NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DEFINING CONDITIONS FOR THE USE OF PERSISTENT SURVEILLANCE

by

Cristina Cameron Fekkes

December 2009

Thesis Advisor:	Erik Dahl
Second Reader:	Nancy Roberts

Approved for public release; distribution is unlimited

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE December 2009	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE Defining Conditions for the Use of Persistent Surveillance	5. FUNDING NUMBERS
6. AUTHOR(S) Cristina Cameron Fekkes	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

Currently, there exists no full definition of persistent surveillance in joint doctrine that allows a clear distinction between persistent and non-persistent collection requirements for collection managers to properly resource surveillance assets. The Joint Forces Command (JFCOM) Joint Concept Development & Experimentation Directorate (J9) attempts to alleviate this shortfall by proposing a definition: "Persistent Surveillance: an operationally focused surveillance approach that uses a full range of strategic, operational and tactical collection methods to dwell on and revisit a target. Persistent surveillance contributes to the detection and recognition of meaningful changes in an adversary's activities that support planning and executing preemptive actions to prevent likely adversary courses of action."

The issue with this definition, as with all current definitions, is the lack of precision in defining what circumstances warrant the use of persistent surveillance. In addition, currently there are no quantifying metrics to determine effectiveness of intelligence, surveillance, and reconnaissance (ISR) collection for the use of the persistent surveillance concept (i.e., metrics to show the duration an asset loiters over a target area and the success rate of meeting mission objectives during this time). Without a clear and distinct definition, and metrics, the concept of allocating assets for collection managers to perform persistent surveillance becomes ambiguous. This thesis is to determine key conditions for allocating the use of persistent surveillance through historical analysis of the use of persistent surveillance between the concept's introduction in the 2001 Quadrennial Defense Review (QDR) and the evolution following the 2006 QDR, when the concept of persistent surveillance was actually declared an operational capability that was vital to the mission in Iraq. This thesis will perform a historical case study on the evolution of persistent surveillance in U.S. Central Command in order to build a more precise definition and allow for better use of persistent surveillance in future military operations.

14. SUBJECT TERMS Persistent Surveillance	15. NUMBER OF PAGES 83
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01–280–5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

DEFINING CONDITIONS FOR THE USE OF PERSISTENT SURVEILLANCE

Cristina Cameron Fekkes
Major, United States Air Force
B.A. Political Science, Pepperdine University, 1995
M.A. Leadership Studies, University of San Diego, 1998

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(DEFENSE DECISION MAKING AND PLANNING)

from the

NAVAL POSTGRADUATE SCHOOL
December 2009

Author: Cristina Cameron Fekkes

Approved by: Erik Dahl
Thesis Advisor

Nancy Roberts
Second Reader

Harold A. Trinkunas, PhD
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Currently, there exists no full definition of persistent surveillance in joint doctrine that allows a clear distinction between persistent and non-persistent collection requirements for collection managers to properly resource surveillance assets. The Joint Forces Command (JFCOM) Joint Concept Development & Experimentation Directorate (J9) attempts to alleviate this shortfall by proposing a definition: "Persistent Surveillance: an operationally focused surveillance approach that uses a full range of strategic, operational and tactical collection methods to dwell on and revisit a target. Persistent surveillance contributes to the detection and recognition of meaningful changes in an adversary's activities that support planning and executing preemptive actions to prevent likely adversary courses of action."

The issue with this definition, as with all current definitions, is the lack of precision in defining what circumstances warrant the use of persistent surveillance. In addition, currently there are no quantifying metrics to determine effectiveness of intelligence, surveillance, and reconnaissance (ISR) collection for the use of the persistent surveillance concept (i.e., metrics to show the duration an asset loiters over a target area and the success rate of meeting mission objectives during this time). Without a clear and distinct definition, and metrics, the concept of allocating assets for collection managers to perform persistent surveillance becomes ambiguous. This thesis is to determine key conditions for allocating the use of persistent surveillance through historical analysis of the use of persistent surveillance between the concept's introduction in the 2001 Quadrennial Defense Review (QDR) and the evolution following the 2006 QDR, when the concept of persistent surveillance was actually declared an operational capability that was vital to the mission in Iraq. This thesis will perform a historical case study on the evolution of persistent surveillance in U.S. Central Command in order to build a more precise definition and allow for better use of persistent surveillance in future military operations.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

BCT	Brigade Combat Team
CCIR	Commander's Critical Information Requirements
CENTCOM	U.S. Central Command
COCOM	Combatant Command
CSIS	Center for Strategic International Studies
DIA	Defense Intelligence Agency
DNI	Director of National Intelligence
DoD	Department of Defense
EEI	Essential Elements of Information
FAA	Federal Aviation Agency
GEOINT	Geospatial Intelligence
IED	Improvised Explosive Device
IPL	Integrated Priority List
ISR	Intelligence, Surveillance, and Reconnaissance
JFC	Joint Force Commander
JFCOM	Joint Force Command
JIC	Joint Integrating Concept
JIEDDO	Joint Improvised Explosive Devise Defeat Organization
J9	Joint Concept Development & Experimentation Directorate
OEF	Operation ENDURING FREEDOM
OIF	Operation IRAQI FREEDOM
PIR	Priority Intelligence Requirement
QDR	Quadrennial Defense Review

QRM	Quadrennial Review of Defense Roles and Missions
RFI	Request for Information
TF ODIN	Task Force Observe, Detect, Identify and Neutralize
TPED	Tasking, Processing, Exploitation, and Dissemination

ACKNOWLEDGMENTS

I would like to thank Dr. Erik Dahl and Dr. Nancy Roberts for all of their support and time in helping me through this process. My deepest appreciation goes to my family for their patience, with a special thank you to Major William Lussier for all of his time during the final hours of getting this project completed.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PERSISTENT SURVEILLANCE

The eighteenth-century utilitarian philosopher Jeremy Bentham envisioned the perfect environment for watching over convicts using persistent surveillance. The design was known as the "panopticon," and it allowed constant surveillance by prison guards unbeknownst to inmates.[1] The panopticon design placed prisoners in cells around a central observation tower. From the tower, convicts could be watched, but could not see who was watching. The architectural design of using surveillance as a threat, Bentham believed, was enough to compel prisoners to behave to the point that actual observation would most likely be unnecessary. Bentham also believed that the concept of persistent surveillance would not only grant unrestrained power to observe whenever desired, but would indirectly lead to the power to control actual behavior of those being watched.

The ideology behind panopticons was not fully appreciated during Bentham's time. Ironically, two centuries later a parallel ideology of persistent surveillance is eagerly being sought by military strategists. Information gained through the use of persistent surveillance is believed essential for U.S. forces against adversarial challenges faced in twenty-first-century warfare.

B. THE PROBLEM

In March of 2007, the Joint Integrating Concept (JIC) for *Intelligence, Persistent Intelligence, Surveillance, and Reconnaissance: Planning and Direction* identified future military operations in the 2014-2026 timeframe: missions that would "require persistence to find, identify, track and determine intent of elusive adversary targets."[2] The JIC indicated that increases in sophisticated denial and deception techniques by adversaries were expected to rise in the future, along with adversaries taking advantage of optimizing

1 Jeremy Bentham, Panopticon (Preface), in Miran Bozovic (ed.), The Panopticon Writings, (London: Verso, 1995), 29–95.

2 Department of Defense, Intelligence, Persistent Intelligence, Surveillance, and Reconnaissance: Planning and Direction JIC, ver. 1.0, March 29, 2005, 3, http://www.dtic.mil/futurejointwarfare/jic.htm.

complex environments against U.S. forces. The JIC's identification of the future threat codified Combatant Commander's (COCOM) on-going concerns for the need of increased persistent Intelligence, Surveillance, and Reconnaissance (ISR) to fill capability gaps in their Integrated Priority Lists (IPL).[3]

Despite identification of future threats and the call from warfighting COCOMs to address the gap with more increased persistent ISR as a solution, the Department of Defense as a whole has yet to provide sufficient metrics for evaluating either the effectiveness of ISR missions or warfighters' needs for the increased ISR assets.[4] Statistical research of past military operations to justify the call for increased persistent ISR does not exist. "DOD currently assesses its ISR missions with limited quantitative metrics such as the number of targets planned versus the number collected against."[5] Although the DoD acknowledges the issue, the department continues to take the risk of perpetuating the problem by fielding "more and more collection capabilities with little regard for how they "plug-in" to the ISR Enterprise as a whole."[6] The Defense ISR Enterprise is made up of globally distributed human and technological systems, combining deployed forces, fixed overseas locations, and Continental U.S. operations.[7]

Without developing metrics and systematically gathering feedback that enables it to assess the extent to which ISR missions are successful in supporting warfighter needs,

---

[3] Department of Defense, *Intelligence, Persistent Intelligence, Surveillance, and Reconnaissance: Planning and Direction JIC,* ver. 1.0, March 29, 2005, 3, http://www.dtic.mil/futurejointwarfare/jic.htm.

[4] Government Accounting Office, Intelligence, Surveillance and Reconnaissance: Preliminary Observations on DOD's Approach to Managing Requirements for New Systems, Existing Assets, and Systems Development (Washington, DC, 2007), 14; at: http://www.gao.gov/new.items/d07596t.pdf.

[5] Ibid.

[6] Department of Defense, *Intelligence, Persistent Intelligence, Surveillance, and Reconnaissance: Planning and Direction JIC,* ver. 1.0, March 29, 2005, 3, http://www.dtic.mil/futurejointwarfare/jic.htm.

[7] Definition of ISR Enterprise derived from statement of John Landon, representative for the Undersecretary of Defense Acquisition, Technology and Logistics, made before the U.S. House of Representatives Subcommittee on Tactical Air and Land Forces Committee on Armed Services and the Subcommittee on Technical and Tactical Intelligence, October 5, 2005, located at: http://www.globalsecurity.org/intell/library/congress/2005_hr/051020-landon.pdf.

DoD is not in a position to validate the true demand for ISR assets, determine whether it is allocating and tasking its ISR assets in the most effective manner, or acquire new systems that best support warfighting needs.[8]

Uncovering the conditions under which persistent surveillance is used is important for defense decision makers and planners. A clear definition of concept utilization allows for better system acquisition, test and evaluation, development of doctrine, and training of concept and asset usage which in turn can provide the greatest support to the warfighter.

Using a systems approach, the dynamics of an unclear and undefined concept of persistent surveillance can be better articulated. By drawing a behavior-over-time graph,[9] based on conditions of key concepts, a better understanding of the current concerns surrounding the issue can be understood. Although the future aspect of the graph is based on speculation, and any projection of the future could be wrong, the speculation nonetheless allows discussions that may otherwise never get surfaced.

The behavior-over-time graph below predicts the relationship among four behavioral concepts involved in the evolution of persistent surveillance as first conveyed in the 1998 DoD Annual Report to the President and Congress.[10] The four concepts are allocation of persistent surveillance assets; the concentration of target collections; the intensity of surveillance; and the amount of actionable intelligence acquired. They are measured against three timeframes (past, present and future).

---

[8] Government Accounting Office, Intelligence, Surveillance and Reconnaissance: Preliminary Observations on DOD's Approach to Managing Requirements for New Systems, Existing Assets, and Systems Development (Washington, DC, 2007), 14; at: http://www.gao.gov/new.items/d07596t.pdf.

[9] Behavior-over-time graphs take key variables as an important first step toward articulating the current understanding of a dynamic system. By graphing speculated future behavior of each variable, the objective is to test assumptions and uncover inconsistencies that may otherwise never get surfaced. Information derived from Guidelines for Drawing Casual Loop Diagrems, written by Daniel H. Kim, available on The Systems Thinker Web site at: http://thesystemsthinker.com/tstgdlines.html.

[10] Text combines the concepts taken from "Chapter 8:Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance" of DoD 1998 Annual Report to the President and the Congress, located on Department of Defense Web site at http://www.dod.mil/execsec/adr98/chap8.html#top.

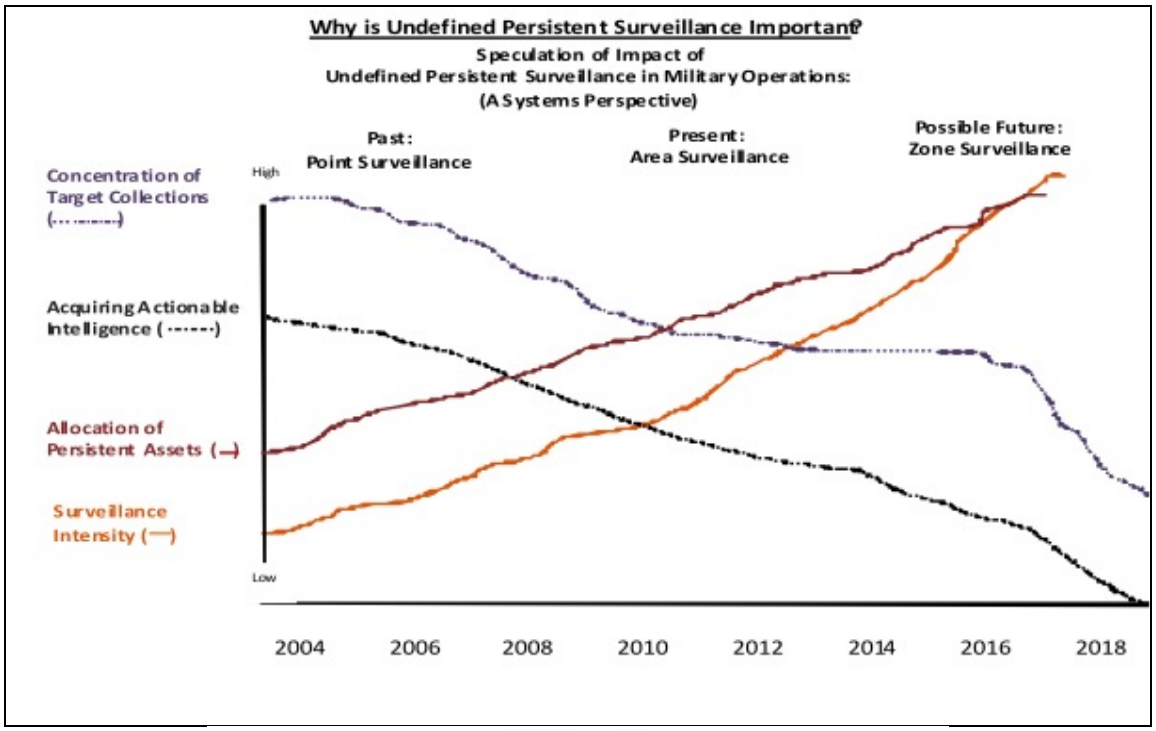
Using the 1998 DoD Annual Report to the President and Congress as a baseline, the evolution of the value of surveillance assets is graphed. Using subsequent reports, in particular the 2001 and 2006 QDR, this thesis speculates that military operations will continue to increase demand for persistent surveillance assets, but questions whether or not such demands are actually warranted. If this prediction holds true, an increased reliance on surveillance assets will be seen as a significant aspect of the 2010 QDR, and as such, the request should be scrutinized by Congress.

