THE VULNERABILITIES OF UNMANNED AIRCRAFT SYSTEM COMMON DATA LINKS TO ELECTRONIC ATTACK

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

JAYSEN A. YOCHIM, MAJOR, US ARMY
B.S., Weber State University, Ogden, Utah, 1998

Fort Leavenworth, Kansas
2010-01

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* 11-06-2010	**2. REPORT TYPE** Master's Thesis	**3. DATES COVERED** *(From - To)* AUG 2009 – JUN 2010

4. TITLE AND SUBTITLE The Vulnerabilities of Unmanned Aircraft System Common Data Links to Electronic Attack	**5a. CONTRACT NUMBER**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) MAJ Jaysen A. Yochim	**5d. PROJECT NUMBER**
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army Command and General Staff College ATTN: ATZL-SWD-GD Fort Leavenworth, KS 66027-2301	**8. PERFORMING ORG REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	**10. SPONSOR/MONITOR'S ACRONYM(S)**
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Unmanned aircraft are fulfilling critical roles in Iraq and Afghanistan. They are integral in base defense plans and the protection of key infrastructure. They enable commanders to monitor activity throughout their area of responsibility and direct action, when required. Many policymakers see Unmanned Aircraft Systems as a cost effective alternative to manned aircraft and a way to prevent risking a pilot's life. These systems have a number of advantages over manned aircraft. They are unbound by human limitations. They can remain airborne for long durations, do not require life support systems, do not need to eat or sleep, and they will never say no to a mission. They may minimize friendly loss of life by conducting missions that have a minimal chance of survival. However, unmanned systems also have some disadvantages when compared to manned aircraft. They are still prone to human error due to their being flown by ground-based operators. Their development and procurement cost has grown exponentially as capabilities increase. Current systems are not autonomous and their control is contingent on uninterrupted communications. Their dependence on a constant control signal has contributed to a UAS accident rate 100 times greater than manned aircraft A threat could exploit this need for an uninterrupted data feed by using Electronic Warfare to disrupt this signal, potentially crippling unmanned systems.

15. SUBJECT TERMS
Unmanned Aircraft Systems, Unmannded Aerial Vehicles, Electronic Warfare, Jamming, Counter-UAV, Common Data Links

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	118	

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

MASTER OF MILITARY ART AND SCIENCE
THESIS APPROVAL PAGE

Name of Candidate: Major Jaysen A. Yochim

Thesis Title: The Vulnerabilities of Unmanned Aircraft System Common Data Links to Electronic Attack

Approved by:

______________________________________, Thesis Committee Chair
Bill J. McCollum, Ed.D.

______________________________________, Member
Kenneth J. Riggins, M.S.

______________________________________, Member
Major Nicholas J. Martin, M.S.

Accepted this 11th day of June 2010 by:

______________________________________, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

THE VULNERABILITIES OF UNMANNED AIRCRAFT SYSTEM COMMON DATA LINKS TO ELECTRONIC ATTACK, by Major Jaysen A. Yochim, 118 pages.

Unmanned Aircraft are fulfilling critical roles in Iraq and Afghanistan. They are integral in base defense plans and the protection of key infrastructure. They enable commanders to monitor activity throughout their area of responsibility and direct action, when required. Many policymakers see Unmanned Aircraft Systems as a cost effective alternative to manned aircraft and a way to prevent risking a pilot's life. These systems have a number of advantages over manned aircraft. They are unbound by human limitations. They can remain airborne for long durations, do not require life support systems, do not need to eat or sleep, and they will never say no to a mission. They may minimize friendly loss of life by conducting missions that have a minimal chance of survival. However, unmanned systems also have some disadvantages when compared to manned aircraft. They are still prone to human error due to their being flown by ground-based operators. Their development and procurement cost has grown exponentially as capabilities increase. Current systems are not autonomous and their control is contingent on uninterrupted communications. Their dependence on a constant control signal has contributed to a UAS accident rate 100 times greater than manned aircraft A threat could exploit this need for an uninterrupted data feed by using Electronic Warfare to disrupt this signal, potentially crippling unmanned systems.

ACKNOWLEDGMENTS

This project would have not been possible without the assistance of the staff at the Combined Arms Research Library, Fort Leavenworth, Kansas. These professionals conducted research, coordinated inter-library loans, and obtained copyrights.

I would like to thank my committee, especially Dr. Bill McCollum for all the work he did as my committee chair. He was always supportive of my direction but knew when to intervene to adjust my course. Dr. Bill went above and beyond, from recruiting other committee members, to proof reading volumes of material.

I would like to thank those who contributed interviews to this project. They broke down this highly technical subject into an understandable language. This study would not have been possible without their support.

I must thank my friend, Mariann Foster, who helped edit this study. She never complained about my lack of writing skills and was always supportive. She is a good friend and I do not know what I would have done without her assistance.

My entire career is the responsibility of Mark and Brenda Yochim, my parents. They always believed in my passion for military aviation and my desire to serve. Their daily example of perseverance and fortitude is what has allowed me to succeed.

Finally, I would like to thank my wife Alisa, my daughter Mara, and my son Jansen. This “family break” at Command and General Staff College was busier than I had advertized. Alisa is my anchor and was always there to tell me to suck it up. She never let me feel sorry for myself and lovingly kept me focused on the goal. I am thankful to my kids for their understanding when daddy had to work. My kids give some of the best back scratches.

TABLE OF CONTENTS

ACRONYMS

AC2	Airspace Command and Control
ADAM	Air Defense Airspace Management
AE	All Environment
AGL	Above Ground Level
AMPS	Aviation Mission Planning System
ANCOC	Advanced Non-Commissioned Officer Course
AO	Area of Operations
APART	Annual Proficiency and Readiness Test
AR	Army Regulation
ASI	Additional Skills Identifier
ATM	Aircrew Training Manual
ATO	Air Tasking Order
AVGAS	Aviation Gas
BAE	Brigade Aviation Element
BAMS	Broad Area Maritime Surveillance
BCT	Brigade Combat Teams
BLOS	Beyond Line of Sight
BNCOC	Basic Non-Commissioned Officer Course
C2	Command and Control
C4ISR	Command, Control, Communication, Computer, Intelligence, Surveillance and Reconnaissance
CA	Coordinating Altitude
CAB	Combat Aviation Brigades

CAB	Combined Arms Battalion
CBO	Congressional Budget Office
CDL	Common Data Link
C-IED	Counter-Improvised Explosive Device
CJCS	Chairman Joint Chiefs of Staff
COCOM	Combatant Command
COMSEC	Communications Security
COP	Common Operational Picture
CRP	Communications Relay Package
CTC	Combat Training Center
DARO	Defense Airborne Reconnaissance Organization
DOD	Department of Defense
DOTMLPF	Doctrine, Organization, Training, Material, Leadership, Personnel, and Facilities
EA	Electronic Attack
ECCM	Electronic Counter-Countermeasures
ECM	Electronic Countermeasures
EHF	Extremely High Frequency
EM	Electromagnetic Jamming
EO	Electro Optical
EP	Electronic Protection
ERMP	Extended Range/Multi-Purpose
EW	Electronic Warfare
EWS	Electronic Warfare Support
FAA	Federal Aviation Administration

FCS	Future Combat System
FM	Field Manual
FMV	Full Motion Video
FYDP	Future Years Defense Plan
GAO	Government Accountability Office
GCS	Ground Control Station
GMTI	Ground Moving Target Indication
GPS	Global Positioning System
HIMEZ	High Altitude Missile Engagement Zone
HMMWV	High Mobility Multi-purpose Wheeled Vehicles
IFF	Identification Friend or Foe
IR	Infra-Red
ISR	Intelligence, Surveillance, and Reconnaissance
JCIGCS	Joint Common Interoperable Ground Control Station
JDDC	Joint Doctrine Development Community
JDPC	Joint Doctrine Planning Conference
JFACC	Joint Forces Air Component Commander
JFC	Joint Force Commander
JP	Joint Publication
LOS	Line of Sight
LRFD	Laser Range Finder Designator
LRS	Long Range Surveillance
MOI	Memorandum of Instruction
MPH	Miles per Hour
MSL	Mean Sea Level

MTT	Mobile Training Teams
NATO	North Atlantic Treaty Organization
NRL	Naval Research Laboratory
NTC	National Training Center
OC	Observer/Controller
OEF	Operation Enduring Freedom
OIF	Operation Iraqi Freedom
OSGCS	One System Ground Control Station
OSRVT	One System Remote Viewing Terminal
PEO AVN	Program Executive Office Aviation
RDT&E	Research, Development, Test and Evaluation
RL	Readiness Level
ROE	Rules of Engagement
RSTA	Reconnaissance, Surveillance, and Target Acquisition
RVT	Remote Viewing Terminal
S-APART	Semi-Annual Proficiency and Readiness Test
SAR	Synthetic Aperture Radar
SATCOM	Satellite Communications
SECDEF	Secretary of Defense
SHF	Super High Frequency
SIP	Standardization Instructor Pilot
SIP	Standardization Instructor Pilot
SME	Subject Matter Expert
SOCOM	Special Operations Command
SUAS	Small Unmanned Aircraft System

SUAV	Small Unit Unmanned Aerial Vehicle
TACS	Theater Air Control System
TC	Training Circular
TF	Task Force
TUAS	Tactical Unmanned Aircraft System
UA	Unmanned Aircraft
UAS	Unmanned Aircraft System
UAV	Unmanned Aerial Vehicle
UHF	Ultra High Frequency
US	United States
USA	United States Army
USAF	United States Air Force
USJFCOM	United States Joint Forces Command
USN	United States Navy
USV	Unmanned Surface Vehicle
UUV	Unmanned Underwater Vehicle
VDL	Video Data Link

ILLUSTRATIONS

TABLES

CHAPTER 1

INTRODUCTION

> We're at a real time of transition, here, in terms of the future of aviation, and the whole issue of what's going to be manned, and what's going to be unmanned, and what's going to be stealth and what isn't. How do we address these threats? . . . . I think we're at the beginning of this change. I mean, there are those that see JSF as the last manned fighter--fighter-bomber--or jet. And I'm one that is inclined to believe that.
>
> — Admiral Michael G. Mullen, USN, Chairman, Joint Chiefs of Staff

Unmanned Aircraft (UA) are fulfilling critical roles in Iraq and Afghanistan. They are integral in base defense plans and the protection of key infrastructure. They enable commanders to monitor activity throughout their area of responsibility and direct action, when required. Many policymakers see Unmanned Aircraft Systems (UAS) as a cost effective alternative to manned aircraft and a way to prevent risking a pilot's life.

These systems have a number of advantages over manned aircraft. They are unbound by human limitations. They can remain airborne for long durations, do not require life support systems, do not need to eat or sleep, and they will never say no to a mission. They may minimize friendly loss of life by conducting missions that have a minimal chance of survival.

However, unmanned systems also have some disadvantages when compared to manned aircraft. UAS are still prone to human error due to their being flown by ground-based operators. Their development and procurement cost has grown exponentially as capabilities increase. Current systems are not autonomous and their control is contingent on uninterrupted communications. Their dependence on a constant control signal has contributed to a UAS accident rate 100 times greater than manned aircraft (Congressional

Research Service 2005, 2). A threat could exploit this need for an uninterrupted data feed by using Electronic Warfare (EW) to disrupt this signal, potentially crippling unmanned systems.

Military aviation is in a transitional phase. Determining the future force structure and the required equipment is a complex proposition, and this transformation demands extensive research and development. The research and development effort will be expensive and time-consuming. US military aviation stands to remain the dominant global airpower force if their vision of the future force is correct, but if their vision is incorrect, it will be fighting to regain airpower relevancy.

Background

The history of unmanned aerial flight is long and diverse, reaching back to the early years of military aviation. Military aviation, as a distinct organization, was first established in 1912 with the formation of the British Royal Flying Corps (Royal Air Force Organization 2009). Military aviation innovation continued to progress and soon military forces began using aircraft to spot for artillery and limited reconnaissance. The combat effectiveness of aircraft supporting ground warfare resulted in the birth of anti-aircraft artillery, but early anti-aircraft gunners were ineffective, due to inadequate training. In 1917, the British Army requested a system that would improve training for anti-aircraft gunners. The government assigned Archibald Montgomery Low, a pre-war physicist, engineer, and inventor who some consider the father of radio guidance, with the task of developing such a system. On 21 March 1917, he designed and tested the first Unmanned Aerial Vehicle (UAV) known as the Ruston Proctor Aerial Target (Bloom 1958, 142).

In World War II, the remotely operated aircraft experienced its next evolution. The most famous unmanned systems of World War II were the German V1 and V2 guided munitions. These systems were pre-programmed with an area target, guided by simple autopilots, and were completely autonomous once launched. While impressive and a critical concern for the British, the German Henschel Hs 293 and Ruhrstahl Fritz-X were the most successful unmanned systems of the war. Both were air launched, radio guided, anti-ship bombs and are credited with damaging or destroying 32 allied vessels (Bogart 1976, 62). The German military also used remotely operated Surface-to-Air and Air-to-Air Missiles (AAM) with minimal success. During this period, remotely operated systems were limited by their inability to reliably maintain communication links.

Throughout the Korean and Vietnam War Eras, the use of unmanned target drones, cruise missiles, and reconnaissance drones expanded. However, similar to the German V-1 and V-2, these systems were auto-piloted, and not remotely guided. In 1986, the UAV entered the modern era with the development of the British Phoenix and United States/Israeli Pioneer. For the first time, these systems integrated remote guidance, range, endurance, payload, and cost into a reliable platform. Since 1986, unmanned system design, procurement, and utilization exploded globally (Goebel 2009). Most modern militaries are or have developed UAS programs and numerous countries are producing UASs. Asymmetric threats are also seeking UASs. In 2006, Israel acquired and shot down an Iranian produced UAS operated by Hezbollah, a non-state actor (Eshel 2006).

The use of unmanned systems is becoming a mainstay on the modern battlefield. Unmanned systems gather intelligence, observe key terrain, disable explosives, clear underwater mines, and perform a myriad of other missions. Future plans call for unmanned systems capable of ground combat, medical evacuation, troop transport, logistical support, and innumerable other functions limited only by the human imagination. UAS have become so integrated in modern military operations that some contest that unmanned systems have spurn an emerging Revolution in Military Affairs (RMA) (Edwards 2009, 4). Undeniably, the use of unmanned systems has spread beyond their original design concept.

Military leaders originally intended to utilize remote platforms on dirty, dangerous, and dull missions (Braybrook 2004). The logic was simple; when military leaders determined a mission profile caused undue risk to personnel, unmanned systems provide expendable options. However, the performance of unmanned systems in combat and the information they provide commanders, has transformed the view of these systems. Once a dispensable tool, they are now an invaluable asset. Military forces have become information dependent organizations were command centers serve as the information hub.

The design and layout of Tactical Operations Centers (TOC) support the gathering, processing, and redistribution of information. The geographic center of most TOCs consists of a digital map, a computerized significant event tracker, and a display showing UAS Full Motion Video (FMV). The real-time information provided by these airborne systems is processed and analyzed within the TOC resulting in the development of intelligence. In essence, the UAS has become the commander’s window to the battlefield. If required, commanders can rapidly redeploy these systems throughout the battle space ensuring the ability to see the operational environment. While these systems have proven important to combatant commanders, has the United States military become over reliant on UAS? If the answer to this question is yes, then protection of the electromagnetic spectrum must be a mission priority.

Remotely operated UASs require two separate radio communications links to operate: one communications link feeds FMV to a Remote Viewing Terminal (RVT) through a Video Data Link (VDL), the other communication link controls the UAS through a Common Data Link (CDL). The VDL uses an omnidirectional antenna to broadcast its communication feed in all directions, allowing any RVT tuned into the UASs VDL frequency to observe the UASs FMV. Video quality and consistency of reception is dependent on the VDL signal strength. The CDL can use either an omnidirectional antenna or a directional antenna that broadcasts only in the direction of the Ground Control Station (GCS) (Hill 2010).

If a CDL experiences frequency interference, the UA executes a self-recovery program known as a “lost link procedure” and attempts to reacquire the CDL from the GCS. If smaller UA, such as the RQ-11 Raven, fails to reacquire the CDL, it continues its self-recovery program and returns to a preprogrammed recovery point. When some larger UA, such as the RQ-7 Shadow, fail to reacquire the CDL, the operators may identify the UA as rogue and deploy a recovery parachute to avoid endangering manned aircraft (Hill 2010).

The scope of this research is limited to Man-Portable and Tactical UAS as defined in Field Manual (FM) 3-04.15, *Multi-Service Tactics, Techniques, and Procedures for the Tactical Employment of Unmanned Aerial Systems,* dated 3 August 2006. These UAS operate in support of tactical commanders and at altitudes less than 10,000 feet. The systems referenced will primarily be US Army systems. This study presumes design philosophies and technologies are common throughout this class of UAS. However, if systems emerge that demonstrate minimal weaknesses, those systems will be identified as recommendations for future development.

The US military has conducted little research on counter Tactical UAS operations. The UAS field is scientifically complex and this researcher is not a scientist. Rather, the focus of this research is on the operational application of scientifically informed theory. Continuing, this research does not address the science of UAS vulnerabilities. Further scientific research is required to adapt UAS to counter threats once identified.

The primary question of this study is: Are UAS CDLs vulnerable to Electronic Attack (EA)? To address this question, the following secondary questions are relevant:

1. What are the ramifications of an EA on UAS CDL systems?

2. What countermeasures can mitigate EAs?

3. Using DOTMLPF, how has the Army prepared for EW?

4. What UAS are most susceptible to EW?

Significance

Today's commanders are using UASs throughout the battlefield. They have become indispensable to combat commanders and their ability to command and control forces. The Joint force has revised doctrine to account for their abilities to shape the battlefield environment. If threat forces develop a technique to deter UAS operations, it could drastically effect how the US, as well as other militaries, operates. Additionally, the design and procurement of UAS has expanded due to the relative reliability of UAS in an uncontested environment. Consequently, due to budgetary constraints the US military has favored increased funding to the research and development of unmanned systems over manned vehicles. Some military analysts have professed an UA might ultimately replace existing and recently developed observation and attack aviation assets as well as fighter platforms. The aircraft affected would include the OH-58, AH-1, AH-64, A-10, F-16, F-22, and F-35 (Allexperts 2005). Thus, innovative research and development of advanced manned aircraft, specifically attack rotary wing, has been limited in the United States. Instead, the United States has favored modernization of current manned aircraft with minimal planning for replacements. While effective in the current environment, if unmanned systems are susceptible to EA, the future force might not receive the vital services manned aircraft currently provide.

