military Operations*, eBook (Washington, D.C: Office of the Joint Chiefs of Staff, 2017), https://fas.org/irp/doddir/dod/jp2_01.pdf.

commander and their staff select the wrong course of action, their CCIRs will drive the intel analysts to develop flawed PIRs that are not answering the “right” questions.

While looking at data management for JICs, there are various policies and practices that are implemented by DST and SMEs within the organization. The primary reason for this is the conglomeration of personnel from a multitude of agencies in support of forward deployed operations. The varied training of different policies and practices to those involved in JICs will, by nature, create vulnerabilities in the “translation” of disseminated information to various military branches. This is also an important factor to note, as the various branches of the military also provide their own doctrine and operational procedures along with the implementation of joint doctrine. This can lead to further issues of translation in circumstances where intelligence coming from reach-back intelligence support operations is used. The lack of the ability to create common data sources can negatively affect plan capability, integration of activity, and overall access for results. The lack of knowledge of the systems in play within the various areas of intelligence collection and analysis can also cause sharing issues, creating a delay in the proper dissemination of desired intelligence from forward deployed units.

INHERENT CHALLENGES TO INTELLIGENCE OPERATIONS

There are, by nature, inherent challenges and issues that arise when any intelligence operations, or change to the process of these operations, are put into motion. Some of these challenges are related specifically to the mission set or process of the intelligence

community; others are challenges that face nearly all complex organizations regardless of their base purpose, i.e. issues within its structure.[81]

Many of the issues found in intelligence operations stem from deficiencies in integration, which in turn lead to short comings in several aspects of the intelligence process-coordination, collection, analysis, information sharing, the relationship between the intelligence and policy communities, congressional oversight, personnel policies, and innovative ideas. These challenges affect infrastructure, agency administrations, and transparency among various IC affiliates. Many of the other issues that face intelligence operations stem directly from these shortcomings of the system. These same deficiencies are present in military intelligence operations as they are inherently similar.

One such challenge is that of preventing the groupthink phenomena. In former community analyses (i.e. examination of the Iraq WMD assessments), all oversight committees involved pointed to the ubiquitous problem of groupthink as a major contributor to issues within the IC.[82] This common phenomena occurs when analysts lapse too readily into agreement based on the vague intellectual notion of a majority.[83] As mentioned previously, intelligence oriented organizations tend to receive the blame for failed and negatively perceived military operations, or other national security issues. Recommendations that are deemed out-of-the-box or radical are often overlooked and ignored in deference to more commonly agreed upon and traditional ideals; a tendency which sometimes causes some intelligence analysts to share more information that coincides with the desired

[81] Patrick Neary, "Intelligence Reform, 2001-2009: Requiescat In Pace?", *Studies In Intelligence* 54, no. 1 (2010), https://nsarchive2.gwu.edu//NSAEBB/NSAEBB370/docs/Document%207.pdf.
[82] J. Tama, *Intelligence Reform: Progress, Remaining Deficiencies, And Next Steps*, eBook (Princeton University, 2005), https://www.princeton.edu/~ppns/papers/intel_reform.pdf.
[83] M. Lowenthal, *Intelligence: From Secrets To Policy* (Washington, DC: CQ Press, 2000).

consensus views.[84] This can cause important and critical intelligence data to slip through the cracks and is a major weakness in the current system as it is designed to protect national security and contributes to the inherent issues of groupthink incidents.[85]

The groupthink phenomena extends past common bureaucratic avenues and into the world of military intelligence operations as well. The by-the-book nature of military operations in general create the perfect environment for groupthink to influence the intelligence process. Collective rationalization and stereotypes of out-groups can lead to an intrinsic fallacy within the military intelligence operation and the correspondence of doctrine. There lies a tendency amongst those in policy support operations to 'appease the masses' as the very jobs they are trusted to do are at risk if the are deemed as going against the grain. Self-censorship and an illusion of unanimity is facilitated through direct pressure being placed on dissenters by policymakers and other peoples of influence to support the standing of those in power. This push to conform can contribute to defective decision-making and faulty military intelligence operations. When exhibited to this fashion, groupthink can have a great and overwhelming impact on the reach back intelligence process as the intelligence

product disseminated to those in need is faulty from the beginning, leading to a domino effect that will affect operations all the way down to a tactical level.