This thesis argues that without a clear definition of what or how the persistent surveillance concept is to be used, the demand for more assets and the continued reliance by the force on the products of the assets have a higher propensity of being mismanaged and underutilized. The lack of a clear vision and end state in the use of increased surveillance assets leaves DoD decision makers no basis for prioritizing investments, assessing progress in achieving strategic goals or identifying where further investment in capabilities may no longer be warranted.[11]

The request for more persistent surveillance has evolved from gaining more actionable intelligence on a specific target set to being a resource in providing situational awareness for broader coverage of areas for tactical missions. By expanding the target search from one that is specific (i.e., named target) to one that is broad (i.e., using surveillance in fighting warfare ideology such as defeating improvised explosion devices (IEDs)) may minimize the efficiency of use of the assets operational intent. This thesis asserts that as the use of persistent surveillance asset allocations continues to increase, the coverage area will broaden. Where the coverage area is broadened, the concentration on a target area becomes less focused. As the target area becomes less focused, the surveillance intensity decreases. A summary of such speculation is depicted in the behavior-over-time graph (Figure 1). This graph illustrates the speculation of how the

[11] Noted in a Government Accountability Office report ro the Subcommittee on Air and Land Forces, Committee on Armed Services, House of Representatives entitled "Intelligence, Surveillance, and Reconnaissance: DoD Can Better Assess and Integrate ISR Capabilities and Oversee Development of Future ISR Requirements," GAO–08–374, March 28, 2008, available at: http://www.gao.gov/products/GAO-08-374.

identified factors may progress into the future, for better or for worse. Such speculation was validated through historical analysis of the persistent surveillance concept used in Iraq between 2003 and 2007.



Definitions of Factors

Allocation of Persistent Surveillance Assets:
Number of surveillance assets given to execute military operations
Concentration on Target Collections
Concentration analysts placed on pre-identified target area/track
Surveillance Intensity:
Time surveillance assets are employed
Actionable Intelligence:
A process of analyzing multi-dimensional facets of actionable information to arrive at an action plan. Definition derived from KPraxis, "Capture of Saddam Hussein: Actionable Information to Actionable Intelligence," at: http://www.kpraxis.com/archives/information_intelligence/000054.html)

Definitions of Factors

Point Surveillance: focused surveillance on a defined person, place or thing
Area Surveillance: Surveillance within a defined space or area of operations
Zone Surveillance: Surveillance defined on transnational terms

Figure 1. Behavior-Over-Time Graph of Persistent Surveillance

These relationships are better understood in the causal loop diagram shown in Figure 2. Causal loop diagrams are constructed to aid in identifying the causal

relationship between different aspects within a system.[12] The relationship within the system is labeled with (S) or (O) to indicate a positive or negative causal effect. An (S) means that change in the concept variable leads to change in the same direction (increase or decrease) in the variable it is being related to. For example, if the definition of persistent surveillance is ambiguous, then this causes an increase in ambiguity in justification for using the concept. Likewise, the relationships identified with an "O" signify an opposite, or negative, effect. For example, as ambiguity in justification for using persistent surveillance increases, the concentration on target collection decreases. This is an opposite, or negative, relationship.

The causal loop diagram in Figure 2 reveals a vicious cycle. The diagram shows that greater ambiguity in the definition of persistent surveillance leads to greater ambiguity in the justification for the concept's use. Where there is greater ambiguity in the concept's use, there is less concentration on target collections. As target collections are less concentrated, so is the level of surveillance intensity. When surveillance intensity is decreased, there is an increase of information but a decrease in actionable intelligence acquired. The lack of actionable intelligence by the surveillance assets perpetuates the notion that there is a lack of available surveillance assets to accomplish the mission, thus an increase in assets in needed in order to resolve the problem.

There is hope in escaping this vicious cycle. The first step is to clearly define how the persistent surveillance concept should be used and the second step is to explore under what conditions persistent surveillance has been effectively used in the past.

[12] Information derived from Guidelines for Drawing Casual Loop Diagrems, written by Daniel H. Kim, available on The Systems Thinker Web site at: http://thesystemsthinker.com/tstgdlines.html.

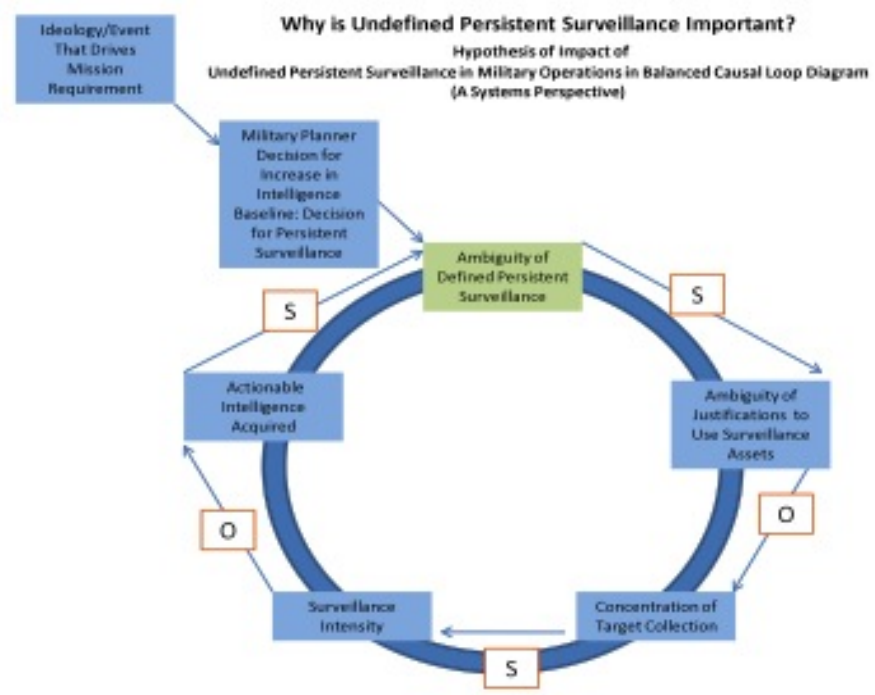


Figure 2. Casual Loop Diagram: Why is Persistent Surveillance Important?

1) Starting with a definition. The definitions of persistent surveillance alone, in military circles, are ambiguous and inconsistent in the realms of intent. Ambiguous definitions can lead to higher probabilities of increased mismanagement of resources: time, money and manpower. Without a singular, concise explanation to justify the requirement for persistent surveillance, collection platforms and resource allocation continue to be trapped in a vicious cycle of mismanagement. Although several definitions currently exist, the proposed JFCOM/J9 definition is the most consistent for how the concept is utilized. The organization defines persistent surveillance as:

> an operationally focused surveillance approach that uses a full range of strategic, operational and tactical collection methods to dwell on and revisit a target. Persistent surveillance contributes to the detection and recognition of meaningful changes in an adversary's activities that support planning and executing preemptive actions to prevent likely adversary courses of action.[13]

[13] JFCOM/J9 definition provided by Post-JIPS Conference, Suffolk, VA, May 26, 2008.

2) Explore when persistence has been used in the past and the conditions under which it is more effective. Only after understanding how persistent surveillance has been employed and with what level of effectiveness is it possible to plan for more efficient and effective use in the future.

This thesis provides a historical case study of the use of the concept of persistent surveillance in the U.S. Central Command (CENTCOM) area of operations from 2003–2007. This time period was chosen because it illustrates the evolution of this concept from the first years of Operation Iraqi Freedom (OIF), soon after persistent surveillance was introduced as an operational goal in the 2001 Quadrennial Defense Review (QDR), to the period of 2006–2007, after the concept had been declared a requirement for defeating terrorist networks in the 2006 QDR.

Examples of persistent surveillance taken from missions executed by CENTCOM during this period show how the concept shifted from a conventional to an irregular warfare resource, and between the strategic and tactical levels of operation. The events chosen to show this include: the rescue of Army POW Private Jessica Lynch (2003), the capture of former Iraqi dictator Saddam Hussein (2003), operations in Fallujah (2004), the capture of insurgent leader Abu Masab al-Zarqawi (2006), the joint effort to counter the IED threat through the creation of the Joint Improvised Explosive Device Defeat Organization (JIEDDO) (2006), and the Army counter-IED effort led by a task force named, Task Force Observe, Detect, Identify and Neutralize (TF ODIN). The methodology as to how and why these events were chosen for the thesis will be discussed in Chapter III.

As will be discussed in Chapter IV, four examples were chosen to represent the evolution of persistent surveillance for the 2003 to 2005 time period. An additional three examples from 2006 to 2007 were used to show the further evolution of persistent surveillance. Chapter five then analyzes those examples to determine whether the persistent surveillance was effective or not. A graphical representation of how each example fits into its respective area (i.e., Jessica Lynch was an example from the 2003 to 2005 time that was effective) is shown in Figure 3.

	Effectiveness	Ineffectiveness
2003-2005	Jessica Lynch POW Mission; Capture of Saddam Hussein; Operation Phantom Fury (Fallujah Operations Nov 2004)	Operation Vigilant Resolve (Fallujah Operations Apr 2004)
2006-2007	Hunt for Zarqawi; Army counter-IED operations (Task Force ODIN)	Joint counter-IED operations (JIEDDO)

Figure 3. Research Design of Cases Chosen to Analyze the Use of Persistent Surveillance

Chapter VI concludes the thesis and warns that the continued use of multiple interpretations of persistent surveillance will have serious implications for the acquisition and allocation of asset prioritization for decision makers and planners into the foreseeable future. An accurate definition for persistence surveillance in preparation for the 2010 QDR is more important than ever.

Due to the nature of classified operations and the disclosure of classified military capabilities, these examples are limited in scope to historic accounts based on unclassified evidence obtained from open-source information of real-world intelligence, surveillance and reconnaissance (ISR).

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

A. PERSISTENT SURVEILLANCE: THE KEY TO SUCCESS IN FUTURE WARFARE

The United States has proudly held the reputation as the "single remaining military superpower" in the modern world.[14] Made up of roughly 2.6 million active and reserve members, the force operates on an annual budget of approximately $700 billion with a supporting budget that supplies the largest inventory of advanced war-fighting equipment in the world.[15] Whereas innovative approaches using technologically advanced systems, such as strategic lift and GPS guided precision munitions, have allowed the U.S. to achieve strategic dominance, they have also fostered a culture of dependency on technology to provide answers to threats being faced in the battlespace. The emerging use of persistent surveillance, as an answer to thwarting the insurgent stronghold in Iraq and Afghanistan today is a perfect illustration of this.

Although the U.S. emerged as the world's military super power at the end of the Cold War, its military has an unsuccessful track record in achieving an offensive dominance in an asymmetric warfare environment. The increasing use of the persistent surveillance concept by U.S. forces in Iraq and Afghanistan has been said to be in response to the call from the warfighter as one of the main resources missing in order to successfully defeat the insurgency.

And when America's conventional military superiority fails "to deliver quick, cheap, and decisive success," as it had failed to do in Vietnam, all levels of the government scramble to find the answers before the American public becomes

[14] Craig Eisendrath and Tom Harkin, *National Insecurity: U.S. Intelligence After the Cold War* (Philadelphia, PA: Temple University Press, 2000), 181.

[15] Statistical data retrieved from the Bureau of Labor Statistics: Occupational Outlook Handbook, 2008–2009 Edition, on the number of active and reserve members in the U.S. armed services, available at: http://www.bls.gov/OCO/ocos249.htm, accessed on November 20, 2009.

"politically demoralized."[16] For military decision makers and planners this means an increase in budgetary requests for the production of "silver bullet" answers, such as that of persistent surveillance.

The events of September 11, 2001, and the military operations that ensued in Operation Iraqi Freedom (OIF) and Operation Enduring Freedom (OEF) emphasized the value of intelligence and the need for operational reform. In a statement before the Senate Armed Services Committee, Under Secretary of Defense for Intelligence Dr. Stephen Cambone explained the need for organizational transformation in the Intelligence Community:

> ISR organization and doctrine—weather in support of political or military leaders—has not been systematically revised for two generations. ISR activities are burdened by legacy policies and stove-piped activities that are de-conflicted, but not integrated either within DoD or between DoD and the Intelligence Community. We are taking measures to create a modern ISR capability.[17]

One of the reforms outlined was horizontal integration: a planned "system-of-systems" that integrates surveillance capabilities across various human and technical intelligence disciplines and national, theater, tactical, and commercial programs.[18]

It was after the call for up-to-the-minute information of near-real-time data in the operating environment that policy makers and military planners gave more attention to the issue of providing persistent surveillance. Just as philosopher Jeremy Bentham envisioned the panopticon being used as a tool to grant unrestrained power to observe the activities of convicts whenever desired, the U.S. military has envisioned that the introduction of persistent surveillance for military operators will provide the same against both known and unknown threats. If Bentham's theory proves to be correct, the U.S.

---

[16] Jeffrey Record, "The American Way of War: Cultural Barriers to Successful Counterinsurgency," *CATO Institute*, Policy Analysis no. 577 (September 1, 2006), accessed on CATO Web site at: http://www.cato.o rg/ pub_ display. php?pub_id=6640.

[17] Stephen A. Cambone, "Intelligence, Surveillance, and Reconnaissance," Statement Before the Senate Armed Services Committee Strategic Forces Subcommittee, April 7, 2004, 11.

[18] Ibid.

military's usage of persistent surveillance may also lead to the power to control behavior. The power to control, for the military, would be in terms of striking the enemy first.

The introduction of persistent surveillance was not only a technologic advancement in multi-sensor operations, but also an introduction to the cultural shift occurring within U.S. politics in defense decision making and planning. Persistent surveillance is a technologic advancement in better understanding the battlespace environment, wherever that may be; a shift from past military strategic practice that focused on a conventional adversary and way of fighting. Persistent surveillance brings into view a more cautionary approach for future U.S. engagement in warfare.

Whether it is gaining knowledge of a country's nuclear proliferation or a known terrorist's whereabouts, the ability to target, track and execute a decision that leads to action in securing national interests requires credible data linked real-time to decision-makers. Timeliness in passing such information has been, and continues to be, of paramount concern in protecting and securing interests. Intelligence is perishable. Therefore, good intelligence on the adversary must be acted upon quickly before the adversary detects surveillance and subsequently changes its mode of operation to conceal its activity.

Currently within the Department of Defense there are various definitions and concepts of what constitutes persistent surveillance. The lack of an agreed upon definition of persistent surveillance introduces an expensive transitional cost to the necessary shift in military leaders' mindset called for by the U.S. Secretary of Defense. As technological capabilities in ISR have improved in the last few decades to deliver real-time information, the numbers of requests for access to information obtained through such means have increased. There has been a surge in requests for unmanned aerial vehicles (UAVs), increased investments in national space-based platforms, as well as an effort to increase recruitment of human intelligence collectors. At the executive level, the U.S. government has initiated several programs to foster information sharing amongst federal agencies, as the value of full spectrum access to information has proven to be essential in national security planning for the asymmetrical threat being faced today.

Access to more information is believed to provide decision makers the ability to plan more accurately, thus achieving a higher probability of mission success.

Most organizations are believed to either rise or fall based on how the introduction of change is assimilated into their systems, especially during tough economic times where the organization is faced with questionable funding to provide the necessary resources for the organization's sustainability.[19] A primary determinant of the future success of an organization is its leadership's ability to articulate clear visions that complement implementation of strategic goals and objectives.[20] For the U.S. military, the organization's success in implementing change with the introduction of persistent surveillance is no different. Not only must the military internally be able to assimilate internal change, but also attempt to manage the ever changing budgetary constraints imposed by the U.S. Congress to fund such technologic innovations as persistent surveillance.

Whereas last year the Secretary of Defense was granted monies by Congress, a year later the U.S. Congressional Research Service and Congressional Budget Office is now advising the House Budget Committee that the Department of Defense should be given less, as much as $7 billion less each year on weapons procurement and research.[21] Such budgetary constraints could adversely affect DOD efforts in implementing the request for integrated ISR,[22]unless the military planners can prove such procurement is essential.

