NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

FEASIBILITY OF INDIRECT FIRE FOR COUNTERING SWARMS OF SMALL UNMANNED AERIAL SYSTEMS

by

Matthew D. Parsons

June 2020

Thesis Advisor: Raymond R. Buettner Jr.
Co-Advisor: Edward L. Fisher

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2020	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE FEASIBILITY OF INDIRECT FIRE FOR COUNTERING SWARMS OF SMALL UNMANNED AERIAL SYSTEMS	**5. FUNDING NUMBERS**
6. AUTHOR(S) Matthew D. Parsons	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

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

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

Counter-Unmanned Aerial Systems (C-UAS) technology struggles to keep up with the evolving threat posed by drones. This threat is compounded by the advent of Small Unmanned Aerial Systems (SUAS) operating together to accomplish tasks as an autonomous entity known as a swarm. The miniaturization of these devices, coupled with rapid growth in their capabilities, presents a challenging problem that must be addressed.

This work explores the design of a counter-swarm indirect fire capability within the existing Marine Corps ground-based air defense and fire support framework. In doing so, this thesis presents a novel solution by defining the parameters of an artillery shell with effects designed to disrupt SUAS operations. Such a shell would target the electromagnetic spectrum vulnerabilities of Unmanned Aerial Vehicles (UAV) by utilizing expendable jammers delivered as a payload in a cargo-carrying projectile. This capability is likely to be effective against the swarm threat and can be used from the rear in support of units under SUAS attack anywhere within range of the artillery piece.

14. SUBJECT TERMS drone swarm, artillery, navigation warfare, Counter-Unmanned Aerial Systems, C-UAS, Small Unmanned Aerial Systems, SUAS, Unmanned Aerial Vehicles, UAV	**15. NUMBER OF PAGES** 123
	16. PRICE CODE

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

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

FEASIBILITY OF INDIRECT FIRE FOR COUNTERING SWARMS OF SMALL UNMANNED AERIAL SYSTEMS

Matthew D. Parsons
Major, United States Marine Corps
BS, U.S. Naval Academy, 2008

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION WARFARE SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
June 2020

Approved by: Raymond R. Buettner Jr.
Advisor

Edward L. Fisher
Co-Advisor

Thomas J. Housel
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Counter-Unmanned Aerial Systems (C-UAS) technology struggles to keep up with the evolving threat posed by drones. This threat is compounded by the advent of Small Unmanned Aerial Systems (SUAS) operating together to accomplish tasks as an autonomous entity known as a swarm. The miniaturization of these devices, coupled with rapid growth in their capabilities, presents a challenging problem that must be addressed.

This work explores the design of a counter-swarm indirect fire capability within the existing Marine Corps ground-based air defense and fire support framework. In doing so, this thesis presents a novel solution by defining the parameters of an artillery shell with effects designed to disrupt SUAS operations. Such a shell would target the electromagnetic spectrum vulnerabilities of Unmanned Aerial Vehicles (UAV) by utilizing expendable jammers delivered as a payload in a cargo-carrying projectile. This capability is likely to be effective against the swarm threat and can be used from the rear in support of units under SUAS attack anywhere within range of the artillery piece.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AAW	anti-air warfare
AGL	above ground level
AI	artificial intelligence
BW	bandwidth
BPSK	binary phase shift keying
C2	command and control
CIA	Central Intelligence Agency
CDMA	code division multiple access
C/A	course/acquisition
CPG	Commandant's Planning Guidance
COTS	commercial-off-the-shelf
C-UAS	Counter-Unmanned Aerial Systems
CW	continuous wave
dB	decibel
dBW	decibel-Watt
DEW	directed energy weapon
DiCER	Disruptive Cyber and Electronic Warfare Round
DOD	Department of Defense
DA	Department of the Army
DON	Department of the Navy
DPICM	dual-purpose improved conventional munition
DSSS	direct sequence spread spectrum
EA	electronic attack
EW	electronic warfare
EM	electromagnetic
EMP	electromagnetic pulse
ES	electronic warfare support
EP	electronic protection
FFT	fast Fourier transform

FHSS	frequency hopping spread spectrum
FPV	first person view
G-BAD	ground-based air defense
GPS	Global Positioning System
GNSS	Global Navigation Satellite System
GAO	Government Accountability Office
GCS	ground control station
HE	high explosive
HPM	high power microwave
HF	high frequency
IED	improvised explosive device
IR	infrared
ISM	industrial, scientific, and medical
ISR	intelligence, surveillance, reconnaissance
JAPCC	Joint Air Power Competency Center
JP	joint publication
J/S	jamming to signal ratio
MADIS	Marine Air Defense Integrated System
MCWP	Marine Corps warfighting publication
NGA	National Geospatial Intelligence Agency
NAVWAR	navigation warfare
OFDM	orthogonal frequency division multiplexing
PL	path loss
PRN	pseudorandom noise
PNT	position navigation and timing
REAP	radio emission attack projectile
RF	radio frequency
RPV	remotely piloted vehicle
SDR	software defined radio
SEAD	suppression of enemy air defense
SUAS	small unmanned aerial system
TFT	tabular firing table

TTPs	techniques, tactics, and procedures
UAV	unmanned aerial vehicle
UAS	Unmanned Aerial Systems
UHF	ultra-high frequency
USMC	United States Marine Corps
USRP	universal software radio peripheral
UON	urgent operational need
VHF	very high frequency
W	Watt
WLAN	wireless local area network

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This thesis is a culmination of a year's worth of research, phone calls, and conferences. Every interaction I had, or research paper read, was a stepping stone to the formation of this concept. I would like to personally thank those who had an impact on the completion of this thesis, but do so with the understanding that I may leave out someone worthy of recognition.

This work would not have been possible without the subject-matter experts and advisors who supported me throughout the process of writing this paper. First, I would like to thank Dr. Ray Buettner and Mr. Ed Fisher, who guided me through this process and provided for its inspiration. Internal to the Naval Postgraduate School, there were also a number of individuals who graciously gave their time to this project. I am grateful for Dr. Phillip Pace, James Calusdian, and Dr. David Jen of the Electrical Engineering Department for sharing their vast expertise on this subject and supplying me with the resources needed to complete the job. I am also deeply indebted to the Graduate Writing Center and especially Mr. Daniel Lehnherr for the many hours of help with the wording in each of the six chapters of this thesis. His genuine interest and excitement about the concept gave me the motivation I needed to become a better writer.

From the Marine Corps Detachment in Fort Sill, Oklahoma, Tim Harvey provided the artillery expertise that was crucial for conveying the fundamental principles of indirect fire delivery mechanisms. Tim, I regard your opinions with such esteem that it was only through your approval that I was convinced that this idea could work. Similarly, Wesley Wang of Picatinny Arsenal, NJ, provided a wealth of knowledge on past and current efforts in the development of electromagnetic spectrum denial weapons.

A thesis takes a significant amount of work and sacrifice to complete. My family understands this more than anyone else, so I would like to express my heartfelt gratitude to my wife, Claire, and daughters, Emilia and Adelaide. Their patience and support were critical for me to focus time and energy on this project.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Unmanned Aerial Vehicles (UAV), also known as drones, are part of the new normal for the 21st century. The ability to send an unmanned platform to accomplish tasks has been embraced by many different commercial sectors, as well as the military. UAVs as part of an Unmanned Aerial System (UAS) can be directed to perform missions as a more cost-effective and expendable asset than traditional manned platforms. Therefore, there has been a significant investment in this technology. This investment has led to a rapid increase in the capabilities of these devices, along with their proliferation. Today there are many types of these airborne platforms available for a growing number of applications.

The proliferation of drone technology presents a challenging problem for the Department of Defense (DOD) and law enforcement agencies. These low-cost and hard to target systems can be utilized as an asymmetric weapon to overwhelm conventional defense platforms and tactics. Not every UAV is a threat, but their ability to carry payloads, bypass physical security systems, and transmit data through communications links makes them an attractive asset for malicious actors. In response, Counter-Unmanned Aerial Systems (C-UAS) technologies have been extensively explored for the defense of airspace surrounding critical infrastructure and military bases. The evolution of drone technology and it's adaptation against specific mitigation measures make some of these methods obsolete. The threat is growing more serious as devices that operate with higher levels of autonomy become available. Similarly, there has been significant research and discussion regarding the use of a multitude of Small Unmanned Aerial Systems (SUAS) acting in unison. These potential "drone swarms" pose an even more severe problem since a number of simultaneous targets could quickly overwhelm defenses. Some have called this drone threat a "wicked" problem.

The Army's Training and Doctrine Command (TRADOC) Pamphlet 525-5-500 "Commander's Appreciation and Campaign Design" defines a "wicked" problem. Wicked in this sense does not relate to the problem's moralistic nature but rather it refers to the difficulty in developing a solution. Unlike structured problems that have standardized

methodologies for solving, wicked problems have no clear action to take. These types of problems are the most challenging to solve since they are complex, non-linear, and chaotic. People will disagree on the nature of the problem as well as the desired end state. Furthermore, there is no way to assume that all possible solutions have been identified since there is rarely only a single variable to consider. Research into the evolving capabilities of drones and related mitigation methods makes it clear that they have become a "wicked" problem.

Like the other services, the U.S. Marine Corps (USMC) does not have a C-UAS swarm solution that addresses the needs of supporting combat operations at the tactical level. The USMC is expeditionary in nature and, therefore, the ideal system must be lightweight, highly responsive, and maneuverable to keep pace with a fast-paced operational tempo. Furthermore, for maximum effect and ease of integration, any new C-UAS system should have an as little organizational impact as possible and be integrated into the existing fire support framework. By exploiting the reliance of these devices on the electromagnetic spectrum, techniques incorporating electronic warfare (EW) can be applied as part of an effective mitigation strategy. This thesis will outline the design requirements for an indirect fire capability that enhances tactical level C-UAS particularly against SUAS swarms.

A. DRONE WARFARE AND THE NEW NORMAL

The adaption of swarming SUASs into the arsenals of our enemies undoubtedly initiated a new dimension of warfare that has the potential to change our battlefield tactics. These tactics will be augmented with innovative solutions to address this threat. This thesis will attempt to look to the future and analyze the capabilities and vulnerabilities of SUAS swarms. In doing so, it will propose an indirect fire countermeasure like the one in the below scenario, so that we are better prepared to face this new normal.

In the not so distant future, a USMC patrol is alerted to the presence of a massive swarm of unmanned aerial vehicles inbound to their position from a distance of 20 kilometers (km). The swarm acts as a singular entity, but individual drones are equipped with intelligence-gathering sensors to seek out valuable targets and engage them with their

small incendiary device payloads. The swarm navigates to the target using positioning data provided by the Global Positioning System (GPS) and feeds information back to its operator via a wireless local area network (WLAN) connection. Outside the range of the patrol's vehicle-mounted directed energy weapon (DEW), as well as that of their handheld jamming devices, the unit calls in a fire mission to its supporting artillery battery. The artillery forward observer keys the handset on his radio:

"Blacksheep, this is Highlander immediate jam, grid 123 456."

There is suddenly a rush of activity in the battery fire direction center (FDC) as the transmission is received and relayed to the gunline. Knowing from the latest intelligence brief that the enemy had a UAS swarming capability, the Battery Commander had ordered each of his 155-millimeter (mm) M777A2 howitzer teams to ready a stockpile of Radio Emission Attack Projectiles (REAPs) for just this occasion. The FDC passes optimal aiming point data along with fuze setting times to each of the guns which are computed by the Advanced Field Artillery Tactical Data System (AFATDS). Each gun fires "when ready."

Less than a minute later the artillery projectile arrives on target and ejects an innocuous-looking payload suspended from a parachute seven hundred meters above the swarm. The swarm immediately loses its navigation control capability and the connection with its controller is lost as the jamming signal transmitted by the payload overpowers the communications frequencies of the drones. Without the ability to self-navigate to their pre-determined waypoint, the drones fall harmlessly to the ground, short of their objective.

B. BACKGROUND AND NEED

There is no single C-UAS solution that adequately addresses the needs of ground combat operations. The future threat from the proliferation of drones on the battlefield, coupled with swarming tactics, cannot be solved with current weapons. Swarm technology is still in its infancy, but it is inevitable that swarming tactics will be embraced as an asymmetric force multiplier by our adversaries. Current counter-drone technology systems are not adequately robust or cost-effective to mitigate the threat posed by a future swarm of drones, and these systems will quickly become obsolete in defending against these kinds

of attacks. These current mitigation strategies lack the flexibility to support highly maneuverable and expeditionary forces in a fluid environment against a dispersed airborne threat. This presents a capability gap that must be filled to defend against SUAS swarms.

The 39th USMC Commandant's Planning Guidance (CPG) acknowledges the capabilities of SUAS swarms and their potential to radically change the nature of warfare (Berger, 2019). When thinking of autonomous vehicles and their potential applications, it is imperative that we study not only their benefits but also the threat that they pose to our forces.

The purpose of this thesis is to investigate the applicability of a specific NAVWAR based Electronic Warfare (EW) technique as a potential solution to the "wicked" drone problem. In doing so, the requirements for a C-UAS artillery shell will be defined. This research advocates the future development of a responsive and low-cost swarm denial weapon system that can be integrated with the current battlefield effects provided by the field artillery.

The benefits of developing a C-UAS artillery payload would not only aid ground units in contact but would also have applications for shipboard and military aircraft implementation. Additionally, the impacts of this research would have benefits outside of the defense establishment to include civilian law enforcement and aviation authorities.

C. PROBLEM STATEMENT

C-UAS technology struggles to keep up with the pace of the evolving threat posed by malicious actors utilizing drones. This threat is increased by the advent of SUASs operating in swarm configurations that have the ability to work together to accomplish specific tasks. The miniaturization of these devices, coupled with rapid growth in their capabilities, presents a "wicked" problem. This problem must be addressed to counter the threat posed to ground combat troops.

D. RESEARCH QUESTIONS

This research will examine the feasibility of using existing artillery pieces as a C-UAS system to support ground combat operations. It will focus on defining the requirements of an artillery shell designed to disrupt SUAS operations. To achieve this result, the research question that will be explored is: What are the design requirements for a C-UAS artillery payload that can counter swarming SUAS?