Yet another intrinsic challenge that faces the intelligence operations and that must be considered when investigating options of any intelligence reform, is that of collection or analytical stove piping. This refers to the tendency of agencies or branches in analogous lines

[84] Tom Cohen, "Tsarnaev Case Raises Questions About Post 9/11 Intelligence Reforms - Cnnpolitics", *CNN*, 2013, http://www.cnn.com/2013/04/24/politics/boston-fbi-russia/.
[85] Cortney Weinbaum et al., "Perspectives and Opportunities in Intelligence for U.S. Leaders," *Perspective: Expert Insights on a Timely Policy Issue.* September 2018. Doi:10.7249/pe287.

of work to compete with one another, often to a wasteful and harmful degree.[86] Stove piping can be further compounded through what is deemed as "stovepipes within stovepipes", an aggregate competitive effect that takes place as separate programs and processes work independently from one another within the same discipline or branch.[87] Although this is, in part, the natural result of the compartmentalization of various programs, it worsens the stovepipe issue, making cross-agency, or in the instance of military intelligence activities cross-branch, strategies increasingly difficult.[88]

While it is acknowledged that the stovepiping issue does not impact modern-day military intelligence operations to the degree that groupthink does, exacerbating the stovepipe issue is the duplication of effort that may derive from such compartmentalization. It stands to reason that without joint collaboration, responses to collection and/or production tasks may not be systemized into one location (i.e. the JIC) leading to issues in obtaining the information through the reach back intelligence process. This also leads to further problems as individual branch intelligence units may provide different answers to the same sets of questions that spurred the collection of particular intelligence and adding another layer of stovepipe issues to the intelligence process.[89]

RECOMMENDATIONS BASED ON THESE FINDINGS:

Expanding on the idea of integration and implementing action more influential to the operational level in asymmetric warfare, there should be more integration amongst the

[86] M. Lowenthal, *Intelligence: From Secrets To Policy* (Washington, DC: CQ Press, 2000).
[87] M. Lowenthal, *Intelligence: From Secrets To Policy* (Washington, DC: CQ Press, 2000).
[88] J. Tama, *Intelligence Reform: Progress, Remaining Deficiencies, And Next Steps*, eBook (Princeton University, 2005), https://www.princeton.edu/~ppns/papers/intel_reform.pdf.
[89] Cortney Weinbaum et al., "Perspectives and Opportunities in Intelligence for U.S. Leaders," *Perspective: Expert Insights on a Timely Policy Issue.* September 2018. Doi:10.7249/pe287.

intelligence services of the various military branches. Currently, each branch of the Armed Forces has its own intelligence unit, operating to some degree under the DIA. While there is an overlying standard of operation guidelines disseminated to the various groups, and also acknowledging the expansion of the control of the DIA in recent reformation measures, each branch's intelligence unit is largely left to its own devices when in actual operation, especially at a tactical level. This creates a void between intel units within the realms of language, doctrine, and other areas of importance that are not specifically outlined within the parameters of joint doctrine.

While it is NOT suggested that these agencies converge into one singular cohesive unit, it is believed that the DIA should be given the responsibility to set more detailed, standardized operational and analytical techniques for collection and analysis purposes.[90] Put simply, the DIA should be made into a central "hub" of military intelligence, beyond the current operational use of the JIC. Not only would this action increase the degree of sharing amongst the military service branches, it will also assist in the necessary "translation" of collected data between branches that operate of different doctrine and require them to meet a higher quality standard than what is currently necessitated and beyond the requirements of the NMJIC in its current construct.