The integration of more ISR is a transformational change for the U.S. military. Transformational change within organizations requires clear vision and precise definitions of how operations are to be achieved. It is in this vein that semantics play a key role, especially in the joint military environment. Unclear terminology can lead to

---

[19] John C. Bruckman, "Overcoming Resistance to Change: Causal Factors, Interventions, and Critical Values," *The Psychologist-Manager Journal*, 1550–3461, Volume 11, Issue 2, 2008, 211–219.

[20] Ibid.

[21] William Welsh, "DoD Budget forecast Threatens New Technology Developments," *Defense Systems*, accessed October 15, 2009, at: http://www.defensesystems.com/Articles/2009/10/15/DOD-budget-analysis.aspx.

[22] Ibid.

costly misunderstandings and change the course of both operations and strategic intent. An example of this confusion has been the semantic impact of the loosely defined term *reachback* in military operations. Reachback has been broadly associated as being "the relationship between forward deployed and in-garrison, geographically separated units."[23]

Unfortunately, the term has developed a negative connotation amongst some operational circles. According to U.S. Air Force Chief of Staff for Intelligence, Lieutenant General David A. Deptula, and Commander of the Air Force's 480th ISR Wing, Colonel James R. Marrs, the term reachback has become synonymous with "not having the same sense of urgency" as the operational units forward. The perception, the AF officers opined, has led forward commanders to question the trustworthiness of ISR that is geographically separated from their forward units. According to Deptula and Marrs,

> Even though these views are in most cases without merit, detractors used the perceived faults of reachback to build a wall between them and any organization not located within the confines of their physical operational space. To them, if it was not organic or they did not control it, it did not matter.[24]

Subsequently, the perception of the term has led to costly arguments between the Air Force and the Army over adoption of ISR distribution and asset allocations.

"You can't bring the soldier back to the farm once he has seen Paris," said the Army's former director of unmanned systems integration about the growing attractiveness of ISR to forward deployed units.[25] The Army skepticism of *ISR reachback* has spurred debates all the way up to Congress over ISR resource allocation. Whereas the Army would like to have ISR assets directly tethered to forward units where they are

---

[23] David A. Deptula and James R. Marrs, "Global Distributed ISR Operations: The Changing Face of Warfare," *Joint Force Quarterly*, issue 54 (3rd Quarter 2009).

[24] Ibid.

[25] Demetri Savastopulo, "U.S. Military in Dogfight Over Drones," *Financial Times*, August 20, 2007, at: http://ebird.afis.mil/ebfiles/e20070820537336.html.

perceived to be most responsive, the Air Force vehemently disagrees, claiming such plans of using ISR assets would provide sub-optimal employment.[26]

> 'All the services are representing their interests…the Army has worked the Alabama delegation as hard as the Air Force has worked the North Dakota and Ohio delegations,' says Colonel Charles Bartlett, head of a special Air Force task force on UAVs…While Richard Shelby, the Republican senator from Alabama, is concerned about the impact on Redstone Arsenal, which manages much of the Army's UAV work, Byron Dorgan, the North Dakota Democratic senator, wants to attract more work for Grand Forks Air Force base, partly to make up for the loss of four refueling squadrons scheduled as part of the Pentagon's base realignment across the U.S.[27]

Although the perception of ISR reachback remains in contention amongst service members and leadership, the executive agent authority over how ISR assets are developed was decided by an order to join the Army and Air force UAV programs under a joint integrated product team by Deputy Defense Secretary Gordon England.[28]

Could all of this bickering been prevented with a clearly defined definition and joint doctrine of the usage of ISR capabilities? Perhaps, but hind sight is always twenty-twenty. Now it is knowledge gained through experience that really matters as the debate on ISR reachback has attracted attention among Congressional members who now are requiring more clarity in going forward.

> U.S. Representative Bud Cramer, D-Huntsville, AL, said moving control of the military's unmanned aerial vehicles, or UAVs, would be disruptive and possibly dangerous to soldiers fighting in Afghanistan and Iraq. "That's what my concern is ultimately. We have to make sure our resources in (Iraq) and around the world are used properly." Cramer inserted language in the 2008 Department of Defense spending bill that would require the Pentagon to carefully review any decision to move Army management of UAVs to the Air Force.[29]

---

[26] Demetri Savastopulo, "U.S. Military in Dogfight Over Drones," *Financial Times*, August 20, 2007, at: http://ebird.afis.mil/ebfiles/e20070820537336.html.

[27] Ibid.

[28] Carlo Munoz, "Services to Lay Groundwork For Joint Unmanned Drone Program," *Inside the Pentagon*, September 20, 2007, at: http://ebird.afis.mil/ebfiles/e20070920546251.html.

[29] Shelby G. Spires, "Army Hoping to Keep UAvs from Air Force," *Huntsville (AL) Times*, August 13, 2007, at: http://ebird.afis.mil/ebfiles/e20070814536331.html.

Thus, as the debate broadens, it is more important than ever to be clear about the definitions of "persistent" and "persistent surveillance" currently in circulation within DoD:

Current Definitions of Persistent:

- "the length of time a sensor system can provide continuous coverage of an area of interest. It's expressed as the average amount of time a sensing capability is able to focus on a particular geographical area of interest."[30]
- "the length of time a sensor can provide continuous coverage of a location, target, or activity of interest. What constitutes persistent varies significantly dependent upon Joint Force Commander's (JFC) mission objectives, operational environment, and target type. The JFC's desire for persistence is founded upon his ability to satisfy commander's critical information requirements (CCIRs), priority intelligence requirements (PIRs), or essential elements of information (EEIs), with the current IRS enterprise due to problems or obstacles generated by friendly and/or adversary actions or capabilities."[31]

The two definitions of persistent cause the following consternation for ISR collection managers: 1) both definitions assume persistence in ISR is limited to sensors (what about human intelligence collection?); 2) both leave the "length of time" undefined (can assets be used persistently for days, months, years?); and 3) neither definition considers full-spectrum ISR collection to be used (the first definition talks of a "sensor system," but it is unclear whether this a singular sensor or a combination of different sensors needed to obtain 'persistence'?; the second definition omits the word "system," suggesting that it is the operating capability of a particular sensor that provides persistent coverage).

Current Definitions of Persistent Surveillance:

---

[30] Department of Defense. "ISR Integration Roadmap" (D). V PB07, January 2007.

[31] DS Strategic Command. "Persistent ISR Planning and Directing Joint Integrating Concept," Version 1.0, 29 March 2007.

- "the integrated management of a diverse set of collection and processing capabilities, operated to detect and understand the activity of interest with sufficient sensor dwell, revisit rate and required quality to expeditiously assess adversary actions, predict adversary plans, deny sanctuary to an adversary, and assess results of U.S./coalition" actions.[32]
- "the integrated management of a diverse set of collection and processing capabilities to detect, locate, characterize, identify, track, target, and possibly provide battle damage assessment and retargeting against activities of interest, with sufficient coverage area, dwell, revisit, responsiveness, and quality to predict an adversary's behaviors, and formulate and execute preemptive activities to deter or forestall anticipated adversary courses of action."[33]
- "a collection strategy that emphasizes the ability of some collection systems to linger on demand in an area to detect, locate, characterize, identify, track, target, and possibly provide battle damage assessment and re-targeting in real or near real time. Persistent surveillance facilitates the formulation and execution of preemptive activities to deter or forestall anticipated adversary course of action."[34]
- "a collection strategy that uses a full range of strategic, operational, and tactical collection systems to dwell on and revisit a target in order to detect, locate, characterize, identify, track, target and assess desired effects. Persistent surveillance contributes to the detection and recognition of meaningful changes in an adversary's activities that support planning and executing preemptive actions to prevent likely adversary courses of action."[35]

---

[32] DS Strategic Command. "Persistent ISR Planning and Directing Joint Integrating Concept," Version 1.0,29 March 2007.

[33] Defense Intelligence Agency. "Joint Persistent Surveillance CONOPS" (D), 31 July 2008.

[34] Joint Publication 2–0. *Joint Intelligence*, 22 June 2007.

[35] JFCOM/J9 definition pre-JIPS conference.

The difference in these definitions leads to a central contentious issue amongst stakeholders who want to use persistent surveillance: Is persistent surveillance *integrated management* or a *collection strategy*? Integrated management is the process of maintaining or diverting readily available resources amongst operations. With regards to persistent surveillance, this would be the allocation of surveillance assets in an operating area without a specific, focused objective for its use. Conversely, the use of the persistent surveillance concept in a collection strategy would involve identifying a specific target set to a specific area with a specific focus during the pre-planning phase of an operation. The answer to this question prompts collection mangers, decision makers, and planners to view persistent surveillance as resource management (integrated management) or as a subsystem (collection strategy) impacting a larger strategic mission. For example, the tracking of a commander's critical information requirement (CCIR) can illustrate the semantic difference between integrated management and a collection strategy.

If persistent surveillance is defined as integrated management, information systems are used to find and report elements to support the CCIR, but fail to report other information that might fall outside "the plan," which if detected and reported, may advance other strategic objectives beyond those gained in the CCIR alone.[36] Conversely, if a CCIR is being sought with persistent surveillance that is viewed as a collection strategy, "information pathways will move information directly to collaborative users (rather than through successive headquarters) and empower all echelons."[37] The difference in definitions not only impacts resource allocation of assets used to achieve the actual surveillance, but also the time, money and manpower required to train and equip DoD facilities, networks, and operators to ensure persistent surveillance can be executed properly.

If persistent surveillance is considered "the guiding vision--a globally coherent national-security system" it will require "a coherent operational system to exercise all

[36] David W. Pendall, "Persistent Surveillance and Its Implications for the Common Operating Picture," *Military Review*, November/December 2005, 43.

[37] Ibid., 44.

elements of national power."[38] This would require a DoD transformation in how business is run; a paradigm shift that has been discussed in length but hesitantly acted on. Over the last two decades DoD has "under-invested" in true intelligence reform.[39]

Technological advancements that enable better ISR collection have unequivocally been made over the last two decades, but the degree of transformation in how analysis is processed and passed to decision makers once the information is obtained has lagged behind.[40] According to author Gregory Treverton, policy officials see the value of intelligence only after an issue becomes important and are looking for perspective on dealing with it. Treverton criticizes policy officials for not seeing the value of intelligence and the information intelligence assets can obtain until it's too late. He asserts that officials are interested in intelligence on their terms and their terms only. Treverton writes,

> Policy officials are likely to want intelligence at three points of an issue. First: when they see an issue becoming important; intelligence gives them a sense of perspective. Secondly: when they have to decide what to do about an issue; at this point they want intelligence to help them to consider alternative ways to approach the issue. Thirdly: when policy officials have made up their minds on how to act they welcome intelligence out only if it supports their view.[41]

In the realms of intelligence, most would agree that having any prior surveillance on a target set is better than having none at all. USSOCOM recognized the need for an intelligence architecture equal to the enemy they faced (the Al-Qaida network); an enemy that was adaptive, flexible, agile and capable of inflicting harm on U.S. interests anytime.[42] But, by having more ISR assets that allow persistent surveillance are decision-makers always better off?

---

[38] David W. Pendall, "Persistent Surveillance and Its Implications for the Common Operating Picture," *Military Review*, November/December 2005, 45.

[39] Robert K. Ackerman, "Persistent Surveillance Comes Into View." *Signal Online*, May 2002.

[40] Gregory F. Treverton, *Reshaping National Intelligence for an Age of Information*, New York: Cambridge University Press, 2001, 183–185.

[41] Ibid.

[42] Judy G. Chizek, "Military Transformation: Intelligence, Surveillance and Reconnaissance." *CRS Report for Congress*, January 17, 2003.

This issue is a contentious one between services, in particular the Air Force and the Army. The debate over how persistent surveillance is allocated and used is divided. Currently each of the armed services is struggling to work together to optimize ISR and UAV capabilities. General Deptula pointed this out when asked about the progress on policy to ease the problems with flying UAVs in battlefield theaters. In reference to the debate between the Air Force and Army over executive agent authority of theater-wide ISR assets General Deptula is under the belief that,

> There are no Air Force targets in Iraq and Afghanistan. The targets belong to the joint force commander. So the issue is between the perspective of the overall joint force commander and a local unit commander. To optimize UAS capability for all, the theater-capable UAVs should be flown in line with what the joint commander needs, while also ensuring there are enough local-capable UAS assets to meet smaller unit commander's needs. It is very important that we follow our tried-and-true joint organizational approaches that have existed since the 1986 Goldwater-Nichols Act. We could be doing it better.[43]

Although the decision to grant executive agent authority to either service was ended with the Deputy Defense Secretary England's decision to create a task force for joint ISR planning in 2007, the Army continues to pursue independent concepts. An example of this was the publication of an article entitled "Tactical Persistent Surveillance" in the summer 2008 issue of the Army's *Military Intelligence Professional Bulletin*.[44]

The article was co-written by the director, deputy director and the ISR division chief of the Army's Concept Development Directorate at the Army Intelligence Center. In this document the authors agreed that despite numerous attempts, DoD had yet to adequately define the term for persistent surveillance—its capabilities and limitations.[45] Instead they proposed an Army-centric definition for "tactical persistent surveillance." The authors claimed the joint endeavor for defining persistent surveillance was focused on the "operational and strategic concerns and typically focused upon space and/or aerial

---

[43] Shiela Vemmer, "Lt. Gen. David Deptula: U.S. Air Force Deputy Chief of Staff for ISR," *Defense News*, January 12, 2009, at: http://www.defensenews.com/story.php?i=3896251.

[44] Sharon R. Hamilton, Richard L. Smith, and Martin C. McCleary, "Tactical Persistent Surveillance," *Military Intelligence Professional Bulletin*, Vol 34, No. 3, July–September 2008, 7, at: https://icon.army.mil/anon/mipb/CurrentMIPB.pdf.

[45] Ibid.

platforms such as UAS," whereas their proposed definition "specifically pointed to tactical echelon support."[46] Yet, the authors also pointed out that "the success of the future modular force brigade combat teams (BCT) depended significantly upon the integration of ISR capabilities at all echelons, and the capability to provide tactical persistent surveillance and exploitation of the area of operations."[47]

While the authors' attempt to clarify the use of persistent surveillance is well intended, the document has the ability to confuse and distort the joint definition for persistent surveillance. The on-going joint endeavor to pursue integrated persistent surveillance requires joint initiatives in budgeting, contracting, and interdependent connectivity between services. The proposal for defining an Army tactical use of persistent surveillance undermines this joint endeavor, an endeavor that Deputy Defense Secretary England sought with the development of the ISR task force in 2007 and the Defense Secretary's plea for joint warfighter support.

Although one can argue that the article was just another concept piece within a military sponsored publication, it is fair to assume the authors are well thought of within the service and as such the article illustrates the mindset of the service's *Concept Development Directorate at the Army's Intelligence Center*. Their definition of persistent surveillance allows latitude for operational interpretation. Latitudes of interpretation can quickly morph from ideology based on the interpretation to standard operating practice within organizations. Once operating practices begin to normalize within an organization they are almost impossible to correct.

One example that illustrates the dangers of poorly defined concepts is the Federal Aviation Agency's (FAA) vague definition of an "installation" as applied to hand-held

---

[46] Sharon R. Hamilton, Richard L. Smith, and Martin C. McCleary, "Tactical Persistent Surveillance," *Military Intelligence Professional Bulletin*, Vol 34, No. 3, July–September 2008, 7, at: https://icon.army.mil/anon/mipb/CurrentMIPB.pdf, 8–9.