E. KEY CONCEPTS

1. Unmanned System Terminology

Many different organizations have varying definitions of the terms relating to the operations of unpiloted aircraft. According to the 2010 *Strategic Concept of Employment for Unmanned Aircraft Systems in NATO* report by the Joint Air Power Competency Center (JAPCC), an Unmanned Aircraft (UA) is "an aircraft that does not carry a human operator and is capable of flight under remote control or autonomous programming" (p. 3). According to USMC Warfighting Publication (MCWP) 3–20.5, *Unmanned Aircraft Systems Operations*, the same term defines a "rotary wing, fixed wing or lighter than air vehicle capable of flight without an on-board crew" (USMC, 2018a, p. 1–3). The USMC then refers back to Joint Publication (JP) 3–52 *Joint Airspace Control* to define the term UAS as "the system, whose components comprise the necessary equipment, network, and personnel to control an unmanned aircraft." As illustrated in Figure 1, these elements are the physical flying platform, the command and control architecture that it utilizes, and any payload it may carry.

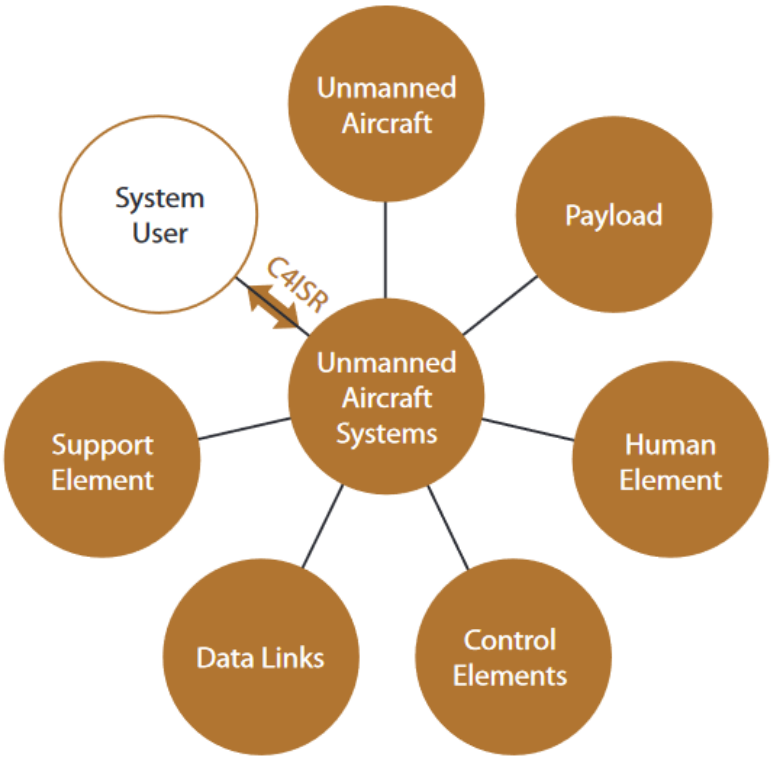


Figure 1. Components of a UAS. Source: Joint Air Power Competence Center (2011).

In many research papers and studies, the term drone is used synonymously with other terms such as unmanned vehicle (UV), unmanned aerial vehicle (UAV) or remotely piloted vehicle (RPV) to describe any autonomous or remotely controlled aircraft that is part of this overarching system (Gilliland, 2019; Valavanis & Vachtsevanos, 2015). For this paper, the different terms and definitions generally relate to the same concept, and therefore a standardized terminology can be established. The terms UAV and drone will be used interchangeably to describe the physical flying mechanism while UAS will refer to the overarching network of system elements that enable flight. Furthermore, the term SUAS will be used to emphasize the physical size of the UAV that is part of this system. Generally, a drone is considered part of a SUAS if it weighs under 55 pounds (Department of Homeland Security [DHS], 2019) . Specifications on types of UAVs, as well as their capabilities and countermeasures, are described in Chapter I.

2. Artillery

Throughout history, artillery is the term used to describe a multitude of direct and indirect firing weapons with a wide range of calibers delivering a variety of munitions (Bailey, 2004). In general, the term artillery refers to a large caliber weapon system that is used to launch a projectile beyond the range of smaller munitions. This system includes the weapon itself as well as the ammunition, support equipment, and personnel needed to operate it (Kinard, 2007). A howitzer is a specific type of artillery piece with a relatively short barrel that utilizes separate loading propellant increments to fire a projectile with either a low or high trajectory (Bailey, 2004). Figure 2 depicts the M777A2 155-millimeter lightweight towed howitzer utilized by the U.S. Army and USMC. For the purposes of this thesis, the M777A2 will be the primary delivery system for the projectile with a C-UAS submunition. However, this concept could also be applied to create projectiles of a variety of calibers to fit a number of different weapons platforms. The utility of artillery as a delivery mechanism for a C-UAS weapon is described in Chapter III.

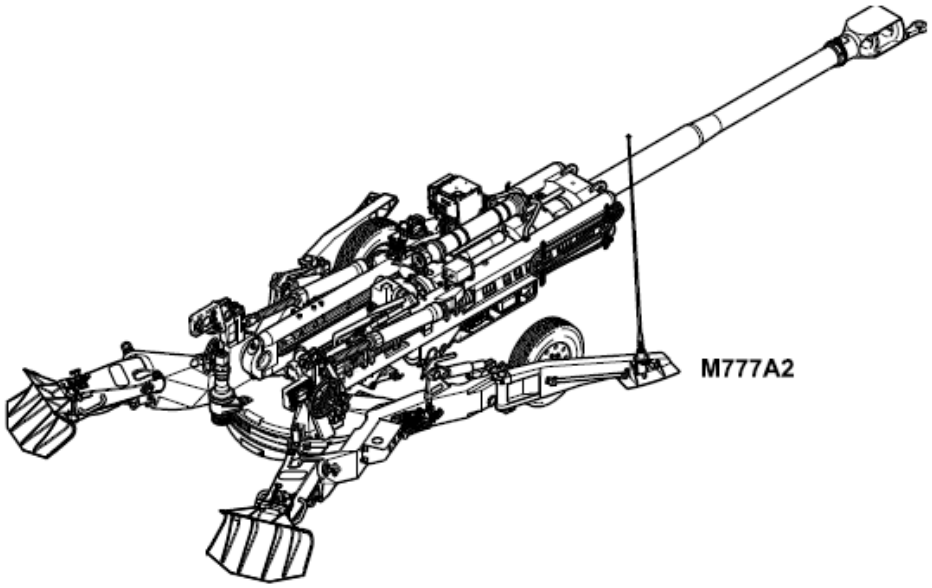


Figure 2. M777A2 155 mm towed howitzer. Source: Department of the Army [DA] (2014).

3. Electronic Warfare

Electronic Warfare (EW) is a discipline that involves "the art and science of preserving the use of the electromagnetic spectrum for friendly use while denying its use by the enemy" (Adamy, 2000). This concept includes the offensive and defensive measures taken to gain and maintain spectrum dominance along with the supporting actions taken to enable friendly activities in this domain. EW is conducted in order to produce an effect which is a change to a condition, behavior, or degree of freedom (Joint Chiefs of Staff [JCS], 2010). Doctrinally, EW is divided into three subdivisions, and each relates to one of these missions. These subdivisions are Electronic Attack (EA), Electronic Warfare Support (ES), and Electronic Protection (EP) (Payne, 2006). Figure 3 is a depiction of how these concepts are interrelated.

a. Electronic Protection

EP represents the defense of the EM spectrum and is the division of EW that involves passive and active means taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize or destroy friendly combat capabilities (JCS, 2012). With regards to UAV operations, EP involves the technologies and techniques used to minimize the effects of intentional or unintentional electromagnetic interference.

b. Electronic Warfare Support:

Electronic warfare support (ES) is defined as the "subdivision of EW that entails the actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated EM energy for the purposes of immediate threat recognition, targeting, planning and conduct of future operations" (JCS, 2012 p. viii). An example of ES would be the interception of radio transmissions to determine their characteristics and location for use in a future attack.

c. Electronic Attack:

EA represents the offensive side of EW, and its effects can either be destructive or non-destructive. Non-destructive actions include electromagnetic suppression or deception, while examples of destructive EA include anti-radiation missiles, jamming or directed energy weapons. EA consists of both offensive and defensive activities to include countermeasures (JCS, 2012). According to the JCS, EA is considered a form of fires.

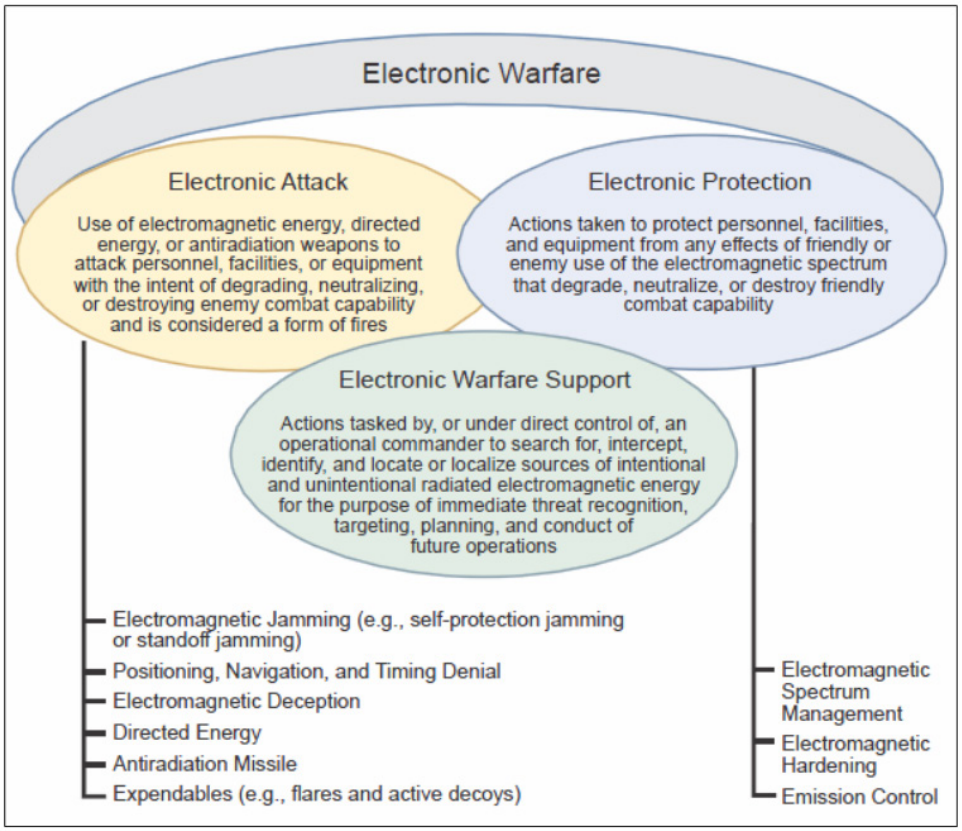


Figure 3. Electronic warfare components. Source: Department of Defense [DOD] (2012).

4. Navigation Warfare

Joint Publication 3-14 "Space Operations" defines navigation warfare (NAVWAR) as "deliberate offensive and defensive actions to assure friendly use and prevent adversary use of PNT (Position, Navigation, and Timing) information through coordinated

employment of space, cyberspace, and electronic warfare capabilities" (JCS, 2018, p. II-3). Since accurate PNT data is a critical component for SUASs operations, the application of NAVWAR via EW techniques against the signals that deliver this information can be an effective strategy for their mitigation. This concept is explored in Chapter IV one potential method of engagement for a C-UAS artillery shell.

F. LIMITATIONS

It is important to note that there is no panacea that will stop all drones. UAS technology is evolving at a rate that makes it challenging to predict all the countermeasures that will be needed to disrupt them. This thesis research attempts to describe a method that has the potential to work against UAVs that rely on GPS signals for navigation and positioning. This vulnerability was chosen since most current drones utilize these satellite signals, and they are critical for swarms operating in autonomous modes. The resulting requirements will inform one aspect of the required system of systems.

G. THESIS OUTLINE

This thesis is organized as follows. Chapter II is an introduction to UAS as well as their command and control methods. The principles of C-UAS techniques are presented along with shortfalls in current mitigation measures. In Chapter III, the concept of an artillery delivered C-UAS weapon is introduced as a means to augment the USMC integrated air defense strategy. Chapter IV outlines the NAVWAR concept as it applies to C-UAS technology. A case study on the capture of an American drone is introduced as a means to show the vulnerability of UAS to NAVWAR techniques. Experiments and studies that have demonstrated the effectiveness of GPS jamming and spoofing on UASs are described along with the utility of software-defined radios (SDRs) for signal generation. Chapter V describes the development of the concept for an artillery-delivered EW device. A simulation is then presented that demonstrates the effective engagement area of such a weapon. Conclusions are presented in Chapter VI, along with tactical employment considerations and recommendations for future study.

II. UNMANNED AERIAL SYSTEMS AND COUNTERMEASURES

Chapter II outlines the background research that was done to develop the reasoning and feasibility for an indirect fire C-UAS weapon. This is accomplished by describing the different types of UAVs and the concepts that relate to their command and control. The application of SUAS swarms as a weapon is presented and existing C-UAS techniques are described, as well as their current shortfalls.

A. INTRODUCTION TO UAVS

UAVs are not a modern invention. As long as pilots have put themselves in harm's way, there have been efforts to develop platforms to carry out their missions to mitigate risk and reduce cost. The earliest use of drones was documented during World War I. (Palik and Nagy, 2019). Known initially as RPVs or Remotely Piloted Vehicles, the technology of these early drones allowed for only primitive capabilities, so they saw limited operational use. This began to change in the early 1990s when UASs such as the Pioneer were adopted as intelligence collection and surveillance assets (Department of the Navy [DON], 2016). From there, military-grade UASs have grown into the highly capable, multipurpose machines we have today.

The rise of military systems foreshadowed the interest and investment in civilian UASs. The proliferation of UASs we see now is fueled by the rapid increase in their functionality, coupled with a reduced cost and miniaturization. This has allowed them to be adopted to a wide variety of military and civilian applications. The global market for drones is estimated to exceed $48.9 billion by the year 2023 (Hindle, 2018). This market is dominated by military spending; however, the demand for hobby and commercial drones is steadily increasing. Today, there are more than 100 different drone manufacturing companies with many different models for consumers to buy. These devices have quickly become part of our everyday lives as prices drop and their growing capabilities give rise to a number of applications.

B. UAS CHARACTERISTICS

There are many different types of UASs. It is first necessary to describe them in broad categories to capture the breadth of their variance. The simplest distinction is either military or civilian application. Military systems include those systems developed for specific operational tasks such as intelligence collection, targeting, or surveillance. Civilian UASs are those that are available for the commercial sector or hobbyists and are generally referred to as COTS (commercial-off-the-shelf) technology by government agencies. These types of UASs are becoming more ubiquitous in our lives as hobby interest in drones grow and they are applied to a variety of fields such as mapping, agriculture, and disaster recovery. The main difference between military and civilian UASs today is cost. Military systems are significantly more expensive than their civilian counterparts yet they are more likely to have more sophisticated technology and incorporate more ruggedized parts for durability.