Policy, procedures, and overall capabilities of JICs must be studied and analyzed on a deeper level in order to determine the need for review and update for policies, procedures, technical actions for sorting, accessing, sharing, and managing intelligence data. The difficulty in finding studies involving the success or faults of JICs in their current state of

[90] D. Shedd and M.F. Ferraro, "Intelligence Reform 2.0", *Defense One*, 2015, http://www.defenseone.com/ideas/2015/04/intelligence-reform-20/110659/.

affairs points to a need for this type of revamp; however, in the scope of this study, it was unrealistic to delve that far into discovery of solutions to the weaknesses of JICs as they stand. This limitation in study constraints will be further acknowledged in the suggestions for future research. It is currently acknowledged, however, that a complete standardization of intelligence and operational data, as well as a standardization of the methods of accessibility to such system data, between the various commands worldwide that effect and impact global/regional plans would help to reduce problems within JICs in their current state. It is also noted that the diminishment of over-classification in intelligence operations would also help streamline the process of reach-back support and applicable operations within JICs, allowing for more efficient and effective intelligence support to forward deployed military operations.

In order to better understand the asymmetric adversary that our military now faces, there must be a stronger reliance on cultural intelligence within the joint intelligence doctrinal guidelines. Standard doctrine should be re-written for today's threat, taking into account that a basic comprehension of all foreign peoples attributed to any joint operations area, regardless of times of war or peace, is fundamental as the relationships with the population of an area directly affects knowledge of the enemy.[91] While the use of cultural intelligence is present in today's intelligence products derived from JICs, the basic joint doctrine, as it stands, does not include the importance of cultural intelligence products in its operational guidelines. Guidance must be addressed in these standard principles as it places

[91] Military Intelligence, Intelligence Studies, Intelligence Operations, National Intelligence, Intelligence Analysis, Gateway to Intelligence, Accessed February 2019. https://www.au.af.mil/au/awc/awcgate/awc-ntel.htm

many forces in foreign missions at a cultural disadvantage, causing hiccups in the operational result of the reach-back intelligence process. Adding and enhancing cultural intelligence to the JIPB process will improve both the operational analysis of space and allow combatant commanders to make better resulting decisions on the battlefield.[92] It is important to remember that JFC are experts in military matters and processes, not cultural specialists; the JIC should be used to bridge that knowledge gap in order to boost the use of reach-back intelligence and its assistance in the design of successful courses of action in military operations on the ground.

ISSUES TO CONSIDER IN ALL RECOMMENDATIONS:

As most of the aforementioned recommendations demonstrate, integration is deemed to be key in implementing successful intelligence reform. Yet, it does not go unnoticed that there are instances when a method of decentralization may operate with a better chance of success, especially given the fact that our more recent security threats are decentralized by nature as asymmetric adversaries.[93] The need to coordinate the activities of the IC should not drive reform to create a fully centralized system. Some amount of decentralization is necessary as it allows for a greater miscellany of approaches and perspectives of collection and analysis; a critical step in the promotion of innovation and prevention of groupthink.[94] This being said, the ultimate goal of any intelligence reform should be the advancement and

[92] Weinbaum, Cortney, John Parachini, Richard Girven, Michael Decker, and Richard Baffa. "Perspectives and Opportunities in Intelligence for U.S. Leaders." *Perspective: Expert Insights on a Timely Policy Issue*, September 2018. doi:10.7249/pe287.
[93] R.L. Hutchings, *The Morning After: How To Reform The Intelligence Reform*, eBook (Princeton University, 2007), https://www.princeton.edu/sites/default/files/content/docs/news/HPSCI_120607.pdf.
[94] R.L. Hutchings, *The Morning After: How To Reform The Intelligence Reform*, eBook (Princeton University, 2007), https://www.princeton.edu/sites/default/files/content/docs/news/HPSCI_120607.pdf.

culture of collaboration while granting individual agencies room to pursue national intelligence objectives in the myriad of ways.[95]

LIMITATIONS OF STUDY:

As an exploratory study investigating various areas of the intelligence and military relationship, the research included in this study is limited by subjectivity, the lack of quantifiable data, and unknown information that may affect the results within. Classification of documents related to the operational process of reach-back intelligence created a difficult hurdle when addressing this operational support system; open-source information and previous research reports related to the topic were used in lieu of documents that were unable to be accessed without proper classification status.