Assumptions

The US military is an expeditionary force that projects its power globally. As such, its equipment tends to be mobile, hardened, and durable. If the equipment requires power, it is often vehicle mounted or tied into a power generation grid. Due to this specialization, US equipment tends to be large and expensive. As an expeditionary force, they tend to fight wars on foreign soil.

Mobility requirements do not bind current or future adversarial forces when planning their internal defenses. Equipment designers do not need to account for mobility or durability in their designs. Their equipment will utilize existing infrastructure and thus have an unlimited power potential. These designs may be technologically advanced, but simple to produce. The simplicity allows for indigenous production. Compiled, these advantages reduce the equipment cost and allow for higher equipment inventories.

Further, an adversary’s mission may not depend on shooting down an UAS. As mentioned earlier, commanders utilize the information provided by UAS to plan, synchronize and execute combat operations. They rely upon UASs to increase their situational awareness and expand their command and control (C2) capabilities to assess effects and direct forces as required to achieve mission objectives. But for the adversary, denying commanders the ability to effectively use a UAS may represent a tactical victory.

Throughout history, warfare has driven the adaptation and production of new equipment. Complex equipment, such as aircraft, requires an expensive and lengthy procurement process. The time required to design effective countermeasures is lengthy if an adversary is able to design an effective counter UAS weapon.

Further, historically adversaries have used the US forces Rules of Engagement (ROE) to their advantage. Future adversaries will continue to use the US ROE to their advantage. Their counter-UAS weaponry will be intermixed with their civilian populace. These tactics mitigate the US military's ability to target such weaponry by conventional means.

Definitions of Key Terms

Listed below is a brief glossary of key terms relevant to this study. Based on Joint and Army Publications, these definitions will aid the reader in understanding the concepts and analysis presented in this paper.

Common Data Link (CDL). The means of connecting an UA to a GCS for the purpose of transmitting and receiving flight command data inputs necessary to control UAS while in flight (US Joint Forces Command 2009b, 111).

Countermeasures. That form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity (US Joint Forces Command 2009b, 101).

Electronic Countermeasures (ECM). A subsection of EW, ECMs defend against forms of EA or surveillance including communication jamming, radar acquisition, and radar tracking (US Joint Forces Command 2009b, 101).

Electromagnetic Interference (EMI). Any electromagnetic disturbance that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics and electrical equipment. It can be induced intentionally, as in some forms of EW, or unintentionally, as a result of spurious emissions and responses, intermodulation products, and the like (US Joint Forces Command 2009b, 135).

Electromagnetic Jamming. The deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of preventing or reducing an enemy's effective use of the electromagnetic spectrum, and with the intent of degrading or neutralizing the enemy's combat capability (US Joint Forces Command 2009b, 135).

Electromagnetic Spectrum. The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands (US Joint Forces Command 2009b, 47).

Electronic Attack (EA). Division of EW involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires (US Joint Forces Command 2009b, 47).

Electronic Warfare (EW). Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. EW consists of three divisions: EA, Electronic Protection (EP), and Electronic Warfare Support (EWS) (US Joint Forces Command 2009b, 137).

Line of Sight (LOS). The unobstructed path from a soldier, weapon, weapon sight, electronic-sending and -receiving antennas, or piece of reconnaissance equipment to another point (Headquarters, Department of the Army 2004, 125).

Man-portable UAS. These UAS are small, self-contained, and portable. They usually operate below the coordinating altitude. Their use supports the small ground combat teams/elements in the field. They are self-contained and controlled at the combat team level. Data is usually direct FMV constrained to LOS to the operator only (Headquarters, Department of the Army 2006a, 14).

Remote Video Terminal (RVT). An RVT enables a user to receive UAS video away from a GCS. RVTs are designed to be portable and compatible for operations in battlefield command vehicles and some aircraft (Headquarters, Department of the Army 2006a, 18).

Tactical UAS. Tactical UAS are larger systems that support maneuver commanders at various tactical levels of command and can also support the small combat teams when so employed. They are deployable among the tactical command levels and are operated by specialized UAS units, locally controlled and operated. Data products can expand beyond FMV depending on UAS payload configuration and can be disseminated to combat teams in real time using an RVT (Headquarters, Department of the Army 2006a, 14).

Theater UAS. Theater UAS are generally deployed to support theater-wide requirements. Theater UAS permit varied support to combat team and subordinate tactical command levels depending on the type of UAS. The theater UAS design and robust C2 architecture permit split site operations. Specifically, the UA can be deployed to theater with mission C2 and data collection, processing and dissemination being conducted locally or outside of theater of operations under reachback conduits (Headquarters, Department of the Army 2006a, 15).

Unmanned Aerial Vehicle (UAV). A powered, aerial vehicle that does not carry a human operator, uses aerodynamic forces to provide vehicle lift, can fly autonomously or be piloted remotely, can be expendable or recoverable, and can carry a lethal or nonlethal payload. Ballistic or semiballistic vehicles, cruise missiles, and artillery projectiles are not considered unmanned aerial vehicles (US Joint Forces Command 2009b, 419).

Unmanned Aircraft (UA). An aircraft or balloon that does not carry a human operator and is capable of flight under remote control or autonomous programming (US Joint Forces Command 2009b, 419).

Unmanned Aircraft System (UAS). That system whose components include the necessary equipment, network, and personnel to control an unmanned aircraft (US Joint Forces Command 2009b, 419).

Video Data Link (VDL). The means of connecting an UA to a RVT for the purpose of transmitting and receiving FMV (US Joint Forces Command 2009b, 111).

Limitations

This study is limited to the Man-Portable and Tactical UAS classes, the most commonly used systems by tactical units. The US military has conducted limited research on counter UAS operations against these classes and this research is beyond the classification of this study. This study will examine the Army Readiness Center research on UAS reliability but these records are incomplete due to inconsistencies in reporting of Man-Portable UAS accidents. Man-Portable and Tactical UAS are untested in an active

EA environment due to the relative age of these technologies. Therefore, no combat findings are available to add to this study. This qualitative study may identify operational theories that require further scientific research. However, it will not present scientifically tested solutions to a known problem, though it may identify an unknown problem that requires a scientific solution. In order to maximize distribution, this study remains unclassified.

Delimitations

The focus of this study is external threats to the UAS CDLs. This study will not cover fully autonomous UAS or their internal navigation control systems. The focus is on UA intended to complete an entire mission sortie through a successful recovery. Therefore, this research does not include remotely guided munitions such as cruise missiles, wire guided missiles, radio guided munitions, or precision guided bombs.

CHAPTER 2

LITERATURE REVIEW

> Technology is not the limitation . . . it's the ability of people to conceive of ways to use the technology.
>
> — Rich O'Lear, VP for Unmanned Aircraft Systems, Lockheed Martin

Six types of literature are relevant to this study. The first is Joint and service doctrine including Joint Publications (JP), Army FMs, and Multi-Service Manuals that concentrate on the training, operation, and command and control of UAS. Second, government white papers, congressional reports, and service studies contain a vast amount of information. Third, professional journals such as Jane's, Armada International, and Journal of Electronic Defense contain information from analysts, researchers, and manufactures. Fourth, books including institutional textbooks, reference books, and history books detail research and experiences involving UAS. Fifth, to the dynamic nature of this studies subject, this study will review numerous blogs as well as print, video, and web based news reports. Lastly, the UAS industry has published numerous fact sheets, brochures, and information papers to advertise their products.

This chapter will first review the types of literature this study may use to answer the primary research question. Next, this chapter analyzes the existing literature in order to identify the gaps in the record and identify pertinent military trends. Lastly, this chapter describes the significance of the thesis in relation to existing literature.

Doctrine

Joint Doctrine

The Joint doctrine regarding UAS is not current and does not reflect lessons learned during combat operations in Iraq and Afghanistan. Consequently, Joint Publications (JP) offer little new information regarding UAS training, employment, or command and control. There are also inconsistencies in UAS terminology.

There are four noteworthy Joint or multi-service publications relevant to this UAS discussion. The base JP for UAS is JP 3-55.1, *Joint Tactics, Techniques, and Procedures for Unmanned Aerial Vehicles,* dated 27 August 1993. The focus of this publication is the Reconnaissance, Surveillance, and Target Acquisition (RSTA) capabilities UAS deliver to the battlefield. It attempts to establish basic terminology, determine UAS classifications, identify airspace considerations, and recommend methods of employment. However, most of the Joint doctrine contained in JP 3-55.1 is outdated and does not incorporate lessons learned in Iraq and Afghanistan, or account for UAS innovation over the last decade. This JP does not address employment or considerations of armed UAS. In addition, the publications doctrine uses inconsistent UAS terminology and individual service doctrine terminology often differs from Joint doctrine.

The most current multi-service UAS publication is FM 3-04.15, *Multi-Service Tactics, Techniques, and Procedures for the Tactical Employment of Unmanned Aerial Systems,* dated 3 August 2006. This publication adds fidelity to the tactics, techniques, and procedures introduced in JP 3-55.1. It discusses planning considerations, employment tactics, and communications procedures for armed and RSTA UAS platforms. However, the classification of UAS platforms in FM 3-04.15 differs from the

UAS classifications in JP 3-55.1. To establish common terminology, this study uses the UAS platform classifications identified in FM 3-04.15.

The primary procedural control publication for UAS is, JP 3-52 *Doctrine for Joint Airspace Control in the Combat Zone, dated*, 22 July 1995. This literature concentrates on procedural control of UAS in congested airspace to mitigate risk. It discusses considerations requiring attention to integrate UAS into manned airspace, such as difficulties using radar to acquiring and tracking UAS due to their unique design, construction and design profile.

The Joint community's primary Electronic Warfare (EW) doctrine is, JP 3-51 *Joint Doctrine for Electronic Warfare*, 7 April 2000. This publication does not specifically address UAS employment, considerations, or vulnerabilities. Rather, the focus of JP 3-51 is the fundamentals and principles of EW. The Joint environment breaks EW into EA, EP, and EWS. This study draws on the EA and EP aspects of this publication. This information allows for determining what type of EW can affect UAS CDL and what protection designs are possible.

Army Doctrine

There are four Army Field Manuals (FM), Training Circulars (TC), or Army Regulations (AR) pertinent to this study. The capstone Army publication is, FM 3-04-155, *Army Unmanned Aircraft System Operations*, dated 29 July 2009. FM 3-04-155 informs commanders, staff, and soldiers on the operation and employment of UAS. It is the foundation for the further refinement of tactic, techniques, and procedures. In addition to the traditional ISR considerations, this manual accounts for lessons learned during operations in Iraq and Afghanistan and employment of armed UAS. Due to its recent update, FM 3-04-155 is relevant in the current operational environment and lays out the Army's vision for future UAS operations.

The Army's primary training publication for Tactical UAS is, TC 1-600, *Unmanned Aircraft Systems Commander's Guide and Aircrew Training Manual*, dated 23 August 2007. As with all Aircrew Training Manuals (ATMs), TC 1-600 standardizes aircrew training and determines flight evaluation procedures. It also establishes crewmember qualification, refresher, and mission readiness training standards for Tactical UAS, such as the MQ-5 Hunter and RQ-7 Shadow. Tactical UAS crewmembers are school trained and are Military Occupational Specialty (MOS) qualified. They must maintain a higher standard of training than operators of Man-Portable UAS and complete an annual flight physical similar to rated aviators.

The primary Man-Portable UAS training publication is, TC 1-611, *Small Unmanned Aircraft Systems and Aircrew Training Manual*, dated 2 August 2006. This ATM standardizes operator training for Man-Portable UAS. The guidelines and standards identified in TC 1-611 are not as strenuous as TC 1-600. Man-Portable UAS operators do not receive the same extensive training as Tactical UAS crewmembers and do not have an MOS qualification. This publication focuses on operators being proficient in the integration of their UAS in combined arms operations.

The AR mandating UAS operations is, AR 95-23, *Unmanned Aerial Systems Flight Regulations*, dated 7 August 2006. This regulation covers UAS operations, UA crewmember training, crewmember currency requirements, and flight rules. In contrast to the ATMs, AR 95-23 focuses on procedural control of planning, training, and execution to ensure safety of operation. This publication is applicable to all Army UAS classifications.

US Governmental Reports

The US government has published four white papers that discuss UAS operations. The most comprehensive of these papers is, *FY2009–2034 Unmanned Systems Integrated Roadmap*, dated April 2009. This paper details the importance of current UAS in the combat environment and lays out the military's future UAS strategy. This paper targets a wide audience including military leaders, academic institutions, UAS industries, and government officials. The purpose of the roadmap is to explain UAS capabilities in the current operational environment and identify potential combat applications on tomorrow's battlefield. This paper culminates with a projection of future UAS technologies, missions, and implications on the 2034 battlefield.

In contrast, the *Defense Science Board Study on Unmanned Aerial Vehicles and Uninhabited Combat Aerial Vehicles*, dated February 2004, focuses on current operations, not future operations. The report details current UAS tactics and technologies found in Iraq and Afghanistan. Unlike the roadmap, this report is a critical review of the current UAS structure and issues recommendations for improvement. One of the issues identified is UAS CDL communications failures (Defense Science Board 2004, 43).

Next, *Unmanned Aerial Vehicles: Background and Issues for Congress*, dated 21 November 2005, is a comprehensive information paper written for members of congress. This article also explains the advantages UAS present on the modern battlefield. This paper includes the implications of UAS production on the American industrial base, and presents considerations for UAS export and possible implications of UAS proliferation.

In considering export potential, this paper details various UAS types including obsolete systems no longer found in the US inventory.

Lastly, the *Unmanned Aerial Vehicle Reliability Study*, dated February 2003, examines current Defense Department UAS to determine the risk posed by unmanned aviation to persons and property due to accidents. The DOD commissioned this study under its campaign to influence the FAA to allow UAS utilization in national airspace. This study attempts to identify issues of reliability and recommend solutions to improve reliability. Pertinent to this research, the study details UAS mishaps related to communication interference.

Professional Journals

Three noteworthy journals contribute to this study. The most important of these is *Jane's Unmanned Aerial Vehicles and Targets*, a non-governmental journal, not subject to UAS industry influence. It details UAS produced in the US and those produced globally. Jane's explains UAS technology with greater fidelity than any other publication and identifies foreign states with active UAS industries. It also details states that actively export UAS technology. This journal allows for examination of commonalities found in UAS globally and threats related to forces being able to obtain similar systems and develop UAS countermeasures.

Armada International is monthly publication focused on the defense industry and issues a comprehensive annual report on UAS. This annual report details current and future UAS globally, although it is not as detailed as *Jane's Unmanned Aerial Vehicles and Targets*. However, where Jane's tends to focus only on current military systems, Armada examines military and prominent civilian systems still in the developmental phase.

The final publication is the *Journal of Electronic Defense* produced by the Association of Old Crows, a nonprofit international professional organization specializing in EW. This journal reports on trends, industry news, and other developments in the EW field. Concerning this study, the journal's EW coverage includes electronic countermeasures (ECM), airborne EA, and command and control warfare.

Books

Four books provide texture to this study. The first of these books is *Advances in Unmanned Aerial Vehicles,* edited by Kimon P. Valaavanis. The book does not focus on military UAS. Rather, it is a compilation of articles written by civilian researchers across the world. It is written and edited by civilians and allows them to share information. The book gives a detailed history of civilian UAS theory and research, and discusses control fundamentals, aspects of navigation, and application of these principles in current projects. Of greatest interest to this study, *Advances in Unmanned Aerial Vehicles* discusses numerous control designs that could provide direction for military UAS CDLs.

In *Modern Communications Jamming Principles and Techniques,* author Richard Poisel explains the science of disrupting modern communications. Dr. Poisel does not write for a military audience. However, the information provided is applicable to military operations. The book discusses the operational use and vulnerabilities of modern communications systems. It identifies forms of jamming including active, passive, structural, and environmental. The book provides examples of jamming techniques and explains their advantages and disadvantages. It also indentifies principles of anti-jamming technology and tactics.

In contrast, *Fundamentals of Electronic Warfare*, by Sergei Vakin, Lev Shustov, and Robert Dunwell is intended for a military audience. The book is a detailed description of EW in modern warfare, and provides a short history of EW and its application in historical context. *Fundamentals of Electronic Warfare* is both a scientific text, which details the mathematical models of EW and an operational text that explains EW tactics. Further, it explains active and passive jamming of electromagnetic energy. Unlike *Modern Communications Jamming Principles and Techniques*, this text concentrates on EW directed against or produced by aircraft.

The final book, *Wired for War*, by P. W. Singer is not a science-based text. Singer conducted an exhaustive study on the science of UAS, current application of UAS technology, and the potential UAS future. Singer believes there is an ongoing UAS RMA and that the proliferation of robotics has changed the face of warfare. This book also identifies robotics limitations and exposes the myth of computer infallibility. Singer discusses the global proliferation of robotics in military and paramilitary organizations, and contends the global proliferation of robotic systems could undermine America's perceived dominance.

Media

This study intends to use two real time sources of information. The first of these is news coverage from print, video, and web based media. On a regular basis, these outlets detail UAS combat operations. However, these sources do have limitations. They report high profile events such as UAS attacks and UAS crashes yet lack many of the relevant facts surrounding these events. Despite these drawbacks, some of these reports may contribute to the depth of this study.

This study also uses a number of professional blogs. The first blog is the Congressional Unmanned Aerial Vehicle Caucus co-chaired by Rep. Howard “Buck” McKeon and Rep. Alan Mollohan of the US House of Representatives. This caucus’ mission is to educate members of Congress and the public on the strategic, tactical, and scientific value of UAVs. Another potential blog for review is UAVforum.org, an online working group that discusses global UAS research and advances. Many of the systems discussed on UAVforum are non-US designs and generally not reported on in US sources.

UAS Industry Releases

This study used fact sheets, brochures, and information papers from UAS manufactures. AeroVironment, Inc. and AAI Corporation produced the most important products due to their share of the UAS market. General Atomics Aeronautical Systems, Inc, Honeywell, and Northrop Grumman information was also reviewed to determine their systems capabilities.

These documents are industry advertizements that tend to espouse capabilites and ignore limitations. This study used these products to develop an understanding of system specifications and capabilites.

Review of Current UAS

To call a UAS a remote control airplane is simplistic. An UAS is a complex integration of various technologies designed to operate in austere environments. They consist of three separate major components an UA, a GCS, and a RVT. Multi-echelon military leaders depend on UAS to increase their situational awareness and enable decision-making. The CDL structure of UAS varies based on the size, mission, and capabilities of the UA.