[47] Ibid., 12.

GPS units in an aircraft. The dilemma began when field inspectors were tasked to interpret whether or not hand-held GPS units were "installed" in aircraft and when the devices technically were not.[48]

> Because of the lack of policy and guidance material regarding the FAA's definition of the installation of a hand-held GPS unit in an aircraft, FAA field inspectors are routinely misinterpreting the FAA's policy. For example, in one region of the United States a FAA inspector may state that the use of Velcro to attach a hand-held GPS unit to the yoke constitutes an installation and requires the filing of a FAA form 337. Meanwhile, in another region of the United States an inspector may state that as long as no tools are needed to remove the hand-held unit from the aircraft, no form 337 or field approval is required. These inconsistent interpretations often cause users of hand-held GPS units to complete unnecessary paperwork or undergo unneeded bureaucratic procedures to legally use their hand-held GPS units on board their aircraft. If nothing else, misinterpretations and misapplications of FAA policy can cause considerable aggravation to users of hand-held GPS units.[49]

A documented lesson learned this example shows the dangers of using undefined or under-defined concepts that in turn lead to operational misapplication and a cycle of wasted resources. Is this the path of persistence surveillance? The broad usage of the term amongst the myriad of applications and justifications give the impression that it is.

Where can true "information and information technologies…significantly increase the likelihood of success"?[50] Do all military operations merit the allocation of assets to provide persistent surveillance? From this author's perspective, the answer is no. Persistent surveillance is costly; costly in terms of system employment, manpower for system operability and most importantly, the security of protecting U.S. tactics and techniques from being manipulated by the enemy. Planning the employment of persistent surveillance needs to be carefully considered; cause and effects of its use critically deliberated, and clearly defined objectives discussed prior to allocation in all military manners.

---

[48] Informational article entitled "Inconsistent FAA Interpretation Leads to Problems with use of Hand-Held GPS Units in Aircraft," accessed on October 20, 2009, on Aircraft Owners and Pilots Association Online at: http://www.aopa.org/whatsnew/regulatory/reghandheld.html.

[49] Ibid.

[50] Franklin D. Kramer, Larry Wentz, and Stuart Starr, "I-Power: The Information Revolution and Stability Operations," *Defense Horizons*, 55, (Washington, DC: National Defense University Press, February 2007).

THIS PAGE INTENTIONALLY LEFT BLANK

III. RESEARCH DESIGN

The overall design and methodology is a historical case study of the use of persistent surveillance in U.S. CENTCOM. This chapter will explain how the various missions used in the study were selected and define the criteria used for the analysis.

A. HISTORICAL EXAMPLES OF PERSISTENT SURVEILLANCE

The research used for this paper was based on analysis of military missions in Iraq, specifically military missions that occurred between 2003 and 2007. The examples selected are: the Jessica Lynch POW mission, the capture of Saddam Hussein, the battles of Fallujah, the hunt for Zarqawi, the joint counter-IED effort led by the Joint Improvised Explosive Device Detection Organization (JIEDDO), and Army counter-IED effort under Task Force ODIN. Due to the nature of classified operations and the restriction on disclosure of classified military capabilities, these historic examples, available from open-source information, provide unclassified evidence of real-world ISR assets that used persistent surveillance. These examples were selected for study because they are all prominent examples of the use of persistent surveillance—either militarily significant, such as the battles of Fallujah, or widely discussed publicly, such as the rescue of Jessica Lynch—for which data is available at the unclassified level.

Why use the 2001 and 2006 QDRs to analyze the evolution of the growing value of persistent surveillance? Whereas the 2001 QDR introduced persistent surveillance as a potential operational goal, the concept evolved during the start of OIF in 2003 and continued through 2005. This led to the 2006 QDR fully declaring that persistent surveillance was an invaluable operational capability and vital to mission success in the war in Iraq. Evaluation of the persistent surveillance concept before, after and between the QDRs shows the impact conditions may have had in the interpretation of how the concept was used by the services.

The intent of the QDR was to understand the Department of Defense's acquisition of new technologies and was directed by the U.S. Congress. After the end of the Cold

War, there was a need to better understand and validate the Department's expenditures. Congress desired more insight in order to help guide budgetary decisions. The law instructing the QDR reads,

> Title 10, Section 118 of the United States Code specifies: "The Secretary of Defense shall every four years, during a year following a year evenly divisible by four, conduct a comprehensive examination (to be known as a "quadrennial defense review") of the national defense strategy, force structure, force modernization plans, infrastructure, budget plan, and other elements of the defense program and policies of the United States with a view toward determining and expressing the defense strategy of the United States and establishing a defense program for the next 20 years. Each such quadrennial defense review shall be conducted in consultation with the Chairman of the Joint Chiefs of Staff."[51]

Thus, the QDR is designed to assess Department of Defense strategy and the reasoning behind the request of technology and systems to counter national security threats in the security environment of the twenty-first-century.[52] After the fall of the Soviet Union and the end of the Cold War, there was a need to understand the reasoning behind defense decision making and planning. The QDR was to serve as the overall strategic planning document for the Department of Defense.[53]

Principal Deputy Undersecretary for Policy, Ryan Henry, believed that the 2006 QDR showed that there was a shift taking place from traditional conventional warfare thinking within the U.S. military. Henry implied that the effectiveness of warfare was no longer calculated by the number of targets achieved, but rather how missions were being accomplished. He stated, "It's not about numbers. Numbers don't tell you if you can get the job done, it's about capabilities."[54] The 2006 QDR stated that the success of the force depended on "an unblinking eye over the battle space through persistent surveillance" in

---

[51] Title 10, Section 118 of the United States Code, available on the Office of Law Revision Counsel, U.S. House of Representatives Web site at: http://uscode.house.gov/uscode-cgi/fastweb.exe?getdoc+uscview+t09t12+54+1++()%20%20AND%20((10)%20ADJ%20USC)%3ACITE%20AND%20(USC%20w%2F10%20(118))%3ACITE.

[52] William S. Cohen, Report of the Quadrennial Defense Review, (Washington, D.C.: Department), May 1997, iv.

[53] Ibid., 2.

[54] Donna Miles, "DoD Releases QDR to Chart Way Ahead to Confront Future," American Forces Press, February 3, 2006, at: http://www.defenselink.mil/news/newsarticle.aspx?id=14953.

order to succeed at future "…operations against any target, day or night, in any weather, and in denied or contested areas."[55] Whether or not the services shared this view helps in understanding how the services approach acquisition for such capabilities.

How was persistent surveillance employed and how effective was that employment? In Iraq, the increased use of persistent surveillance is believed to be based upon the unique operational needs of ongoing irregular warfare.[56] But the breadth of missions and the emerging need for persistent surveillance challenged the force. The tasking, processing, exploitation, and dissemination (TPED) associated with each intelligence discipline (signals, imaging, etc.) differed amongst the services, combat support agencies, and from national to tactical assets and applications.[57] Did the missions reviewed warrant the use for persistent surveillance or did services feel compelled to use persistent surveillance based upon stronger dissent of military commanders from the "silk scarf syndrome?"[58] The answer to this question provides the basis for the analysis of effectiveness discussed in Chapter V.

The assessment of the effectiveness of persistent surveillance is based on three criteria: 1) the environment the sensor platforms were used in (i.e., was it an optimal performance environment (weather, climate, operating altitude, degree of interoperability with other sensors); 2) the experience of the operators (i.e., had the operators using the intelligence gathered by persistent surveillance worked in the area being collected on before? Or was this the first time they were learning of the environment); and 3) the clarity of the use of persistent surveillance (i.e., how focused was the surveillance area? Narrow, broad, undefined?). Creation of the criteria was based on abstracted information believed to play a critical role in the evolution of the surveillance concept as depicted by news articles and Congressional testimony during the analyzed time periods.

---

[55] QDR 2006, 67, accessed on Department of Defense Web site at: http://www.defenselink.mil/qdr/report/Report20060203.pdf.

[56] In preparing for the upcoming QDR 2010, a Quadrennial Roles and Mission Review (QRM) was conducted by the Secretary of Defense to assess what has transpired in the military's capabilities since publication of the 2006 QDR. Information derived from the posted January 2009 QRM, 32, accessed on the Department of Defense Web site at: http://www.defenselink.mil/news/Jan2009/QRMFinalReport_v26Jan.pdf.

[57] Information from 2009 QRM, 26, accessed from Department of Defense Web site at: http://www.defenselink.mil/news/Jan2009/QRMFinalReport_v26Jan.pdf.

[58] Silk scarf syndrome meant the commander's preference of using manned aviation n over unmanned aerial vehicles; concept was used in Elizabeth Bone and Christopher Bolcom, "Unmanned Aerial vehicles: Background and Issues for Congress," Report for Congress, The Library of Congress, April 25, 2003, 1.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. PERSISTENCE SURVEILLANCE 2003–2007

Now that we have outlined the methodology used in examining this historical case study, this chapter will explore historical events that used the persistent surveillance concept from 2003-2007. This chapter will also discuss how these historical events transformed the concept's perceived importance in military operations. As mentioned in Chapter III, the historical events explored will include: the rescue of Army POW Jessica Lynch in 2003; the capture of hiding Iraqi President Saddam Hussein in 2003; Operations in Fallujah in 2004; the value of persistent surveillance in the capture of insurgent leader Abu Musab al-Zarqawi in 2006; and two different efforts focused on the problem of Improvised Explosive Devices (IEDs), the Army's Task Force ODIN project and in the Department of Defense's Joint Improvised Explosive Device Detection Organization (JIEDDO).

A. THE INTRODUCTION OF PERSISTENT SURVEILLANCE (2003–2005)

The use of persistent surveillance in Operation Iraqi Freedom (OIF) represented an evolutionary development for surveillance tactics as much as it did a revolutionary development[59] in how warfare was fought. The increased awareness of persistent surveillance, stemming from the 2001 QDR, allowed military planners to incorporate the concept in OIF operational planning. Conventional forces grew increasingly aware and attracted to the use of persistent surveillance at the onset of the conflict. Unfortunately, the majority of the conventional force lacked experience with the capabilities of the surveillance, as it was practically nonexistent prior to 2003, except in operations involving Special Forces.

The use of the concept began in earnest at the onset of OIF. Military analysts, planners and decision makers were constantly submitting requests for information (RFI) to intelligence collection operators to fill critical intelligence gaps in the war. In

[59] Carlo Kopp, "Intelligence, Surveillance, and Reconnaissance During Operation Iraqi Freedom," at: http://www.ausairpower.net/DT-ISR-OIF-04.pdf.

executing missions that fulfilled the RFIs, the newly fielded persistent surveillance assets quickly earned the confidence of DoD leadership as an invaluable resource.

Lieutenant General Walter E. Buchanan III, Commander of U.S. Central Command Air Forces, acknowledged this during testimony before the House Armed Services Committee in 2004. He stated that "prior to launching the first weapons to rid Iraq of Saddam Hussein, Predators flew above Baghdad gathering data, monitoring HVTs and providing us real-time intelligence information."[60]

The first example of the capabilities Gen. Buchannan referenced had been made public a year earlier in the rescue efforts of captured American prisoner of war, Army Private Jessica Lynch in April 2003. Decision makers viewed the rescue live from the persistent Predator full-motion video surveillance streams. Once Private Lynch was safe in U.S. custody, the video of the complex joint rescue mission was released for public consumption. The New York Times reported the mission as being "the most prominent example of this complexity."[61] The paper stated,

> As it unfolded, Marine Corps artillery created a diversion, while Army Rangers seized the perimeter of the hospital where she was held and Navy Seals pulled her out on a stretcher. Air Force AC-130 gunships were on call to bring their withering cannon fire into play if the rescuers ran into trouble.[62]

The all-weather, through the cloud, surveillance performance of the Predator[63] provided the experienced rescue teams the capability to have real-time insight of the operations from above. This gave a bird's eye view of the mission simultaneously to decision makers and operators for seamless coordination.

---

[60] Walter E. Buchannan III, "Intelligence, Surveillance, and Reconnaissance." Statement Before the House Armed Services Committee, Subcommittee on Tactical and Land Forces regarding unmanned combat air vehicles (UCAV) and unmanned aerial vehicle (UAV), March 17, 2004, at: http://www.globalsecurity.org/military/library/congress/2004_hr/04-03-17buchanan.htm.

[61] Tom Shanker and Eric Schmitt, "A Nation at War: Special Operations," *New York Times*, April 6, 2003, at: http://www.nytimes.com/2003/04/06/world/nation-war-special-operations-covert-units-conduct-campaign-invisible-except-for.html?pagewanted=all.

[62] Ibid.

[63] Capabilities of the Predator RQ-1/MQ-1/MQ-9 Reaper can be located at: http://www.airforce-technology.com/projects/predator/.

Once made public, the surveillance gave Americans, and the world, a glimpse of operations as "they happened," garnering public support for both the technology and on-going military missions in OIF.

The next example of the successful use of persistent surveillance was the employment of around-the-clock surveillance coverage to assist in the capture of exiled Iraqi President Saddam Hussein. Hussein was considered to be the number one high value target in Iraq at the time, and his capture was deemed a huge success for coalition forces, and the performance of persistent surveillance was lauded with further public approval for its employment.

"Operation Red Dawn," as the capture was referred to, occurred on December 13, 2003. The operation consisted of approximately 600 soldiers from the 4th Infantry Division, coalition forces, and special operations forces.[64] The mission objective was clear, the target known, and the force working on the mission was inherently "joint" from the operation's conception.

In this case, intense persistent human intelligence collection via interrogations of close associates of Saddam Hussein had been conducted in an effort to close in on the dictator's location.[65] In order to verify the gathered clues, persistent aerial surveillance was used. A tip that Saddam had been driving around in a battered old cab was an example of such a clue hunted by aerial surveillance assets.[66] Acting quickly, the location of the hiding dictator was narrowed to an area right outside his hometown of Tikrit, where raids of hideouts revealed traces that the dictator had in fact been in the area.[67] Raids within the area intensified until forces eventually found Saddam Hussein.

Public accounts of both events attributed much of their success to the use of persistent surveillance. The concept quickly began to earn a large vote of confidence

---

[64] Information about Operation Red Dawn accounts found on Global Security Web site, at: http://www.globalsecurity.org/military/ops/red-dawn.htm.

[65] Evan Thomas and Rod Nordland, "How We Got Saddam," *Newsweek*, December 22, 2003.

[66] Ibid.

[67] Ibid.

from DoD decision makers and planners, who began to increase the concept's usage—just as enemy tactics began to shift from conventional to insurgent warfare on the ground.

U.S. forces in particular were not prepared for such a fight, largely because American leaders could not come to an agreement that the conventional war they had entered had now shifted to a type of warfare they were unprepared for. The insurgent warfare that erupted on the ground took American leadership by surprise. Instead of taking the advice of Karl von Clausewitz, who had argued, "…the most far reaching act of judgment that the statesman and commander have to make is to establish ... the kind of war on which they are embarking,"[68] American decision makers took on a semantic disagreement over what type of warfare coalition partners were involved in.