UAVs are generally classified as being a fixed-wing or rotocopter design (DHS, 2019). This attribute defines the flight characteristics of the UAV and carries with it the inherent capabilities and vulnerabilities related to rotary versus fixed-wing aircraft. Most military systems utilize a fixed wing design which gives them an increased payload capacity and longer flight endurance. The most popular types of commercially available UAVs have a rotocopter configuration that gives them vertical take-off and target hovering capabilities. Some types of UAVs incorporate both of these physical attributes into a single platform, but this is less common. Figure 4 is an image of a fixed wing versus a rotocopter design.

Figure 4. Fixed-wing and rotocopter design UAV. Source: DHS (2019).

Apart from their external design or application, there are several other ways that UASs can be classified. UASs differ in regards to their size, speed, endurance, max altitude, and payload capacity. The DOD uses a number of these attributes as a basis for defining five major groups of UASs. These groups are presented in Table 1 and are from the 2011 Department of Defense *Unmanned Aircraft Systems Airspace Integration Plan*.

Table 1. DOD UAS classification: Source: DOD (2011).

<table>
<tr><th>UAS Groups</th><th>Maximum Weight (lbs) (MGTOW)</th><th>Normal Operating Altitude (ft)</th><th>Speed (kts)</th><th colspan="2">Representative UAS</th></tr>
<tr><td>Group 1</td><td>0 – 20</td><td><1200 AGL</td><td>100</td><td>Raven (RQ-11),
WASP</td><td>  </td></tr>
<tr><td>Group 2</td><td>21 – 55</td><td><3500 AGL</td><td rowspan="2">< 250</td><td>ScanEagle</td><td>  </td></tr>
<tr><td>Group 3</td><td>< 1320</td><td rowspan="2">< FL 180</td><td>Shadow (RQ-7B),
Tier II / STUAS</td><td>  </td></tr>
<tr><td>Group 4</td><td rowspan="2">>1320</td><td rowspan="2">Any Airspeed</td><td>Fire Scout (MQ-8B, RQ-8B),
Predator (MQ-1A/B),
Sky Warrior ERMP (MQ-1C)</td><td>  </td></tr>
<tr><td>Group 5</td><td>> FL 180</td><td>Reaper (MQ-9A),
Global Hawk (RQ-4),
BAMS (RQ-4N)</td><td>  </td></tr>
</table>

The miniaturization of drone technology in recent years has created the need for further classification of Group 1 UASs to include the mini, micro, and nano designations. These UASs are distinguished by a smaller size as well as a more limited speed, endurance, and payload capacity. The majority of COTS UASs fall into one of these group 1

subcategories and are collectively referred to as small unmanned aerial systems SUASs (Rhode and Shwarz, 2015). These types of UASs are rapidly becoming the most prolific in the airspace.

Table 2. SUAS classifications. Source: Rhode and Shwarz (2015).

Drone type	Payload (g)	Speed (km/h)	Endurance (min)	Altitude (m)	Operating Radius (km)
Mini	600 - 3000	30 - 100	15 - 90	2000 - 3000	< 15
Micro	50 - 600	< 50	< 30	< 600	< 2
Nano	< 50	< 20	< 10	< 300	< 0.1

C. UAS COMMAND AND CONTROL

Generally, UASs are dependent on wireless communications. These communications consist of the data links that provide the information necessary for the UAV to carry out specific tasks. These data links are required for functions such as navigation, the transfer of telemetry data, and video or imagery transfer. The challenge for the design of a UAS with respect to these data links is how to optimize the desired signal

strength while protecting it from intentional or unintentional interference. It is essential to understand the fundamental principles of Radio Frequency (RF) communications and how it relates to these data links in order to learn how EW can be applied against a SUAS. With this groundwork laid, a strategy for the development of an artillery delivered C-UAS weapon is developed in Chapter III.

1. UAS Communication

Communication methods for UASs is dependent on the electromagnetic spectrum. Light visible to the naked eye is only a small portion of the entire range of frequencies that make up this spectrum. The frequencies in each of these bands have different characteristics that make them suitable for various applications such as TV, radio, or X-rays. UAS communication is reliant on these frequencies as carriers to transmit the information necessary to carry out tasks. These signals are transmitted in the radio wave portion of the spectrum with frequencies in the MHz to GHz range. Figure 5 is a depiction of the electromagnetic spectrum.

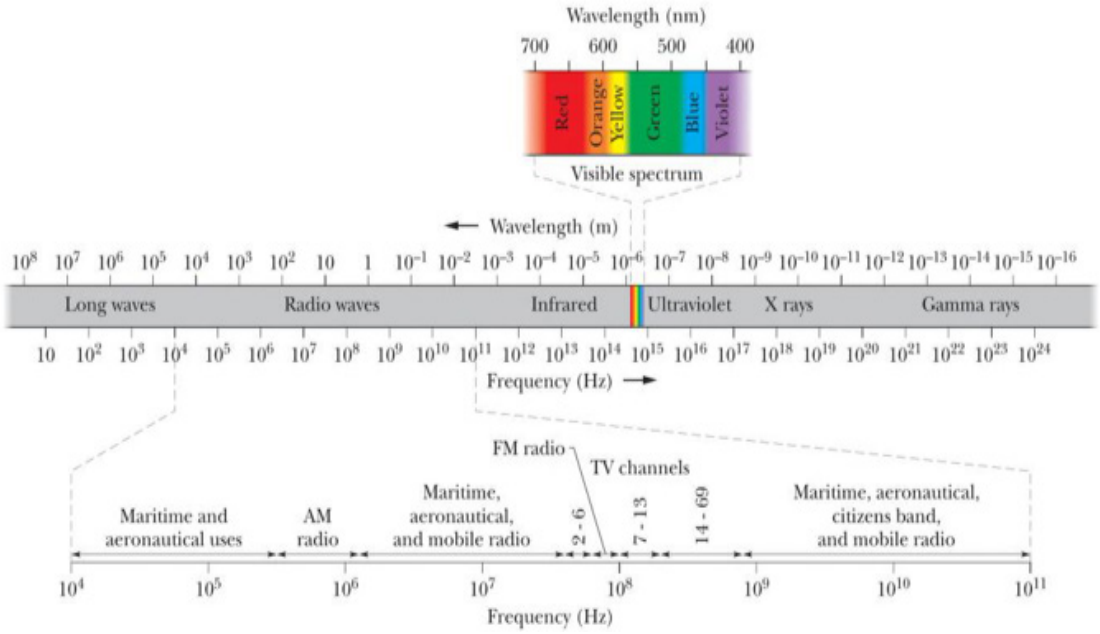


Figure 5. The electromagnetic spectrum. Source: Halliday, Walker, and Resnick (2014, p. 973).

The spectrum requirements for UAS operation depend on the desired data links and flight characteristics of the UAV's design. The ability of a device to successfully transmit and receive a specific type of signal is determined by the operating frequency, bandwidth, antenna characteristics, and modulation scheme (Rochus, 1999). These characteristics are outlined below as they relate to UAS operations.

a. Frequency

Frequency is the number of occurrences of something over a set time period. With regard to radio wave propagation, this term refers to the number of repetitions a sinusoidal wave makes in one second and measured with the unit of (Hz). The wavelength of a given frequency is defined as the distance that a given point will travel on a wave during one cycle (Stanley & Jeffords, 2006). Electromagnetic waves travel at the speed of light, which is approximately 3×10^8 meters per second. The wavelength, λ, is derived by dividing the speed of light, c, by the frequency, f, as seen in the below equation.

$$\lambda = \frac{c}{f}$$

Lower frequencies with longer wavelengths can propagate farther yet have a reduced capacity to carry information. Higher wavelengths can transfer data at higher rates but do so with a reduced range, often requiring a line of sight for data transfer. Commercial UAVs often incorporate several different frequencies to optimize command and control data links for maximum range and data transfer. The most common frequencies used in modern COTS UAVs for remote control are in the industrial, scientific, and medical (ISM) bands of 2.4 or 5.8 GHz; however, lower frequencies at UHF (433 MHz) or HF (27, 25 or 72 MHz) are sometimes used. The 2.4 and 5.8 GHz bands have the limitation of requiring a line of sight for data transfer but have a higher capacity of information they can transmit.

b. Spectrum Bandwidth

Bandwidth refers to the range of frequencies that are utilized for transmitting a signal. It is a finite resource that determines the rate of data transfer for a given time segment (Rochus, 1999). Microwave data links in UAVs have the capacity for large

bandwidths that allow the transfer of video. Lower frequency data links in the HF range have a smaller bandwidth and are generally not used for video or imagery.

c. Antennas

An antenna is a spatial amplifier that concentrates RF energy to transmit and receive communication messages (Stutzman & Thiele, 2014). Four parameters describe antennas with regards to SUAS operations and the scope of this research. These are the directivity, radiation pattern, polarization, and bandwidth. These parameters determine the characteristics of the physical size, type, and ability of an antenna to focus RF energy.

(1) Directivity

Directivity, D, is the measure of an antenna's ability to focus RF energy in a particular direction. This value is a ratio of the power transmitted in a specific direction to the power transmitted by an isotropic antenna that transmits uniformly. The amount of RF energy received at a location is referred to as the power density, S. A very directive antenna has a narrow beam and high power density versus a less directive one with a wide beam. Antenna radiation patterns are also commonly described by the term gain, G. Gain is a ratio of the power actually transmitted in a direction defined by azimuth and elevation angle (θ, ϕ) to a hypothetical situation where all the energy was radiated isotropically. Gain is computed from directivity, D, by multiplying it by the radiation efficiency of the antenna , e_r, as seen in the equation $G = e_r D$.

The combination of the antenna's gain and the transmitter's power is referred to as the effective radiated power (ERP). The relative power levels and gains associated with the transmission of RF energy is typically expressed in decibels. Decibels are a way to compare a value to a logarithmic scale to give a relative intensity level. Multiplication and division of decibel values are converted to addition and subtraction, respectively, because the scale is logarithmic. Therefore, in this form, the ERP of the transmitter is calculated by simply adding the antenna gain to the transmitter output power.

(2) Radiation Pattern

An antenna's radiation pattern, $F(\theta,\phi)$, is a representation of the variation of the level of RF energy emitted at an angle around a transmitter (Stutzman and Thiel, 2013). Typically, a radiation pattern is comprised of the main beam along with any number of side lobes. The ability of a UAV antenna to receive a communications signal is dependent on its location within this pattern and the relative power level associated with the angle it occupies. UAV antennas are typically oriented so that they receive a communication signal with a maximum transmitted power within this radiation pattern. Figure 6 is a depiction of an antenna transmitting a signal to a UAV receiver. The dotted line represents an isotropic antenna that radiates its energy uniformly in all directions. The solid line represents a real antenna radiation pattern consisting of the main lobe and several smaller side lobes. To receive the maximum signal power level, the UAV in the image is positioned within the main lobe of the antenna.

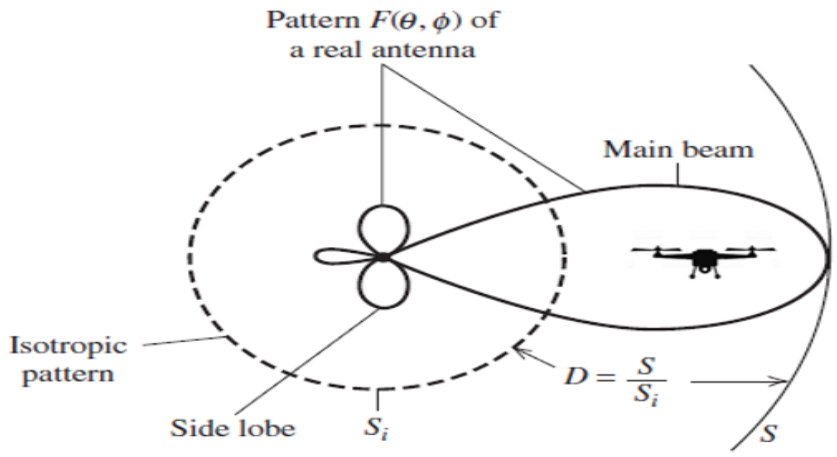


Figure 6. Antenna radiation pattern $F(\theta,\phi)$. Adapted from Stutzman and Thiele (2013).

(3) Polarization

Polarization refers to the vector field representation of the electric fields radiated by the antenna (Stutzman & Thiele, 2013). Antennas can emit linear, circular, or elliptical

polarization. A wave from a transmitter antenna is matched to the receiving antenna when they have identical polarization states. The polarization efficiency, p , is a value between 0 and 1 that describes the level of similarity between the polarized state of the transmitter and receiver. A cross-polarized state ($p = 0$) exists when there is a complete match between the two antennas (Stutzman & Thiele, 2013). In communications systems like the ones used in UAVs, a matched pair of polarization is optimal to reduce the excess power requirements needed to overcome antenna misalignment.

(4) Antenna Bandwidth

An antenna's bandwidth describes the span of operating frequencies that it can transmit and receive. It is defined as BW = $(f_u - f_L)/2$ where f_u and f_L represent the upper and lower frequencies, respectively. Antennas with a large BW are referred to as broadband or wideband antennas. Ones with a small BW are known as narrowband.

SUASs generally have several antennas for different control links. Because of their dimensions, SUASs are limited in the antennas that they can use and generally utilize low-cost omnidirectional antennas. These antennas have varying degrees of gain and polarization, depending on their specific application. When transmitting information at higher frequencies, these devices require more focused RF beams with a higher gain in order to receive the transmitter's signal. Lower gain antennas are typically used for satellite transmissions in order for the SUAS receiver to have a full view of the sky.

d. Spreading Mode/Modulation Scheme

UAV systems incorporate communication techniques to reduce interference and protect the integrity of the transmitted signal. The most common spreading modes used in these devices are frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS) (Rohde and Schwarz, 2015). In FHSS systems, the carrier frequency of the signal is pseudo-randomly changed at a designated hopping rate. A shared code between the transmitter and receiver allows for the message to be transferred and interpreted. In DSSS systems, the signal is spread over the entire bandwidth and only decoded by a shared P-code. Downlink modes of data video transfer include standard Wi-

Fi over a wireless local area network (WLAN) or Bluetooth. Data can be modulated through a variety of schemes to include frequency shift, phase shift keying, or orthogonal frequency division multiplexing (OFDM).