The differing service components have had their own UAS classifications. To prevent confusion, this research utilize the broad multi-service UAS classification as defined in FM 3-04.15, *Multi-Service Tactics, Techniques, and Procedures for the Tactical Employment of Unmanned Aerial Systems*, dated 3 August 2006 (see table 1). This multi-service manual categorizes UAS into three main classes: Man-Portable, Tactical, and Theater UAS. The employment philosophies of differing classes are similar, but the limitations of some airframes require tactical adaptations. UAS within these classifications have similar CDL structure due to common manufactures, similar operational environments, and DOD mandated interoperability directives.

Table 1. UAS Capabilities

	Speed (knots)		*Maximum Altitude*	*Maximum Endurance*[1]	*Maximum Range*
	Cruise	Dash			
Man-portable					
Desert Hawk	50	50	1,000 AGL	1 hr	10 km[2]
Dragon Eye	45	45	500 AGL	1 hr	10 km[2]
Pointer	45	45	985 AGL	1 hr	5 km[2]
Raven	34	60	1,000 AGL	1 hr	10 km[2]
Silver Fox	50	50	1,000 AGL	10 hrs	32 km[2]
Tactical					
Hunter	70	100	15,000 MSL	8-9 hrs	125 km[2 & 4]
IGNAT	70	120	25,000 MSL	30 hrs	500 nm[2]
Pioneer	65	110	15,000 MSL	5 hrs	185 km[2]
Scan Eagle	70	70	19,000 MSL	15 hrs	110 km[2]
Shadow	70	105	15,000 MSL	5 hrs	50 km[2]
Fire Scout	80	125	20,000 MSL	6 hrs	280 km[2]
ERMP	70	150	29,000 MSL	36 hrs	1200 km[2]
Theater					
Global Hawk	310	340	60,000 MSL	28 hrs	5,400 nm[3]
Predator	70	117	26,000 MSL	20 hrs	500 nm[3]
Predator B	90	220	45,000 MSL	16 hrs	500 nm[3]

[1] Endurance equals total time from takeoff to landing.
[2] Range equals range from GCS.
[3] Range equals total mechanical range of UA.
[4] With retransmission, range equals 200 km.

Source: Headquarters, Department of the Army, FM 3-04.15, *Multi-Service Tactics, Techniques, and Procedures for the Tactical Employment of Unmanned Aircraft Systems* (Washington, DC: Government Printing Office, 2006), 21.

Man-Portable UAS

Man-Portable UAS are small, self-contained, portable systems often employed at the lowest levels of command. This class of UAS operates at lower altitudes and often shares airspace with manned rotary-wing aircraft. Most tactical organizations that employ these systems have a single operator, selected from within the unit, who has attended a qualification course. Man-Portable UAS operators are required to attend a certification course, but do not receive an Additional Skills Identifier (ASI).

Current Man-Portable UAS are either hand-launched, bungee launched, or take-off vertically. The operator commands the UAS by maintaining a CDL between the UA and the GCS. The UAS broadcasts its FMV to any RVT within range of the system, which is monitoring the correct VDL. Man-Portable UAS have shorter ranges than other systems due to their dependence on LOS communications and lower operating altitudes (Headquarters, Department of the Army 2006a, 14).

These UAS use omnidirectional antennas for both their CDL and VDL. In theory, the simplicity of the antenna design improves CDL reliability and maximizes VDL distribution. Additionally, the omnidirectional antenna configuration and interoperability allows any GCS broadcasting the appropriate CDL frequency to command the UA. This flexibility enables multiple operators to command a single UA by transferring command using a CDL "*handshake*", effectively extending the range of a single UAS. However, an incorrectly performed handshake can result in a disruption of the CDL and cause a crash. Man-Portable UAS rarely utilize this function to avoid risk of an accident (Hill 2010).

Current Man-Portable UAS in include the RQ-16 Tarantula Hawk (T-Hawk), RQ-11 Raven, RQ-14 Dragon Eye, Puma AE, and Wasp. The following is a review of the design characteristics of these current UAS designs (Headquarters, Department of the Army 2006a, 21).

RQ-16 Tarantula Hawk

The RQ-16 T-Hawk, produced by Honeywell Aerospace, is the newest Man-Portable UAS in the US Army inventory. The original Army designation for the system was the XM156 Class 1 UAS and was a subsystem of the Army's Future Combat System (FCS) (Department of Defense 2009, 86). The DODs review of the Army's FCS left the

T-Hawk's future in doubt, but seeing the systems potential, the Navy adopted the XM156. In January 2008, the Navy surprised many by placing a surprise order for 186 XM156s and re-designated the system as the RQ-16 Tarantula Hawk (Trimble 2008). In Iraq, the Navy led Multi-Service Explosive Ordnance Disposal Group is currently using 20 T-Hawks to combat roadside bombs.

The T-Hawk is gasoline operated, has a range of up to 10 kilometers, and can remain airborne for 50 minutes (see figure 1). The system includes a GCS, a ground support package, and two UAs. The UA takes off vertically, flies to 100 waypoints at up to 46 Miles per Hour (MPH), can establish a stationary hover over a desired location, and communicates on L-band Ultra High Frequency (UHF). The UAS has a gimbaled sensor capable of recording Electro Optical (EO) and Infra-Red (IR) images. The GCS is capable of recording up to 240 minutes of FMV imagery. The T-Hawk is limited to LOS communications and cannot operate in moderate rain, heavy wind, or high temperatures (Honeywell Aerospace 2008).

Figure 1. RQ-16 Tarantula Hawk
Source: FY2009–2034 Unmanned Systems Integrated Roadmap, DOD (Photo, FY2009–2034 Unmanned Systems Integrated Roadmap, DOD, 6 April 2009).

RQ-11 Raven

The RQ-11 Raven, produced by AeroVironment, Inc., is the most common Man-Portable UAS in the US military. In 2002, AeroVironment's Flashlight UAS won the Army's small UAV competition and was redesignated the RQ-11 Raven (Net Resources International 2010). The Raven is one of the world's most popular UAS with over 9,000 UAs produced for international clients, including all US military service branches and eight other international partners.

The Raven uses an electrical engine, has a range of up to 10 kilometers, and can remain airborne for up to 110 minutes (AeroVironment Inc. 2009c) (see figure 2). The system includes the Joint Common Interoperable Ground Control Station (JCIGCS), six individual sensor payloads, and three UAs (AeroVironment Inc. 2009e). The RQ-11 is hand-launched, flown either manually or on a preprogrammed route, flies up to 50MPH at 500 feet AGL, and performs a conventional belly landing. The Raven UAS has two sensor payloads; a dual forward and side-look EO nose camera with a stabilized electronic pan-tilt-zoom feature for daytime operations, and a forward and side-look IR nose camera for night operations. The JCIGCS is an AeroVironment designed interoperable GCS that provides FMV, captures screen images, stores data for playback during target assessment, communicates on L-band UHF frequencies, and is compatible with all other AeroVironment UAS. The Raven is limited to LOS communications and cannot operate in moderate rain or high winds (AeroVironment Inc. 2009c).

Figure 2. RQ-11 Raven
Source: Courtesy AeroVironment, Inc., Media Gallary, www.avinc.com (accessed 10 January 2010).

RQ-14 Dragon Eye/Swift

The RQ-14 Dragon Eye is an original Naval Research Laboratory (NRL) project, but AeroVironment designed the latest version of the UAS (AeroVironment Inc. 2009a). Production has been limited with the Navy, Marines, and Special Operations Command

(SOCOM) being the primary users. The RQ-14s production run is complete with approximately 630 systems produced (Department of Defense 2009, 84). The RQ-14 is being phased out and replaced by the RQ-11 Raven.

The RQ-14 is a dual engine UAS, which uses electric engines (see figure 3). The system has a range of up to 10 kilometers and can remain airborne for up to 60 minutes. The RQ-14s UA is bungee launched, flown using an autopilot or on a preprogrammed Global Positioning Satellite (GPS) route, flies up to 40MPH at 500 feet AGL, and performs a conventional belly landing. The RQ-14 uses an EO payload for daytime operations and an IR payload for night operations. The Dragon Eye includes three interchangeable payloads: a GCS, three UAs, and two RVTs (AeroVironment Inc. 2009a). The improved Swift variant includes four interchangeable payloads, an AeroVironment JCIGCS, four UAs, and two RVTs. The JCIGCS provides FMV, captures screen images, stores data for playback during target assessment, and communicates on L-band UHF frequencies. The RQ-14 is limited to LOS communications and cannot operate in moderate rain or high winds (AeroVironment Inc. 2009e).

Figure 3. RQ-14 Dragon Eye / Swift
Source: Courtesy AeroVironment, Inc., Media Gallary, www.avinc.com (accessed 10 January 2010).

Puma AE

The Puma AE, produced by AeroVironment, is an All Environment (AE) UAS intended for land or maritime operations but is still in the developmental phase (AeroVironment Inc. 2009b). The primary proponent for the Puma AE is SOCOM, but no orders have yet been placed. The Puma AE is comparable to the RQ-11 Raven but the Puma AE is waterproof and can land in water (Department of Defense 2009, 67).

The Puma AE has an electric engine, a range of up to 15 kilometers, and can remain airborne for up to 120 minutes (see figure 4). The Puma AE is hand launched, flown on a pre-programmed GPS route, flies up to 45MPH at 500 feet AGL, and performs a conventional belly landing on land or water. The Puma AE utilizes a gimbaled payload that pans plus or minus 180 degrees, tilts plus 10 to minus 90 degrees, uses both an EO and IR sensor, and contains an IR illuminator. The Puma AE uses the AeroVironment JCIGCS, which provides FMV, captures screen images, stores data for playback during target assessment, and communicates on L-band UHF frequencies (AeroVironment Inc. 2009e).

Figure 4. Puma
Source: Courtesy AeroVironment, Inc., Media Gallary, www.avinc.com (accessed 10 January 2010).

WASP III

The WASP III, produced by AeroVironment, is the smallest UAS in the US inventory. Its primary users are the Air Force, Navy, and Marine Corps (AeroVironment Inc. 2009d). The WASP III is a Micro-UAV but the DOD has not established a separate classification for micro systems. The DOD procurement plan does not detail the systems anticipated end strength, but AeroVironment has completed hundreds of systems with production continuing until 2012 (Department of Defense 2009, 68).

The WASP III uses an ultra-quiet electrically powered engine, has a range of up to 5 kilometers, and can remain airborne for up to 45 minutes (see figure 5). The WASP III is hand launched, flown manually or on a preprogrammed route, flies up to 40MPH at 1000 feet AGL, and performs a conventional belly landing. Three payloads are available for the WASP III: a forward and side-look EO camera, a high-resolution EO camera with electronic pan/tilt/zoom, and an IR imager. It uses the AeroVironment JCIGCS, which provides FMV, captures screen images, stores data for playback during target assessment, and communicates on L-band UHF frequencies (AeroVironment Inc. 2009e). The WASP III is limited to LOS communications and cannot operate in moderate rain or high winds. AeroVironment is also upgrading the WASP III and in the near future plans to offer a waterproof version (AeroVironment Inc. 2009d).

Figure 5. Wasp
Source: Courtesy AeroVironment, Inc., Media Gallary, www.avinc.com (accessed 10 January 2010).

Other Man-Portable UAS

This review of Man-Portable UAS is not exhaustive but represents a cross section of the current US military fleet. The Silver Fox UAS is another UAS program of record produced by BAE Systems. This study did not review the Silver Fox due to its low production, lack of a procurement plan, and limited DOD interest in future development. The Desert Hawk III is a Lockheed Martin design and is primarily used by the Air Force and allied military forces. This study did not review the Desert Hawk III due to limited US procurement. Other UAS may be in the design phase of procurement but due to lack of information, these systems are included in this review (Department of Defense 2009).

Tactical UAS

Tactical UAS are larger than Man-Portable UAS and operates in support of maneuver commanders. These systems operate under restrictions similar to manned aircraft and require a more robust support structure than Man-Portable UAS. Tactical UAS belong to ground brigades, but Combat Aviation Brigades (CAB) often provide oversight as aviation safety experts (Hill 2010). CABs have a limited number of Tactical UAS but plans call for an expansion in CAB systems (Ford 2010). Brigades C2 these systems but they can operate in support of any organization with access to a RVT.

Tactical UASs may be launched using external power, such as a pneumatic catapult, or take off under its own power. In the US inventory, UASs in this class all land by conventional means, but some foreign made Tactical UAS land by parachute (Armada International 2009). These systems require extensive training to operate and pilots must maintain standards similar to rated-aviators. Tactical UAS require high-power mobile GCS to maintain control and are often dependant on maintaining constant LOS communications. These systems have more sophisticated sensors than Man-Portable UAS and use a single sensor payload for all mission profiles. The current fleet of Tactical UAS includes the RQ-7 Shadow, RQ-5 Hunter, I-GNAT, and MQ-1C Sky Warrior/Gray Eagle (Headquarters, Department of the Army 2006a, 21).

RQ-7 Shadow 200

The RQ-7 Shadow, produced by AAI Corporation, is the most common Tactical UAS in the US inventory and is in use by both the Army and Marine Corps (Department of Defense 2009, 89). The RQ-7 Shadow 200 is the flagship airframe of AAI's Shadow family of UAS. The Shadow family includes the Shadow 400 and Shadow 600 (AAI Corporation 2009a). These other Shadow UAS are larger than the RQ-7 and the US military has not shown interest in them. The US Army currently has 63 RQ-7 UAS in its inventory and procurement plans call for 115 systems in total (Department of Defense 2009, 89). In 2006, the Marine Corps selected the RQ-7 as a replacement for the aging RQ-2 Pioneer UAS, but the Marines have not determined their final system strength (Department of Defense 2009, 89).

The RQ-7B uses an Aviation Gas (AVGAS) fueled pusher prop engine, has a range of up to 125 kilometers, and can remain airborne for up to 6 hours (see figure 6). The Shadow 200 is launched using a trailer mounted pneumatic catapult rail system, flown manually, flies up to 140MPH at 14,000 feet MSL, and uses an automated Take Off and Landing System (TALS) to land conventionally on fixed landing gear (Department of Defense 2009, 89). The RQ-7B is equipped with plug-in optical payload (POP) 300, an Israeli made payload that includes a thermal imager, an EO sensor, a laser range finder (LRF), and an IR illumination for target identification (Tamam Division

2010). The Shadow 200 uses the Army One System Ground Control Station (OSGCS) which can simultaneously operate numerous UA. This is housed in a climate-controlled shelter, provides UA health and fault monitoring, conducts video coding and decoding, and can archive up to 30 days of ISR data (AAI Corporation 2009b). The Shadow is limited to LOS communications and operates using S-band UHF/SHF frequencies for its CDL and C-band SHF frequencies for its VDL (Hill 2010). The Shadow 200 cannot operate in moderate-rain, extreme-winds, or turbulence (AAI Corporation 2009a).

Figure 6. RQ-7 Shadow 200
Source: FY2009–2034 Unmanned Systems Integrated Roadmap, DOD (Photo, FY2009–2034 Unmanned Systems Integrated Roadmap, DOD, 6 April 2009).

MQ-5 Hunter

The MQ-5 Hunter, produced by Northrop Grumman Corporation, is the latest variant of the RQ-5 medium-range Tactical UAS first introduced in 1996 (Department of Defense 2009, 79). The Army is only user of the Hunter and its service life is yet to be determined. The Army has cancelled and recalled the Hunter on numerous occasions out of operational necessity. The Hunter's first operational deployment was in support of NATO operations in the Balkans and it is currently operating in Afghanistan and Iraq (Department of Defense 2009, 79).

The MQ-5 operates using a heavy fuel engine, which incorporates a conventional and pusher prop in combination (see figure 7). The Hunter has a range of up to 200 kilometers, can remain airborne for up to 18 hours, and flies up to 125MPH at altitudes up to 18,000 feet MSL. The Hunter takes off conventionally, is manually flown, and lands using fixed landing gear (Department of Defense 2009, 79). The MQ-8 is equipped with an advanced payload that includes an EO/IR sensor, an IR illuminator, a laser range finder designator (LRFD), and a communications relay package (CRP). The MQ-5 can use the GBU-44/B, Viper Strike, a glide bomb that uses the Hunter's LRFD to attack targets. The Hunter uses the same OSGCS as the Shadow 200 allowing for simultaneous operation of numerous UA, is housed in a climate-controlled shelter, provides UA health and fault monitoring, conducts video coding and decoding, and can archive up to 30 days of ISR data (AAI Corporation 2009b). The Hunter is limited to LOS communications and uses a C-band SHF frequency for both its CDL and VDL (Northrop Grumman 2010).

Figure 7. MQ-5 Hunter
Source: FY2009–2034 Unmanned Systems Integrated Roadmap, DOD (Photo, FY2009–2034 Unmanned Systems Integrated Roadmap, DOD, 6 April 2009).

I-GNAT

The I-GNAT, produced by General Atomics Aeronautical Systems, is an improved version of the GNAT 750 first introduced in 1989 (Department of Defense 2009, 75). The Army procured the I-GNAT in response to a congressional request for additional UAS to support operations in Afghanistan and Iraq. General Atomics Aeronautical Systems produced 25 I-GNATs in numerous variants, but its production run is complete. I-GNATs support operations until their service life expires. The MQ-1C is replacing these systems (Department of Defense 2009, 75).

Depending on the variant, the I-GNAT operates using either an AVGAS or a heavy fuel pusher prop engine with a LOS range of up to 250 kilometers or a BLOS range of 2500 kilometers, can remain airborne for up to 40 hours, and flies up to 140MPH at altitudes up to 25,000 feet MSL (see figure 8). The I-GNAT takes off conventionally, is manually flown, and lands using retractable landing gear. The system is equipped with an advanced payload that includes an EO/IR sensor, a LRFD, and a CRP

(General Atomics Aeronautical Systems 2009b). The I-GNAT uses the OSGCS allowing for simultaneous operation of numerous UA, is housed in a climate-controlled shelter, provides UA health and fault monitoring, conducts video coding and decoding, and can archive up to 30 days of ISR data (AAI Corporation 2009b). Most of the I-GNAT variants are limited to LOS communications operating on C-band SHF frequencies. However, some I-GNATs are equipped to use a BLOS satellite communications (SATCOM) radio operating on Ku-band EHF frequencies (General Atomics Aeronautical Systems 2009b).