One limitation derived when examining the current manifestation of the JIC is the little quantifiable information available publicly to point towards this approach's possibility of success and/or failure. There are few accessible reports and studies available to scrutinize the organizational structure, policies, and procedures associated with JICs in order to determine fault lines of weakness. The study conducted by Lou Anne DeMattei supported this realization by noting on page 96 the "*very limited corpus of scholarly research and systematic empirical evaluation"*[96]*,* and the current research exhibited a shortfall of available information. Many studies into the JIC and its operational success were dated; some beyond a period of twenty years. Due to this fact, many of the suggestions were based on a subjective

[95] R.L. Hutchings, *The Morning After: How To Reform The Intelligence Reform*, eBook (Princeton University, 2007), https://www.princeton.edu/sites/default/files/content/docs/news/HPSCI_120607.pdf.
[96] DeMattei, Lou Anne. "Knowledge Management in Joint Intelligence Operations Centers." *American Intelligence Journal*31, no. 2 (2013). https://www-jstor-org.easydb.angelo.edu/stable/26202080?read-now=1#page_s.

nature rather than on objective studies, as the more current quantifiable studies are inaccessible without clearance. This information usually becomes public after a designated period of time and could contribute to the study in the future. This means that all the data used and collected for research purposes was either unclassified or open sourced.

While noting these limitations, it is not believed that any conclusions or recommendations were negatively impacted; rather they are based on logical and conceptual understandings of current circumstances and pitfalls regarding intelligence and military operations in the fight against the asymmetric threat. These limitations are also negated in suggested efforts for future research.

SUGGESTIONS FOR FUTURE RESEARCH:

It is recommended that each of the specific issues addressed in this paper be individually analyzed through further qualitative study as it is acknowledged that 'success' in the realm of intelligence operations is, by nature, a subjective study. It is acknowledged that by separating the issues addressed here via a thorough and individual study, a deeper and more comprehensive understanding of the intelligence and military relationship would be made, contributing to an effective use of resources and assets in the fight against asymmetric adversaries. This would help to make recommendations to policy change more detailed and easier to codify. It is also recommended that future studies be conducted by researchers with a level of credential that will allow for deeper analysis of classified information in regard to how each of these issues effect intelligence and military operations against the asymmetric threat; this will also help to decrease the level of use of open source information for a study

of this magnitude. This would not only assist in negating the limitations exhibited by this research, it will also help to increase the quality of research in future studies.

It is also suggested that a push for more empirical studies on the operational success of JICs, as well as into the current process of reach back intelligence, be supported in the military intelligence world. Many intelligence officers, as well as active duty military personnel (i.e. Warrant Officers) are required to conduct research and continue to make advancements and suggestions for growth in their respective fields of expertise. There is a need in this area for operational and organizational analysis to be conducted on the JIC in order to assure that action is taken to help boost its operations to the most efficient and effective levels.

REFERENCES

Ball, Tim. "Replaced? Security Force Assistance Brigades Vs. Special Forces", *Texas National Security Network*, 2017, https://warontherocks.com/2017/02/replaced-security-force-assistance-brigades-vs-special-forces/.

Brown, Harold and A. Aspin. "Aspin Brown Report on the Intelligence Community." *The Commission on the Roles and Capabilities of the US Intelligence Community*. https://www.govinfo.gov/content/pkg/GPO-INTELLIGENCE/html/int014.html

Burch, James. "The Domestic Intelligence Gap: Progress Since 9/11? - HOMELAND SECURITY AFFAIRS", *HOMELAND SECURITY AFFAIRS*, 2008, https://www.hsaj.org/articles/129.

Carter, Ashton B. and William J. Perry, *Countering Asymmetric Threats*, eBook (Washington D.C.: The Brookings Institution, 1999), https://www.belfercenter.org/sites/default/files/legacy/files/kte_ch5.pdf.