2. UAS Control Modes

The technical characteristics of the modes of control links for a UAS can be divided into three broad categories that relate to the operator's level of interaction with the device. These are signal control, first-person view (FPV), and autonomous. Signal control refers to the use of the radio data link from a ground station to the device that allows the controller to direct the UAV to perform functions such as navigation and payload deployment. In this type of control the controller has limited visibility on the UAV unless it is within line of sight. A UAV data link using FPV allows the controller to manipulate the drone via video piloting. This allows for the controller to direct the UAV's actions without line of sight limitations. Autonomous UAVs can be preprogrammed with instructions to carry out tasks without the input from a controller. Instructions for the UAV are programmed into the system prior to launch allowing for it to accomplish its mission without human intervention.

There are various levels of autonomous control for a drone that range from no autonomy to full autonomy. The highest level of this kind of command and control structure is a UAS with the ability to perform all tasks without the aid of an operator. Current drone swarm command and control architectures have not displayed this high level of autonomy. In most cases, each individual drone is controlled by a single ground station computer. This is known as infrastructure-based architecture (Campion et al., 2019). These computers transmit and receive telemetry data from the swarm components in order to send navigation signals and tasking commands. Figure 7 depicts an infrastructure based SUAS swarm. In this configuration, each UAV communicates directly with a ground station controller.

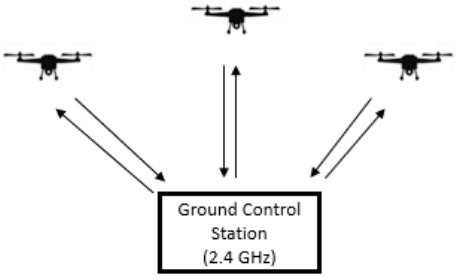


Figure 7. Infrastructure based UAS swarm architecture. Adapted from Campion et al. (2019).

Higher levels of swarm autonomy would allow for the swarm itself to make decisions by interpreting data through onboard computers. This would require an established communications channel between every SUAV within a swarm to transfer data without human intervention, such as using an ad hoc wireless network-based architecture, or other conduits for sharing information. Higher levels of autonomy allow a SUAS to have an extended range since they are no longer limited by the remote-control frequency; however, they are more reliant on satellite communications for accurate positioning data. Figure 8 illustrates an example of a networked swarm architecture. In this configuration, the ground station communicates directly with one SUAS "mothership" that relays information to the other SUAVs in the swarm.

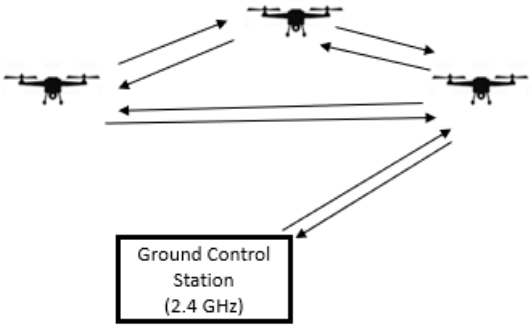


Figure 8. Networked swarm architecture. Adapted from Campion et al. (2019).

D. UAS NAVIGATION AND POSITIONING

In the modern world, accurate navigation data are taken for granted. This capability has become an integral part of our society. It is relied upon for everything from precision-guided munitions to turn-by-turn directions to the nearest supermarket on our mobile devices. The use of satellite navigation is also critical for a UAS or swarms of SUASs operating in an autonomous mode without augmentation by an inertial navigation system.

1. Global Navigation Satellite System

Navigation data is provided through constellations of satellites collectively known as the Global Navigation Satellite System (GNSS). The most used of these systems are the Global Positioning System (GPS) developed by the United States military and GLONASS by Russia. Europe and China have more recently launched their own satellite networks known as Galileo and Beidou, respectively. This thesis focuses on GPS since a majority of existing COTS SUASs utilize this system as the primary means of navigation. The first GPS satellite was launched in 1974, and currently, there are 31 GPS satellites in low Earth orbit. This system is managed by the U.S. Air Force and the National Geospatial-Intelligence Agency (NGA). Ground stations on Earth are used to monitor these systems and adjust the satellite's internal clocks to establish their position in orbit accurately.

GPS receivers rely on the signal from at least three satellites to determine a location. This is done through the use of trilateration. Trilateration is the process of mathematically determining the position of an object on the surface of the earth using the calculated distances from fixed control points. By measuring one distance from one satellite and comparing it with the distance to that of other satellites, an intersection point that represents the UAVs location can be established. Figure 9 shows this concept relating to UAS operations. In this image, the distance from each satellite that the UAV receiver measures is the radius of each of the circles.

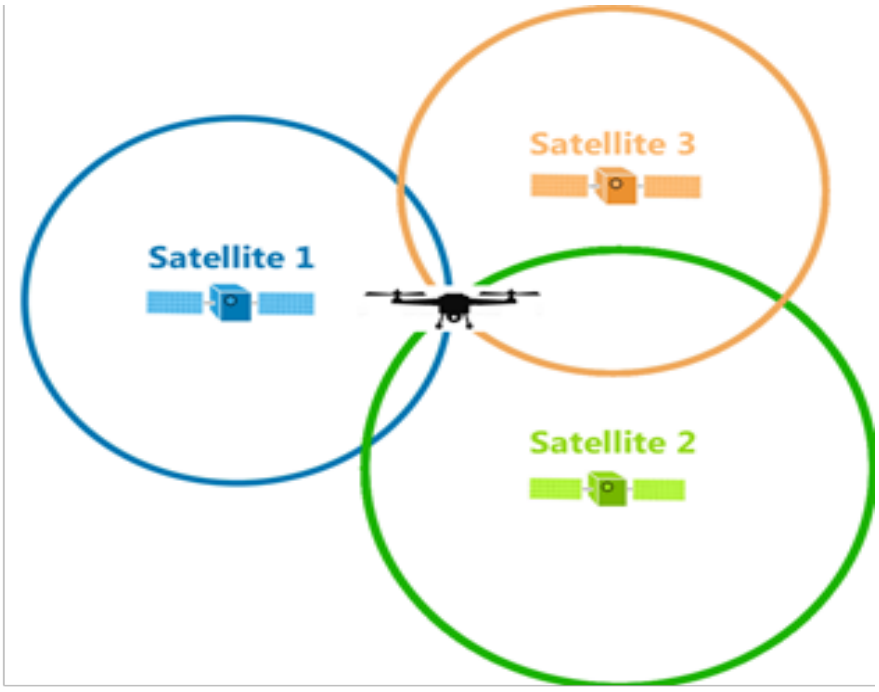


Figure 9. GPS trilateration. Adapted from GISGeography.com (2016).

With GPS, the location is determined by measuring the time it takes for an electromagnetic signal to be sent and received by a satellite from a known position. This distance, d, is calculated by multiplying the speed of the propagating signal, c, with the time required for the signal to be transmitted, t. Mathematically, this is illustrated by the equation below (Wang et al., 2015).

$$\sqrt{(x-x_1)^2+(y-y_1)^2+(z-z_1)^2}=ct_1$$

In this equation, x, y, and z represent the position on the earth while the subscripted characters represent the known coordinates of a specific satellite. The speed of light is measured in meters/second and t is the signal propagation time in seconds. When integrating n satellites, this equation can then be solved simultaneously for each of the satellites to determine the UAV's position (Hermans and Gommans, 2018). The below equation demonstrates this concept.

$$\sqrt{(x-x_n)^2+(y-y_n)^2+(z-z_n)^2}=ct_c$$

2. GPS Signal Frequencies

Several types of signals and codes are used over the EM spectrum to allow for accurate navigation. Satellites generate two GPS signals which are propagated via carrier waves at separate L-Band frequencies. The L_1 carrier signal is at 1575.42 MHz and L_2 at 1227.6 MHz. The L_1 band is primarily used by the civilian sector for navigation, and the majority of UASs rely on these signals.

The GPS signal is modulated using binary phase-shift keying (BPSK) to generate two pseudo-random noise codes (PRN) that are unique to each satellite. These codes are the basis for accurate positioning (Herring, 2012). The C/A code is used for civilian access and the P-code is for precision. The C/A code is shorter, used for civilian applications, and is intended for faster satellite acquisition. This PRN code has a length of 1,023 chips or time increments before it repeats and is repeated every millisecond resulting in a frequency of 1.023 MHz. The P-code is a 37 week long set of binary data generated at 10.23 MHz. Each satellite is assigned a specific portion of this code to repeat every seven days. All ground GPS receivers have a stored database of the PRN codes for each satellite, which is then used to match signals to specific satellites and establish the receiver's position by trilateration. Military systems utilize an encrypted P-code known as the Y-code. This makes the navigation message more secure from spoofing or unauthorized access.

GPS signals overcome interference by using two techniques. Code division multiple access (CDMA) is the process that allows multiple satellites to transmit at the same frequency without interference. Additionally, GPS communications systems utilize the DSSS modulation scheme that distributes the message over a wide bandwidth. Using this technique, only a small portion of the navigation message can be corrupted by narrowband interference. This is known as the processing gain of the system.

3. GPS Navigation Message

The navigation message is sent on the carrier wave which is transmitted from the satellite at a rate of 50 bits/second or 50 baud. This message is comprised of 25 frames, each consisting of 5 subframes that contain ten words composed of 30 bits each. Within this message is contained the satellite's position data, known as the ephemeris, and an

additional almanac of the data for all other GPS satellites. Including the almanac allows the receiver to focus its satellite search on only those that would be visible at the time. Additionally, it provides correction data for atmospheric delays and correction data for clock offset.

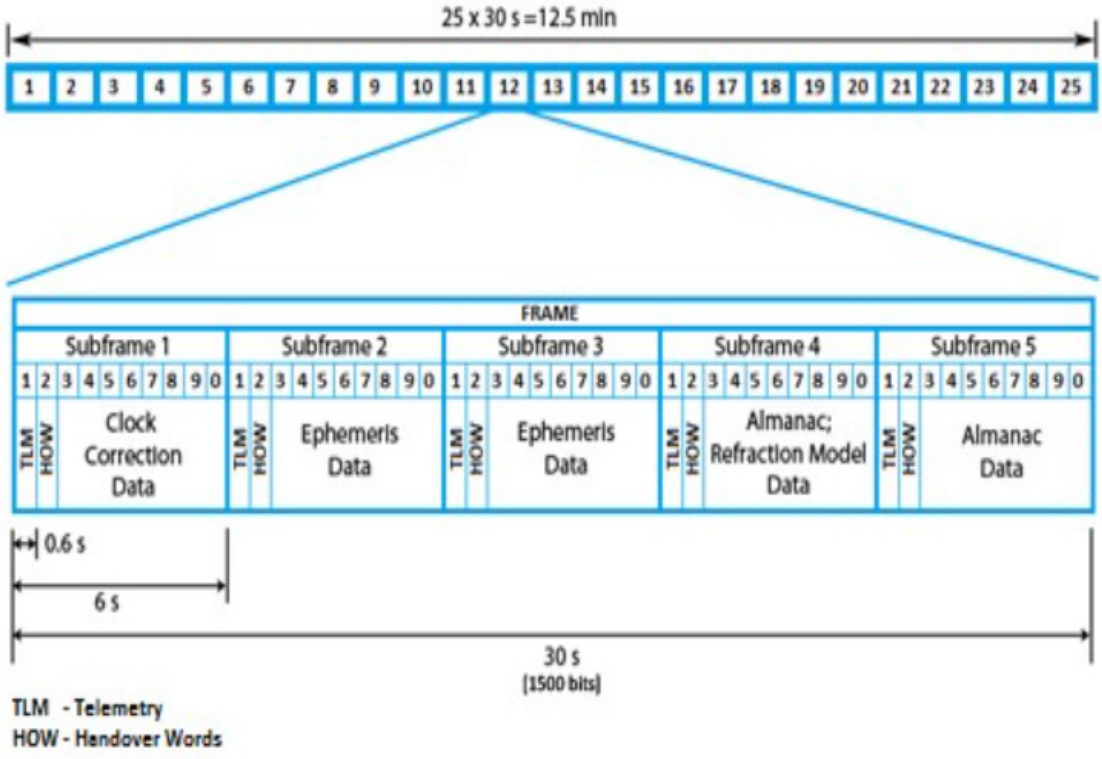


Figure 10. Structure of the GPS navigation message frame. Source: National Instruments (2019).

4. UAV Signal Propagation

The Friis equation is used to describe the propagation of RF energy through free space (Friis, 1946). The power of a signal received can be calculated by an adaptation of the Friis equation known as the one-way radar equation. The formula depicted below gives received power, P_r, in relation to the power of the transmitter, P_t, and the associated gains of the transmitter and receiver along with the wavelength of the propagating frequency (Stutzman and Thiele, 2013).

$$P_r = P_t \frac{G_t G_r \lambda^2}{(4\pi R)^2}$$

In decibel form, this adaptation of the Friis equation can be written as

$$10LogP_r = 10LogP_t + 10LogG_t + 10LogG_r - 20LogR - 20Log(f) - 32.44$$

where R = the range in km and the frequency, f, is expressed in MHz.

The Friis equation demonstrates that the attenuation of a given signal is directly related to the frequency and proportional to a factor of 1 divided by the range squared. This is known as path loss. Figure 11 illustrates the signal path loss at different UAS operating frequencies as a function of distance. From the graph, it is apparent that data links at higher frequencies, such as WLAN connections, attenuate faster than lower frequencies data links like GPS.

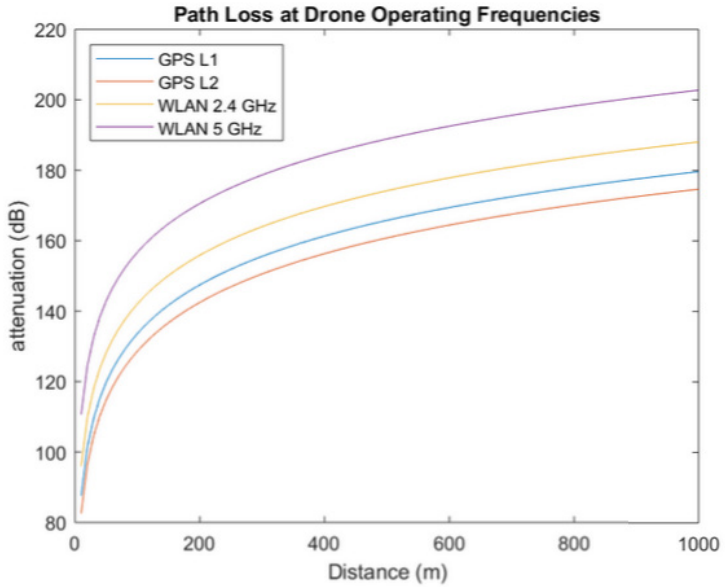


Figure 11. 1000-meter path loss of drone operating frequencies

Due to the large distance that the carrier wave must travel, GPS signal strength at the receiver is minimal compared to other types of communications signals. For reference, these signals are on the magnitude of one million times smaller than that of an FM radio

station. For GPS signals, this path loss is caused by atmospheric attenuation they experience from the satellite to the Earth's surface. This distance is averaged to be approximately 2×10^7 meters.