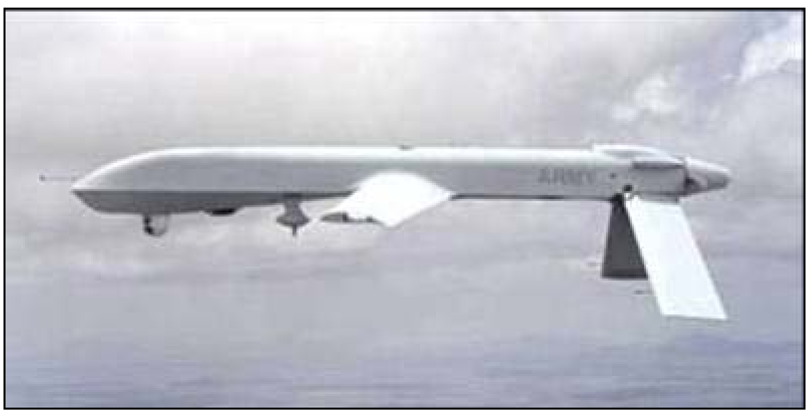

Figure 8. I-GNAT
Source: FY2009–2034 Unmanned Systems Integrated Roadmap, DOD (Photo, FY2009–2034 Unmanned Systems Integrated Roadmap, DOD, 6 April 2009).

MQ-1C Sky Warrior/Gray Eagle

The MQ-1C Gray Eagle, produced by General Atomics Aeronautical Systems, is an upgrade of the MQ-1 armed Predator UAS produced specifically for the Army. The MQ-1C is the end product of the Army's Extended Range/Multi-Purpose (ERMP) development program. It was original designation was the Sky Warrior, but the Army has recently re-designated the UAS as the Gray Eagle (Jensen 2010). Production of the MQ-1C is ongoing and systems are operating in Iraq and Afghanistan in support of the War on Terror. The Army plans to procure 11 complete systems with a total production of 132 airframes (Department of Defense 2009, 78).

The MQ-1C operates using a heavy fuel pusher prop engine with a LOS range of up to 500 kilometers or a BLOS range of up to 1200 kilometers, can remain airborne for over 30 hours, and flies up to 170MPH at altitudes up to 29,000 feet MSL (General Atomics Aeronautical Systems 2009a) (see figure 9). The MQ-1C takes off conventionally, is manually flown, and lands using retractable landing gear. The system is equipped with a payload that includes an EO/IR sensor, a Synthetic Aperture Radar/Ground Moving Target Indication (SAR/GMTI) sensor, a LRFD, and a CRP. The MQ-1C can use up to four laser guided AGM-114, Hellfire missiles, which use the systems LRFD to attack targets. The MQ-1C uses the OSGCS allowing for simultaneous operate numerous UA, is housed in a climate-controlled shelter, provides UA health and fault monitoring, conducts video coding and decoding, and can archive up to 30 days of ISR data (AAI Corporation 2009b). The Gray Eagle is capable of either LOS or BLOS communications using Ku-band EHF frequencies (General Atomics Aeronautical Systems 2009a).

Figure 9. MQ-1C Sky Warrior / Gray Eagle
Source: FY2009–2034 Unmanned Systems Integrated Roadmap, DOD (Photo, FY2009–2034 Unmanned Systems Integrated Roadmap, DOD, 6 April 2009).

Analysis of Literature

Current doctrine focuses on the employment of UAS. The doctrine does address considerations when operating an UAS in vicinity of other friendly activity and cites concerns with UAS control in vicinity of Counter-Improvised Explosive Device (C-IED) jammers. The doctrine recommends avoiding flight within a set distance of active jammers, turning jammers off when using UAS, or programming jammers to not broadcast against the UAS designated frequency. The doctrine also states that operation of multiple UAS in a concentrated area could cause CDL interference.

The government reports recognize the occurrence of CDL communication jamming. One report claims that 11 percent of UAS accidents are a result of communications failures (Office of the Secretary of Defense 2003, 53). Unlike the doctrine that identifies the likely sources, government reports do not reference possible sources of signal interference. The reports recommend technological development to mitigate CDL interference.

Only one book, *Wired for War*, by P. W. Singer, directly addresses incidents of military UAS CDL interference. In addition, this book identifies sources of natural interference not addressed in any of the governmental publications. Like other military tactics, EW is a continuously adapting field of countermeasures. The books do offer civilian applications, which could be altered for military UAS operations.

Gaps in the Record

Doctrine openly acknowledges that US equipment can interfere with UAS data links. CDL communications appear to be susceptible to both jamming and mimicking. The government reports identify improvements required in CDL technology. The books suggest that any radio frequency can be jammed.

There is limited literature addressing enemy counter-UAS attacks. However, doctrine does acknowledge the possibility that enemy forces may attack UAS. It does not identify possible vulnerabilities the enemy may exploit, nor does it provide recommendations to counter an enemy attack against UAS.

Trends

The ongoing trend in the military is to increase and expand unmanned operations. Most of the government publications stress the integration of UAS throughout the operational environment and detail the advantages UAS provide to the combat leader.

Generally, current doctrine focuses solely on UAS employment. The military has not acknowledged or addressed contingencies when operating in a non-permissive UAS environment. The most troubling trend is a sense of ignorance regarding UAS limitations.

Significance of Thesis in Relation to Existing Literature

Existing literature focuses on the advantages of UAS employment. In comparison, this study focuses on vulnerabilities in a non-permissive UAS environment. Literature has identified the CDLs susceptibility to communications failure. However, these failures are attributed to specific scenarios involving operations in the vicinity of C-IED jammers or multiple UAS. Civilian literature attests such failures could occur from numerous manmade or natural sources. Therefore, to determine these vulnerabilities, this study will identify occurrences of UAS failure during training and execution of combat operations.

As seen in this review, these six types of literature provide a comprehensive view of UAS CDL and possible vulnerabilities to these control structures. The Joint doctrine establishes some common terminology between services but is limited by the age of the documents. Army doctrine is tactically based and draws on lessons learned during combat operations. It details considerations for the employment of UAS in the operational environment. Books explain the science of UAS communications and the possibility of interference with UAS data links. Professional journals provide information by subject matter experts (SME) in the field of UAS, communications, and EW. Finally, media sources are the most dynamic literature and provide near real time information on current UAS operations. This review has also identified gaps in the record and trends in existing literature.

CHAPTER 3

RESEARCH METHODOLOGY

> Discovery is to see what everybody else has seen, and to think what nobody else has thought.
>
> — Albert von Szent-Gyorgyi

While some literature is available on UAS CDLs, the current information does not provide sufficient detail to identify the scope of the problem. To answer the research questions presented in chapter 1, this qualitative study of UAS CDL structures analyzes the current record and conducts interviews to add to the record. In order to achieve a comprehensive answer, this process includes an evaluation of current and developmental military and civilian UAS CDLs. This study will propose recommendations to change military UAS planning to account for operations in a non-permissive UAS environment.

This chapter explains the steps taken previously to gather available information. This study identifies information that necessitates interviews with experts and those with experience in the field pertaining to this study. Lastly, this chapter describes the research methodology and the advantages and disadvantages to the methodology.

Information Gathering

To identify relevant doctrine, regulations, and unclassified publications, this study extensively reviewed Joint, Army, Navy, Marine, and Air Force electronic publications. Due to the dynamic nature of UAS technology, numerous web-based resources have been reviewed, including Association for Unmanned Aircraft Systems International, Congressional Unmanned Aerial Vehicle Caucus, The Association of Old Crows, Space Media Network, and the Air Force Research Institute. The US Army Combined Arms

Research Library in Fort Leavenworth, Kansas, provided access to UAS development and procurement plans. Combined Arms Research Library research librarians provided government reports, journals, and other relevant literature.

Interview Selection

Limited information is available in current literature regarding vulnerabilities to UAS CDLs. Consequently, this study necessitated conducting interviews to gather relevant institutional knowledge. Either the military or the civilian UAS community may help answer the research question. This study interviews experts from both communities in order to conduct a comprehensive study. Additionally, numerous variables have been identified that could affect the results of this study. The interviews must address these variables to minimize information gaps relevant to the primary question.

The initial interviews were conducted with experts in UAS development. The US Army UAS Project Managers at Redstone Arsenal, Huntsville, Alabama were the primary target of these interviews. These project managers are experts on the operational design of current and future Army UAS. These interviews were intended to identify known limitations to UAS CDLs and the Army's attempts to mitigate these risks in current and future UAS.

This study also interviewed civilian UAS engineers and designers currently conducting research and development. The purpose of this interview was to compare and contrast the differing design characteristics. This study determines if civilian and military designs suffer from similar limitations. Where design differences exist, what civilian applications have potential military applications?

In addition, this study interviewed Observer/Controllers (OCs) from the National Training Center (NTC), Fort Irwin, California, to determine the frequency of UAS CDL failures in a permissive peacetime environment. This was intended to help determine how often CDL interference occurs and what systems are most vulnerable. However, not all incidents of UAS CDL interference amount to an accident that requires an official accident investigation. Due to this, the official accident statistics may only account for UAS accidents requiring an investigation, thus limiting the validity of accident data.

Lastly, this study interviewed experts in the EW community. These experts assist in understanding the science of EW. Understanding the science of EW helps determine if UAS CDLs are vulnerable to UAS attacks. Additionally, if the study finds that UAS CDLs are susceptible to EW attacks, the EW expert may recommend changes to improve UAS communications security.

These interviews were conducted using 20 base questions and additional secondary interview questions determined during the course of the interview. Interview participants provided answers based on individual knowledge when possible. Some interviewees were not capable of answering certain questions. A digital recorder was used to capture information and ensure obtained data is not lost. The basic interview questions were:

1. On what radio bands do UAS CDL and VDL communicate? Please explain communication bands used for current and future Man-Portable and Tactical UAS.

2. Do current UAS CDLs experience interference? What conditions contribute to possible interference?

3. Are certain UAS or classes of UAS more likely to experience interference?

4. What is shadow jamming or self-jamming? How common is this phenomenon?

5. FM 3-04.15, *Multi-Service Tactics, Techniques, and Procedures for the Tactical Employment of Unmanned Aerial Systems*, dated 3 August 2006, states, "Users must be aware of enemy actions and environmental factors that can limit the effectiveness of UAS communications." What enemy actions or environmental conditions affect UAS communications?

6. How often do incidents of UAS CDL interference occur in Iraq or Afghanistan?

7. Do C-IED systems employed in Iraq and Afghanistan interfere with UAS CDLs? What classes of UAS are more susceptible to C-IED interference?

8. Are beyond line of sight (BLOS) communications more or less likely to encounter interference?

9. What are the lost link procedures for current and future UAS?

10. How can commanders or UAS operators mitigate CDL interference risks?

11. The *Unmanned Aerial Vehicles: Background and Issues for Congress*, dated 21 November 2005, reported that UAS have 100 times greater accident rate than manned aircraft. Is this still a valid statistic or has UAS reliability improved?

12. On 17 December 2009, *The Wall Street Journal*, reported that insurgents had compromised UAS VDL communications. Have insurgents successfully compromised UAS CDL communications?

13. On 31 December 2008, *CBS News*, reported that Palestinian militants issued an open request on an extremist blog seeking assistance in developing technology with the capability to "detect, intercept and jam UAV signals". Have similar additional threats been issued? Does such requests factor into UAS design considerations?

14. Do current UAS possess adequate electronic countermeasure (ECM) protection? What ECM modifications will current UAS receive?

15. What size issues must Program Executive Office Aviation (PEO AVN) consider when developing ECM devices? What size concerns are most difficult to overcome?

16. What redundancy is built into current UAS CDLs? What redundancy is being designed into future UAS CDLs?

17. Do current UAS Doctrine, Organization, Training, Material, Leadership, Personnel, and Facilities (DOTMLPF) accurately account for UAS shortcomings or vulnerabilities? What adjustments are required in the UAS DOTMLPF to account for UAS shortcomings or vulnerabilities?

18. Does PEO AVN research civilian UAS CDLs for possible military applications?

19. Does PEO AVN participate in the Navy's annual Black Dart counter-UAS exercise at Naval Air Weapons Station, China Lake? Should PEO AVN participate in this exercise?

20. What additional publications can advance this study?

Research Methodology

This study used the DOTMLPF construct to address the primary and secondary questions posed in chapter 1. It focused mainly on the adequacy of Joint and Army doctrine to prepare for EW, structure of UAS organizations to provide oversight of EW preparations, the training operators receive to identify EW, and materials that affect a

CDLs ability to cope with interference. This use of the doctrine, organization, training, and material portions of DOTMLPF will continue throughout chapters 4 and 5.

Advantages and Disadvantages of Methodology

The advantage to this methodology is the inclusion of interviews with the US Army's experts in UAS design and EW fields. This technique directly addressed the gaps identified during the literature review. Additionally, including the civilian UAS community brought a fresh perspective and potential alterations to military UAS designs.

The disadvantage to this methodology is that identified issues may not have near term solutions. It may not be possible to incorporate ECM on some UAS classifications due to size and weight limitations. The field of EW research and development is also very dynamic and ECM devices effectiveness may be short lived. While this study may find that UAS CDLs are vulnerable, those vulnerabilities may be acceptable due to a number of other considerations.

As seen in this chapter, this study relied heavily upon interviews to address gaps identified in the available record. Interviews with both military and civilian UAS researchers allowed the researcher to compare and contrast differing design philosophies. This study used interviews, doctrine, and government reports to recommend changes to the UAS DOTMLPF construct. Experts across the UAS spectrum were interviewed to ensure this study is comprehensive. However, technological limitations may not allow an adequate recommendation for all UAS classifications.

CHAPTER 4

ANALYSIS

> I am concerned about the continued decline in research-and-development funding. From 1980 through today, our investment in basic defense research as a percentage of gross domestic product has declined by 50 percent. . . . choosing to win in Iraq and Afghanistan should not mean our country must also choose to assume additional risk. . . . Who is thinking about the war in 2015? Or the war in 2030?
>
> — Rep. Howard "Buck" McKeon, US House of Representatives

This chapter focuses on the doctrine, organization, training, and material portions of the DOTMLPF construct. This study analyzes the UAs identified as Man-Portable and Tactical UAS in FM 3-04.15, *Multi-Service Tactics, Techniques, and Procedures for the Tactical Employment of Unmanned Aerial Systems*, dated 3 August 2006. First, this chapter defines criteria for Man-Portable UAS classification and reviews the design, capabilities, and employment of the major systems. The study then examines the criteria for Tactical UAS and conducts a similar review of major Tactical UASs. Lastly, the analysis focuses on the doctrine, organization, training, and material considerations that influence UAS CDLs.

Doctrine

Doctrine is composed of the fundamental principles and codified briefs direct action or motive to a common philosophy. Historically, the armed services have struggled to nest their individual service doctrines in a manner that supports mutual operations. To force cooperation, The Chairman of the Joint Chiefs of Staff (CJCS) issues guidance known as Chairman of the Joint Chiefs of Staff Instruction (CJCSI). This directive dictates the procedure for the development of collaborative Joint doctrine. In CJCSI

5120.02B, *Joint Doctrine Development System*, dated 4 December 2009, the CJCS charges the Commander, United States Joint Forces Command Commander (CDRUSJFCOM), to oversee Joint doctrine production. This qualitative study examines both Army and Joint doctrine to determine the adequacies of their considerations for UAS operations in an EW threat environment.

This section reviews Army and Joint doctrine to determine planning considerations, recommendations, or mitigations for operating Man-Portable and Tactical UAS in an EW rich environment. The RQ-11 Raven is the primary example of Man-Portable UAS due to its extensive use throughout the Joint forces. The RQ-7 Shadow is the primary example of Tactical UAS due to its use by both the Army and Marines. Findings for these systems are transferable within their classifications due to system commonalities and interoperability.

Joint and Multi-Service

The first mission of Joint operations is to establish a common language, but dissimilar terminology has posed a problem for Joint UAS operations. UAS technology is dynamic and defining language today might not account for systems in development. The services might have differing logic behind their language structure. Some UAS classifications are based by system specifications and capabilities, and some describe the environment in which the system operates. A consistent naming convention allows for universal understanding by system operators and non-operators. Clear classification becomes critical if this study determines certain system criteria, such as their operational environment, increases susceptible to CDL disruption and EA.

In recent years, UAS have held numerous classifications depending on the source and age of the defining publication. For example, the RQ-11 Raven has held numerous classifications including a Close Range-UAV (CR-UAV), Small-UAS (SUAS), Man-Portable UAS, Tier-1 UAV, Tactical-1 UAS, and Group-1 UAS. This study reviewed various publications including JP-55.1, *Joint Tactics, Techniques, and Procedures for Unmanned Aerial Vehicles,* dated 27 August 1993, FM 3-04.15, DODs UAS strategic planning document, *FY2009–2034 Unmanned Systems Integrated Roadmap,* dated April 2009, and FM 3-04.15, *Multi-Service Tactics, Techniques, and Procedures for the Tactical Employment of Unmanned Aerial Systems*, dated 3 August 2006 to determine classifications.

JP 3-55.1, *Joint Tactics, Techniques, and Procedures for Unmanned Aerial Vehicles,* dated 27 August 1993, is the capstone Joint UAS manual. The validity of this publication in the current operational environment is limited due to its age. The JP 3-55.1 identifies smaller systems, such as the RQ-11 Raven, as CR-UAVs and larger systems, such as the RQ-7 Shadow, as Medium Range-Unmanned Aerial Vehicle (MR-UAV). This classification is not in any other service publication but these are common system descriptions in the civilian UAV community (Blyenburgh 2008, 5)(see table 2). The UAVs capabilities determine the identification, not the environment in which the system operates (US Joint Forces Command 1993, 14).

Table 2. Civilian UAS Classes					
Classification	Description	Weight	Range	Altitude	Endurance
Mini-UAV	Miniature	Less than 25 kilograms	Less than 10 kilometers	Less than 500 feet	Less than 2 hours
CR-UAV	Close-Range	25 – 150 kilograms	10-30 kilometers	Less than 10,000 feet	2-4 hours
SR-UAV	Short-Range	50 – 250 kilograms	30-70 kilometers	Less than 10,000 feet	3-6 hours
MR-UAV	Medium-Range	150 – 500 kilograms	70-200 kilometers	Less than 16,500 feet	6-10 hours
MALE	Medium-Altitude Long-Endurance	1000 – 1500 kilograms	Over 500 kilometers	16,500-25,000 feet	24-48 hours
HALE	High-Altitude Long-Endurance	Over 2000 kilograms	Over 2000 kilometers	Less than 65,000 feet	24-48 hours
STRATO-UAV	Stratospheric	Over2500 kilograms	Over 2000 kilometers	Over 65,000 feet	24-48 hours

Source: Created by author using data from *EASA UAS Workshop*, European Aviation Safety Agency, Blyenburgh, 2008.

The *FY2009–2034 Unmanned Systems Integrated Roadmap*, dated April 2009, is the DODs strategic planning guidance for all current and forecasted unmanned systems. The roadmap identifies smaller UAS, such as the RQ-11 Raven, as a Group 1 UAS and larger UAS, such as the RQ-7 Shadow, as a Group 3 UAS. The specifications and performance of the UAS determines its classification, not the UASs operational environment. The group identification is broad and does not account for the growing micro-UAS field (see table 3). Additionally, this group identification is of little value to a non-operator who does not know the specifications and performance parameters of a specific UAS (Department of Defense 2009, 110).