During General John Abizaid's first press conference as the Commanding General of CENTCOM, he made reference that the shift being witnessed on the Iraqi battlefield was that of a "classical guerrilla-type campaign."[69] In a poignant disagreement with such claims, the Secretary of Defense, Donald Rumsfeld, argued that there was no guerilla war in Iraq and that "…it would be a misunderstanding and a miscommunication… to the people of the country and the world" to say that there was one, instead argued that there were "five different things" going on in Iraq: "looters, criminals, remnants of the Ba'athist regime, foreign terrorists, and those influenced by Iran."[70]

The underlying issue of the argument was publicly admitting that the insurgent warfare posed a significant challenge for the conventionally trained U.S. forces. The challenge was to be able to separate the good guys from the bad within a population that now harbored the enemy. There was virtually no distinction between those who targeted coalition forces and the innocent civilian among whom they lived.

---

[68] Carl von Clausewitz, *On War*, Michael Howard and Peter Paret, eds., (Princeton NJ: Princeton University Press, 1976), 88.

[69] See BBC, "US faces Iraq guerrilla war," July 16, 2003, available at http://news.bbc.co.uk/2/hi /middle_east/ 3072899.stm.

[70] Department of Defense News Briefing with Secretary Rumsfeld and General Myers, June 30, 2003, available at http://www.defenselink.mil/transcripts/transcript.aspx? transcriptid=2767. When a reporter read the DoD definition of guerrilla war—"military and paramilitary operations conducted in enemy-held or hostile territory by irregular, predominantly indigenous forces"—and asked whether that described the situation in Iraq, Secretary Rumsfeld replied, "It really doesn't."

So when U.S. President George Bush demanded military objectives be achieved while limiting affects on the civilian population,[71] much more emphasis was placed on verifying the "target" before engaging the enemy than ever before. It was this new emphasis that gave the persistent surveillance concept a larger operational necessity. Collateral damage on mistaken targets had the propensity of having large operational and strategic political implications for the coalition forces engaged in Iraq. The use of persistent surveillance was believed to help minimize false targets.

The use of persistent surveillance as a resource to aid in filtering the "good from the bad" with more fidelity drove military planners to incorporate the persistent surveillance concept into more operational missions. Seen as a more reliable and capable means of gaining and verifying intelligence in the new batllespace environment of insurgent warfare in Iraq, the use of multi-sensor aircraft, unmanned aerial vehicles, and human intelligence sources on the ground in close coordination grew to be viewed as the "best way forward" in beating the enemy. Under this assumption, military planners began to further integrate the allocation of multi-sensing platforms into operations. Whether it was answering a commander's need for an essential element of information (EEI) or providing an update on a known insurgent's location, requests for and the allocation of surveillance assets in operations began to soar in 2004. A Congressional Research Service report highlighted the increase of appropriated funding of DoD budget requests for more UAVs:

> The growing awareness and support in Congress and the Department of Defense for UAVs, investments in unmanned aerial vehicles have been increasing every year. The Fiscal Year 2001 (FY01) investment in UAVs was approximately $667 million, while the FY03 funding totaled over $1.1 billion dollars. The Pentagon has asked for $1.39 billion in procurement and development funding for FY04, with much more planned for the out years.[72]

---

[71] President George Bush delivered a televised speech aboard the USS Abraham Lincoln on May 1, 2003. The speech focused on the fighting in OIF shifting to stability operations. Specifically, the President stated, "With new tactics and precision weapons, we can achieve military objectives without directing violence against civilians." Transcript of the speech can be found on British news site, *The Guardian*, at: http://www.guardian.co.uk/world/2003/may/01/usa.iraq.

[72] Elizabeth Bone and Christopher Bolcom, "Unmanned Aerial vehicles: Background and Issues for Congress," Report for Congress, Congressional Research Service, April 25, 2003, 2.

The growing investment by the DoD in UAVs indicated there was an increased emphasis on both the use of and the confidence in using more surveillance. Even with no public acknowledgment or precise definition as to how and for what the surveillance would be used in operations, requests for budget increases passed without question. And with more surveillance assets in circulation for use without clear and concise parameters for allocation, military decision makers and planners began to assign assets with little operational justification.

The start of ambiguous persistent surveillance usage was illustrated in two major operations that used persistent surveillance in Fallujah in 2004; the first in April and the other in November. Each operation used persistent surveillance, but each operation had a different outcome. The successful usage of the surveillance concept occurred when planners took more time to coordinate the concept amongst units involved prior to the onset of operations.

In the early part of 2004 in Fallujah, insurgents ambushed four American contractors working for Blackwater while they were driving through the city, their bodies mutilated and hung from a bridge.[73] The grisly event caused grave concern amongst the leaders in Baghdad, Washington and within the capitals of invested coalition partners partaking in securing an Iraq after Saddam.

> Under the old Iraqi regime, Fallujah had enjoyed some special prerogatives and had produced a number of senior leaders in Iraq's various security forces. Many residents therefore had some reason to be concerned about their place in the post-Saddam Iraq.[74]

Despite some political reservations on both Iraqi and coalition partners, a counter-response to the insurgent factions believed to be responsible for the American contractor deaths in Fallujah commenced on April 4, 2004. Operation Vigilant Resolve, as it was called, "featured 1,300 marines from I MEF, along with some Iraqi participants. The

[73] Catherine Dale, "Operation Iraqi Freedom: Strategies, Approaches, Results, and Issues for Congress," Congressional Research Service (RL34387), April 2, 2009, 70.

[74] Ibid.

marines surrounded the city, and then teams made forays into it in an attempt to locate those responsible for the slayings and draw out other insurgents."[75]

Once again, surveillance assets were requested for the operation in addition to Air Force AC-130 gunships to support the Marine contingent on the ground. Due to limited information about those responsible for the deaths, both Marines on the ground and aerial surveillance assets allocated to the fight had limited intelligence to go on in finding the culprits within Fallujah. Up against non-conventional forces, the coalition force tried to separate civilians between insurgent factions by warning civilians to leave the city before the armed conflict would begin. According to the Congressional Research Service,

> The Marines began the Fallujah operations by setting conditions—turning off electrical power, and urging the civilians of Fallujah to leave the city. The vast majority of residents did depart—leaving about 500 hardcore fighters, who employed asymmetrical tactics against a far larger, stronger force…The operation reportedly included 540 air strikes, 14,000 artillery and mortar shells fired, and 2,500 tank main gun rounds fired. Some 70 U.S. personnel were killed, and 609 wounded.[76]

There were allegations of numerous civilian casualties in the battles, so much so that within days of Operation Vigilant Resolve's commencement, operations were halted.[77]

Although the decision to halt operations was a political one and not due to any specific operational failure, the public criticized the use of the persistent surveillance concept during Operational Vigilant Resolve largely due to misrepresentation by media. The surveillance assets were seen as having been ineffective. A joint effort began soon after Operation Vigilant Resolve ended to re-evaluate the use of the concept; and at the same time, planners drew up a new plan for Fallujah.

Operation Phantom Fury, the second battle of Fallujah, commenced in November 2004. Of specific concern to Iraqi's future stability, U.S. and coalition forces were

---

[75] Rebecca Grant, "The Fallujah Model,"*Air Force Magazine*, February 2005, at: http://www.airforce-magazine.com/MagazineArchive/ Pages/2005/February%202005/ 0205fallujah.aspx.

[76] Catherine Dale, "Operation Iraqi Freedom: Strategies, Approaches, Results, and Issues for Congress," Congressional Research Service (RL34387), April 2, 2009, 71.

[77] Rebecca Grant, "The Fallujah Model."

focused on defeating the Zarqawi insurgent network, believed to be based in Fallujah.[78] According to Michèle Flournoy, senior adviser for the Center of Strategic International Studies (CSIS) International Security Program, the operation was critical to OIF. She stated,

> This battle has the potential to be a turning point in Iraq — putting the country on the road to greater stability, elections and hope or causing it to backslide further into violence and despair. The real challenge for the U.S. and Iraqi forces in Fallujah will be to win this battle without losing the war — that is, to defeat the insurgents without turning the Iraqi population against them.[79]

In an account of Operation Phantom Fury, *AIR FORCE* magazine contributing editor, Dr. Rebecca Grant, described persistent surveillance as a key component in fighting against insurgents. She wrote,

> Counterinsurgency efforts across Iraq relied heavily on persistent intelligence, surveillance, and reconnaissance from air and space platforms. Operation Enduring Freedom and Operation Iraqi Freedom had already proved the value of persistence. Now, for stability operations, the role of persistent surveillance was doubly important.[80]

Operation Phantom Fury was a meticulously planned joint operation that took months of planning. Planners had mapped Fallujah "down to the street addresses," which was considered to be one of the "…huge successes of Fallujah II…" according to military operators involved in planning the operation.[81]

The planners, as well as the operators involved in the mission, were all experienced with the region and effectively allocated surveillance assets, such as the Predator, to provide persistent situational awareness of changes to the battlespace. In Dr. Grant's article, the persistent surveillance was described as "…a God's-eye picture for

---

[78]Secretary of Defense Rumsfeld and Joint Chiefs of Staff Chairman Richard Myers conducted a news media briefing at the Pentagon discussing Zarqawi network and Fallujah on April 7, 2004, transcript located at: http://www.america.gov/st/washfile-english/2004/April/ 200404080833551CBnosnhoJ2.296084e-02.html.

[79] News release by CSIS analysts November 9, 2004 on the Fallujah offensive can be found on CSIS Web site at: http://csis.org/files/media/csis/press/pr04_60%5B1%5D.pdf.

[80] Rebecca Grant, "The Fallujah Model."

[81] Ibid.

troops on the ground…," saving lives every day as restricted lines of sight that had once favored defenders were overcome by the persistent surveillance concept achieved by the Predator and other tactical UAVs such as Pioneer.[82]

Operation Phantom Fury also had the benefit of almost unlimited access and allocation to ISR assets for optimal sensor performance. Sensors had a high degree of fidelity with interoperability, allowing "direct feeds via satellite to command centers and selected forces on the ground opened up a full-motion video perspective on the street battle" near-real-time, all the time unbeknownst by insurgent forces.[83]

The battle of Fallujah in November 2004 was the first large contingency of joint "conventional forces" to experience the benefits of streaming situational awareness, soon to be known in the field as geospatial intelligence (GEOINT), derived from the persistent surveillance concept. A shift in the cultural mindset was occurring amongst the forces. With a better understanding of what persistent surveillance could provide to engaging forces on the ground, the requests by the warfighter to have the capability in daily operations grew astronomically. For example, a former Marine involved in the operation recalled the value of GEOINT gained from the persistent surveillance,

> The expansion of GEOINT and the Marines' familiarization with it became the catalyst for its exponential growth in the field. During Operation Phantom Fury, the Marines executed the missions assigned with the tools they were given… The Marines who had now "grown up" with GEOINT support wanted it all the time and knew exactly what to ask for—and they weren't waiting around for it. It was no longer viewed as a "nice to have"; it was a "must have."[84]

The success of Operation Phantom Fury inspired more interest in persistent surveillance throughout the halls of Congress and the Pentagon.

---

[82] Rebecca Grant, "The Fallujah Model."

[83] Ibid.

[84] Stephen Kahn, "GEOINT's Evolution Energizes military Capabilities," *Pathfinder*, The National Geospacial-Intelligence Agency magazine, volume 6, number 4, July–August 2008, 5–7, posted at: https://www1.nga.mil/Newsroom/Pathfinder/0604/Documents/0604.pdf.

In 2005 Marine commanders listed persistent surveillance as one of their top priority needs.[85] The request sparked a joint research project between graduate students at the Air Force Institute of Technology and scientists at Los Alamos National Laboratories. The joint venture developed a tactical persistent surveillance asset known as Angel Fire. Without a clearly defined definition of persistent surveillance for guidance of the concept's use in operations, the program developers created this definition for Angel Fire:

> …persistent, city-sized surveillance…by providing real-time imaging capabilities, IED and other threats … can be detected, prevented and/or negated. Angel Fire is particularly well-suited to provide enhanced situational awareness to forces operating in an urban environment, convoy operations or other ground operations.[86]

Although the intent of the project was to meet the needs of the warfighter in the most expeditious way possible to fight the fight, the acquisition of the newly fielded persistent surveillance asset was delayed in getting out to the field because of controversy between services. At the same time Air Force and Marines were pushing for the acquisition of Angel Fire, the Army was pushing another tactical asset for inter-service application of providing persistent surveillance. Their asset was called Constant Hawk. According to a press report,

> Gary Stradling, the Angel Fire project leader at Los Alamos, e-mailed Marine and Air Force officials to warn them the Army was pushing Constant Hawk "specifically to pre-empt USMC/Angel Fire." He also urged the Marines and Air Force to seek help from members of Congress, including Sen. Pete Domenici, R-N.M…Other e-mails were sent directly to staff members at the Senate and House of Representatives, urging them to raise the issue with their bosses and help speed delivery of Angel Fire.[87]

Without a clear and concise joint definition of the usage of persistent surveillance, each service began to independently interpret how the surveillance should and could be used. Despite good intentions of fulfilling requests from the field for more surveillance

---

[85] Tom Vanden Brook, "Spy technology Caught in Military Turf Battle," USA TODAY, October 17, 2007, at: http://www.usatoday.com/news/military/2007-10-02-angel-fire_N.htm.

[86] Ibid.

[87] Ibid.

assets, each of the armed services requested more money to fund more persistent surveillance assets, sparking multiple independent acquisition programs. Each service justified their requests as a "top priority request" from the field that needed to be put in operation as soon as possible in order to prevail in the battlefields of Iraq. What the services failed to understand was that the persistent surveillance concept depended on several factors, not just having access or control of the asset alone.

The outgrowth of persistent surveillance from 2003-2005 experienced both effective and ineffective employment. Factors that played into effective use of the surveillance concept included: 1) the environment the sensor platforms were used in (i.e., was it an optimal performance environment (weather, climate, operating altitude, degree of interoperability with other sensors); 2) the experience of the operators (i.e., had the operators using the intelligence gathered by persistent surveillance worked in the area being collected on before? Or was this the first time they were learning of the environment); and 3) the clarity of the use of persistent surveillance (i.e., how focused was the surveillance area? Narrow, broad, undefined?).

B. THE CALL FOR MORE PERSISTENT SURVEILLANCE (2006–2007)

By 2006, persistent surveillance had become so popular that the call for its usage had expanded tenfold. The concept had morphed almost completely from usage for high value targets and missions to an everyday resource ground commanders believed was necessary in order to conduct operations taking place in Iraq. Persistent surveillance had gone from fulfilling intelligence gaps in baseline intelligence assessments for mainly strategic objectives to actively seeking unknown gaps for tactical operations.

While the services were battling both Pentagon and Congressional resources to fund their requests for more surveillance assets, strategy in Iraq focused on neutralizing the use of improvised explosive devices (IEDs) used by insurgents that gave them an offensive advantage against coalition forces and defeating the insurgent network at its core.

In 2006, persistent surveillance was considered essential in the take down of the man was believed to be the insurgent leader of all of Iraq, Abu Musab al-Zarqawi. The

"unblinking eye" was considered invaluable to tracking, verifying and (at the end) guiding the bombs that would end Zarqawi's life.

> A reconnaissance-surveillance team from Delta Force's B Squadron, assigned to TF 145's Task Force North, infiltrated the area to get "eyes on" the house, said a source in the special operations community. Sources said a Predator unmanned aerial vehicle was overhead.[88]

During a June 2006 mission debriefing to the press, Army General Bill Caldwell explained that for "the first time that we … had definitive, unquestionable information as to exactly where he was located," in a place where he could be hit "without causing collateral damage to other Iraqi civilians and personnel in the area.[89] Operators involved in the operation were once again experienced, they were familiar with the operating terrain, and they had conducted a great deal of coordination amongst assets prior to commencing operations. Along with this, the target was known and the use of the surveillance assets was used in a narrowly defined search area.