Using the average distance $R = 2\times10^7$ meters and the wavelength, $\lambda = \frac{c}{f} = 19cm$ for the L1 signal, the free space path loss can is calculated by the below equation.

$$L_s = \left(\frac{\lambda}{4\pi R}\right)^2$$

In decibel form, this equation can be written as $L_s = 20\log(R) - 20\log(f) - 32.44$

where R is the distance in kilometers (km) and f is the frequency in megahertz (MHz). Solving this equation results in a path loss of approximately -182 decibel-watts (dBW).

To interpret the C/A code for the GPS signal, the UAV receiver power level must be at least -158.5 dBW (NavtechGPS, 2019). With this information it is now easy to calculate the necessary ERP of the satellite by adding the absolute value of the path loss to the required received power. Doing so results in an ERP of approximately 23.5 dBW. While this number seems high compared with the minimal required receiver power, it is important to note that it is the result of the losses incurred over the vast distance that this signal must travel from a satellite in orbit to the surface of the earth. Reducing the distance between the transmitter and receiver will consequently result in a decrease in the required transmission power. This concept is visualized in Figure 12.

.

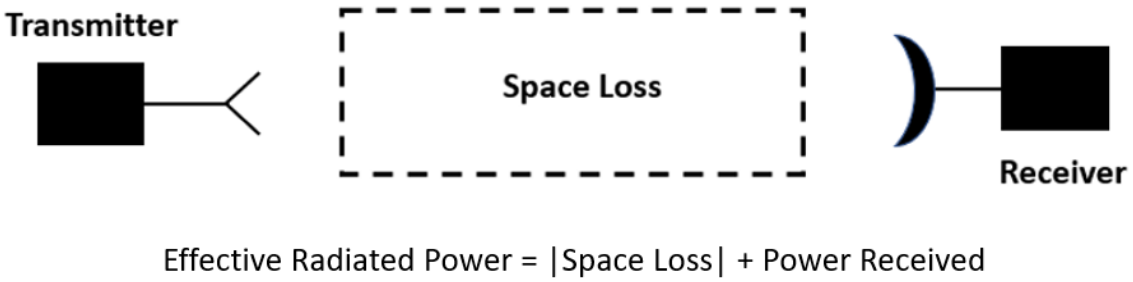


Figure 12. Visualization of free space signal propagation. Adapted from Naval Air Systems Command (1993).

The miniscule signal power required from a satellite for a UAV to successfully navigate means that these GPS signals are exceptionally vulnerable to both intentional and unintentional interference. If a UAV loses its GPS signal due to one of these reasons, it may respond by either attempting to land safely or hover in place until the signal is reestablished depending on its design. Similarly, any other command and control frequency used by the UAV becomes weaker the further that it travels from its ground station controller. For optimal performance UAVs operating in signal control or FPV are limited to a set operational range that is determined by the ERP of the transmitter. Outside of this range the UAV becomes unresponsive or executes a return to home function if it has been programmed to do so.

E. SUAS THREATS TO COMBAT OPERATIONS

The threat from SUAS technology poses a growing concern to the DOD. These low-cost and hard-to-target systems are seen as asymmetric weapons to overwhelm our conventional defense platforms and tactics. Not all SUASs are a threat, but their ability to carry payloads, bypass physical security systems, and transmit data through communications links makes them an attractive asset to malicious actors and our other adversaries.

1. SUAS Weaponization

SUAS weaponization is a growing threat on the battlefield. The small size and limited capabilities of these devices mean that they lack the sophistication or firepower of their larger military-grade counterparts, yet they can still deliver an explosive payload with a high level of accuracy. These can have devastating effects if their payloads are dropped over fighting positions or onto sensitive equipment.

The proliferation of drone technology has the potential to challenge the air superiority that has traditionally been the domain of nation-state militaries. Utilizing COTS devices like the $1,500 DJI Phantom, anyone now has the ability to cheaply develop a miniaturized air force (Pomerleau, 2017). This model has an endurance of 30 minutes and can fly at speeds of 10 meters/second (DJI, 2020). With a single battery charge and carrying a small payload, it is capable of a range of 11 miles. These types of SUASs can operate

from a high vantage point to gather information and send back video imagery via data links to a ground control station. This can provide the information required to plan and coordinate attacks. For example, Russia's recent incursion into Ukraine was aided by drones used to target ground troops. Ukrainian units quickly learned that drone sightings overhead were quickly followed by barrages of artillery fire (Freedburg, 2015).

Recent incidents have also highlighted terrorist organizations like ISIS and Hezbollah utilizing UAVs such as the Phantom that have been rigged to drop a grenade or mortar round above a target (Figure 13). Similarly, the drones themselves can be rigged to explode, essentially turning them into flying improvised explosive devices (IEDs). (Sims, 2018). This form of "aerial terrorism" is becoming increasingly common (Lele and Mishra, 2009, p. 61).

Figure 13. A COTS drone rigged with an explosive payload. Source: Pomerleau (2017).

UAS technology is also used to create a platform to deliver precision-guided munitions as well. Recently, Kalashnikov unveiled is KUB-BLA drone at the International Exhibition of Arms in Abu Dhabi (Sly, 2019). It operates as a "kamikaze" UAS with coordinates fed into the vehicle and an advanced computer algorithm that can distinguish between different targets. By using an autonomous waypoint mode, this system is a fire-and-forget type weapon that does not rely on a ground station controller. Additionally, this

group 1 style device boasts a three-kilogram payload, 30-minute flying time, and top speed of over 80mph. The drone's low cost and simplicity to use has the potential to revolutionize warfare in the same way that the company's AK-47 assault rifle did decades before. Figure 14 is a depiction of the Kalashnikov drone.

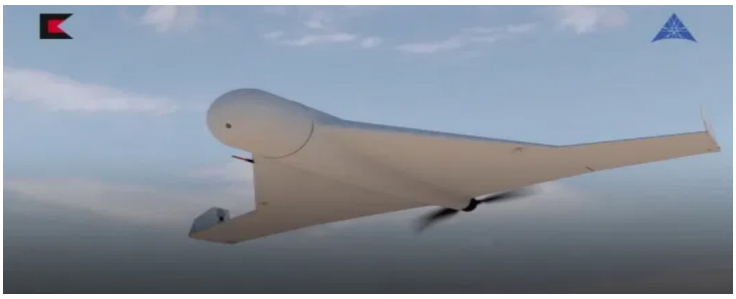


Figure 14. Kalashnikov drone. Source: Parsons (2019).

2. SUAS Swarming

It is becoming apparent that SUAS have the potential to "change the nature of warfare" (Stiles, 2017, p.1). One recent phenomenon of SUAS that is driving this change is the adaptation of swarming. A swarm is defined as "a group of entities that together coordinate to produce a significant or desired result" (Campion et al., 2017). Conceptually, SUASs operating in a swam configuration would exhibit the characteristics of a flock of birds or a group of insects that appear to have a collective consciousness. This could be achieved by integrating artificial intelligence (AI) algorithms into a group of SUAS that enables decisions without the aid of a human operator.

The use of weaponized swarms is still in its infancy; however, there have been several instances of multiple UAVs conducting a coordinated attack. For example, on September 14, 2019, a series of drone strikes on a Saudi Arabian Oil facility resulted in a significant disruption of the world's daily oil production (Mena, 2019). In January of 2018, Russia reported that a swarm of thirteen drones armed with explosives attacked a base in Syria from a position estimated to be more than 50 km away (Hambling, 2018). Although the drones and their explosive payloads were crudely constructed, this attack is the most

significant military use of SUAS swarming to date. While these instances demonstrate coordinated attacks by multiple drones, they do not exhibit true swarming characteristics.

In a short film titled "Slaughterbots," the possibilities of a SUAS swarm were captured in a near-future scenario (McFarland, 2017). Hundreds of nano-sized quad-copters were weaponized with a small shaped charge and augmented with artificial intelligence. These drones were capable of discriminating between targets with such accuracy that they could seek out individuals based on facial recognition or uniform. Nuclear weapons were determined to be obsolete since this swarm could be bought for a modest price and without the risk of collateral damage.

"Slaughterbots" may be science fiction for the moment, but it does not mean that it is a far-fetched idea. A May 2016 study at the Naval Postgraduate School (NPS) demonstrated this by the successful deployment of 50 fixed wing *ZephyrII* UAVs that conducted cooperative autonomous flight operations for ten minutes (Chung et al., 2016). Each of these UAVs were built from off-the-shelf components and 3D printed parts. Figure 15 is an image of the *ZephryII* UAV.

Figure 15. NPS ZephyrII UAV. Source: Chung et al. (2016).

Building on the success of the NPS project, the Defense Strategic Capabilities Office demonstrated the capabilities of a swarm of 103 Perdix drones deployed from an F-

18 in October of 2016 (Slavin, 2017). These drones weigh less than a pound but can fly at speeds of up to 68 mph. Operating as a collective organism, they successfully conducted several missions autonomously. Similarly, other types of drones developed for this type of mission set by the U.S. include DARPA's Gremlins and the Office of Naval Research's Low-Cost UAV Swarming Technology (LOCUST) programs. These devices are programmed to "think" independently and to respond in a specific manner when confronted with different situations, similar to a football player's playbook (Jeffery, 2017).

The low cost of micro and nano-sized UAVs means that they are expendable assets, which increases their viability for future conflicts. A mass of these devices could move at a speed that could easily overwhelm an enemy force and paralyze command and control. Using swarming tactics means that they could also quickly overcome radar and air defense systems by either providing too many small targets to engage or by masking a more significant attack. Additionally, swarming tactics with these devices can be viewed as a low risk and cost-effective means to conduct traditionally dangerous missions in hostile environments.

F. C-UAS TECHNOLOGY AND TACTICS

Counter-Unmanned Aerial Systems (C-UAS) is the term used to describe those methods used as a means to render a UAV non-operational. It refers to an approach of threat mitigation by attacking the entire system that allows the UAV to conduct its mission. Recognizing the need for innovative solutions, the 2019 National Defense Budget, congress has allocated $1.5 billion dollars to the research and development of C-UAS technologies (Klien, 2018). From the need to address the threat from UASs, an industry focused on finding effective means of detection, identification, and defeating UASs has been created. C-UASs differ both in the methods used to defeat UAS and in the systems used to accomplish this objective.

1. UAS Detection/Identification

The detection and identification of a hostile UAV target are accomplished through a number of different sensor mechanisms. Often, several of these techniques are integrated into a single device. An overview of these techniques is outlined below:

Sight: Humans and optical sensors may be able to distinguish a UAV. This can be inhibited by intervening terrain, structures, weather, or foliage that prevent a visible signature from being determined.

Sound: Some UAVs emit an audible signature that can be detected.

Radar: UAVs can be detected by radar if their radar cross-section is sufficiently large.

Infrared (IR) and Ultraviolet (UV): IR and UV radiation emitted from a UAV can be detected by sensors.

Radio Frequency: Electromagnetic signals which are used for command and control of the UAV or for information downlink (video, etc.) can be detected and tracked.

2. UAS Defeat

There have been numerous studies by both civilian and military agencies that have experimented with a variety of methods for defeating a UAS. These types of defeat mechanisms are generally subdivided into the categories of "Hard Kill" (kinetic attacks) or "Soft Kill" (non-kinetic attacks) (Schleher, 1999). Kinetic studies have shown how nets, bullets, or even birds of prey can be effective means to defeat a drone. Non-kinetic techniques such as jamming or directed energy weapons (DEWs) have demonstrated the ability to disrupt communications or render a UAV inoperable through the destruction of electronic components with high energy bursts.

Interdiction methods can be further separated into the magnitude of their effects on the target. The exploitation of a UAV for intelligence purposes could allow for the attribution of an attack. While some soft-kill methods may allow for follow on exploitation, hard-kill tactics typically inflict enough damage that this is not possible. An overview of C-UAS interdiction techniques is outlined below and visualized in Figure 16.

a. Hard Kill C-UAS

Nets: Trapping mechanisms have been employed through various means to include specialized firearms or another UAV adapted for C-UAS capabilities.

Conventional firearms: Small arms and anti-aircraft artillery shot at the UAV can be highly effective at disabling or destroying the target.

Birds of prey: Raptors trained for C-UAS purposes have proved to be effective against smaller drones.

Surface-to-air missile (SAM) systems: Both radar-guided and IR SAMs can be effective against individual UAVs. This included man-portable (MANPAD) systems.

Air interception: Using aerial vehicles to attack UAVs can be accomplished through manned combat aircraft using gun systems, air-to-air missiles, or by UAVs operating in a C-UAS role.

Lasers: Directed beams of light energy can create physical damage to a UAV by damaging its onboard optical sensors.

High Power Microwave (HPM): HPMs use directed RF or microwave energy to damage the electrical hardware of a UAV.

Electromagnetic pulse (EMP): EMPs are blasts of electromagnetic energy with enough power to destroy any electrical components that are not shielded. This is similar in concept to HPM but done so with a higher power.

b. Soft Kill C-UAS

Jamming: To jam a UAV, a signal is generated at a higher power to interfere with the intended message and effectively block communications.

Spoofing: Spoofing involves imputing false data into the UAV in an effort to deceive it. This can be done either through RF or cyber means.

Hacking: Using malware to infect the drone can allow for a defender to take over control of a UAV or destroy its flight guidance programming.