Table 3. Joint UAS Groups

UAS Category	Weight	Altitude	Speed
Group 1	Less than 20 pounds	Less than 1,200 feet AGL	Less than 100 knots
Group 2	21-55 pounds	Less than 3,500 feet AGL	Less than 250 knots
Group 3	Less than 1320 pounds	Less than 18,000 feet AGL	Less than 250 knots
Group 4	Over 1320 pounds	Less than 18,000 feet AGL	Any speed
Group 5	Over 1320 pounds	Over 18,000 feet AGL	Any speed

Source: Created by author using data from *FY2009–2034 Unmanned Systems Integrated Roadmap*, Department of Defense, 2009.

The FM 3-04.15, *Multi-Service Tactics, Techniques, and Procedures for the Tactical Employment of Unmanned Aerial Systems*, dated 3 August 2006, is the most relevant UAS publication with Joint considerations. It identifies smaller UAS, such as the RQ-11 Raven, as a Man-Portable UAS, and larger UAS, such as the RQ-7 Shadow, as a Tactical UAS. The operational environment of the UAS and general system capabilities determine this classification (see table 4). This operational environment class identification means a similar system may fall into multiple categories dependant on utilization. For example, the FM 3-04.15 calls the MQ-1B Predator a Theater UAS and the MQ-1C Sky Warrior a Tactical UAS due to the MQ-1Cs planned employment (Headquarters, Department of the Army 2006a, 21).

Table 4. Multi-Service UAS Classifications

Classification	Size	Altitude	Characteristics
Man-Portable UAS	Small, self-contained	Below coordinating altitude	-controlled at the combat team level. -Data is usually FMV constrained by LOS. -Data may be disseminated to brigade/battalion TOCs. -Imagery processing/interpretation is limited to the combat team.
Tactical UAS	Larger systems with more robust requirements	Above coordinating altitude	-Operated by specialized UAS units. -Products can expand beyond FMV depending on payload. -Imagery processing/interpretation may be conducted by intelligence units. -Communication may be LOS dependant.
Theater UAS	Large systems	Above coordinating altitude	-Operated by specialized UAS units. -Numerous products available depending on payload. -Imagery processing/interpretation may be conducted by local intelligence units or reach back intelligence organizations. -BLOS Communications.

Source: Created by author using data from *Multi-Service Tactics, Techniques, and Procedures for the Tactical Employment of Unmanned Aerial Systems*, Headquarters, Department of the Army, 2006.

UAS terminology is continuing to evolve as new systems are developed and fielded. The current Joint community classification is the group identification associated with the *FY2009–2034 Unmanned Systems Integrated Roadmap*. The roadmap includes five UAS groups separated by gross weight, operating altitude, and airframe speed (Department of Defense 2009, 110). The group system in the roadmap requires knowledge of a specific UAS, but the class system in the FM 3-04.15 requires general knowledge of the UAS (Headquarters, Department of the Army 2006a, 21). This study is using the class system identified in FM 3-04.15, *Multi-Service Tactics, Techniques, and*

Procedures for the Tactical Employment of Unmanned Aerial Systems, due to its ease of use for a general audience.

This study defines threats to UASs and evaluates doctrinal mitigation of these threats. The focus of research is EW threats directed against Man-Portable and Tactical UAS but minimal information was available due to their limited employment. Information was available for attacks against larger Tactical and Theater UAS but these systems experienced conventional attacks, not EAs. There are three verifiable accounts of attacks against UAS conducting operations and these incidents provide direction for this study.

The first incident occurred in Israel during the 2006 Israel-Hezbollah War in southern Lebanon. On 7 August 2006, an Israeli F-16 shot down an Iranian built Ababil-T UAS using an AAM (Weiss 2006). Israel reported shooting down two additional Iranian UAVs less than a week later, but these claims are in dispute. These attacks each used fighter aircraft employing conventional air superiority tactics.

The next incident occurred in Georgia during the 2008 build up to the South Ossetia War. On 21 April 2008, the Georgian government operated an Israeli built Hermes UAS over their disputed Abkhazian region. The Georgian government accused the Russians of shooting down their aircraft, a claim the Russian government denied. The Georgian government released a video it claims shows a Russian MIG-29 attacking their UAV using an AAM (BBC News 2008).

The last confirmed incident occurred in 2009 during Operation Iraqi Freedom. Coalition forces did not confirm the incident for a month, but coalition forces reportedly tracked the Iranian UAV over Iraq for 70 minutes before shooting it down. A coalition fighter shot down the UAV but the report did not state how the aircraft downed the UAV. The Iranian system was an Ababil-3, similar in size to the MQ-1B Predator (Reid 2009).

These incidents all involved fighter aircraft attacking Theater UAS using conventional air superiority tactics. The value of these attacks in identifying threats to Man-Portable and Tactical UAS is limited. Such tactics could be effective against larger Tactical UAS but would be impractical against Man-Portable UAS. Countering smaller Tactical and Man-Portable UAS requires unconventional methods either not yet produced or not yet released to the public.

In 2008, the effective Israeli airstrikes of Operation Cast Lead resulted in a more realistic and plausible threat against these smaller systems. These airstrikes decimated the Hamas terror network leadership within the Gaza Strip and prompted militants to request external technological support (Ronen 2008). On 31 December 2008, a militant group identified as “The Sons of Palestine” used a jihadist Blog, m3ark forum, to request assistance from “anybody who could suggest a way to detect, intercept and jam the electronic signals transmitted by Israeli reconnaissance UAVs” (CBS News Investigates 2008). This insurgent group had somehow identified the ability to EA UAS but it is unknown how they came to this determination. There is no evidence that this group received the assistance they sought, but this request demonstrates the technological networking capability of asymmetric threats.

This study reviewed the Joint and service publications to identify perceived UAS threats and examine the adequacy of threat mitigation. The focus of this study is threats to UAS CDLs, but this study reviewed all forms of counter-UAS to be comprehensive.

JP 3-55.1, *Joint Tactics, Techniques, and Procedures for Unmanned Aerial Vehicles*, dated 27 August 1993, the capstone Joint UAS publication is woefully inadequate in its counter-UAS planning guidance. It identifies UAS employment opportunities, but fails to address any threat to UAS operations.

JP 3-30, *Command and Control for Joint Air Operations*, dated 12 January 2010, is the newest JP that addresses UAS operations and does a better job in identifying the potential implications of disrupting CDL communications. It explains that UAS and manned aircraft operate similarly, but that operating UAS requires special considerations. JP 3-30 states, "In the event of lost communications, a manned aircraft will typically press with the mission . . . (UAS) rely on a nearly continuous stream of communications to successfully complete a mission . . . communications security, and specifically bandwidth protection (from both friendly interference and adversary action) is imperative" (US Joint Forces Command 2010, 83). Despite the publication not being a UAS manual, JP 3-30 is the best Joint planning tool for UAS operations.

Lastly, this study reviewed FM 3-04.15, the multi-service publication that fills the void in Joint UAS doctrine. FM 3-04.15 addresses conventional threats to UAS operations once and its mitigation guidance is only applicable to Theater UAS. It states, "Cloud decks may make it desirable to station the UAS in a low-altitude environment, but minimum altitude limitations and/or enemy threat systems may restrict this option. Against an overcast cloud background, the UA may be highlighted, aiding AAM, antiaircraft artillery (AAA), and surface-to-air missile (SAM) threat operators." The counter-UAS threats identified are not practical means for use against Tactical or Man-

Portable UAS and it makes no mention of EW threats. This guidance is of little value to these lower altitude systems.

US Army

This study took a different approach reviewing Army publications and split its focus into two areas. First, this study examined Army maneuver doctrine to determine the adequacy of employment planning and considerations when integrating UAS into operations. Second, the study examined how well Army doctrine addresses EW threats to UAS operations.

The tactically focused review of maneuver doctrine included FM 3-90.6, *The Brigade Combat Team*, August 2006, FM 3-90.5, *The Combined Arms Battalion*, dated April 2008, FM 3-20.96, *Reconnaissance Squadron*, dated September 2006, and FM 3-21.10, *The Infantry Rifle Company*, dated July 2006. These publications all do an outstanding job integrating UAS in to all aspects of operations including all types of offensive, defensive, security, and reconnaissance operations. However, these manuals do not address threats to UAS operations or contingency planning when operating a non-permissive UAS environment. The only Army publication that addresses limitations to UAS operations is FM 3-20.971, *Reconnaissance and Cavalry Troop*, dated August 2009. FM 3-20.971 identifies issues such as vulnerability to enemy fire, acoustic signature, and LOS communications that may limit UAS operations. Most of these publications discuss EW, but none offer planning considerations for UAS operations on an electronic battlefield.

The capstone Army UAS publication is, FM 3-04.115, *Army Unmanned Aircraft Systems Operations*, dated July 2009. This study extracts two major contributions from this publication. First, *Army Unmanned Aircraft Systems Operations* identifies the susceptibility of UAS CDLs to disruption by EMI and friendly EW jamming systems. Second, FM 3-04.115 is the only publication that addresses counter-UAS threats and how enemy forces may attack all classes of UAS. It addresses multiple conventional counter-air threats but it is also identifies the potential for an EA (Headquarters, Department of the Army 2009a, 34).

UAS CDL susceptibility to EMI, coupled with the militant request for EW assistance, presents a reasonable direction for counter-UAS development. This study was unable to find any evidence of EA against UAS. The relative age of Man-Portable and Tactical UAS technology has limited their use on an electronic battlefield and these systems are largely untested against EW threats. Reason dictates that if UAS CDLs are susceptible to passive EMI, they are also vulnerable to an active EA.

In discussing disruption due to EMI, FM 3-04.115 states, “UAS operations are susceptible to interference from military and civilian communications systems. Terrestrial microwave systems using high energy directional antennas (MSE and tropospheric systems employed by Army and Marine units) may cause significant frequency interference problems and should be avoided (Department of the Army 2009a, 43).” These high-energy communications systems are common in major population centers and on an increasingly technologically dependant battlefield. This study continues to examine EMI on UAS CDLs and implications of such interference throughout this chapter.

Army Unmanned Aircraft Systems Operations discussed EW threats against UAS in general terms. Although it identifies the potential threat of EW systems, it fails to identify possible means to conduct an EA against UAS. It states, “UAS may be subjected to offensive EW, computer network attacks, computer network exploitation, and signal intelligence exploitation (Department of the Army 2009a, 43)."

This study examined Joint, multi-service, and Army publications to identify perceived threats, threat mitigations, and employment considerations for all classes of UAS. Multiple manuals contribute to the discussion of these aspects, but no single publication adequately examines each of these topics. Tactically focused maneuver manuals such as FM 3-20.971, *Reconnaissance and Cavalry Troop*, dated August 2009, explains how UAS are effective combat multipliers and provides the ground commander with some UAS considerations. An aviation centric manual such as FM 3-04.115, *Army Unmanned Aircraft Systems Operations*, dated July 2009, identifies possible threats to UAS but it does not adequately support counter EW planning for UAS.

Organization

This study conducted an organizational review of Tactical and Man-Portable UAS units to assess their ability to plan for EW against UAS. This examination was conducted separately due to the differing command and control structure of these UAS. Units that employ Man-Portable UAS range from as large as Combined Arms Battalion (CAB) to as small as a Long Range Surveillance (LRS) teams. Man-Portable UAS operate below Joint airspace coordinating altitudes and do not require the same airspace control and control (AC2) considerations as larger platforms. Tactical UAS are Brigade level systems that may operate in support of subordinate unit operations. These systems operate above Joint airspace coordinating altitudes and require stringent AC2 measures to ensure de-confliction with manned aircraft.

Man-Portable UAS

TC 1-611, *Small Unmanned Aircraft System Aircrew Training Manual*, dated August 2006, is the primary training publication for Man-Portable UAS. This training circular standardizes Man-Portable UAS training and is a byproduct of Army Aviation adoption of UAS prepotency. Army aviation attempted to standardize Man-Portable UAS organizations and used manned aviation units as a design template. The organization built mirrors manned aviation units, but the Man-Portable UAS units lack the expertise of their manned counterparts (Headquarters, Department of the Army 2006c, 7). This lack of SMEs limits their ability to conduct detailed UAS planning.

In accordance with TC 1-611, the commander of an organization equipped with Man-Portable UAS is responsible for the training, planning, and mission execution of their combat system. The commander identifies an experienced operator to serve as the unit UAS Master Trainer and act as the technical and tactical expert in Man-Portable UAS operations. Man-Portable UAS operators must obtain and maintain a set level of proficiency by completing mission preparation training, compulsory training requirements, and a Semi-Annual Proficiency and Readiness Tests (Headquarters, Department of the Army 2006c, 10).

Similarly, commanders of manned Army Aviation units are responsible for the training, planning, and mission execution their pilots. An experienced warrant officer serves as the units Standardization Instructor Pilot (SIP), who is the technical and tactical expert in the employment of their airframe. Rated aviators must obtain and maintain a set level of proficiency by completing Readiness Level (RL) progression training, compulsory semi-annual training requirements, and an Annual Proficiency and Readiness Tests (APART) (Headquarters, Department of the Army 2006g).

The Man-Portable UAS organizational structure looks similar, but it fails to meet the intent of TC 1-611 due to a lack of expertise for three reasons.

First, the commander of a manned aviation unit is a rated aviator who maintains the same standards as the pilots they lead and is proficient in the employment of their combat system. Commanders of units equipped with Man-Portable UAS are unlikely operators and they receive no specific Man-Portable UAS training. They may not recognize the implications of CDL disruption or what can be done to mitigate interference.

Second, the SIP of a manned aviation unit is not only an experienced pilot. They have also received advanced training to assist their service as a standardization authority. An SIP receives additional training on techniques for training and evaluating individuals, designing comprehensive training programs, and maintaining aviation-training records. Conversely, Man-Portable UAS Master Trainers may themselves be inexperienced operators (Hicks 2008). The ability of a UAS Master Trainer to train operators on EW considerations is dependent on their individual experiences.

Lastly, rated aviators are board selected and undergo a ridged evaluation process. These professional pilots, especially warrant officers, are in career fields that ensure continuous growth throughout their service and this constant progression ensures a healthy talent pool. Man-Portable UAS operators are unit commander selections and there is no minimal requirement to become an operator. They do not receive a Military Occupation Specialties (MOS) career code and may only serve as an operator once in their career. Without ensuring Man-Portable UAS operators remain in the community, it is impossible to develop a healthy talent pool. This lack of collective knowledge limits the intellectual growth potential of the Man-Portable UAS organizations. This stagnant knowledge pool hampers their ability to cope with contingences, such as an EA, against their aircraft.

Tactical UAS

TC 1-600, *Unmanned Aircraft Systems Commander's Guide and Aircrew Training Manual*, dated August 2007, is the primary training publication for Tactical UAS. This TC standardizes Tactical UAS training and is a byproduct of Army Aviation adoption of UAS prepotency. Army aviation standardized Tactical UAS organizations and using manned aviation units as a design template (Headquarters, Department of the Army 2007, 7).

In accordance with TC 1-600, the commander of an organization equipped with a Tactical UAS is responsible for the training, planning, and mission execution the systems. A UAS Standardization Officer/NCO, who is often a warrant officer, assists the commander and serves as the technical and tactical expert for Tactical UAS operations. The commander may assign additional experienced Tactical UAS pilots to serve as Evaluator/Unit Trainers. The remaining pilots are either Mission Commanders or Unmanned Aircraft Crewmembers depending on their level of experience. Tactical UAS operators and rated aviators maintain similar standards. Tactical UAS pilots must complete RL progression training, compulsory semi-annual training, an Annual Proficiency and Readiness Tests (APART), and be medically cleared for flight duties (Headquarters, Department of the Army 2007, 21).

The Tactical UAS organizational structure looks similar and the expertise of its members allows for its successful operation.

First, the commander of a manned aviation unit is a rated aviator who maintains the same standards as the pilots they lead and is proficient in the employment of the combat system. Commanders of Tactical UAS units are not qualified to operate the systems, but the inclusion of a Standardization Officer/NCO mitigates their lack of experience.

Second, the SIP of a manned aviation unit is not only an experienced pilot, he/she has also received advanced training to assist their service as a standardization authority. An SIP receives additional training on techniques for training and evaluating individuals, designing comprehensive training programs, and maintaining aviation-training records. Tactical UAS Standardization Officer/NCO is either an experienced Tactical UAS operator or often a permanently grounded rated aviator. There is no additional training for a Standardization Officer/NCO. They rely upon their individual or collective experience to varying degrees of success (Hill 2010).

Lastly, rated aviators are board selected and undergo a ridged evaluation process. These professional pilots, especially warrant officers, are in career fields that ensure continuous growth throughout their service and this constant progression ensures a healthy talent pool. Tactical UAS operators enlist into the career field and must satisfactorily complete an extensive entry level training program that includes Federal Aviation Administration (FAA) ground school. Tactical UAS pilots are in the MOS 15W career field and will continue to progress throughout their service (Thomas 2006). This progression ensures the development of a healthy Tactical UAS talent pool. This pool of talent allows organizations to constantly grow and mature. This growth enables such organizations to cope with unplanned contingences, such as an EA, against their aircraft.

Training

This study reviewed training required to become a Tactical or Man-Portable UAS operator. The training plans have been examined separately due to the stark differences between the training programs. A Man-Portable UAS operator is not a unique MOS and the operators do not receive an ASI after qualification. Tactical UAS operators enlist into a career field they will remain in throughout their career.

Man-Portable UAS

There are no prerequisites for becoming Man-Portable UAS operators, but they should be technically savvy individuals. Man-Portable UAS operators in this study included infantrymen, fire supporters, mechanics, engineers, and cooks. In 2007, all RQ-11 Raven operators received their training during a 10-day course of instruction at Redstone Army Arsenal, Alabama. However, various alternate Raven qualification courses are now available due to an expansion of Man-Portable UAS utilization and constrained home-station training timelines (Hicks 2008).

In 2009, Man-Portable UAS operators received training at Redstone Army Arsenal, Alabama, Fort Benning, Georgia, Mobile Training Teams (MTTs), and Combat Training Centers (CTCs). The RQ-11 qualification course Memorandum of Instruction (MOI) includes UA familiarization, flight controls and EMI indicators, basic aerodynamics, mission planning, and UAS emergency procedures. RQ-11 operators receive a certificate of completion and an operator’s qualification card once they complete the training (Hicks 2008).