In a separate, but similar type of use against insurgent warfare, the Army sought out a tactical source to aid in the hunt for improvised explosive devices (IEDs)-- the most notorious weapon against U.S. and coalition troops in Iraq.[90] A task force, once confined in secrecy, was created by order of the Army's Vice Chief of Staff, General Richard A. Cody; the task force was named Task Force Observe, Detect, Identify and Neutralize (TF ODIN).[91] The program was said to have been triggered "by the limited numbers of USAF Predator UAVs in Iraq, and consequent refusal of many Army requests"[92] from ground commanders for operational surveillance. Considered a success, TF ODIN is said to be responsible for enabling Army ground commanders to mount a full surveillance and strike effort in Iraq. According to one report, since its conception in July 2007 to June

---

[88] Sean D. Naylor, "Inside the Zarqawi Takedown; Persistent Surveillance Helps End 3-Year Manhunt," *Defense News*, June 12, 2006, Vol. 21, No. 4, 1.

[89] Ibid.

[90] Brad Knickerbocker, "Relentless Toll to U.S. troops of Roadside Bombs," *The Christian Science Monitor*, January 2, 2007, at: http://www.csmonitor.com/2007/0102/p01s03-usmi.html.

[91] David Pugliese, "Task Force ODIN: In the Valleys of the Blind," *Defense Industry Daily*, January 15, 2009, at: http://www.defenseindustrydaily.com/Task-Force-ODIN-In-the-Valleys-of-the-Blind-05250/.

[92] Ibid.

2008, the effort killed more than 3,000 adversaries, and led to the capture of almost 150 insurgent leaders.[93] TF ODIN's biggest advantage is believed to be the persistent surveillance capability along with sensor scans that can detect signatures of disturbed earth or new pavement, which signals ground units to be wary of newly buried IEDs.

> ODIN's current workhorses in Iraq are eight Warrior Alpha UAVs equipped with full-motion video cameras and other imagery systems, and about 10 C-12 King Air turboprops, most equipped with video cameras and, on occasion, signals intelligence sensors. They are linked by radio to brigade commanders and to such aircraft as Apache helicopters that can quickly swoop in for a kill. Using computer software, intelligence analysts assigned to the task force have pieced together pattern-of-life imagery to trace the movements of insurgents suspected of planting IEDs along convoy routes. [94]

TF ODIN was welcomed and commended by the Army with open arms. Like the Marines and other conventional forces that had experienced the benefits of persistent surveillance, operators would no longer be content with anything less than having the availability of constant coverage and situational awareness of their forward operating area at the time of their choosing.

Although the Army had gone solo on the creating and acquisitioning TF ODIN, both the Department of Defense and Congress soon became convinced of the Army's efforts and charged that if more surveillance assets, such as those used in TF ODIN, were available, more lives would be saved and the fight against insurgent led IEDs could be defeated.

In February 2006, the Department of Defense stood up the Joint Improvised Explosive Device Defeat Organization (JIEDDO). The organization's mission was to "…focus (lead, advocate, coordinate) all Department of Defense actions in support of

---

[93] David Pugliese, "Task Force ODIN: In the Valleys of the Blind," *Defense Industry Daily*, January 15, 2009, at: http://www.defenseindustrydaily.com/Task-Force-ODIN-In-the-Valleys-of-the-Blind-05250/.

[94] Jon W. Glass, "Taking Aim in Afghanistan," *CISR Journal*, February 5, 2009, available at: http://www.c4isrjournal.com/ story.php?F=3825704.

Combatant Commanders' and their respective Joint Task Forces' efforts to defeat improvised explosive devices as weapons of strategic influence."[95]

Included in the mission was the use of increased persistent surveillance for attacking the insurgent network at the tactical level. Congress responded in the National Defense Authorization Act for Fiscal Year 2007, to which the House of Representatives Committee on Armed Services recommended $100 million in Title XV for the rapid procurement of no less than ten manned, aerial, persistent surveillance platforms for tactical operations. The decision was based on the recognition that,

> …there is a critical tactical mission requirement in OIF and OEF for additional manned, aerial, persistent surveillance platforms to combat asymmetric threats such as IED. The committee understands IEDs continue to be the primary cause of casualties for U.S. armed forces in OIF and OEF. The committee is aware that current surveillance platforms deployed in OIF and OEF are used almost exclusively for intelligence gathering missions rather than direct support of tactical operations such as interdiction of IED emplacement and convoy security.[96]

Additionally, the committee expected that,

> …manned, aerial, persistent surveillance platforms be rapidly procured for use by ground commanders in OIF and OEF. The committee believes that if these platforms are employed in tactical operations, such as conducting persistent road surveillance missions, then these platforms could prevent the emplacement of IEDs and counter other threats faced by U.S. armed forces on the roads in Iraq. The committee expects these platforms to be configured and staffed so that they can be rapidly deployed and easily maintained without placing additional, unnecessary logistic burdens on U.S. armed forces. The committee also expects these platforms to be equipped for day and night surveillance and for simple, direct communication with ground- and air-based quick reaction forces.[97]

Considered to be a huge win for tactical units in the field, the success of expansion of persistent surveillance assets in actually contributing to successfully hunting IEDs was

---

[95] Mission statement of JIEDDO, as directed by DoD Directive 2000.19E on February 14, 1966, on the JIEDDO site at: https://www.jieddo.dod.mil/index.aspx.

[96] Information gathered from House Report 109-452 – National Defense Authorization Act for Fiscal Year 2007, located at: http://thomas.loc.gov/cgi-bin/cpquery/?&dbname= cp109&sid= cp109KAbKU&refer=&r_n=hr452.109 &item=&sel=TOC_783424&.

[97] Ibid.

difficult to quantifiably measure. Current U.S. strategies used to counter insurgent activity, particularly IEDs, although well intended, have been reactive, defensive and dynamic. In an op-ed column titled, "IEDs: Combating Roadside Bombs," Brigadier General Anthony Tata, Deputy Director for Operations, Joint Improvised Explosive Device Defeat Organization, explains the great difficulty in the efforts against IEDs. He opined,

> We have a major focus on attacking the IED networks underway. JIEDDO operates along three lines of operation: defeat the device; attack the networks; and train the force. Attacking the networks is where we see the biggest dividends in stopping the shipment, construction and emplacement of IEDs…Once coalition forces separate the enemy from the people, they bring in indigenous police forces to hold the security gains and then build trust and confidence as well as conduct reconstruction. We see tips go way up; we see bomb makers turned in; we see IED networks dissolve. There is no greater ambassador for the American people than a war-fighter on the ground interfacing with the local population; and that works. [98]

The main issue with insurgencies, as faced in Fallujah in April 2004, is separating civilians from "the enemy." This is the same issue Gen. Tata speaks of. The problem with irregular warfare is that "…insurgents can infiltrate as civilians, no matter what screening processes the U.S. establishes."[99] Unless specific intelligence has been prepared to narrow the focus area and identifying the target beforehand, it will always be difficult to measure the effectiveness of persistent surveillance assets allocation for ambiguous target sets. But without a precise definition of how the concept is to be used, commanders, contractors and operators loosely tailored justification to have assets that provided persistent surveillance. The question is, at what cost and to whose benefit?

---

[98] Anthony Tata, "IEDs: Combating Roadside Bombs," Washington Post, October 2, 2007, at: http://www.washingtonpost.com/wp-dyn/content/discussion/2007/09/28/DI2007092801469_pf.html.

[99] Anthony H. Cordesman, "The Fallujah Objectives: What Meaningful 'Victory' Really Means," Center for Strategic International Studies, 2, at: http://csis.org/files/media/csis/pubs/iraq_fallujahvictory.pdf.

THIS PAGE INTENTIONALLY LEFT BLANK

V. ANALYSIS AND DISCUSSION

This chapter analyzes the evolution of the persistent surveillance concept based on the historical events discussed in the previous chapter and how the under-defined concept has impacted military acquisitions, planning and operations. As it is with all evolutionary processes, the use of persistent surveillance between 2003 and 2007 experienced both effective and ineffective employment. The measurement of effective or ineffectiveness was based on the following criteria: 1) the environment the sensor platforms were used in (i.e., was it an optimal performance environment (weather, climate, operating altitude, degree of interoperability with other sensors); 2) the experience of the operators (i.e., had the operators using the intelligence gathered by persistent surveillance worked in the area being collected on before? Or was this the first time they were learning of the environment); and 3) the clarity of the use of persistent surveillance (i.e., how focused was the surveillance area? Narrow, broad, undefined?). This chapter also discusses the impact past and present use of the persistent surveillance concept may have on future defense decision makers and planners based on the historic facts outlined in this thesis.

A. THE EFFECTIVENESS AND INEFFECTIVENESS OF PERSISTENT SURVEILLANCE

The premise of insurgent warfare is the gradual inversion against traditional strengths of large armed forces from an advantage to a disadvantage.[100] Guerrilla warfare, small wars, partisan wars, and low-intensity conflict have all been used to describe insurgency warfare of the past. Regardless of the warfare title, the underlying premise of such insurgent warfare has been the same: "warfare on the cheap."[101] Without a clear definition of such warfare there is no clear strategy or acquisition of the proper resources for the force to contend with such an adversary. According to retired Navy Captain Jeff Huber,

[100] Donald M. Snow, *Distant Thunder: Patterns of Conflict in the Developing World*, (Armonk, New York: St. Martin's Press, 1993), 57.

[101] Ibid.

> Our "Good War" military was suited to symmetrical enemies whose political behavior could be compelled by defeat of their armed forces. We haven't had a foe like that since the Berlin Wall came down; arguably, the Soviets ceased to be a serious military threat years if not decades before then. Yet the preponderance of our defense budget is spent on gee-wizardry to deter or fight a peer competitor that will never emerge. At the low-tech end of the spectrum, the Obama administration intends to continue increasing the size of our ground forces to conduct the "long war" against "radical extremists," despite analysis by Rand Corporation that concludes the best way to proceed in our misnamed war on terror is "with a light U.S. military footprint or none at all."[102]

The author of *Distant Thunder: Patterns of Conflict in the Developing World*, Donald M. Snow, says the ability to define insurgency can allow the correct military means and political ends for which insurgent warfare is fought to be properly prescribed. He states,

> In terms of means, insurgency refers to how forces are used strategically and tactically in front of an enemy. As a strategy, it attempts to wear down and weaken a militarily superior foe over time. Its major goal, attrition, is accomplished by prolonging war and exhausting a less dedicated foe. Tactically, insurgency usually involved irregular, part-time, often non-uniformed forces who employ such tactics as ambush, hit-and-run, and avoidance of contact where superiority at the point of engagement does not guarantee victory.[103]

American forces for decades have organized for large-scale conventional operations against like adversaries. In conventional warfare, American forces have succeeded, but forces have experienced setbacks when up against insurgencies. Failures by American forces against insurgencies have been costly; costly not only in the number of service members' lives lost, but also in resources and political influence.

> The U.S. defeat in Vietnam, embarrassing setbacks in Lebanon and Somalia, and continuing political and military difficulties in Afghanistan and especially Iraq underscore the limits of America's hard-won conventional military supremacy. That supremacy has not delivered decisive success against non-state enemies practicing protracted irregular

---

[102] Jeff Huber, "Sticker Shock and Awe," *The American Conservative*, April 6, 2009, at: http://www.amconmag.com/article/2009/apr/06/00025/.

[103] Donald M. Snow, *Distand Thunder: Patterns of Conflict in the Developing World*, 57.

> warfare; on the contrary, America's conventional supremacy and approach to war—especially its paramount reliance on firepower and technology—are often counterproductive.[104]

The reason why American forces have often been ineffective and counterproductive has been because U.S. forces are at an information disadvantage when fighting against insurgents. According to Naval Postgraduate School professor Gordon H. McCormick's *Systems Model of Insurgency*,

> Insurgents begin with an overwhelming information advantage but a force disadvantage. Their primary concern must be to overcome the state's force advantage. The counter insurgency begins with an overwhelming force advantage but an information disadvantage. Its efforts must focus on neutralizing the insurgents' information advantage. The first side that overcomes its disadvantage wins.[105]

As U.S. strategic planners focus countering the insurgent threat environment with a technologic fix to tip the insurgent information advantage, it may be that high-tech gadgetry may not produce a solution to the problem. But how does a technologically driven force begin to think that there could be something other than a high-tech answer? Such thinking would require an exhausting strategic paradigm shift within the Department of Defense (DoD); a paradigm shift requiring less emphasis on the acquisition and role of technologic hardware in executing warfare (i.e., missiles, fighter aircraft).

This was apparent in a survey done in 2000 of some 1,900 officers attending U.S. professional military education that found that most U.S. military officers were "technological optimists."[106] Many of the officers surveyed believed advanced technology was essential to success. Officers who took the survey believed there was

---

[104] Jeffrey Record, "The American Way of War: Cultural Barriers to Successful Counterinsurgency," *CATO Institute*, Policy Analysis no. 577 (September 1, 2006), accessed on CATO Web site at: http://www.cato.o rg/ pub_ display. php?pub_id=6640.

[105] Gordon H. McCormick, "A Systems Model of Insurgency," Department of Defense Analysis, Naval Postgraduate School, Monterey, CA, 13–14. Presented to CIA-RAND Insurgency Board, June 22, 2005.

[106] Thomas G. Mahnken and James R. FitzSimonds, *The Limits of Transformation: Officer Attitudes toward the Revolution in Military Affairs*, Newport Paper 17 (Newport, RI: Naval War College Press, 2003), ch.6.

correlation between operational success and the availability of technology for military operations. The survey conducted indicated three main beliefs of what technology offered: 1) technology was necessary in granting U.S. forces the advantage in engaging in high-intensity operations with substantially reduced risk of casualties; 2) having advanced technology would allow for a shortened duration of engagement in future conflicts; and 3) having advanced technology at the military's disposal made it easier for the United States to use force to achieve decisive battlefield victories.[107] Unfortunately, the officers failed to acknowledge the challenges of insurgent warfare and the events of September 11, 2001.

Understanding the influence persistent surveillance had on decision makers to further employ the surveillance concept is one of the key elements to uncovering the conditions for which persistent surveillance was used throughout the four year span covered in this thesis.

Historical analysis of effective and ineffective operations using persistent surveillance in Iraq between 2003 through 2005 and 2006 through 2007 reflected a shift in strategic usage of the surveillance concept. Operations using persistent surveillance in Iraq between 2003 through 2005 were conducted in a conventional fashion: surveillance was used to enhance pre-gathered intelligence against known targets, conducted by experienced operators in pre-coordinated operations. In contrast, following the 2006 QDR call for persistent surveillance as "vital to mission success in Iraq," persistent surveillance between 2006 and 2007 was used with little to no pre-gathered intelligence, had an increased role against unknown targets and appeared to be used more by inexperienced operators in ad hoc operations.

Between 2003 and 2005, the rescue of Jessica Lynch, capture of Saddam Hussein and success of Operation Phantom Fury were all effective operations that used the persistent surveillance concept. In all of these events, there were three consistent similarities between the operations: planners used persistent surveillance to validate

[107] Thomas G. Mahnken and James R. FitzSimonds, *The Limits of Transformation: Officer Attitudes toward the Revolution in Military Affairs*, Newport Paper 17 (Newport, RI: Naval War College Press, 2003), ch.6.

known intelligence; surveillance search areas were pre-defined based on a known target; and operators had previous experience using the surveillance concept. These operations set the groundwork for how persistent surveillance could be effectively used, but also showed other potentially larger uses. Of course, there were also examples of failures during this time frame, such as operations in Fallujah in April 2004 that proved to be both a learning tool as well as a catalyst for increased persistent surveillance in the future.