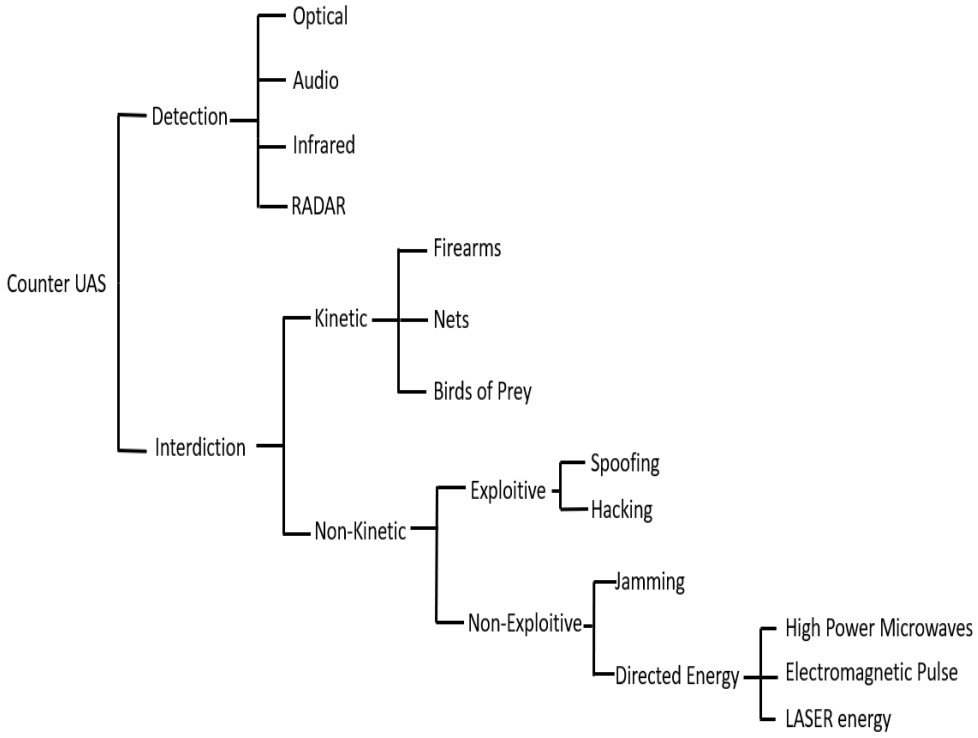


Figure 16. Counter-UAS detection and interdiction

3. Constraints and Limitations of Current C-UAS

Current C-UAS devices can be either handheld, vehicle-mounted, ground fixed, or airborne delivered. A 2019 report by the Journal of Electronic Defense outlined more than 250 different C-UAS products made by more than 100 different companies (Knowles and Swedeen, 2019). Each of these current attack options has limitations that affect their ability to mitigate the SUAS threat. These constraints are separated into three general categories: line of site engagement, range/mobility, and collateral damage.

Current C-UAS technologies apply their mitigation strategies through direct-fire means. This requires the defender engaging the UAS to place themselves within the range and visibility of the attacking aircraft. For hard kill techniques such as firearms, direct fire is easily understood by the straight trajectory of a bullet to its target. With this method of engagement, any intervening crests between the weapon and the target would cause this C-UAS system to fail. Similarly, the effects of soft kill interdiction techniques are limited by

the physics of RF energy propagation. The higher frequencies utilized by SUASs require line-of-sight for engagement, and the effectiveness C-UAS methods that use them are also degraded in transit due to interference from foliage, buildings, or weather.

All C-UAS techniques have a limited engagement range. For kinetic methods, this distance is determined by the caliber and type of the weapon, along with the ballistic characteristics of the projectile's flight path. For non-kinetic methods using RF energy, this distance is most directly related to the effective radiated power. A more substantial power supply or larger antenna would result in a greater range, but the size and weight of these systems would proportionally increase. This limitation can be overcome by producing more mobile systems; however, there is a trade-off between the mobility of a system and distance that it is sufficient for mitigating the threat.

The correlation between mobility and range is demonstrated through three different technologies developed by CACI International of Alexandria, VA. CACI International is an industry leader in providing C-UAS technology solutions. As part of a technology suite, CACI has developed three variations of its Skytracker system for grid fix, vehicle-mounted, and man-portable employment options (Knowles, 2019). Each of these variations can disrupt control links, and jam GPS/GNSS signals. The Skytracker "CORIAN" is designed for a fixed position and has a range of 10 kilometers, the "AWAIR" is its vehicle-mounted variant with a range of 5 km, while the man-portable option called the "Small Form Factor" has a range of only 2 km.

The employment of hard and soft kill C-UAS techniques both require the defender to consider the collateral damage from their effects. While kinetic options such as using bullets can be effective, this method could become hazardous when faced with a multitude of simultaneous targets. Without significant coordination between the shooters, the potential for crossfire would quickly become a significant risk. Additionally, due to the line-of-sight requirement for non-kinetic tactics, RF energy will affect not only the UAS but also any other friendly devices that are operating at the same frequency within the radiation field. This is an especially important factor to consider when employing navigation jamming devices. The weak nature of GNSS signals means that a relatively low transmitter power can also jam friendly ground units or friendly aircraft in the vicinity.

4. C-UAS Performance Metrics

Sandia National Laboratories (SNL) has developed C-UAS performance metrics to aid in the production of drone mitigation solutions. These metrics help to define the design and evaluation process for the effectiveness of a given system. Their research states that the performance of a specific system is determined by parameters that constrain its sensing ability, assessment capability, and neutralization effectiveness. Sensing the presence of a target UAV is a factor determined by the probability of sensing, P_s, and the sensing range, R_s. The ability to accurately assess the threat is dependent on the probability of assessment P_a, the assessment range, R_a, and the time needed for assessment, T_a. Finally, the ability of a C-UAS system to neutralize a threat is characterized by the probability of neutralization, P_n, the neutralization range, R_n, and the time needed for neutralization or T_n. Figure 17 is a graphical depiction of these variables involved in calculating the effectiveness of a given C-UAS system.

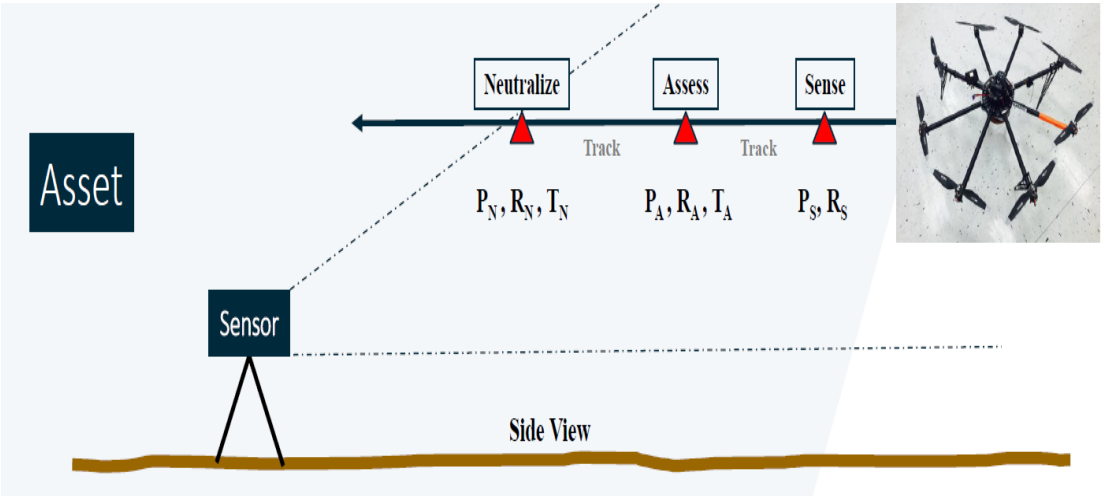


Figure 17. C-UAS system effectiveness. Source: Russel (2019).

Using this methodology, the probability of detection, P_D, and an estimate of the overall effectiveness of a specific C-UAS system, P_e, can be determined from the following equations:

$$P_D \cong P_s \times P_a$$

$$P_e \cong P_D \times P_n$$

For a notional C-UAS system, the following variables are estimated in daylight with optimal visibility;

$P_s = 0.9$ at a range of 1,000 meters

$P_a = 0.8$ at a range of 500 meters

$P_n = 0.9$ at a range of 400 meters

$T_n = 60$ Seconds

Plugging these numbers into the above equations then yields the probabilities of detection and effectiveness for the system;

$$P_D \cong (.9)(.8) \cong .7$$

$$P_e \cong (.7)(.9) \cong .6$$

With these estimated parameters, this notional system has a 60% probability of neutralizing the threat at its maximum range of 400 meters. Hypothetically, this system can only neutralize one target every 60 seconds. These performance metrics will change when variables such as the speed of the UAS are added, but it is apparent that a single C-UAS system will have limited effects on a swarm of SUASs at its maximum range. To achieve the maximum level of threat protection from a swarm, multiple C-UAS systems like the Skytracker variants would need to be employed.

5. USMC Integrated Air Defense Strategies

Antiair warfare (AAW) is defined by Joint Publication (JP) 1–02, *Department of Defense Dictionary of Military and Associated Terms,* as "actions required to destroy or reduce to an acceptable level the enemy air and missile threat." The USMC Tactical Publication (MCTP) 3–20C, *Antiair Warfare,* states that this capability serves the dual purposes of force protection and air superiority. C-UAS is not explicitly addressed in this document, but the airborne nature of the threat implies that its mitigation should fall under AAW principles. These principles state that successful AAW operations are based on the concept of destruction-in depth. This term encompasses the two requirements of threat detection and destruction from as far from a designated area to be defended as possible and for as long as the threat exists (USMC, 2018b). In other words, the protection from an airborne threat should be accomplished through integrating mutually supporting assets to provide overlapping detection coverage and engagement envelopes. This allows for a continuity of engagement if a single AAW weapons system fails.

The USMC has heavily invested in C-UAS detection and defeat systems as part of its ground-based air defense (G-BAD) program (LaGrone, 2018). These systems can be integrated in order to provide an overlapping defensive coverage from an airborne threat. According to the *Advanced Technologies Investment Plan (ATIP)* published in 2019 by Program Executive Officer, Land Systems (PEO LS), this program is designed to defeat the full spectrum of low-altitude/low observable threats with a low cost per shot and a high probability of kill against a Group 1 UAS.

As part of the G-BAD program, the Marine Air Defense Integrated System (MADIS) has been developed from an urgent operational need (UON) to defeat UASs and has recently become a full program of record for the USMC. It is an integrated system of systems designed for the neutralization of drones with built-in detection and kinetic and non-kinetic attack options. The less mobile variant of this system is the expeditionary MADIS (E-MADIS) and designed for stationary defense. Figures 18 is an image of the E-MADIS.

Figure 18. Expeditionary (E)-MADIS. Source: USMC PEO LS (2019).

The light MADIS (L-MADIS), is a mobile variant of this system that has been configured onto a vehicle for on-the-move (OTM) detection, tracking, and neutralization. In July of 2019, the L-MADIS system received significant media attention due to its successful downing of an Iranian drone from the deck of the *USS Boxer* (LaGrone, 2019). Figure 19 is an image of the L-MADIS.

Figure 19. Light (L) -MADIS. Source: Swanbeck (2018).

The current handheld solution that is being tested and employed by ground combat units in the USMC is the Drone Defender made by Battelle. This C-UAS device resembles a rifle and uses RF jamming to disrupt UAV frequencies for control and navigation with a beamwidth of 30 degrees. Additionally, it has a maximum range of 400 meters, weighs 15 pounds, and has a two-hour battery life. As opposed to the MADIS, this device is reliant on visual confirmation of the target before aiming and employing. To defend against a SUAS swarm, many of these devices would need to be employed along with their necessary battery requirements. Figure 20 is a depiction of the Drone Defender.

Figure 20. Drone Defender handheld C-UAS. Source: Battelle Memorial Institute (2019).

G. SCOPE FOR THIS THESIS

Chapter II defined the wicked problem that drones present and established the basic parameters that define an UAS. The physical characteristics of these devices, as well as their command and control architectures and spectrum requirements, are highlighted to provide the background information that is necessary to understand the principles of C-UAS techniques. From this research, it is apparent that a defensive SUAS swarm strategy must integrate multiple weapons platforms to develop an overlapping defense in depth. While each C-UAS system in the overarching strategy will have its inherent limitations, these are overcome by the collective effects of multiple engagement methods that target the swarm at the maximum detected distance.

C-UAS technologies also need to adapt to keep up with evolving technologies like swarming to provide an effective offensive and defensive capability for ground combat troops. This conclusion highlights the fact that the USMC's current G-BAD concept negates the use of indirect fires as a potential C-UAS delivery mechanism. Chapter III will explore this concept and explain how C-UAS is an applicable mission for the field artillery.

III. ARTILLERY AS A C-UAS STRATEGY

A. THE EVOLUTION OF CANNON ARTILLERY

The adaptation of artillery to serve in a G-BAD role against drones is a natural progression of its tactical evolution throughout military history. J.B.A. Bailey is a retired Major General in the British Army who has been a significant contributor to the development of innovative concepts and military doctrine. In his book *Field Artillery and Firepower,* Bailey describes the role of artillery in combat. He states that "Artillery supports other arms by hitting targets in their immediate vicinity but beyond the range of their own weapons, or where the fire of the supported arms alone would be insufficient" (Bailey, 2003, p. 15). The earliest artillery pieces fired cannonballs with relatively low accuracy against large enemy formations or fortifications. Exploding shells were invented in the late 18th century by adding a fuse to a hollowed-out iron shell filled with musket balls and an exploding charge. This configuration spread the lethal effects of artillery over a wider area (Kinard, 2007). The range and magnitude of the effects were later enhanced by the implementation of larger caliber weapons and changing the shape of the projectiles.

Until the 20th century, artillery was applied primarily as a direct fire weapon whereby the weapon system is fired with a direct line of sight to its target. It was not until World War I that artillery became utilized in an indirect role as a tactical self-defense method to support troop movements across the battlefield. This breakthrough led to the most significant advances in artillery with increased precision and the ability to engage targets with a multitude of effects (Bailey, 2003). Precision in this context does not necessarily mean the ability to destroy a point target but rather the application of artillery to deliver the desired effects within a designated space and specified time.

The increasing technological sophistication of the modern battlefield has expanded the definition of effects beyond the brute force delivered by exploding munitions. In an article titled "Meeting the Future: State of the Field Artillery in 1999," the Army's Chief of Field Artillery, Major General Leo J. "Lee" Baxter, argued that "we must prepare to deliver full-spectrum effects from massed area fires to precision strikes to disabling

equipment with non-lethal fires whatever the force commander requires." His intent was to change the concept of artillery from managing weapons systems to managing their effects. It was a major paradigm shift regarding the roles of artillery in combat. This vision of the future of artillery was dubbed "cutting edge fires" and was needed for artillery to remain relevant on the modern battlefield. The mission of artillery, as defined by the USMC today, personifies this vision with the term "fire support," which represents the range of effects needed for the supported unit's success. The USMC defines the mission of artillery "to furnish close and continuous fire support by neutralizing, destroying, or suppressing targets that threaten the success of the supported unit" (USMC, 2018c). The three major components of this mission are the timely, accurate, and continuous delivery of fire support, providing depth to combat and counterfire. The design of an artillery shell that targets SUASs should accomplish these three requirements.