The RQ-11 qualification course discusses EMI indicators and some common sources of this interference. This EMI discussion focuses on passive environmental sources such as radio towers, high-frequency antennas, meteorological interference, and self-imposed interference. The qualification course does not cover enemy threats to UAS or contingency planning for operations in an active EW environment (Hicks 2008).

Tactical UAS

Tactical UAS operators attend a 23-week qualification course at Fort Huachuca, Arizona. This Aviation Professional Training program includes a fully certified FAA ground school, aerodynamics, and meteorology is the first phase of training (Thomas 2006). They next receive training on image analysis, aviation maintenance management, use of the Aviation Mission Planning System (AMPS), and aviation safety considerations. Students transition to field operations once they complete classroom instruction. Field instruction includes establishment of a Tactical UAS operating base, UAS mission preparation, operating a Tactical UAS, and displacement of a Tactical UAS operating base (Thomas 2006).

Tactical UAS is a professional career field that offers advancement and career enhancement opportunities as operators gain experience. These operators attend military schools such as Basic Non-Commissioned Officer Course (BNCOC) and Advanced Non-Commissioned Officer Course (ANCOC) as they advance (Thomas 2006). They are competitive for leadership opportunities including Platoon Sergeant and First Sergeant positions. Senior operators may choose to become Warrant Officers as MOS 150U, Tactical Unmanned Aerial Vehicle (TUAV) Operations Technician (Ayers 2008). This independent career field supports retention and encourages operators to remain in the UAS community.

The Tactical UAS qualification course focuses on UAS employment in support of maneuver operations and students do not study threats to UAS. The course MOI does not discuss either environmental EMI on UAS CDLs or EW threats to UAS CDLs. Interviews conducted with OCs at the NTC, Fort Irwin, California, confirmed a lack of EW education within the Tactical UAS community (Hill 2010). The NTC has identified this lack of EW education and aviation trainers will soon implement scenarios that train EW planning considerations (Hill 2010).

Material

This study examines vulnerabilities of UAS CDLs to an EA but these systems have not served on an active EW battlefield. However, publications such as FM 3-04.115, *Army Unmanned Aircraft Systems Operations*, dated July 2009, explain UAS susceptibility to EMI. Signal interference is the root cause behind both EMI on an UAS CDL and an EA against an UAS CDL, therefore the symptoms of both these events are similar. This section will review how such interference occurs and what material measures may be taken to mitigate this interference.

The primary subjects of this UAS CDL security review are *Unmanned Aerial Vehicle Study*, dated February 2003, the *Unmanned Aerial Vehicles: Background and Issues for Congress*, dated 21 November 2005, *Airspace Integration Plan for Unmanned Aviation*, dated November 2004, and *Unmanned Aircraft Systems FY05-FY09 Class A-C Accident Analysis*, dated 4 December 2009. Despite a wide variation in their production dates, the information in these reports is consistent and lends credence to the reliability of these reports.

UAS CDL Reliability

The intent of UAS is to be a cost effective alternative to manned aircraft and a way to prevent risking a pilot's life. Human needs and emotions such as fatigue, hunger, ambition, and fear do not bind unmanned systems. They dutifully carry out any assigned task, without regard to their survival or need for reward. Some believe they are incapable of committing human errors that often contribute to aviation accidents and there is a common perception that UAS never fail (Singer 2010, 63).

However, reports indicate that UAS are 100 times more likely to succumb to failure than their manned counterparts (Congressional Research Service 2005, 2). The most common causes for these failures are malfunctioning power plant or props, flight control malfunctions, human error, and communications failures (Office of the Secretary of Defense 2003, 39). According to those interviewed, determining the cause of communication failure or disruption is difficult but accident investigators often suspect EMI (Hill 2010).

A September 2009 report found that the MQ-1B Predators, an Air Force Theater UAS, experienced an estimated accident ration of 40 aircraft for 100,000 hours of flight time, an increase over the 30 aircraft for 100,000 hours of flight time ratio the previous year (Dunnigan 2009). The Air Force had anticipated a reduction in the MQ-1B accident rate to ratio of 15/20 aircraft for 100,000 hours of flight time as the technology matured (Office of the Secretary of Defense 2003, 34). Communications failure is the primary cause of 11 percent of these accidents and this rate has been consistent over time (Office of the Secretary of Defense 2003, 39).

The Army's Tactical UAS losses are even higher with the US Army Combat Readiness/Safety Center reporting 246 RQ-7 Shadow accidents during 421,071 flight hours over a four period. This equates to a Tactical UAS loss ratio of approximately 60 aircraft for 100,000 of flight time (Air Task Force 2009, 5).

It is impossible to estimate an accident to flight hour loss ratio for Man-Portable UAS due the Army not tracking these systems by flight hours. The Army tracks Man-Portable UAS by the number of missions an airframe completes, but information is available that allows us to examine their reliability. The US Army Combat Readiness/Safety Center reported 128 Class C accidents over a four-year period, 125 involving the RQ-11 and 3 involving the RQ-16 (Air Task Force 2009, 11).

However, this number is misleading due to many accidents causing less than $20,000 in damage, below the Class C accident threshold that requires an official report (Headquarters, Department of the Army 2009e, 32). Interviews conducted with a former NTC OC found that Man-Portable UAS operators experience CDL failure 5 to 10 times per week. Most of these crashed systems experience minimal damage and no accident report is required (Gaub 2010). NTC safety trends indicate that one Tactical UAS is damaged for every 90 hours of flight and one Man-Portable UAS is damaged for every 20 hours of flight (Key 2010, 16).

Communications failure was the primary cause for 15 percent of Army UAS reportable accidents (Air Task Force 2009, 6). The Army's higher communication failure ratio is due in part to the operational environment in which Tactical and Man-Portable UAS operate.

Man-Portable UAS operators in Iraq and Afghanistan have lost airframes due to EMI causing CDLs communications failure. Units use traditional and unique methods to ensure the recovery of their UAS. One unusual technique stated, “Another thing we put on there is a bilingual label in Arabic and English that says, ‘If found, return to the nearest coalition forces base for a reward,’ We’ve had several turned in that way.” (Army Magazine 2005) Commanders consider the recovery of lost UAS a priority mission due to security and strategic message concerns. If enemy forces delve into the inner workings of a captured UAS, they may be able to exploit this information and develop countermeasures. In addition, an insurgent force may score a strategic communications victory by displaying a captured UAS in their propaganda.

The accident rate of manned aircraft is marginal in comparison to unmanned systems and even innovative immature aircraft, such as the F-22, is much more reliable than unmanned systems. An operational F-22 Raptor has an estimated loss ratio of six aircraft for 100,000 hours of flight time and the Air Force estimates two aircraft for every 100,000 hours of flight time its technology matures (Dunnigan 2009). The F-16 Fighting Falcon has a loss ratio of four aircraft for 100,000 hours of flight time but some have advocated its replacement by an armed UAS (Dunnigan 2009). The Army helicopter accident rate ranged from the loss of five aircraft for 100,000 hours of flight for the AH-64, to two aircraft for 100,000 hours of flight for the UH-60 (Lucas, Thompson, and Davis 2007, 1).

EW Threats

The more dependent on technology a military force, the more vulnerable the force is to EW. The Army has lagged behind the rest of the services in the development of EW, but they are now building a comprehensive EW program. In March 2009, the Army established EW career fields that will develop Soldiers whose expertise is fighting in the electromagnetic spectrum.

EW is a set of measures and actions performed by conflicting sides to detect and attack enemy electronic systems for the control of forces and weapons, including high precision weapons, as well as to electronically defend one's own electronic systems and other targets from technical intelligence, jamming and non-deliberate interference (Vakin, Shustov, and Dunwell 2001, 1).

The symptoms of an EA on a UASs CDL and the results of EMI on a UAS CDL are similar. An EA against a UAS CDL is a likely threat scenario due to the CDLs susceptibility to EMI being public knowledge. This attack would come in the form of an active jammer designed to drown out the CDLs communications.

Jamming is a form of EA using an electronic device, known as a jammer, to transmit high power signal at receiver to disrupt signal quality (Vakin, Shustov, and Dunwell 2001, 1). The three forms of jamming this study reviewed is broadband noise, tone, and swept jamming (Poisel 2003, 213). These jammers each have advantages and disadvantages on the modern EW battlefield but their limiting factor is the power available to apply to the jamming signal.

The goal of noise jamming is to send a threat signal sufficient strength to "out shout" the transmitter sending the attacked frequency (Schlesinger 1961, 13). Noise jamming disrupts the communication waveform by inserting noise onto the receiver. The bandwidth of the signal may be as wide as the entire spectrum used by the communications system or it may occupy only a single channel (Poisel 2003, 216).

Broadband jamming is also known as full band or barrage jamming. This type of jamming can be effective against all forms of anti-jamming (AJ) communication systems (Poisel 2003, 216). This type of jamming raises the background noise level at the receiver, creating a higher noise environment for an AJ system. If the noise is increased, it makes it difficult for a communications system to operate. Effective noise jamming may reduce the range of the communications or if the noise is sufficient, the jammer may deny communication (Poisel 2003, 216). An effective noise jamming attack can disrupt UAS CDL communications and cause the UAS to execute its lost link programming.

The greatest advantage of broadband noise jamming is the simplicity of the system. A jammer operator selects a frequency band and creates as much noise as possible to degrade an entire frequency spectrum. It does not require a smart means to acquire the specific transmitting frequency or the need to chase a frequency hopping system. The greatest disadvantage of broadband noise jamming is the strength of the jamming signal. The larger the spectrum being jammed, the less power is available to create noise.

Sweep jamming, or swept jamming, occurs when narrowband noise is swept across a frequency band of interest (Poisel 2003, 235). The jammer focuses on a specific frequency and a small portion of the band around the single frequency. This sweep can jam a selected band in rapid succession and have effects similar to a barrage jammer. However, a swept jammer concentrates its full power against specific frequencies on the band of interest and this allows swept jammers to have greater range than broadband jammers.

The greatest advantage of swept jamming is the ability to jam a broadband while maintaining adequate power to project its signal (Vakin, Shustov, and Dunwell 2001). Timing is the key to effective sweep jamming and if timing is correct, the jammer can hop around a spectrum with sufficient power to degrade communications. Timing is also the greatest disadvantage to swept jamming. If the jammer hops the spectrum too quickly, it may not loiter on a selected frequency long enough to achieve the degradation desired (Poisel 2003, 235).

Spot jamming, or single tone jamming, occurs when a jammer concentrates all of its power on a single frequency (Poisel 2003, 229). These jammers are effective against communications systems that do not hop and are in use by the opposition. Spot jamming does not move along the frequency spectrum and this limits the utility of such jammers against modern military equipment.

The greatest advantage of spot jamming is the power available to project on its disrupting power at a target. These jammers may have greater range than systems that attack a broad frequency spectrum (Vakin, Shustov, and Dunwell 2001). The greatest disadvantage of spot jamming is its inability to target modern frequency hopping communications and the intelligence requirement of identifying the specific target frequency (Poisel 2003, 230).

Man-Portable UAS are the systems most likely to experience an EA against their CDLs. These systems operate at low altitudes and in close proximity to threat forces. Their flight profile allows enemy forces to visually or acoustically acquire and track the system throughout their mission. Man-Portable UAS CDLs communicate on an L-band UHF frequency that is easy to jam (Poisel 2003, 213). The CDL does not use any electronic protection (EP) such as a frequency hopping radio or a coded receiver. Lastly, the UAS uses an omnidirectional that can receive commands from any direction throughout its flight profile. The C-IED devices in Iraq and Afghanistan use this type of jammer and their tendency to jam UAS CDLs is a testament to the vulnerabilities of these systems (Gaub 2010).

Tactical UAS are less likely to experience an EA against their CDLs but it is still at greater risk than Theater UAS. These systems operational altitudes are higher than Man-Portable UAS but are often within audio or visual range of threat forces (Hill 2010). Directing a jamming signal able to disrupt Tactical UAS CDLs would likely require an advanced directional antenna in order to project and focus its signal (Wilson 2010). Tactical UAS Man-Portable UAS CDLs operates using S-band UHF/SHF frequency and although more jam resistant than the L-band, it is still vulnerable to jamming (Poisel 2003, 214). Lastly, the UA uses an omnidirectional that can receive commands from any direction throughout its flight profile but the GCS transmits its signal using a directional antenna (Hill 2010)

If a CDL experiences frequency interference, the system executes a self-recovery program known as a “lost link procedure” and attempts to reacquire the CDL from the GCS. If a Man-Portable UAS fails to reacquire its CDL, it continues its self-recovery program and attempts to return to a preprogrammed recovery point. If a Tactical UAS fails to reacquire its CDL, the operators may identify the UA as rogue and deploy the systems recovery parachute to avoid endangering manned aircraft.

Electronic Protection

EP is the subdivision of EW where military forces take action to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability (US Joint Forces Command 2007a, 8). Some experts refer to EP as the fixes to the faults exploited by ECM (Schlesinger 1961, 2). EP three subcategories are spectrum management, Electromagnetic (EM) hardening, and emission control. This study will focus on EM hardening of UAS as the only subcategory that is a defense measure against EA. It will also review self-protective measures such as counter-jammers (Headquarters, Department of the Army 2009c, 13) and Communications Security (COMSEC) measures (Headquarters, Department of the Army 2009b, 13).

In an unconstrained environment, vulnerabilities or flaws in military systems would be quickly repaired, but in reality, modifications take time. An aerospace engineer interviewed discussed a constant struggle to balance considerations of weight, size, form, and technological capabilities into component design (Macdonald 2010). A component designed for one system might not work for another system due to variation in design parameters and space available on a given airframe. EP components designed for use in Tactical UAS might be too large or heavy for use in a Man-Portable UAS. EP requirements for Man-Portable UAS might not be required for a Tactical UAS due to its higher operational altitude. Designers must consider the compromise of all these parameters and cost when developing new systems (Macdonald 2010).

Designing equipment that protects personnel, facilities, and equipment by filtering, attenuating, grounding, bonding, and shielding against undesirable effects of

EM energy is hardening(US Joint Forces Command 2007a, 24). EM hardening is a design consideration for all UAS and hardening is one of the key differences between civilian and military UAS (Macdonald 2010). All military electronic equipment receives some hardening such as filtering, attenuating, grounding, and bonding during the production process (Wilson 2010). Most military systems receive some degree of shielding but the amount varies depending on the system. EM shielding can drastically increase the weight of a system and weight is a major concern for aircraft designers (Macdonald 2010).

Systems at risk from EW may execute a preemptive attack against a threat using defensive EA. These measures use the electromagnetic spectrum to protect personnel, facilities, capabilities, and equipment. A vulnerable system conducts a defensive EA to deny an enemy the use of the electromagnetic spectrum to attack the system (Headquarters, Department of the Army 2009c, 13). This fix to system vulnerability is referred to as electronic counter-countermeasures (ECCM) (Schlesinger 1961, 55). A common defensive EA component designed for aircraft is a counter-jammer.

An airborne counter-jammer jams in the same manner as a ground based system. They detect a jamming signal directed against an aircrafts communications system and transmit a counter-jamming signal toward the threat jammer (Puttre 2004, 57). Various self-protection electronic systems are currently available and some larger UAS have tested systems such as the AN/ULQ-21 (Puttre 2004, 67). It is very difficult to develop a completely effective ECCM system due to the dynamic nature of EW. Military forces may invest millions of dollars and an incredible amount of time to develop an ECCM that is obsolete soon after fielding. ECCM equipment often countered by electronic counter-

counter countermeasures (ECCCM) and countering portion of the ECCM term can be carried to the ridiculous extreme (Schlesinger 1961, 55).

An overarching EW philosophy is that designers cannot make a communications system jam-proof but they can make a communications system jam-resistant. The ability to jam communications or the ability to resist jamming is a question of power. If sufficient power is available, any frequency within the electromagnetic spectrum can be jammed (Wilson 2010).

It would be difficult for a Man-Portable or Tactical UAS to produce sufficient power to resist an EA. Most Man-Portable UAS are battery powered and do not have the capability to produce their own power. Any power diverted for electronic self-protection would drastically affect their mission (Hill 2010). A Tactical UAS generates the power required to operate its systems but its ability to support additional power requirements is questionable (Hill 2010). The power production capability of a UAS is limited and the power potential of a UAS counter-jammer will be equally limited.

Denying unauthorized forces information of value that might be derived from the possession and study of telecommunications is COMSEC. These protective measures mislead or deny unauthorized persons attempting to interdict friendly communication (Headquarters, Department of the Army 2009b, 253). UAS program offices are working to improve COMSEC by applying cryptographic measures (Jensen 2010). The emphasis of these COMSEC improvements is UAS VDLs due to the publicized security breach of UAS video security by insurgents in Iraq (Gorman, Dreazen, and Cole 2009). The development of some of this COMSEC equipment is complete and fielding is ongoing (Hill 2010).

These COMSEC systems encrypt a communications signal with a code prior to transmission and the receiver must decrypt the signal with a key to interpret the information. Coding communications does provide some EP to the transmitted signal. A smart jammer attempting to hop over a specific signal will fail unless it has the correct timing and frequencies (Poisel 2003, 237). This does not mean that a coded signal is jam-proof but it is more jam resistant. Some forms of jamming, such as broadband jamming, are not dependant on timing or frequency specificity. If enough power is available, a jammer can jam any frequency along the spectrum it is targeting (Poisel 2003, 214).

This chapter began with an extensive review of the primary Man-Portable and Tactical UAS. It analyzed existing Joint and Army doctrine, UAS organizational structure, UAS operator training, and materials that influence UAS CDL security. Each of these components play a part in UAS CDL vulnerabilities but the material aspect has the greatest degree of influence. This study has shown that UAS CDLs are susceptible to EMI and that threat technology is available to attack these flaws making the UAS vulnerable. Measures are available that provide some EP to improve the security of these systems and electronic self-protective devices could be incorporated. These modifications must account for factors such as weight, size, form, technological capabilities, and cost into any modification design. Lastly, this study found that no communications signal is jam-proof weight but designers can develop a system that is resistant to jamming.

CHAPTER 5

CONCLUSION AND RECOMMENDATIONS

> [Y]ou may fly over a land forever; you may bomb it, atomize it, pulverize it and wipe it clean of life--but if you desire to defend it, protect it, and keep it for civilization, you must do this on the ground, the way the Roman legions did, by putting your young men into the mud.
>
> — T. R. Fehrenbach

Conclusions

The procurement and utilization of UAS has exploded globally and these systems have changed the face of 21st century warfare. They are a mainstay on the modern battlefield gathering intelligence, observing key terrain, and targeting threat forces. Time will tell if the world is experiencing an UAS RMA or if these weapons are products of simple innovation. What is clear is the faith the US government has placed in UAS and their intent to lead the global development of this technology.