As discussed in Chapter III, the measurement of effective or ineffective was based on the following criteria: 1) the environment the sensor platforms were used in (i.e., was it an optimal performance environment (weather, climate, operating altitude, degree of interoperability with other sensors); 2) the experience of the operators (i.e., had the operators using the intelligence gathered by persistent surveillance worked in the area being collected on before? Or was this the first time they were learning of the environment); and 3) the clarity of the use of persistent surveillance (i.e., how focused was the surveillance area? Narrow, broad, undefined?).

As the use of the surveillance concept began to be accepted by the general force, the request for assets that could perform persistent surveillance at both the tactical and strategic planning levels began to have a large impact on Department of Defense budgetary allocations and Congressional funding.

At its inception as an operational goal when first introduced in the 2001 QDR, the under-defined persistent surveillance concept served as an additional tool for operators in obtaining information. What was unseen at the time was that the concept of persistent surveillance had the strength of becoming an organizational catalyst of change for how wars were to be fought. The magnitude of how much of an impact the persistent surveillance concept would actually have on military operations and planning was staggering. According to organizational change theory, the evolution of the persistent surveillance concept began to take place as established military institutional standards of conventional warfare techniques (surveillance techniques and reporting procedures) began to lose their competitive advantage.[108] Whereas the U.S. dominated in

[108] Baraba Czarniawska and Guje Sevon, *Translating Organizational Change*, (Berlin:Germany, 1996), 146–148.

conventional warfare, the insurgency that erupted in Operation Iraqi Freedom (OIF) exposed U.S. vulnerabilities that stunned decision makers, planners, and operators alike. The new surveillance assets and techniques delivered by the persistent surveillance concept, although under-defined on its usage, shed optimism in regaining the offensive advantage now taken by the enemy. It was a concept introduced at the right time, tested by choice, and proven through a combination of chance and calculated consequence.

The operational effectiveness of persistent surveillance in the case of rescuing Private Lynch was possible due to several factors. First, the use of the surveillance asset was conducted in its most optimal performance capacity taking advantage of all facets such as weather and lighting. Second, the mission was a classic joint operations mission accomplished by some of the finest in the force, to include, Army Rangers, Air Force pilots and combat controllers, U.S. Marines, and Navy Seals.[109] The operators were all experienced, having been properly trained and equipped for such missions and familiar with the search and rescue techniques and procedures. In other words, there was proper utilization of the persistent surveillance concept to accomplish their mission. Finally, the asset was on target, at an arranged time, providing overview to specific consumers on a specific location. Therefore, all three effective criteria were met.

The use of persistent surveillance in the hunt for Saddam Hussein was another effective use of the concept. Considered to be the number one high value target in Iraq at the time, the operational effectiveness of persistent surveillance in this case was once again possible due to several factors. First, the surveillance assets, both human intelligence and aerial surveillance vehicles, were focused on a single target (thereby meeting the third criteria for effective use). This allowed for the forces searching for Saddam Hussein to have in their favor the availability of identifiable markings and understanding of his modus operandi (i.e., they knew what he looked liked and knowledge of his habits). This allowed for intensified persistent use of aerial surveillance to verify tips gathered by human intelligence assets for corroboration in a specific area

[109] Comments made by Brigadier General Vincent Brooks during a CENTCOM briefing the day after Private Lynch was rescued on NewHour with Jim Lehrer, transcript posted on April 2, 2003, available at: http://www.pbs.org/newshour/bb/middle_east/jan-june03/lynch_04-02.html.

during the most optimal periods (i.e., the first criteria). Second, the mission was a classic joint operations mission accomplished by a large coalition force. The operators were experienced and had the benefit of both "black" and "white" world intelligence assets. Black world is the use of covert operatives and systems, such as the Central Intelligence Agency's Task Force 121's involvement in the hunt for Saddam. White world assets are conventional force assets. The availability to use both types of assets gave greater surveillance coverage and accuracy in achieving persistent coverage.

These two monumental operational successes in 2003 boded well for the use of persistent surveillance and the concept picked up momentum as war tactics began to shift. Operation Phantom Fury also had the benefit of almost unlimited access and allocation to ISR assets for optimal sensor performance. Sensors used in Operation Phantom Fury had a high degree of fidelity with interoperability, allowing "direct feeds via satellite to command centers and selected forces on the ground opened up a full-motion video perspective on the street battle" near-real-time, all the time unbeknownst by insurgent forces.[110] Coupled with experienced operators on the ground, a focused surveillance area with multiple assets to provide layered coverage, and a clearly defined operational objective, the use of the persistent surveillance concept was effective.

B. INFLUENCE OF DECISION MAKING ON USING PERSISTENT SURVEILLANCE

Leadership examined these successes and failures and now saw other, potentially greater (or so they hoped) uses for persistent surveillance. In contrast to the 2003 to 2005 time frame, the events analyzed between 2006 and 2007 had not emphasized a need to use the concept during optimum operating environments, with pre-coordinated planning by experienced operators, or used with specific target or surveillance areas identified prior to allocating assets. Rather, decision makers placed greater emphasis on the concept as providing the resource of persistent surveillance in an "on call" fashion to be used at the requester's avail. It is during this time that the concept gained momentum as an axiom

[110] Comments made by Brigadier General Vincent Brooks during a CENTCOM briefing the day after Private Lynch was rescued on NewHour with Jim Lehrer, transcript posted on April 2, 2003, available at: http://www.pbs.org/newshour/bb/middle_east/jan-june03/lynch_04-02.html.

for operational success against irregular warfare challenges, to include countering IEDs and hunting down insurgent networks, amongst the mainstream conventional force structure. Under this belief the use of persistent surveillance shifted from an operational goal to an operational concept that operators felt necessary to have at their tactical disposal. The catalyst for the shift stemmed from knowledge that the concept could achieve far greater insight into a possible "future" than the resources currently at hand. Although the "unblinking eye" is not capable of predicting adversary actions, GEOINT did lend the potential for the user to be better prepared for what was in their path, or forewarn of an adversary soon to be faced.

The operators on the ground were desperately trying to take back a tactical advantage against a technologically disadvantaged adversary and hoped that persistent surveillance could provide the "edge." Although technologically disadvantaged, the adversary continuously proved to have the offensive advantage, a fact that proved extremely frustrating. This fact, coupled with a lack of strategy amongst leadership to overcome such an enemy, raised the value of persistent surveillance assets for operators and how operations were planned.

During conventional operations (i.e., warfare that consisted of good guys versus bad guys and a reason for hostilities), operational plans were made in advance. Strategic objectives began with proper training, while simultaneously resourcing the force with the right equipment to gain the offensive advantage against a known adversary. Such strategy becomes crippled when faced with the elements of irregular warfare. The challenge of irregular warfare begins with identifying the good and the bad guys amongst the population Next comes the understanding of the adversary's operational intent (i.e., why, how and where are they operating out of and against whom with what). This information ultimately leads to locating and neutralizing the adversary. Persistent surveillance, if utilized properly, can fill in any missing gaps and aid in mitigating these challenges.

The use of persistent surveillance has been very effective when integrated with forces in conventional operations. However, the effectiveness of the persistent surveillance concept when used solely for gaining actionable intelligence in irregular warfare scenarios is still difficult to assess. The surveillance is believed to provide a

sense of security for leadership and forces operating in dynamic environments, such as irregular warfare. The question is to what end will forces depend on persistent surveillance in providing information that leads them to achieving the real security they actually seek? Persistent surveillance is clearly a valuable asset on today's battlefields. However, the question remains, how is persistent surveillance best used in current and future operations? At this point, the individual services once again decide to split in not only how persistent surveillance is viewed, but how it should be used. This leads to yet another question, "Does the future hold an agreed upon definition and concept of operation?"

C. THE FUTURE OF PERSISTENT SURVEILLANCE IN THE 2010 QDR

Whereas the 2001 QDR introduced persistent surveillance as a potential operational goal and the 2006 QDR fully declared persistent surveillance as an invaluable operational capability vital to mission success in the war in Iraq, what might the 2010 QDR say about the use of persistent surveillance? As the purpose of the QDR is to shape the Department of Defense's plans, policies, and programs into a broader strategy, which will then find its way into the Presidential budget request, there is no better time than now to fully define what persistent surveillance should be and how it should be allocated. Is persistent surveillance a true ISR asset? Or can forces have the persistent surveillance capability in order to provide tactical situational awareness without any "intelligence" attached?

The historical analysis of persistent surveillance conducted in this thesis implies future employment of persistent surveillance will have large budgetary consequences if the concept is not fully defined, its use is not clearly stated in doctrine, and qualitative metrics of effectiveness are not incorporated into U.S. joint warfare.

The concern of implications that stem from an under-defined and loosely justified persistent surveillance concept is illustrated in the debate of using the concept as a means to gain the offensive advantage against the insurgency in Afghanistan, where the three factors of effective usage of the persistent surveillance are less likely to be present.

Commander of U.S. Central Command has made clear acknowledgement that the successful counterinsurgency strategies of Iraq will not work in Afghanistan.[111] Without any clear delineation of usage, the Army has continued to go forward independently in providing persistent surveillance capability to ground commanders. Modeled after the TF ODIN initiative in Iraq, the Army was said to employ TF ODIN-A, giving lower-ranking tactical commanders the real-time persistent surveillance typically reserved for senior leadership and strategic decision makers in Afghanistan.[112] Although classification has hindered verification of such employment, Defense Secretary Gates was believed to be all for it. The *Wall Street Journal* reported that,

> The expansion of the program into Afghanistan hasn't been formally announced, but Defense Secretary Robert Gates alluded to the plan during a congressional hearing last week. Mr. Gates told lawmakers from the House Armed Services Committee that he was going to "re-create" the Iraq effort and "replicate it in Afghanistan with additional assets."[113]

But it's just not the Army fighting in Afghanistan. What assets are Marines, Air Force and coalition partners using? Are the systems interoperable? How much is each sortie costing? And if units are working "jointly," whose asset gets used and who foots the bill?

> Whether a newly formed Task Force ODIN can pull off the same feat when it begins arriving in Afghanistan in 2009 remains an open question. Afghanistan's mountainous terrain, extreme weather conditions and a comparatively weak U.S. and NATO communications infrastructure will be obstacles. In addition, the tactics of Afghan enemy forces have differed from the urban battle of pacification in Iraq, with Taliban fighters actively engaging U.S. and coalition troops in firefights and then disappearing into mountainous hideouts. Rather than taking the exact blueprint… in Iraq and putting it in Afghanistan, you've got to tailor it for that environment…[114]

Unless specific intelligence has been prepared to narrow the focus area and identifying the target beforehand, it will always be difficult to measure the effectiveness

---

[111] Donna Miles, "Petraeus Notes Differences Between Iraq, Afghanistan Strategies," *Department of Defense News*, April 22, 2009, at: http://www.defenselink.mil/news/newsarticle. aspx?id=54036.

[112] Yochi J. Dreazen, "U.S. to Expand Drone Use, Other Surveillance in Afghanistan," Wall Street Journal, September 18, 2008, at: http://online.wsj.com/article/SB122169509501550021.html.

[113] Ibid.

[114] Jon W. Glass, "Taking Aim in Afghanistan," *CISR Journal*, February 5, 2009, available at: http://www.c4isrjournal.com/ story.php?F=3825704.

of persistent surveillance assets allocation for ambiguous target sets. JIEDDO has yet to verifiably prove with quantitative data the effectiveness of using persistent surveillance techniques to find IEDs against the total amount of time, money, and manpower spent in the total of missions the concept was employed in. Of how many total missions were the surveillance assets allocated and used in? How much did each mission's loiter over surveillance area cost? These are the real questions and the implications. Such concern was highlighted in the National Defense Authorization Act for Fiscal Year 2010 Senate report. The report states,

> The committee continues to be concerned that the Department cannot adequately oversee JIEDDO's budget, manpower, and activities in a manner that ensures the most efficient and effective delivery of equipment and capabilities to U.S. forces. The committee urges that the Department consider reexamining JIEDDO's oversight structure to determine whether a principal staff assistant could devote time and attention to JIEDDO's activities commensurate with the size of its activities.[115]

Furthermore:

> As noted elsewhere in this report, the Secretary of Defense has stated in testimony before the Senate Appropriations Committee, Subcommittee on Defense, that the ISR task force should be phased out, while at the same time, the Department has decided to institutionalize JIEDDO. Just as the committee is concerned about the possible hasty demise of the ISR task force, so too the committee is concerned about the premature decision to make JIEDDO permanent. The committee urges the Department to clarify the criteria it is using to determine which institutions should become permanent and which should not, and to demonstrate how these criteria are being consistently applied across organizations.[116]

For all these reasons, and many more involving the acquisition of newly fielded assets to provide persistent surveillance, are all the more reasons why a clear definition of persistent surveillance must be made by joint share holders.

---

[115] Information found in Senate Report 111–035, National Defense Authorization Act for Fiscal Year 2010: Overseas Contingency Operations, available at: http://www.thomas.gov/cgi-bin/cpquery/?&sid=cp11184yHn&refer=&r_n=sr035.111&db_id=111&item=&sel=TOC_704580&.

[116] Ibid.

Under the current definitions, persistent surveillance has a different meaning throughout the DoD. For the U.S. Strategic Command persistent surveillance is defined as:

> the integrated management of a diverse set of collection and processing capabilities, operated to detect and understand the activity of interest with sufficient sensor dwell, revisit rate and required quality to expeditiously assess adversary actions, predict adversary plans, deny sanctuary to an adversary, and assess results of U.S./coalition" actions.[117]

The Joint Intelligence 2–0 publication defines persistent surveillance not as an integrated management of collection capabilities, but rather a collection strategy. The publication calls persistent surveillance a:

> collection strategy that emphasizes the ability of some collection systems to linger on demand in an area to detect, locate, characterize, identify, track, target, and possibly provide battle damage assessment and re-targeting in real or near real time. Persistent surveillance facilitates the formulation and execution of preemptive activities to deter or forestall anticipated adversary course of action.[118]

While the Joint Forces Command (JFCOM), like the Joint Intelligence publication, also defines persistent surveillance as a collection strategy, JFCOM specifically states that persistent surveillance is capable of using the "full range" of collection platforms. JFCOM defines persistent surveillance this way:

> a collection strategy that uses a full range of strategic, operational, and tactical collection systems to dwell on and revisit a target in order to detect, locate, characterize, identify, track, target and assess desired effects. Persistent surveillance contributes to the detection and recognition of meaningful changes in an adversary's activities that support planning and executing preemptive actions to prevent likely adversary courses of action.[119]

Defining persistent surveillance as a collection strategy using the "full range of strategic, operational, and tactical collection systems" allows justification for conventional military

---

[117] DoD Strategic Command. "Persistent ISR Planning and Directing Joint Integrating Concept," Version 1.0, 29 March 2007, available at: www.dtic.mil/futurejointwarfare/concepts/jic_persistentisr_1_0.doc.

[118] Joint Publication 2–0. *Joint Intelligence*, 22 June 2007.

[119] JFCOM/J9 definition pre-JIPS conference.

planners to incorporate national reconnaissance systems, typically reserved for strategic planners at the highest levels of U.S. decision makers, for tactical operations.