B. C-UAS FIRE SUPPORT

Fire support refers to the delivery of the required effects within the battlespace to facilitate the actions of maneuver elements. There are a variety of munitions available that produce various effects, but none that specifically target SUASs. The standard 155 mm shell utilized by the M777A2 Lightweight Howitzer is the M795. This shell is comprised of a steel forged body packed with high explosives. A fuse is attached to the tip of the projectile that is set to initiate the explosive train for point detonation, proximity, or time delay. Kinetic effects on a target are achieved through the fragmentation of the projectile body, which has devastating effects within a designated blast radius. Except for precision-guided munitions like the M982 Excalibur, the effects of cannon artillery are intended for dispersed targets. The concentration of the effects is achieved by a battery of six guns shooting at a single aim point; however, firing data is typically computed with each howitzer firing a separate aim point in the vicinity of the target. Figure 21 is a diagram of a high explosive artillery shell for reference.

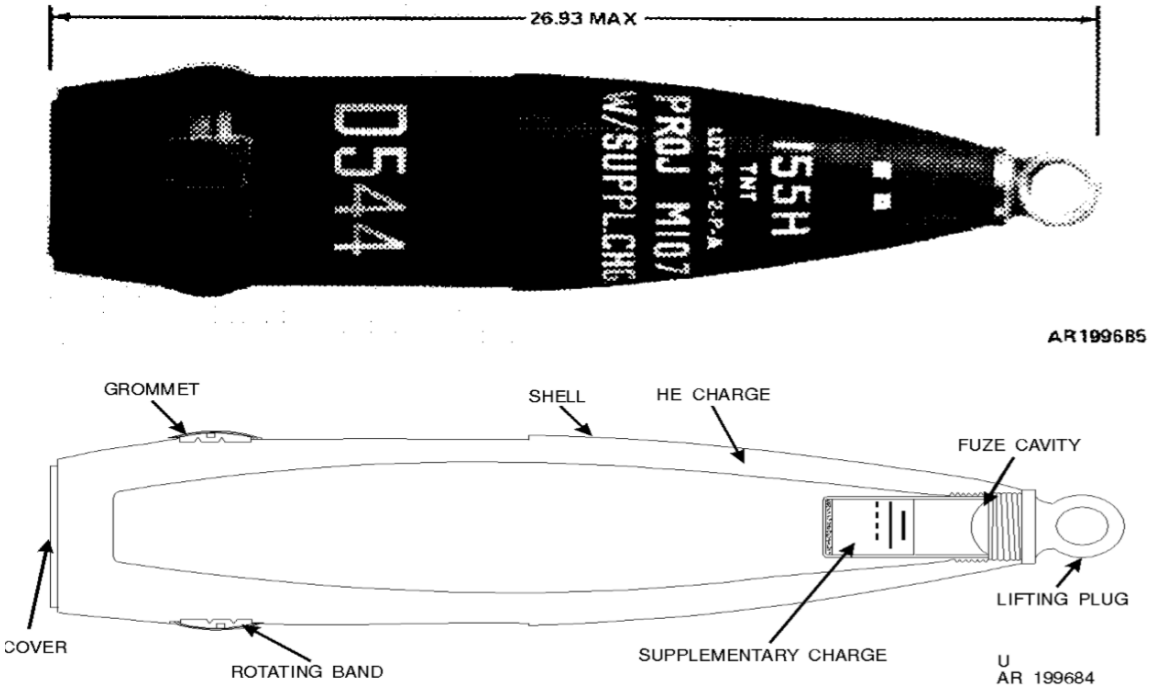


Figure 21. Artillery high explosive shell (without fuse) Source: DA (1994).

The cavity of the shell can be altered for the delivery of other types of payloads. The base-ejecting family of projectiles operates by using the force generated by a timed fuse to expel the back of the round and deliver the encased cargo. For example, the M483A1 Dual-Purpose Improved Conventional Munition (DPICM) delivers submunition bomblets that are scattered by the centrifugal force of the spinning round. Cargo artillery rounds have also been designed to provide non-lethal effects. The earliest known carrier projectiles for this purpose were designed during WWI to deliver communication messages on the battlefield (Imperial War Museums, 2020). This concept grew to include the use of projectiles for the delivery of logistics supplies into hostile areas (Dean, 1997) and even toxic gas agents to be used against personnel.

Cargo rounds are also used for the delivery of effects to influence the electromagnetic spectrum. Their effects can be distinguished by being in the visible or non-visible frequencies. Those shells that have been developed to control the visible spectrum are part of the current inventory for the USMC. Non-kinetic munitions to deliver effects

outside of these frequencies have been researched and tested but have seen limited fielding to date.

1. Visible Spectrum Munitions

a. M485A2 Illumination shell:

The M485A2 Illumination shell has a maximum range of 17.5km and offers one million candle power. It can illuminate an area measuring 1,000-meters in diameter. Larger areas can be illuminated by firing multiple rounds with offset aim points. This projectile uses a base ejecting parachute combined with a white phosphorous "candle" that burns for 120 seconds. When longer durations of illumination are requested, the command "continuous illumination" is given with a duration in minutes. Multiple shells are then fired at intervals that allow for an area to remain illuminated for the desired length of time. The standard height of burst is defined in the Tabular Firing Table (TFT) AM-2 as 600 meters above the target area.

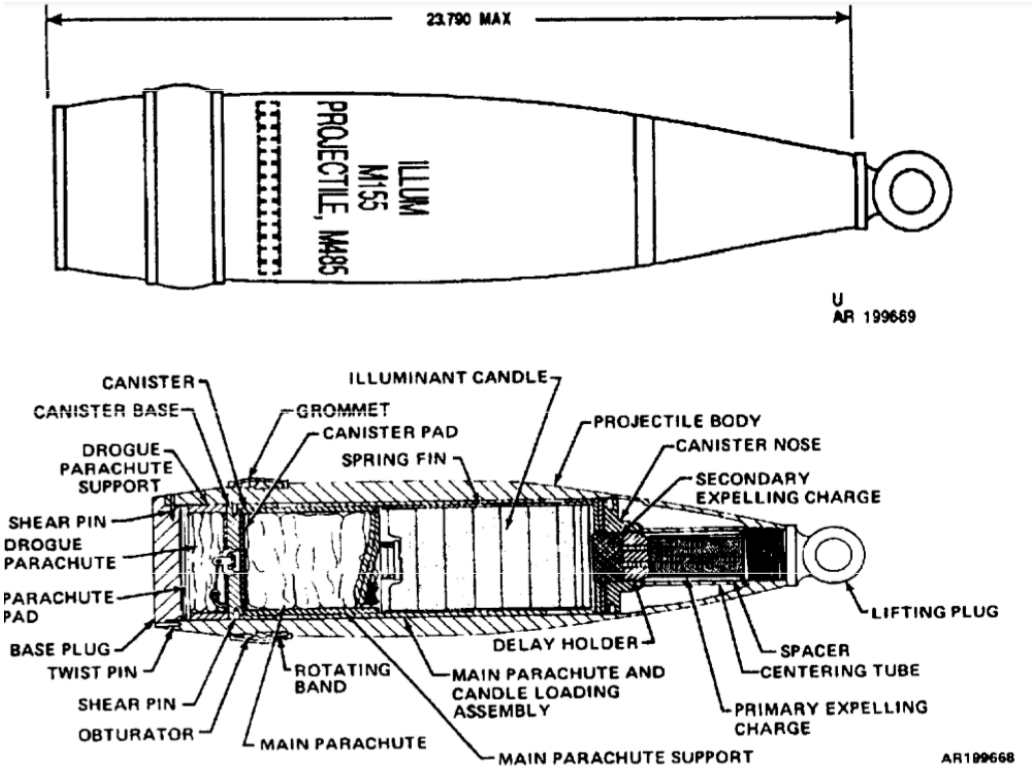


Figure 22. M485 illumination shell (without fuse) Source: DA (1994).

b. M825 White Phosphorus Shell:

The M825 is another base ejecting projectile that delivers 116 white phosphorus soaked felt wedges. These wedges produce an effect that blocks the visible portion of the EM spectrum. This smoke effect lasts for 5 to 15 minutes depending on weather conditions and is employed to screen friendly movement from enemy vision.

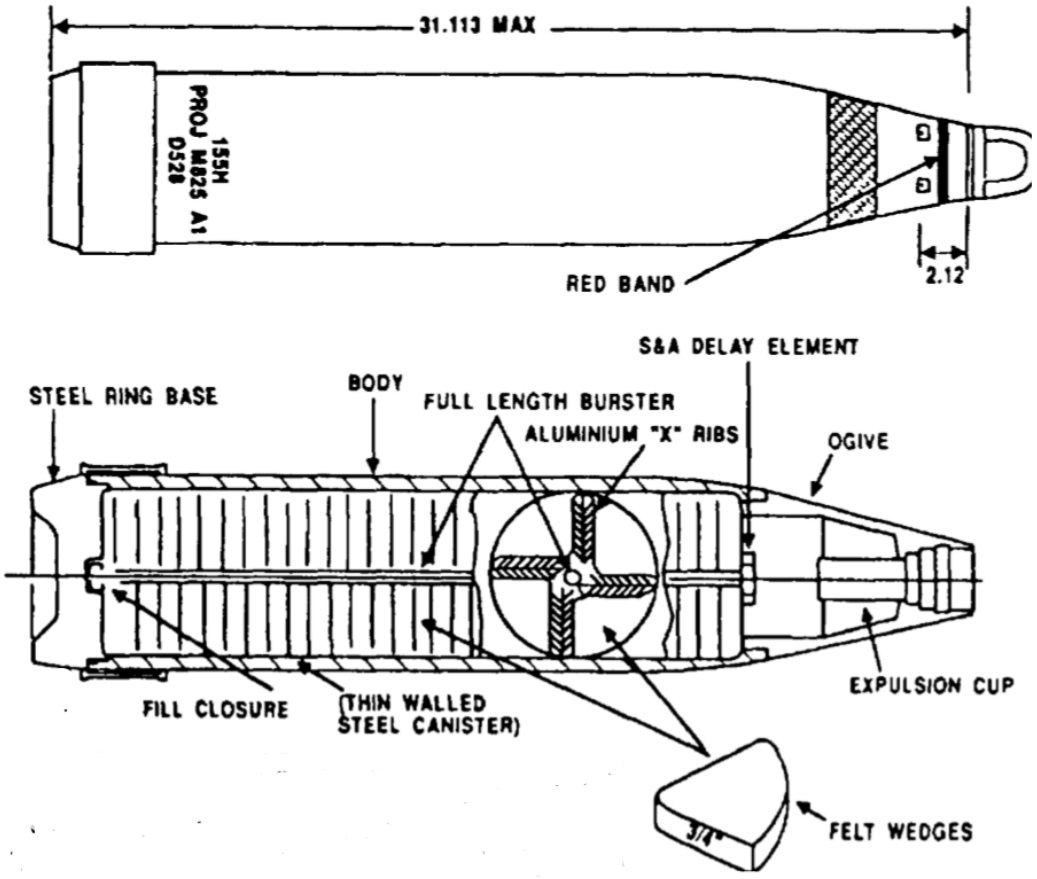


Figure 23. M825 white phosphorus shell. Source: DA (1994).

2. Non-visible Spectrum Munitions

a. M1066 IR Illuminating Shell:

The M1066 contains a cartridge that produces infrared light outside of the visible spectrum. The light emitted is only visible through night vision devices and has two times

the coverage area as traditional illumination rounds for the same time duration. Figure 24 is an image of the M1066.

Figure 24. M1066 IR illuminating Projectile. Source: Robillard (2019).

b. SAMEL-90 PLC Artillery Jamming Shell:

Samel-90 PLC is a Bulgarian based company that has developed a tactical jamming round, which comes in multiple calibers designed to target HF and VHF communications (Samel-90 PLC, 2019). These shells are designed to stick into the ground with a protruding antenna and have a max range dependent on the weapon system firing. For complete coverage of the HF and VHF bandwidths, eight projectiles are fired, with each one covering a specific portion of the spectrum. With more detailed intelligence, a commander may target a specific frequency to jam or fire all eight with overlapping bandwidths for complete coverage. These shells are designed to jam the desired frequency ranges for a duration of 60 minutes. By blocking enemy communications, these rounds can have significant effects on command and control and lead to a tactical advantage in combat. This type of shell is currently not in the U.S. inventory.

Figure 25. Bulgarian artillery jamming shell company. Source: Samel-90 PLC (2019).

c. Artillery Delivered Expendable Jammer (AD-EXJAM):

In the 1980s, the U.S. Army developed a concept of employment for the Air Delivered-Ground Deployed Expendable Jammer (AD-EXJAM). This project modified a M483A1 artillery shell to hold expendable signal generators that would activate once they hit the ground. The original intent of the program was to develop a delivery system for electronic countermeasures that could "seed" a target area and deny the adversary the use of the spectrum. (Taylor et al., 1997) Although demonstrated to be feasible, this program was terminated in the mid-1990s (Requested Decreases Disapproved, 1995).

d. Disruptive Cyber and Electronic Warfare Round (DiCER):

Currently in development at the Joint Center for Gun and Ammunition is the DiCER (Disruptive Cyber and Electronic Warfare Round) program. This program builds on the artillery delivered expendable jammer concept pioneered by AD-EXJAM. These rounds are developed primarily as a means for the extended-range deployment of non-kinetic RF effects to remotely disrupt, degrade, deny, deceive, and monitor adversary spectrum dependent networks and devices (W. Wang, PowerPoint Side, August 14, 2019). These projectiles carry a payload of hardened radio frequency emitters, which are ground

delivered on the battlefield with a wideband antenna for the primary purpose of deception or spectrum denial.

C. C-UAS DEPTH TO COMBAT

Just as the DiCER extends cyber and electronic warfare effects, a howitzer could also deliver C-UAS effects outside of the range of current systems and beyond the line of sight. Artillery in a C-UAS role can add depth to combat by shaping the battlespace at greater distances and providing an additional force protection capability to forward troops. Utilizing indirect fire for an air defense mission against UASs would be effective given that the unit firing has accurate targeting information provided by forward observers who can detect the target signature and ordnance designed to deliver the necessary effects.

The M777A2 utilizes separate-loading ammunition. The projectile and propellant are detached, giving the option for either increasing or decreasing the amount of explosive charge used to propel the round. This means that it can deliver its effects at greater and more flexible ranges than current C-UAS methods. By changing the amount of charge and altering the elevation of the howitzer barrel, the effective range of the system can be manipulated to the desired distance. Figure 26 gives a generic overview of the range capability of an artillery system firing specific charges. The overlapping portions show how more than one charge can be used to reach a given distance.