Reliability of the UAS communications structure is a major concern and failure of CDL communications due to EMI has resulted in numerous UAS accidents. The omnidirectional antennas the aircraft uses to establish the CDL leaves the system open to interference. Environmental EMI from communications systems produce sufficient energy to disrupt CDLs and are responsible for 15 percent of Army UAS accidents (Air Task Force 2009, 6). Man-Portable UAS CDL experience communications failure more frequently but accurate statistics are not available due to lack of reporting (Gaub 2010).

An adversary can exploit this susceptibility to EMI by conducting an EA against the CDL. The indicators of an EA and the symptoms of EMI disrupting UAS CDLs are similar. Jammers capable of disrupting CDLs may be simple range omnidirectional systems or smart systems that can project a signal far away from the transmitter. Interviews conducted confirmed that any communications signal can be jammed if the appropriate technique is used and sufficient power is available (Wilson 2010). Simple jammers are easy to make and these improvised jammers can attack UAS CDLs.

This chapter presents the findings and recommendations of this study using the doctrine, organization, training, and material portions of the DOTMLPF construct. These findings and recommendations are not all inclusive, but they do present the key issues that require attention to shape the future force.

Doctrine

This study's review focused the adequacy of Joint and Army doctrine to prepare for EW. The Joint doctrine review examined the establishment of a common operational language, Joint UAS employment planning, and considerations for UAS CDL protection. This study took a different approach reviewing Army publications and split its focus into two areas. First, this study examined Army maneuver doctrine to determine the adequacy of employment planning and considerations when integrating UAS into operations. Second, the study examined how well Army doctrine addresses EW threats to UAS operations.

The Joint community has failed to establish a language. Development of Joint terminology is the responsibility of US Joint Forces Command (USJFCOM) but this process is complicated due to the dynamic nature of UAS innovation. Operators and non-operators alike should clearly understand Joint terminology. The language must be ridged enough to minimize ambiguity but retain the flexibility that allows for system innovation and growth. Clearly defining classes is critical, especially if findings demonstrate that some classes are more susceptible to EW.

The failure to establish flexible Joint terminology has resulted in continuous changes in UAS classifications. There has been at least five different UAS naming conventions, and at one time the Air Force, Army, and Marines all used service-specific terminology. The *FY2009–2034 Unmanned Systems Integrated Roadmap,* dated April 2009, contains the most recent UAS categories. It specifies groupings based on aircraft specifications and performance. This group identification is of little value to a non-operator who does not know the specifications and performance parameters of a specific UAS (Department of Defense 2009, 110). It also lacks flexibility and the fielding of new micro UASs will require a revised terminology.

This study used the UAS classifications found FM 3-04.15, *Multi-Service Tactics, Techniques, and Procedures for the Tactical Employment of Unmanned Aerial Systems,* dated 3 August 2006, which establishes three classes based on a systems operational environment and general system capabilities. It classifies systems as Man-Portable UAS, Tactical UAS, and Theater UAS. These general groupings allow non-operators to understand system capabilities but their general description may lack the specificity some desire.

Joint planning considerations for UAS employment and considerations for CDL protection within the JPs is acceptable. There is room for improvement but the newest manual, JP 3-30, *Command and Control for Joint Air Operations,* dated 12 January 2010, is excellent.

This study then conducted a review Army maneuver publications to determine their understanding of UAS capabilities and limitations. Maneuver forces have embraced UAS and they have a good understanding of its capabilities. They integrate unmanned systems in all operations: offensive, defensive, and tactical enabling. However, these forces lack a general understanding of UAS limitations and survivability planning considerations. They do not stress UAS dependence on uninterrupted communications, their susceptibility to EMI, or their vulnerability to EW. The only maneuver publication that addresses UAS limitations is FM 3-20.971, *Reconnaissance and Cavalry Troop*, dated August 2009. *Reconnaissance and Cavalry Troop* discusses their vulnerability to enemy fire, acoustic signature, and dependence on LOS communications.

This study next examined the adequacy of UAS threat planning. The primary document for this review was FM 3-04.115, *Army Unmanned Aircraft Systems Operations*, dated July 2009, the Army's capstone UAS planning publication. *Army Unmanned Aircraft Systems Operations* is the only Army publication that addresses both UAS CDL susceptibility to EMI and threats to UAS (Headquarters, Department of the Army 2009a). However, most of the threats identified are conventional and EW threats against UAS are mentioned just once in FM 3-04.115. This study finds that planning considerations and threat mitigation to improve UAS survivability against EW is inadequate.

Other Army aviation manuals, such as FM 3-04.126, *Attack Reconnaissance Helicopter Operations*, February 2007, is an excellent template for improvement. *Attack Reconnaissance Helicopter Operations* dedicates an entire appendix to planning considerations for aircraft survivability from a variety of threats, unlike the few paragraphs in *Unmanned Aircraft Systems Operations*.

Organization

This study examined the organizational structure of Man-Portable and Tactical UAS units to determine if the structure is adequate for EW planning. Aviation branch is the prepotency for UAS and they have progressively standardized UAS operations. Aviation branch has organized UAS units under the same design as their manned units. This has produced mixed results depending on the airframe.

It is unrealistic for units using Man-Portable UAS to mirror the manned aircraft organizational design. These units lack the SMEs found either manned aircraft or specialized UAS units. These units do not have leaders trained as UAS operators and unit UAS Master Trainers may themselves be inexperienced (Gaub 2010). This lack of experts limits their ability to identify indicators of EW or plan to counter an EA. Man-Portable organizations must expand their knowledge base to improve their EW planning capacity.

Tactical UAS units mirror their manned counterparts well. Aviation branch has exerted greater control over these units since their assimilation from Military Intelligence branch. These specialized UAS units have are standardized and professionals in the aviation community. Commanders of Tactical UAS units are not operators, but they have numerous SMEs advisors to mitigate their lack of training. These SMEs are capable of coping with and plan to counter EW if properly trained.

A ridged quality control process ensures Tactical UAS operators are thoroughly vetted professionals. Requirements for enlisting as a Tactical UAS operator are high and these Soldiers enter a career field that ensures continued progression. This ensures that only quality Soldiers receive training as an operator and keeping operators in the community ensures a consistently healthy talent pool (Thomas 2006).

Training

This study examined the training Man-Portable and Tactical UAS operators receive to identify EW training requirements. Training for these operators is different due to their specific operational environments.

Qualification training for Man-Portable UAS operators is very good. Soldiers from various MOSs and skill levels receive training by quality civilian and military trainers. Infantrymen, fire supporters, mechanics, engineers and cooks often train as Man-Portable UAS operators. These Soldiers attend a 10-day qualification course that focuses on learning about their UA, flight controls and EMI indicators, basic aerodynamics, mission planning, and UAS emergency procedures. The qualification course covers environmental forms of EMI, but does not discuss EW threats to aircraft survivability (Hicks 2008). Once qualified, operators receive a certificate of course completion but do not receive an ASI.

Initial entry training for Tactical UAS operators is excellent. The 23-week initial entry training course includes a fully certified FAA ground school, aerodynamics, meteorology, image analysis, aviation maintenance management, use of the AMPS, and aviation safety considerations (Thomas 2006). One critique of the initial entry course is an absence of instruction on threats to UAS survivability and counter EW planning.

Tactical UAS operators train as professionals entering a community through which they progress throughout their career. Unlike Man-Portable UAS operators, these

Soldiers attend developmental military schooling such as the Army's Noncommissioned Officer Course (ANCOC) as they advance, and will have leadership opportunities (Thomas 2006).

Material

This study examined the vulnerabilities of UAS CDLs to an EA. These systems have not been exposed to a highly saturated EW battlefield due to their recent development but findings can be extracted by their performance against other forms of interference. The root cause of both EMI on an UAS CDL and an EA against an UAS CDL is signal interference. UAS reaction to either EMI or an EA will be similar due to both being a result of signal interference. Disruption of UAS CDLs is reflected in a systems reliability and accident rate.

This study found the reliability and accident rate of UAS surprising. In 2005, the Congressional Research Service issued a report that UAS have an accident rate 100 times greater than manned aircraft (Congressional Research Service 2005, 2). Accident data remained consistent throughout this study and data supports the findings of the 2005 Congressional Research Service report (Dunnigan 2009). Communications failure accounts for 11% of all Theater, Tactical, and Man-Portable UAS accidents (Office of the Secretary of Defense 2003, 39). Communications failure in Army systems accounts for 15% of all reportable accidents but most incidents of communication failure for Man-portable UAS go unreported (Air Task Force 2009, 6).

EW technology is available that exploits UAS CDL susceptibility to EMI. These EW systems disrupt CDLs by transmitting a more powerful signal than that produced by a UASs GCS. These systems are jammers that "out yell" a friendly transmitter using the electromagnetic spectrum to send data. This form of EA will cause signal interference similar to what CDLs experience due to EMI. This study reviewed three forms of jamming: broadband noise, tone, and swept jamming (Poisel 2003, 213).

Jamming disrupts communication waveforms by flooding a receiver with noise and any signal can be jammed with sufficient power. Effective noise jamming may reduce as systems communications range or it may completely deny communications (Poisel 2003, 216). Disruption of UAS CDLs will cause a system to execute its lost link programming and force an aircraft to depart the mission area (Gaub 2010).

It is possible to defend against an EA by using EP measures or conducting a defensive EA. EM shielding is means by which designers can improve systems susceptibility to external interference. Shielding can be effective, but it can also add significant weight to the aircraft (Macdonald 2010).

Defensive EA uses the electromagnetic spectrum to execute a preemptive attack against a threat system before it can conduct an EA (Headquarters, Department of the Army 2009c, 13). A counter-jammer is a device commonly used for defensive EA. These counter-jammers detect a jamming signal and transmit a counter-jamming signal toward the threat (Puttre 2004, 57). These improvements are plausible but one must consider second and third order effects when implementing such changes. Any modification used to improve UAS CDL security must account for factors such as weight, size, form, technological capabilities, and cost into any modification design (Macdonald 2010).

COMSEC can also increase UAS CDL security, but it may not prevent CDL jamming. COMSEC imparts a code on data when sending a signal and a key is required to translate the code on the receiving end. These protective measures mislead or deny unauthorized persons attempting to interdict friendly communication (Headquarters, Department of the Army 2009b, 253). Coding communications does provide some EP to the transmitted signal. A smart jammer attempting to hop over a specific signal will fail unless it has the correct timing and frequencies (Poisel 2003, 237). PEO AVN is working to improve COMSEC on all Army UAS (Jensen 2010). COMSEC does not make a signal jam-proof but it may make a signal jam resistant. If sufficient power is available, any frequency within the electromagnetic spectrum can be jammed (Wilson 2010).

Recommendations

This study used the DOTMLPF construct to focus the analytical process and it will continue to use this design when making recommendations to mitigate CDL vulnerabilities.

Doctrine

This study recommends the Joint community adopt classifications aligned with the Joint levels of war: Tactical UAS, Operational UAS, and Strategic UAS. The study recommends the addition of a fourth class, Theater UAS, to reflect systems above the Operational level but below the Strategic level, such as the MQ-9 Reaper. Using the doctrinally accepted levels of war eases ambiguity, prevents continuous redefining of classes, and allows non-operators to understand the general capabilities of a system. These descriptions may be too broad for use by operators and subcategories within these classes may be required for detailed planning.

This study recommends the Army clearly explain limitations and survivability considerations for UAS in maneuver doctrine. This community understands the benefits of this combat multiplier but many are ignorant to their limitations. This lack of understanding may be a contributing factor to the frequency of UAS CDL disruption. These forces have been trained to utilize unmanned systems, but they must be taught how to preserve these systems.

This study recommends the Army conduct a comprehensive review of counter-UAS threats and include its findings in changes to FM 3-04.115, *Army Unmanned Aircraft Systems Operations*. The audience for the revised manual is UAS operators, planners, and leaders. *Army Unmanned Aircraft Systems Operations* must be a standalone document that is applicable to all levels of war. It must account for conventional counter-air threats and EW threats against all UAS. Doctrine must dispel the belief that UAS are expendable. No UAS is expendable and the Army must do more to improve system survivability.

Organization

This study recommends a reexamination of the intent behind current Man-Portable UAS design. It is unrealistic to expect units equipped with MAN-Portable UAS to replicated manned organizations without increases in quality control and in the number of SMEs. This lack of expertise degrades the organizations ability to cope with unforeseen threats, such as an EA.

The Army must generate a standardized screening process for Man-Portable UAS operators and establish a minimum set of requirements to receive training. UAS Master Trainers must be an experienced UAS operator that understands and can plan for threat activity. Master trainers must have enough time in service to advocate UAS limitations and survivability concerns with leadership.

UAS operators should receive an ASI on completion of initial training and they should remain proficient throughout their careers. This will allow these systems to develop a healthy talent pool comparable to Tactical UAS. This will allow Man-Portable organizations to cope with an unplanned event, such as an AE. These recommendations will increase requirements on units equipped with Man-Portable UAS. If these changes prove too disruptive, Aviation branch must reconsider the organizational design for these units.

This study has no organizational recommendations for Tactical UAS. The manned unit design is well suited for these specialized UAS organizations.

Training

This study recommends that counter EW and airframe survivability planning considerations be included in all UAS qualification training.

Man Portable UAS is the system most likely to encounter enemy contact but these operators receive limited threat training. The Man-Portable qualification course discusses environmental EMI but it does not cover EW threats to aircraft survivability. The qualification course should stress the importance of accident reporting, especially when operators suspect EMI. Accident reporting from these systems is poor and ascertaining causes of UAS failures is difficult without this data (Gaub 2010). Lastly, those who complete the qualification course should receive an ASI and be tracked throughout their careers.

Initial entry training for Tactical UAS is excellent but it lacks sufficient threat training. Aviation branch must determine threats to UAS from small arms, Air Defense Artillery (ADA), and EW. Tactical UAS training must be updated to account for these threats and focus its efforts on airframe survivability. These operators must understand that their systems are not expendable and they are responsible for managing its survival.

Material

This study recommends an increased effort to improve CDL protection and security. These improvements will not be universal due to the differing airframes involved. Engineers designing modifications must consider weight, size, form, technological capabilities, and cost considerations. Improvements may not be practical if they impede on system capabilities or substantially increase unit cost. Improvements of smaller systems may be limited to passive measures such as EM shielding and application of COMSEC. Larger systems may be able to integrate active measures, such as counter-jammers, into their systems. Airborne counter-jammers, such as the AN/ULQ-21, are available but current technology may not be appropriate for Army systems (Puttre 2004, 67).

Summary

UAS CDLs are vulnerable to EA and these systems may be targeted using low tech, easy to produce, jamming weapons. Jammed UAS will not complete their assigned mission, but will execute a lost link procedure in an attempt to reestablish link (Hill 2010). Disrupted UAS may reestablish their CDLs but many crash due an inability to reconnect with their GCS. The solution to rectify these flaws will not be uniform for all airframes.

Man-Portable UAS have the greatest threat of experiencing an EA, but the size of the airframe limits EP or defensive EA design options. Any modifications to Man-

Portable UAS that increases weight or substantially raises unit cost may not be worth the effort. The solution for these systems may be improved training for operators and education for leaders. Man-Portable UAS users must plan and account for aircraft survivability when conducting pre-mission planning.

Tactical UAS are less likely to experience an EA but it is possible, especially from a sophisticated threat. The size of Tactical UAS airframes allows greater options to improve CDL protection and security. Engineers still must consider size, weight, and cost when designing modifications. An upgrade that reduces current system capabilities is inadvisable but airframe survivability must be a consideration in future designs.

This study did not focus on Theater UAS but sufficient information is available to determine that these systems are least threatened by a ground based EA. These systems are still vulnerable to EA but most likely by an airborne EW platform. The size of Theater UAS allows numerous options to improve CDL protection and security.

Military aviation is in a transitional phase. Determining the future force structure and the required equipment is a complex proposition. This transformation demands extensive research and development. US military aviation stands to remain the dominant global airpower force if their vision of the future force is correct but if their vision is incorrect, it will be fighting to regain airpower relevancy. Understanding the advantages and disadvantages of manned and unmanned aircraft is vital in determining future force structure.

Manned aircraft have a number of advantages over unmanned aviation. Statistics show that the most accident prone manned aircraft lost five aircraft for every 100,000 flight hours as opposed to the least accident prone UAS losing 40 aircraft for every

100,000 flight hours. This lower accident rate is due to higher standards for manned aircraft design and ability of a pilot to evaluate and react to an in-flight emergency.

Manned aircraft also have a number of disadvantages when compared to unmanned systems. Combatant commanders must consider the limitations and vulnerability of pilots when assigning missions. It is unconscionable to send such airframes on a mission that has little chance of survival or a mission that presses pilots beyond human limitations. Manned aircraft are more expensive to produce and maintain than their unmanned counterparts. The weak link in manned aviation is the man.

Unmanned systems have a number of advantages over manned aircraft. The systems are unbound by human limitations. They can remain airborne for long durations, do not require life support systems, do not need to eat or sleep, and they will never say no to a mission. They may minimize friendly loss of life by conducting missions that have a minimal chance of survival.

Unmanned systems also have a number of disadvantages in comparison to manned aircraft. They have a relatively high accident rate and the cost of the systems have grown exponentially. Ground based operators control these systems and they are still prone to human error. UAS operators have minimal options if an in-flight emergency occurs and such emergencies often result in the airframe being lost. Current systems are not autonomous and depend on communications with a GCS. The weak link for UAS is their dependence on continuous communications.

The best long-term solution for the military is a balanced air force structure. The military must continue to embrace UAS technology and invest in future systems. They must also remember the self-balancing nature of warfare and diversify their employment options. Over dependence on a single technology can leave a force unprepared for combat. In World War II, the Army Air Corps did not recognize limitations their strategic bombing doctrine and numerous lives were lost as they scrambled to produce a viable pursuit aircraft. In the Korean War, the government did not recognize the limitations of Atomic deterrence and spent months rapidly modernizing its obsolete force. In Vietnam, the Air Force had overestimated the ability of their AAMs and modified their shortsighted fighter designs with guns. The US must prepare for future combat operations against all threats whether high intensity conflict, hybrid, or asymmetric. It cannot afford to be unprepared when an unknown adversary decides to attack.

GLOSSARY

Abort. To terminate a mission for any reason other than enemy action. It may occur at any point after the beginning of the mission and prior to its completion (US Joint Forces Command 2009b, 8).

Above Ground Level (AGL). Above ground level is the height in which an aircraft is above the ground (Headquarters, Department of the Army 2007b, 19).

Acoustical Surveillance. Employment of electronic devices, including sound-recording, receiving, or -transmitting equipment, for the collection of information. (US Joint Forces Command 2009b, 8).