All the definitions above lack three basic elements found to be key with using persistent surveillance: the use of persistent surveillance to further investigate a known target; a set limit to loiter time for the assets; and set parameters of the area in which the surveillance should be used in. Without these, each definition allows the use of persistent surveillance to be left up to interpretation of the element using it. Ultimately, without a clear and precise definition of how persistent surveillance should be used, the vicious cycle of mismanaged resources will continue.

However, the 2010 QDR has an opportunity to slow down, and possibly even stop, this vicious cycle from continuing. If the 2010 QDR is geared to drive future acquisitions to counter future threats, then the Department of Defense must clarify the use of persistent surveillance. Therefore, for proper use of the concept, the definition should be precise and leave decision makers and planners little room for misinterpretation as to what justifies the request, acquisition, application, and employment of persistent surveillance. Decision makers and planners must know the consequences of mismanagement and concept misapplication. In addition, standards with quantifiable assessments, that measure the effectiveness of the surveillance concept, should be created and applied amongst all services.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

Historical analysis showed the persistent surveillance concept is useful for missions where objectives are clear; the concept is incorporated in the pre-planning stages of operations; and experienced operators use the products of persistent surveillance. Although many would like to believe the surveillance concept is a cure all, or a panopticon that achieves success in gaining the information advantage necessary to defeat the enemy in every operation the concept is employed in, the fact is it is not.

While this thesis does not propose a precise definition for persistent surveillance, it does highlight the damage an undefined concept can make if left to interpretation. This thesis proposed that the Department of Defense create a clear definition that identifies how, when, and to what extent persistent surveillance should be used. Specifically the definition should identify loiter time, surveillance area parameters and how the concept's effectiveness is to be assessed. Without an accepted and clearly defined use of persistent surveillance in today's joint warfare documents, decision makers and planners are allowed to interpret the concept loosely, justifying the concept's use as each of the armed services sees fit to respond to the needs of their warfighter. Without a collective joint effort, the increased use of this under-defined surveillance concept fuels the vicious cycle of mismanagement—wasting valuable resource of time, money and manpower.

As the conflict in Iraq shifted from conventional battle to stability operations, there was an increased call for more persistent surveillance. Each of the armed services began to independently advocate the need for persistent surveillance. Under the perception the Air Force was not sufficiently allocating enough surveillance assets, the Army and the Marine Corps began seeking alternative means to gain persistent surveillance. As IEDs became the number one cause of force casualties in Iraq, the hunt for IEDs soon became the number one reason why persistent surveillance should be granted to tactical units. And with such pursuit, so began the debate of how viable persistent surveillance was to operations.

Part of the driving factor that warrants the increased need for persistent surveillance is the American reliance on technology for answers. When the technologically-dominant U.S. military found itself at the mercy of an adversary that used handmade improvised explosive devices to successfully gain the offensive advantage, the U.S. government was quick to codify the use of persistent surveillance into operations as the "technological fix" needed to tip the scale.

However, the lack of a clear definition of persistent surveillance may have tipped the scale to the adversary's advantage to an even greater degree as our nation continues to contribute millions of dollars to a "technological fix" that may not be warranted in missions where it is currently being applied. Threats of today and of tomorrow require much more than technologically advanced weapons and much more "sensing" than any technologic surveillance techniques will ever be able to provide.

> While there are those who characterize technology as not making much difference relative to the human dimension of warfare, the truth is that the appropriate mix of both is what has given U.S. joint forces critical advantage in warfare.[120]

[120] David A. Deptula and James R. Marrs, "Global Distributed ISR Operations: The Changing Face of Warfare," *Joint Force Quarterly,* issue 54 (3rd Quarter 2009).

LIST OF REFERENCES

Ackerman, Robert K. "Persistent Surveillance Comes Into View." *Signal Online*, May 2002.

Aircraft Owners and Pilots Association. "Inconsistent FAA Interpretation Leads to Problems with use of Hand-Held GPS Units in Aircraft." Aircraft Owners and Pilots Association, October (2009). http://www.aopa.org (accessed November 2009).

BBC Television. "US faces Iraq guerrilla war." British Broadcasting Company, July 16, 2003. http://news.bbc.co.uk (accessed September 2009).

Bentham, Jeremy. *Panopticon (Preface)*, in Miran Bozovic (ed.), *The Panopticon Writings*. London: Verso, 1995.

Bone, Elizabeth, and Christopher Bolcom. "Unmanned Aerial vehicles: Background and Issues for Congress." *Report for Congress*, The Library of Congress (2003): 1–2.

Brook, Tom Vanden. "Spy technology Caught in Military Turf Battle." *USA TODAY*, (2007): http://www.usatoday.com/news/military/2007-10-02-angel-fire_N.htm (accessed September 2009).

Bruckman, John C. "Overcoming Resistance to Change: Causal Factors, Interventions, and Critical Values." *The Psychologist-Manager Journal*, Issue 2 (2008): 211–219.

Buchannan, Walter E., III. "Intelligence, Surveillance, and Reconnaissance." Statement Before the House Armed Services Committee, Subcommittee on Tactical and Land Forces, (2004): 11. http://www.globalsecurity.org (accessed March 2009).

Bureau of Labor Statistics. "Occupational Outlook Handbook, 2008–2009 Edition: Number of Active and Reserve Members in the U.S. Armed Services." Bureau of Labor Statistics, http://www.bls.gov (accessed September 2009).

Cambone, Stephen A. "Intelligence, Surveillance, and Reconnaissance." Statement Before the Senate Armed Services Committee Strategic Forces Subcommittee, April 7, 2004: 11.

Chizek, Judy G. "Military Transformation: Intelligence, Surveillance and Reconnaissance." *CRS Report for Congress*, January 17, 2003.

Clausewitz, Carl von. "On War." Michael Howard and Peter Paret, eds., (Princeton NJ: Princeton University Press, 1976), 88.

Cohen, William S. “Report of the Quadrennial Defense Review.” Department of Defense (1997): iv.

Cordesman, Anthony H. “The Fallujah Objectives: What Meaningful ‘Victory’ Really Means.” *Center for Strategic International Studies*, 2. http://csis.org (accessed October 2009).

Dale, Catherine. “Operation Iraqi Freedom: Strategies, Approaches, Results, and Issues for Congress.” *Congressional Research Service (RL34387)*, April 2, 2009, 70–71.

Defense Intelligence Agency. “Joint Persistent Surveillance CONOPS.” (D), July 31, 2008.

Department of Defense. “Chapter 8: Command Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance.” *1998 Annual Report to the President and the Congress*, Department of Defense, 2008. http://www.dod.mil (accessed September, 2009).

Department of Defense. “Intelligence, Persistent Intelligence, Surveillance and Reconnaissance Planning and Direction, Joint Integrating Concept Version 1.0.” Department of Defense, http://www.dtic.mil (accessed August 2009).

Department of Defense. “ISR Integration Roadmap.” (D). V PB07, January 2007.

Department of Defense. “Mission statement of JIEDDO.” *DoD Directive 2000.19E*, Department of Defense, February 14, 1966, on the JIEDDO site at: https://www.jieddo.dod.mil (accessed September 2009).

Department of Defense News Briefing with Secretary Rumsfeld and General Myers. June 30, 2003, available at http://www.defenselink.mil (accessed August 2009).

Department of Defense. “Quadrennial Defense Review.” Department of Defense (2006): 67. http://www.defenselink.mil (accessed September 2009).

Department of Defense. “Quadrennial Roles and Missions Review (QRM).” Department of Defense, January 2009: 32. http://www.defenselink.mil (accessed September 2009).

Department of Defense Strategic Command. “Persistent ISR Planning and Directing Joint Integrating Concept.” Version 1.0, March 29, 2007. http//www.dtic.mil (accessed May 2009).

Deptula, David A., and James R. Marrs. “Global Distributed ISR Operations: The Changing Face of Warfare.” *Joint Force Quarterly*, Issue 54 (3rd Quarter 2009).

Dreazen, Yochi J. "U.S. to Expand Drone Use, Other Surveillance in Afghanistan." *Wall Street Journal*, September 18, 2008. http://online.wsj.com (accessed August 2009).

Eisendarth, C., and T. Harkin. *National Insecurity: U.S. Intelligence After the Cold War*. Philadelphia, PA: Temple University Press, 2000.

Glass, Jon W. "Taking Aim in Afghanistan." *CISR Journal*, February 5, 2009: http://www.c4isrjournal.com (accessed August 2009).

Government Accountability Office. "Intelligence, Surveillance, and Reconnaissance: DoD Can Better Assess and Integrate ISR Capabilities and Oversee Development of Future ISR Requirements." *Report on Subcommittee on Air and Land Forces, Committee on Armed Services*, House of Representatives (GAO–08–374), http://www.gao.gov (accessed September 2009).

Government Accounting Office. Intelligence. "Surveillance and Reconnaissance: Preliminary Observations on DOD's Approach to Managing Requirements for New Systems, Existing Assets, and Systems Development." Government Accounting Office, http://www.gao.gov (accessed September 2009).

Grant, Rebecca. "The Fallujah Model."*Air Force Magazine*, February 2005, at: http://www.airforce-magazine.com (accessed August 2009).

Hamilton, Sharon R., R. Smith, and M. McCleary. "Tactical Persistent Surveillance." *Military Intelligence Professional Bulletin*, Vol. 34, No. 3, July–September (2008): 7. Military Intelligence Bulletin via, https://icon.army.mil (accessed September 2009).

Huber, Jeff. "Sticker Shock and Awe." *The American Conservative*, April 6, 2009: http://www.amconmag.com (accessed August 2009).

Information about Operation Red Dawn accounts found on Global Security Web site, at: http://www.globalsecurity.org (accessed August 2009).

Joint Forces Command. "Definition of Persistent Surveillance." *Post-Joint Integrated Persistent Surveillance Conference*, Joint Forces Command, Suffolk, VA, May 26, 2008.

Joint Publication 2–0. *Joint Intelligence*, June 22, 2007.

Kahn, Stephen. "GEOINT's Evolution Energizes military Capabilities." *Pathfinder*, The National Geospacial-Intelligence Agency magazine, volume 6, number 4, (2008): 5–7. https://www1.nga.mil (accessed September 2009).

Kim, Daniel H. "Guidelines for Drawing Casual Loop Diagrems." *The Systems Thinker*, 2009. http://thesystemsthinker.com (accessed October 2009).

Knickerbocker, Brad. "Relentless Toll to U.S. troops of Roadside Bombs," *The Christian Science Monitor*, January 2, 2007. http://www.csmonitor.com (accessed September 2009).

Kopp, Carlo. "Intelligence, Surveillance, and Reconnaissance During Operation Iraqi Freedom." http://www.ausairpower.net (accessed September 2009).

Kramer, F., L. Wentz, and S. Starr. "*I-Power: The Information Revolution and Stability Operations."* Defense Horizons February (2007*)*: 55.

Landon, John. "Definition of ISR Enterprise." *Transcript of statement made before the U.S. House of Representatives Subcommittee on Tactical Air and Land Forces Committee*, October 5, 2005. http://www.globalsecurity.org (accessed October 2009).

Mahnken, Thomas G., and James R. FitzSimonds. *The Limits of Transformation: Officer Attitudes toward the Revolution in Military Affairs.* Newport Paper 17. Newport, RI: Naval War College Press, 2003.

McCormick, Gordon H. "A Systems Model of Insurgency." Transcript of Speech to Department of Defense Analysis, Naval Postgraduate School and presented to CIA-RAND Insurgency Board, June 22, 2005: 13–14.

Miles, Donna. "DoD Releases QDR to Chart Way Ahead to Confront Future." *American Forces Press* (2006): http://www.defenselink.mil (accessed August 2009)

Miles, Donna. "Petraeus Notes Differences Between Iraq, Afghanistan Strategies." *Department of Defense News*, April 22, 2009. http://www.defenselink.mil (accessed August 2009).

Munoz, Carlo. "Services to Lay Groundwork For Joint Unmanned Drone Program." *Inside the Pentagon*, September 20, 2007, http://ebird.afis.mil (accessed September 2009).

Naylor, Sean D. "Inside the Zarqawi Takedown; Persistent Surveillance Helps End 3-Year Manhunt." *Defense News*, Vol. 21, No. 4, (2008): 1.

News release by CSIS analysts November 9, 2004 on the Fallujah offensive, can be found on CSIS Web site at: http://csis.org/files/media/csis/press/pr04_60%5B1%5D.pdf (accessed September 2009).

Office of Law Revision. "Title 10, Section 118 of the United States Code." U.S. House of Representatives, 2009. http://uscode.house.gov (accessed October 2009).

Pendall, David W. "Persistent Surveillance and Its Implications for the Common Operating Picture." *Military Review*, November/December (2005): 43.

Pugliese, David. “Task Force ODIN: In the Valleys of the Blind.” *Defense Industry Daily*, January 15, 2009: http://www.defenseindustrydaily.com (accessed August 2009).

Record, Jeffrey. “The American Way of War: Cultural Barriers to Successful Counterinsurgency.” *CATO Institute*, Policy Analysis no. 577, September 1, 2006. http://www.cato.org (accessed September 2009).

Savastopulo, Demetri. “U.S. Military in Dogfight Over Drones.” *Financial Times*, August 20, 2007, http://ebird.afis.mil (accessed September 2009).

Secretary of Defense Rumsfeld and Joint Chiefs of Staff Chairman Richard Myers conducted a news media briefing on April 7, 2004, transcript located at: http://www.america.gov (accessed September 2009).

Senate Report 111–035. “Overseas Contingency Operations.” *National Defense Authorization Act for Fiscal Year 2010*. http://www.thomas.gov (accessed October 2009).

Shanker, Tom, and Eric Schmitt. “A Nation at War: Special Operations.” *New York Times,* April 6, 2003. http://www.nytimes.com (accessed September 2009).

Snow, Donald M. *Distant Thunder: Patterns of Conflict in the Developing World*. Armonk, New York: St. Martin’s Press, 1993.

Spires, Shelby G. “Army Hoping to Keep UAvs from Air Force.” *Huntsville (AL) Times*, August 13, 2007, http://ebird.afis.mil (accessed August 2009).

Tata, Anthony. “IEDs: Combating Roadside Bombs.” *Washington Post*, October 2, 2007. http://www.washingtonpost.com (accessed August 2009).

Thomas, Evan, and Rod Nordland. “How We Got Saddam.” *Newsweek*, December 22, 2003. http://www.newsweek.com (accessed September 2009).

Transcript of President George Bush, aboard the USS Abraham Lincoln on May 1, 2003. *The Guardian*, at: http://www.guardian.co.uk (accessed August 2009).

Treverton, Gregory F. *Reshaping National Intelligence for an Age of Information*. New York: Cambridge University Press, 2001.

U.S. Air Force. “Capabilities of the Predator RQ–1/MQ–1/MQ–9 Reaper.” U.S. Air Force. http://www.airforce-technology.com/projects/predator/ (accessed August 2009).

U.S. House of Representatives. “House Report 109–452.” *National Defense Authorization Act for Fiscal Year,* U.S. House of Representatives, 2007. http://thomas.loc.gov (accessed September 2009).

Vemmer, Shiela. “Lt. Gen. David Deptula: U.S. Air Force Deputy Chief of Staff for ISR.” *Defense News,* January 12, 2009, via Defense News, http://www.defensenews.com (accessed August 2009).

Welsh, William. “DoD Budget forecast Threatens New Technology Developments.” *Defense Systems*, October 15, 2009. Defense Systems, http://www.defensesystems.com (accessed October 2009).

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California