Coffman, Edward M., Allan R. Millett, and Peter Maslowski. "For the Common Defense: A Military History of the United States of America." *Military Affairs*50, no. 1 (1986): 51. doi:10.2307/1988538.

Cohen, Tom. "Tsarnaev Case Raises Questions About Post 9/11 Intelligence Reforms - Cnnpolitics", *CNN*, 2013, http://www.cnn.com/2013/04/24/politics/boston-fbi-russia/.

Coles, Lt. Commander John P. USN, *Cultural Intelligence & Joint Intelligence Doctrine*, report, Graduate Studies. USAF Air University (USAF AU).

Commission of the Roles and Capabilities of the Defense Intelligence Agency a. Report no. 011. Archives, USAF Air University. USAF AU.

"Congressional Record", *Congress.Gov*, 2004, https://www.congress.gov/crec/2004/09/29/CREC-2004-09-29/pdf.

Daley, Dan. *Asymmetric Warfare: The Only Thing New Is The Tactics*, eBook (Washington D.C.: National War College, 2000), http://www.dtic.mil/dtic/tr/fulltext/u2/a433588.pdf.

DeMattei, Lou Anne. "Knowledge Management in Joint Intelligence Operations Centers." *American Intelligence Journal*31, no. 2 (2013). https://www-jstor-org.easydb.angelo.edu/stable/26202080?read-now=1#page_s

Fox, MAJ Amos C. *Hybrid Warfare: The 21st Century Russian Way of Warfare*. Master's thesis, School of Advanced Military Studies, 2017. United States Army Command and General Staff College.

Hutchings, R.L. *The Morning After: How To Reform The Intelligence Reform*, eBook (Princeton University, 2007), https://www.princeton.edu/sites/default/files/content/docs/news/HPSCI_120607.pdf.

Joint Chiefs of Staff, Joint Publication 1-02 DOD Dictionary Of Military And Associated Terms (Washington, DC: 12 April 2001)

Joint Chiefs of Staff, Joint Publication 2-01.3, Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace (Washington, DC: The Joint Staff, May 24,

2000).

Joint Publication 3-30 | Command And Control Of Joint Air Operations, eBook (Washington D.C.: Office of the Chairman of the Joint Chiefs of Staff, 2014), https://fas.org/irp/doddir/dod/jp3_30.pdf.

Jones, C. *Intelligence Reform: The Logic Of Information Sharing*, eBook (University of Maryland, 2016), http://gvpt.umd.edu/sites/gvpt.umd.edu/files/pubs/Jones_IntellReform.pdf.

Lowenthal, M. *Intelligence: From Secrets To Policy* (Washington, DC: CQ Press, 2000).

McDonnel, Janet A. *Adapting to a Changing Environment: Defense Intelligence Agency in the 1990s*. DIA Historical Research Division. Defense Intelligence Historical Perspectives. 2013. http://www.dia.mil/Portals/27/Documents/About/History/HistoricalPerspectiveVol3_Web.pdf.

Metz, Janet A. and Douglas Johnson II, *Asymmetry And U.S. Military Strategy: Definition, Background, And Strategic Concepts*, eBook (repr., Carlisle, PA: Strategic Army War College, 2001), http://ssi.armywarcollege.edu/pdffiles/PUB223.pdf.

Military Intelligence, Intelligence Studies, Intelligence Operations, National Intelligence, Intelligence Analysis, Gateway to Intelligence. 1. accessed February 2019. https://www.au.af.mil/au/awc/awcgate/awc-ntel.htm

NATIONAL INTELLIGENCE COUNCIL., *GLOBAL TRENDS 2030* ([S.l.]: U S GOVT PRINTING OFFICE, 2013).

Neary, Patrick. "Intelligence Reform, 2001-2009: Requiescat In Pace?", *Studies In Intelligence* 54, no. 1 (2010), https://nsarchive2.gwu.edu//NSAEBB/NSAEBB370/docs/Document%207.pdf.