Air Defense Artillery (ADA). Weapons and equipment for actively combating air targets from the ground. (US Joint Forces Command 2009b, 18).

Air Surveillance — The systematic observation of airspace by electronic, visual or other means, primarily for the purpose of identifying and determining the movements of aircraft and missiles, friendly and enemy, in the airspace under observation. (US Joint Forces Command 2009b, 28).

Airspace Management. The coordination, integration, and regulation of the use of airspace of defined dimensions. (US Joint Forces Command 2009b, 27).

Barrage/Broadband Jamming. A type of electronic attack intended for simultaneous jamming over a wide area of frequency spectrum. (US Joint Forces Command 2009b, 47).

Chairman of the Joint Chiefs of Staff instruction. A replacement document for all types of correspondence containing Chairman of the Joint Chiefs of Staff policy and guidance that does not involve the employment of forces. An instruction is of indefinite duration and is applicable to external agencies, or both the Joint Staff and external agencies. It remains in effect until superseded, rescinded, or otherwise canceled. Chairman of the Joint Chiefs of Staff instructions, unlike Joint publications, will not contain Joint doctrine (US Joint Forces Command 2009b, 62).

Command and Control (C2). The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission (US Joint Forces Command 2009b, 79).

Communications Jamming. Electronic measures taken to deny the enemy use of communications means (Headquarters, Department of the Army, 2004, 52)

Coordinating Altitude. A procedural airspace control method to separate fixed- and rotary-wing aircraft by determining an altitude below which fixed-wing aircraft will normally not fly and above which rotary-wing aircraft normally will not fly (US Joint Forces Command 2009b, 98).

Directed-Energy Warfare. Military action involving the use of directed-energy weapons, devices, and countermeasures to either cause direct damage or destruction of enemy equipment, facilities, and personnel, or to determine, exploit, reduce, or prevent hostile use of the electromagnetic spectrum through damage, destruction, and disruption. It also includes actions taken to protect friendly equipment, facilities, and personnel and retain friendly use of the electromagnetic spectrum (US Joint Forces Command 2009b, 125).

Doctrine. Fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application (US Joint Forces Command 2009b, 130).

Drone. A land, sea, or air vehicle that is remotely or automatically controlled (US Joint Forces Command 2009b, 131).

Electromagnetic Hardening. Action taken to protect personnel, facilities, and/or equipment by filtering, attenuating, grounding, bonding, and/or shielding against undesirable effects of electromagnetic energy (US Joint Forces Command 2009b, 135).

Electromagnetic Spectrum. The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands (US Joint Forces Command 2009b, 136).

Laser Rangefinder / Designator (LRFD). A device which uses laser energy for determining the distance from the device to a place or object. A device that emits a beam of laser energy which is used to mark a specific place or object (US Joint Forces Command 2009b, 233).

Mean Sea Level (MSL). Determined based on barometric pressure, MSL altitude is the distance above where sea level would be if there were no land (Headquarters, Department of the Army 2007b, 19).

Meteorology. The study dealing with the phenomena of the atmosphere including the physics, chemistry, and dynamics extending to the effects of the atmosphere on the Earth’s surface and the oceans (US Joint Forces Command 2009b, 253).

Reachback. The process of obtaining products, services, and applications, or forces, or equipment, or material from organizations that are not forward deployed (US Joint Forces Command 2009b, 331).

Remotely Piloted Vehicle. An unmanned vehicle capable of being controlled from a distant location through a communication link. It is normally designed to be recoverable (US Joint Forces Command 2009b, 338).

Spot/Tone Jamming. The jamming of a specific channel or frequency (Headquarters, Department of the Army, 2004, 187)

Sweep/Swept Jamming. A narrow band of jamming that is swept back and forth over a relatively wide operating band of frequencies (Headquarters, Department of the Army, 2004, 193)

REFERENCE LIST

AAI Corporation. 2009a. Shadow RQ-7B system. http://www.aaicorp.com/pdfs/shadow_200.pdf (accessed 18 Decembr 2009).

———. 2009b. The next generation in one system technology. http://www.aaicorp.com/pdfs/ugcs41709a.pdf (accessed 23 October 2009).

Adamy, David L. 2004. *EW 102: A second course in electronic warfare.* Boston: Artech House Publications, Inc.

———. 2009. *EW 103: Tactical battlefield communications electronic warfare.* Boston: Artech House Publications, Inc.

AeroVironment Inc. 2009a. Dragon eye. http://www.avinc.com/downloads/Dragon_Eye_AV_datasheet.pdf (accessed 19 October 2009).

———. 2009b. Puma AE. 1 January 2009. http://www.avinc.com/downloads/AV_PUMAAE_V10109.pdf (accessed 23 October 2009).

———. 2009c. Raven RQ-11B. 1 January 2009. http://www.avinc.com/downloads/AV_RAVEN-DOM_V10109.pdf (accessed 23 October 2009).

———. 2009d. Wasp III. 1 January 2009. http://www.avinc.com/uas/small_uas/wasp/ (accessed 23 October 2009).

———. 2009e. Joint common interoperable ground control station. 1 January 2009. http://www.avinc.com/downloads/AV_GCS_V10109.pdf (accessed 23 October 2009).

Air Task Force, US Army Combat Readiness/Safety Center. 2009. Unmanned aircraft systems FY05-FY09 Class A-C accident analysis. Accident Report. Fort Rucker, AL: US Army Combat Readiness/Safety Center.

Allexperts. 2005. F-35 Lightning II. 26 December. http://en.allexperts.com/e/f/f/f-35_lightning_ii.htm (accessed 16 September 2009).

Armada International. 2009. *Complete guide drones 2009.* Zurich: Armada International.

Army Magazine. 2005. Raven UAV. Association of the United States Army. 1 January. http://www3.ausa.org/webint/DeptArmyMagazine.nsf/byid/CCRN-6CCSFL (accessed 18 December 2009).

Ayers, Richard. 2008. Warrant officer prerequisites and duty description. US Army Recruiting Command. 5 March. http://www.usarec.army.mil/hq/warrant/prerequ/WO150U.html (accessed 23 December 2009).

BBC News. 2008. Russia “shot down Georgia drone.” 21 April. http://news.bbc.co.uk/ 2/hi/europe/7358761.stm (accessed 19 October 2009).

Bloom, Ursula. 1958. *He lit the lamp: a biography of Professor A. M. Low*. London: Burke.

Blyenburgh, Peter van. 2008. EASA UAS Workshop. European Aviation Safety Agency. 1 February. http://www.easa.europa.eu/ws_prod/g/doc/Events /2008/February/1-Overview%20of%20the%20UAV%20Industry%20(UVS).pdf (accessed 10 March 2010).

Bogart, Charles H. 1976 German remotely piloted bombs. *United States Naval Institute Proceedings* (November): 62-64.

Braybrook, Roy. 2004. Three “D” missions--dull, dirty and dangerous!. Armada International. 1 February.

CBS News Investigates. 2008. Palestinian militants try to find ways to overcome Israeli UAVs on Jihadi forums. 31 December. http://www.cbsnews.com/8301-502684_162-4693780-502684.html?tag=contentMain%3bcontentBody (accessed 19 October 2009).

Congressional Desk. 2010. McKeon Statement on the President's Fiscal Year 2011 Budget Request for the Department of Defense. 12 February. http://www.americanchronicle.com/articles/view/141330 (accessed 16 March 2010).

Congressional Research Service. 2005. CRS Report for Congress, *Unmanned aerial vehicles: Background and issues for congress.* Washington DC: Foreign Affairs, Defense, and Trade Division.

Defense Science Board. 2004. *Defense science board study on unmanned aerial vehicles and uninhabited combat aerial vehicles.* Washington, DC: Government Printing Office.

Department of Defense. 2009. *FY2009–2034 Unmanned systems integrated roadmap*. Washington, DC: Government Printing Office.

Dunnigan, James. 2009. Predators falling from the sky everywhere. 9 September. http://www.strategypage.com/dls/articles/Predators-Falling-From-The-Sky-Everywhere-9-21-2009.asp (accessed 18 December 2009).

Edwards, Victoria. 2009. Stealth hornets: Unmanned aerial vehicle and unmanned combat aerial vehicle UAV/ACAV version of a revolution in military affairs. Conference of Defence Associations. April. http://www.cda-cdai.ca/cdai/ uploads/cdai/ 2009/04/edwards03.pdf (accessed 15 September 2009).

Eshel, David. 2006. Israel intercept two attack UAV launched by Hezbollah. 7 August. http://defense-update.com/2006/08/israel-intercept-two-attack-uav.html (accessed 15 September 2009).

Ford, Kyle L. 2010. “A full spectrum capability”--Leaders navigate state of Aviation Branch during conference. Official Homepage of the United States Army. 4 February. http://www.army.mil/-news/2010/02/04/33968-a-full-spectrum-capability----leaders-navigate-state-of-aviation-branch-during-conference/ (accessed 15 April 2010).

Gaub, Darin. 2010. Interviewed by author. Fort Leavenworth, Kansas. 21 April.

General Atomics Aeronautical Systems, Inc. 2009a. Sky Warrior: Armed persistence. http://www.ga-asi.com/products/aircraft/pdf/Sky_Warrior.pdf (accessed 18 December 2009).

———. 2009b. I-GNAT ER/Sky Warrior Alpha. General Atomics Aeronautical. http://www.ga-asi.com/products/aircraft/pdf/ARMY%20I-GNAT%20ER.pdf (accessed 18 December 2009).

Gorman, Siobhan, Yochi J. Dreazen, and August Cole. 2009. Insurgents hack US drones. 17 December. http://online.wsj.com/article/SB126102247 889095011.html (accessed 18 December 2009).

Goebel, Greg. 2009. Unmanned Aerial Vehicles. vectorsite. 1 January. http://www.vectorsite.net/twuav.html (accessed 24 October 2009).

Headquarters, Department of the Army. 1994. Army Regulation (AR) 385–40, *Accident reporting and records.* Washington DC: Government Printing Office.

———. 2006a. Field Manual (FM) 3-04.15, *Multi-Service tactics, techniques, and procedures for the tactical employment of unmanned aircraft systems.* Washington DC: Government Printing Office.

———. 2006b. Army Regulation (AR) 95-23, *Unmanned aircraft systems flight regulations.* Washington DC: Government Printing Office.

———. 2006c. Training Circular (TC) 1-611, *Small unmanned aircraft system aircrew Training Manual.* Washington DC: Government Printing Office.

———. 2006d. Field Manual (FM) 3-21.10, *The infantry rifle company*. Washington DC: Government Printing Office.

———. 2006e. Field Manual (FM) 3-20.96, *Reconnaissance squadron.* Washington DC: Government Printing Office.

———. 2006f. Field Manual (FM) 3-90.6, *The brigade combat team.* Washington DC: Government Printing Office.

———. 2006g. Training Circular (TC) 1-210, *Aircrew training program commander's guide to individual, crew, and collective training.* Washington DC: Government Printing Office.

———. 2007. Training Circular (TC) 1-600, *Unmanned aircraft systems commander's guide and aircrew training manual.* Washington DC: Government Printing Office.

———. 2009a. Field Manual (FM) 3-04.115, *Army unmanned aircraft systems operations.* Washington DC: Government Printing Office.

———. 2009b. Field Manual (FM) 6-02.53, *Tactical radio operations*. Washington DC: Government Printing Office.

———. 2009c. Field Manual (FM) 3-36, *Electronic warfare in operations.* Washington DC: Government Printing Office.

———. 2009d. Field Manual (FM) 3-20.971, *Reconnaissance and cavalry troop.* Washington DC: Government Printing Office.

———. 2009e. Army Regulation (AR) 95-23, *The Army safety program.* Washington DC: Government Printing Office.

Hicks, Joseph. 2008. Small unmanned aircraft system (SUAS) school training. Memorandum of Instruction. Fort Benning.

Hill, Issac. 2010. Interviewed by author. Fort Leavenworth, Kansas. 3 March.

Honeywell Aerospace. 2008. T-Hawk MAV. September. http://www51.honey well.com/aero/ common/documents/myaerospacecatalog-documents/ Defense_Brochures/T-Hawk_MAV.pdf (accessed 12 November 2009).

Key, Dave. 2010. *NTC Safety Trends*. Fort Irwin: NTC Operations Group.

Lucas, Nancy, Mary Ann Thompson, and Glen Davis. 2008. Fiscal 2007: An update. *Knowledge*: Official Safety Magazine of the US Army. July. https://safety.army.mil/Knowledge_Online/Portals/july2008/Fiscal%202007%20 An%20Update.pdf (accessed 18 December 2009).

Macdonald, John. 2010. Interviewed by author. Fort Leavenworth, Kansas. 2 February.

McDaniel, Martin. 2010. Interviewed by author. Fort Leavenworth, Kansas. 10 February.

Net Resources International. 2010. RQ-11 Raven unmanned aircraft system. SPG Media Limited. http://www.army-technology.com/projects/rq11-raven/ (accessed 3 January 2010).

Northrop Grumman. 2010. MQ-5B Hunter. http://www.as.northropgrumman.com/ products/hunter/assets/MQ-5B-05.pdf (accessed 3 January 2010).

Office of the Secretary of Defense. 2003. *Unmanned aerial vehicle reliability study*. Washington, DC: Government Printing Office.

Poisel, Richard A. 2003. *Modern communications jamming principles and techniques.* Boston: Artech House.

Puttre, Michael., ed. 2004. *International electronic countermeasures handbook.* Norwood: Horizon House Publications.

Reid, Robert H. 2009. Iranian drone shot down by US over Iraq: military admits. 16 March. http://www.huffingtonpost.com/2009/03/16/iranian-drone-shot-down-b_n_175375.html (accessed 19 October 2009).

Ronen, Gil. 2008. Operation 'Cast Lead' begins; one Israeli and 205 arabs are dead. Arutz Sheva News. 27 December. http://www.israelnationalnews.com/News/ News.aspx/129052 (accessed 19 October 2009).

Royal Air Force Organization. 2009. The development of British military aviation. M. B. Barrass. http://www.rafweb.org/RAF_History.htm (accessed 19 October 2009).

Schlesinger, Robert J. 1961. *Principles of electronic warfare.* Englewood Cliffs: Prentice Hall, Inc.

Singer, P. W. 2009. *Wired for war: The robotics revolution and conflict in the 21st century*. New York: The Penguin Press.

Tamam Division. 2010. POP 300: Plug-in optronic payload, lightweight compact multi sensor stabilized electro-optical system. Israeli Aerospace Industries. http://www.iai.co.il/ sip_storage/FILES/5/33885.pdf (accessed 1 April 2010).

Thomas, Buford. 2006. *Unmanned aircraft systems (UAS) training.* Fort Rucker: US Army Aviation Warfighting Center.

Trimble, Stephen. 2008. US Navy unveils surprise order for ducted-fan UAVs. 28 January. http://www.flightglobal.com/articles/2008/01/25/221092/us-navy-unveils-surprise-order-for-ducted-fan-uavs.html (accessed 23 October 2009).

US Congress. Senate. Committee on Armed Services. 2009. *Hearing to receive testimony in review of the defense authorization request for Fiscal Year 2010 and the future years defense program*. 111th Cong, 1st sess. SR-325.

US Joint Forces Command. 1993. Joint Publication (JP) 3-55.1, *Joint tactics, techniques, and procedures for unmanned aerial vehicles.* Suffolk: Doctrine and Education Group.

———. 1995. Joint Publication (JP) 3-52, *Doctrine for Joint airspace control in the combat zone.* Suffolk: Doctrine and Education Group.

———. 2000. Joint Publication (JP) 3-51, *Joint doctrine for electronic warfare.* Suffolk: Doctrine and Education Group.

———. 2006. Joint Publication (JP) 5-0, *Joint operation planning.* Suffolk: Doctrine and Education Group.

———. 2007a. Joint Publication (JP) 3-13.1, *Electronic warfare*. Suffolk: Doctrine and Education Group.

———. 2007b. Joint Publication (JP) 3-50, *Personnel recovery.* Suffolk: Doctrine and Education Group.

———. 2008. Joint Publication (JP) 3-0, *Joint operations.* Suffolk: Doctrine and Education Group.

———. 2009a. Joint Publication (JP) 1-0, *Doctrine for the armed forces of the United States.* Suffolk: Doctrine and Education Group.

———. 2009b. Joint Publication (JP) 1-02, *Department of Defense dictionary of military and associated terms.* Suffolk: Doctrine and Education Group.

———. 2010. Joint Publication (JP) 3-30, *Command and control for Joint air operations.* Suffolk: Doctrine and Education Group.

Vakin, Sergei A., Lev N. Shustov, and Robert H. Dunwell. 2001. *Fundamentals of electronic warfare.* Norwood: Artech House, Inc.

Valavanis, Kimon P., ed. 2007. *Advances in unmanned aerial vehicles: State of the art and road to autonomy.* Dordrecht: Springer.

Washington Technology. 2009. DOD requests $5.4 billion for unmanned systems budget. http://washingtontechnology.com/Articles/2009/06/16/Unmanned-System-Spending.aspx?Page=1 (accessed 16 June 2009).

Weiringa, Jeffery A. 2010. Nonrecurring cost (NC) recoupment charge significant change-Shadow 200 (RQ-7B) unmanned aerial vehicle, DSCA policy memo 10-12. Defense Security Cooperation Agency. 16 February. http://www.dsca.mil/samm/policy_memos/2010/DSCA%2010-12.pdf (accessed 28 April 2010).

Weiss, Efrat. 2006. Hizbullah drone shot down over Israel. ynet news. 7 August. http://www.ynetnews.com/articles/0,7340,L-3287862,00.html (accessed 23 October 2009).

Wilson, Chet. 2010. Interviewed by author. Fort Leavenworth, Kansas. 1 February.

Wise, Jeff. 2007. Civilian UAVs: No pilot, no problem. *Popular Mechanics*. April. http://www.popularmechanics.com/science/space/4213464 (accessed 22 October 2009).

INITIAL DISTRIBUTION LIST

Combined Arms Research Library
U.S. Army Command and General Staff College
250 Gibbon Ave.
Fort Leavenworth, KS 66027-2314

Defense Technical Information Center/OCA
825 John J. Kingman Rd., Suite 944
Fort Belvoir, VA 22060-6218

Dr. Bill J. McCollum
Department of Command and Leadership
USACGSC
100 Stimson Avenue
Fort Leavenworth, KS 66027-2301

Kenneth J. Riggins
Department of Command and Leadership
USACGSC
100 Stimson Avenue
Fort Leavenworth, KS 66027-2301

Major Nicholas J. Martin
US Air Force Element
USACGSC
100 Stimson Avenue
Fort Leavenworth, KS 66027-2301