Oakley, David. "Adapting To Change: Strategic Turning Points And The CIA/Dod Relationship", *Interagency Journal* 5, no. 1 (2014), http://thesimonscenter.org/wp-content/uploads/2014/03/IAJ-5-1Winter-2014-3-11.pdf

Pike, John. "FM 3-11.22 Appendix G, Reach-Back Capability And Federal Response Assets", *Globalsecurity.Org*, 2018, https://www.globalsecurity.org/security/library/policy/army/fm/3-11-22/appg.htm

Radzikowski, Phillip .*'Reach Back'- A New Approach To Asymmetrical Warfare Intelligence*, eBook (ARMY, 2008), https://www.ausa.org/sites/default/files/FC_Radzikowski_1208.pdf.

Rathmell, Andrew. "Towards Postmodern Intelligence," *Intelligence and National Security* 17, no. 3 (2002): , doi:10.1080/02684520412331306560.

Report of Intelligence Activities in the Pacific Ocean Areas, report, Archives, Joint Forces Staff College, US Pacific and Pacific Ocean Areas.

Rosenbach, Eric and A. J. Peritz. "Intelligence Reform | Belfer Center For Science And International Affairs", *Belfercenter.Ksg.Harvard.Edu*, 2009, http://belfercenter.ksg.harvard.edu/publication/19154/intelligence_reform.html.

Shedd, D. and M.F. Ferraro. "Intelligence Reform 2.0", *Defense One*, 2015, http://www.defenseone.com/ideas/2015/04/intelligence-reform-20/110659/.

Sun, Ben, Ken Langdon and Karen McCreadie. *Sun Tzu's The Art Of War* (Oxford: Infinite Ideas, 2008).

Tama, J. *Intelligence Reform: Progress, Remaining Deficiencies, And Next Steps*, eBook (Princeton University, 2005), https://www.princeton.edu/~ppns/papers/intel_reform.pdf.

Targeting, Headquarters, Department of the Army § ATP 3-60 (FM 3-60) (2015). https://fas.org/irp/doddir/army/atp3-60.pdf

"The Evolution And Relevance Of Joint Intelligence Centers — Central Intelligence Agency", *Cia.Gov*, 2018, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol49no1/html_files/the_evolution_6.html.

Thornton, Rod. *Asymmetric Warfare* (Cambridge: Polity Press, 2008).

Watts, Larry. "Intelligence Reform In Europe's Emerging Democracies", *Cia.Gov*, 2007, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no1/article02.html.

Weinbaum, Cortney, John Parachini, Richard Girven, Michael Decker, and Richard Baffa. "Perspectives and Opportunities in Intelligence for U.S. Leaders." *Perspective: Expert Insights on a Timely Policy Issue*, September 2018. doi:10.7249/pe287.

BIOGRAPHY

Heather Marie Port was born in Fayetteville, North Carolina and raised in the smaller suburb town of Hope Mills. Her mother is a former banker and her father is a retired CW3 and former Green Beret, currently working with USASOC. She has a younger sister, Jessica Stephenson, who is an elementary school teacher.

Heather attended South View High School, where she graduated in 2003. She continued her education at Fayetteville Technical Community College, transferring to Fayetteville State University in 2005. After three years of attending school, Heather took a brief hiatus from her educational career. During this time, she received her North Carolina Emergency Medical Technician- Basic Certification. She returned to Fayetteville State University in 2015 and graduated with her Bachelor of Arts in Political Science in May 2016. She started attending Angelo State University through its online graduate program in August 2016 in pursuit of a Master of Arts in Intelligence, Security Studies, and Analysis. Here, she thrived in her studies, earning an invitation into The Order of the Sword and Shield, a National Honor Society dedicated to those in the fields of Homeland Security, Intelligence Studies, and all other protective security disciplines. Her estimated date of graduation is May 2019.

Heather now resides with her husband, Tanner Port, and their three daughters in Fort Wainwright, Alaska where her husband currently serves in the U.S. Army. Preferring the country life and with a plan to return to it, Heather's permanent mailing address for correspondence related to this thesis is listed as 421 Halltown Road, Autryville, NC, 28318.