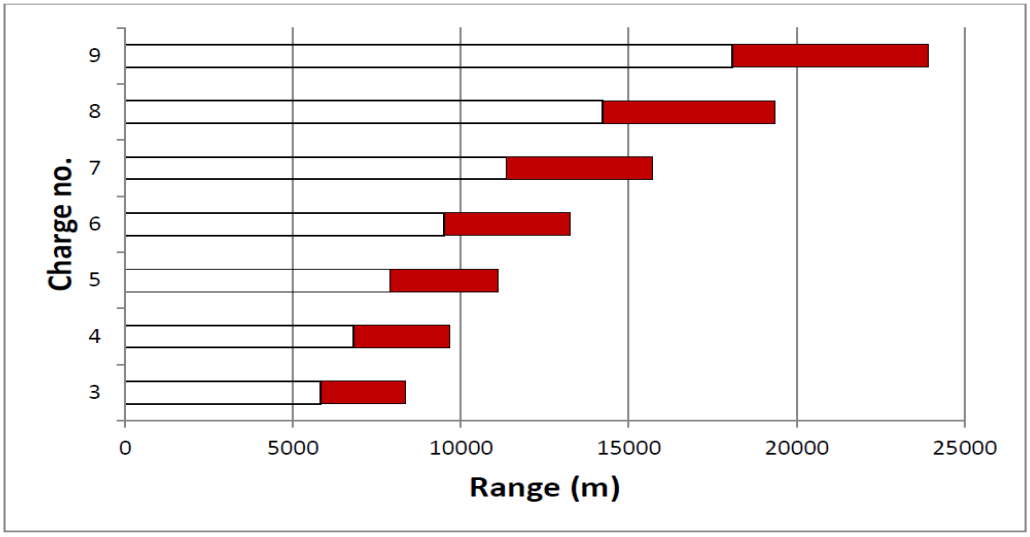


Figure 26. Range comparison for different propellant charges. Source: Dullum et al. (2017).

The use of artillery for the G-BAD mission would add an additional layer to the defense-in-depth provided by the ground-based, vehicle-mounted, and handheld devices currently in use. Figure 27 is a diagram of this concept, demonstrating how artillery can fit in as part of an integrated C-UAS air defense strategy.

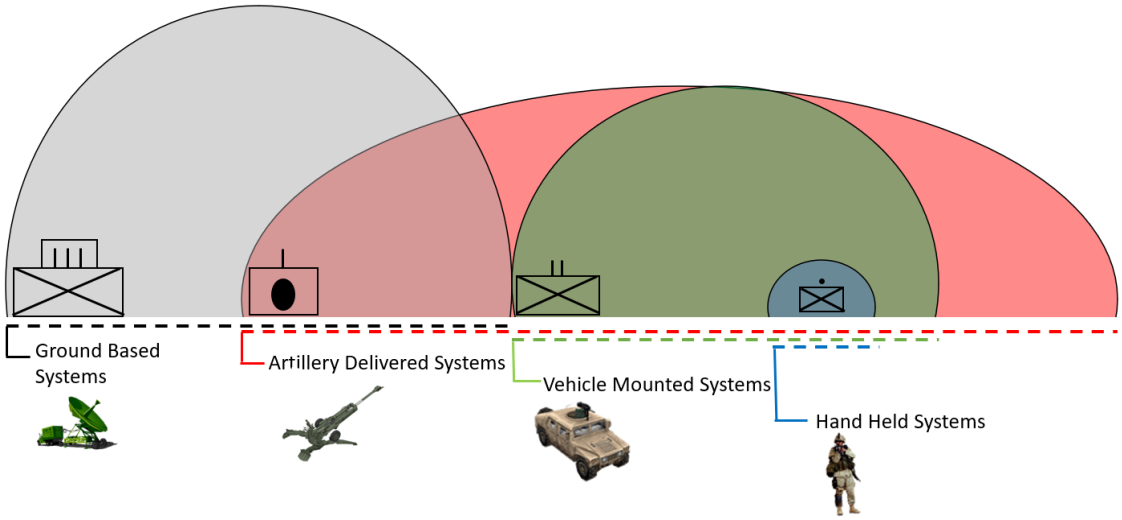


Figure 27. A notional example of a C-UAS defense-in-depth integrating cannon artillery.

This depiction shows how artillery can be used to support overlapping engagement areas to provide a C-UAS force protection capability to the entire battlespace from the rear to the forward line of troops. Shaping operations beyond this area could also be conducted by the creation of UAS denial zones or engaging these devices before they are an immediate threat.

D. C-UAS COUNTERFIRE

Counterfire is the destruction or neutralization of an enemy's weapons systems in order to allow friendly freedom of maneuver in the battlespace. These types of missions are given the highest priority since their execution ensures the freedom of action for the supported unit. The initial engagement of an artillery counterfire mission is "intended to suppress the hostile fire support system long enough for a more decisive engagement to be developed and executed" (HQ USMC, 2018 p. 7–3). This mission is accomplished by attacking either the command and control (C2) architecture, the target acquisition systems, or the physical weapon itself.

Pacer threats such as Russia have been known to use UAS as a means for target acquisition. This means that their destruction would effectively neutralize their indirect fire capabilities and support the counterfire mission. Similarly, when applied directly against a swarm of SUASs, a counterfire artillery mission could attack the swarm's C2 architecture, effectively killing the swarm by denying navigation data or blocking communications.

E. CHAPTER SUMMARY

Chapter III described how the role of artillery in combat has always focused on the delivery of effects outside of the range of direct fire munitions. Technological advancements over the past 200 years allowed for the expansion of the types of effects that are used to shape the battlefield. The projectiles that these weapons fire are redesigned to facilitate the delivery of a variety of payloads to support operational needs at extended ranges. The need to address the SUAS swarming threat is no different. A projectile specifically designed to attack the spectrum vulnerabilities of these devices would add to the defense-in-depth from UAS as part of an integrated G-BAD concept. Such a weapon

would provide a non-kinetic solution that would dramatically extend the effective range of weapons used to defeat SUAS swarms and protect the maneuver of USMC forces.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. NAVIGATION WARFARE AND C-UAS

This chapter begins with a discussion of a specific incident of a C-UAS technique applied against a U.S. combat drone. The possible techniques that were used are investigated as well as the feasibility of developing a weapon to create these effects with an expendable jamming system. Prior research into NAVWAR techniques against as a C-UAS weapon is described as they relate to the design requirements for an artillery shell with similar effects.

A. CASE STUDY: THE CAPTURE OF AN AMERICAN UAS

On December 5, 2011, a CIA stealth drone was conducting surveillance of nuclear energy sites over Iran. Approximately 140 miles from the border of Afghanistan, the drone was detected by an Iranian cyber warfare unit that initiated an electronic attack. Immediately after the incident, Iranian officials claimed that by exploiting a known vulnerability of the device, they were able to capture it. U.S. officials rejected the claim, and although they acknowledged the loss of the UAS, it was believed that the drone was shot down or crashed, leaving them with only pieces to put back together. Shortly afterward, a video was released showing several Iranian officials inspecting an intact and highly classified RQ-170 Sentinel stealth drone. Minor damage to the underside of the aircraft suggested that it may have experienced a rough landing. Still, the fact remains that Iran now possessed an intact and top-secret U.S. intelligence asset.

Before this incident, Iranian engineers had been studying U.S. reconnaissance drones since 2007. By reverse-engineering other less advanced drones taken down inside their borders, they were able to understand their vulnerabilities and how to exploit them. Intelligence collected explicitly on the RQ-170 was done by observing its operations in Afghanistan, where it was deployed since 2009. According to at least one of the Iranian engineers who was involved in the project, Iran realized that GPS navigation was the weakest point of the UAS (Schwartz, 2011). Therefore, they focused their efforts on developing a method for the disruption or alteration of these signals.

Iran claims that their cyberwarfare unit successfully jammed the remote control communications frequency of the drone, which caused it to resort to using the civilian C/A GPS code for its latitude, longitude, altitude, and velocity (Schwartz, 2011). By then introducing a false navigation message, the aircraft was forced to land by making it think that it was at its final destination. The scuff marks that were identified from the video suggest that an altitude miscalculation most likely caused them. Figure 28 is an image taken from a television report released by Iran that shows two officials inspecting the drone.

Figure 28. RQ-170 Sentinel UAV captured by Iran. Source: Gardner (2011).

While the validity of Iran's claims on how it captured the UAS is questionable, it raises questions concerning the vulnerability of these systems to NAVWAR attacks. The drone should have been using the more protected military GPS codes for navigation, and therefore, the injection of a false message should have been impossible. However, if the military signal was jammed, the UAS may have been designed to default to the civilian C/A code, which would make it vulnerable for deception. The remainder of this chapter will detail how this could be accomplished and how this technique can be built into an artillery shell with the same effects against low tech SUAS.

B. NAVIGATION WARFARE TACTICS

The intentional introduction of interference that affects the navigation message delivered to the UAS is classified as signal denial or signal deception (Godson and Wirtz, 2000). The denial of the navigation message is accomplished through overpowering the weaker signal, known as jamming. GPS deception involves inputting a false or "spoofed" signal into the receiver to trick it into accepting the interference signal as genuine.

In his 2001 book *Electronic Warfare 101*, David Adamy states that "the most basic concept of jammer application is that you jam the receiver, not the transmitter" (2011, p. 177). Jamming occurs through the interruption of the data link at the receiver by transmitting noise at a higher power level than the transmitted signal. This type of interference deteriorates the signal and causes it to degrade its accuracy or lose the signal completely. The higher the power of the jamming signal, the greater the effect it will have on the receiver.

Jamming can be accomplished through a variety of techniques to include, barrage, tone, or sweep jamming. The simplest forms of jammers utilize the barrage jamming method to produce a broadband noise interference signal that covers the bandwidth of the GPS signal. Tone jammers can target specific frequencies within the signal bandwidth to create narrowband interference. Intelligent jammers can be designed with prior knowledge of the receiver structure to generate sweeping waveforms that maximize the power efficiency of the jamming transmitter.

The deception or "spoofing" of a GPS receiver is done by broadcasting a transmission designed to resemble an authentic set of GPS signals. This technique is similar to jamming in that the original message is corrupted with a higher power signal. In contrast to merely blocking the signal, spoofing is a more sophisticated type of NAVWAR technique that attempts to take control of a GPS receiver's PNT solution. In so doing, the victim will unknowingly accept the spoofed location signal as valid. These types of attacks can either be done by recording a genuine GPS navigation message and replaying it or by generating an entirely new signal. Military systems are protected from less sophisticated spoofing attacks; however, civilian GPS signals are publicly known and easily replicated

(Jones, 2011). Even when the target receiver fails to recognize the false signal, spoofing can still create enough errors in the message to jam PNT information over large areas (Sathyamoorthy et al., 2012).

To successfully jam communications systems such as GPS, the jammer must overcome the processing gain of the receiver as well as the losses incurred during the distance the signal is propagated. The relative effect of the strength of the jamming signal on a receiver is referred to as the J/S (jammer to signal) ratio. This ratio is computed by subtracting the received signal strength as well as the path loss and gains of the transmitting and receiving antennas from the power of the interference signal. The following equation is the formula for the J/R with all values in decibels (Adamy, 2001).

$$J/S = ERP_J - ERP_s - L_J + L_s + G_{RJ} - G_R$$

In this equation, ERP refers to the effective radiated power of the jammer and signal and is defined as the product of the transmitter power and the gain of the transmitting antenna, respectively. This value represents the total power in watts radiated by an actual antenna versus that from a half-wave dipole reference antenna. G_{RJ} Represents the antenna gain from the UAV receiver in the direction of the jammer and G_R is the gain from the UAV receiver antenna. If the UAV is assumed to have an omnidirectional antenna and is within line of sight of the jamming source, these gain values are negated. Figure 29 is a depiction of the relationship between the J/S ratio and the relative signal strengths of the jammer and desired signal.

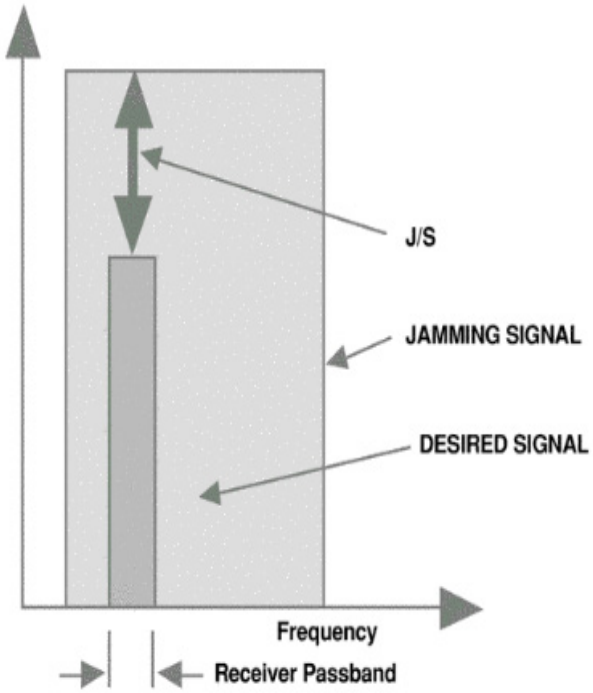


Figure 29. Jamming to signal (J/R) relationship. Source: Adamy (2011).

In a paper titled "The Civilian Battlefield: Protecting GNSS receivers from Interference and Jamming," author Michael Jones details the relative ease by which navigation signals can be jammed or spoofed. Figure 30 demonstrates the effect of jammers operating at different power levels by plotting their theoretical J/S values against the distance from the GPS receiver. According to the figure, the prevention of a GPS receiver from obtaining a C/A code is accomplished with a J/S of 27 dB. To cause a receiver to lose a C/A lock after it is already obtaining PNT information, a J/S of 47 dB is required. It is apparent from the figure that the more powerful the jammer, the greater the distance it will be able to affect the receiver. Due to the weakness of the GPS signal strength, the graph shows that even a 10-milliwatt (mW) jammer will be able to prevent a receiver from obtaining its C/A code at a distance of 10 km. At a distance of 1 km, it will lose its PNT information entirely. This graph shows that the same jamming power can disrupt even the more protected Y-code at a distance of only 400 m. Most current military systems also rely on first acquiring the C/A-code to obtain the Y-code, so jamming of the C/A signal could be sufficient to deny the initial PNT lock (Sklar, 2003).

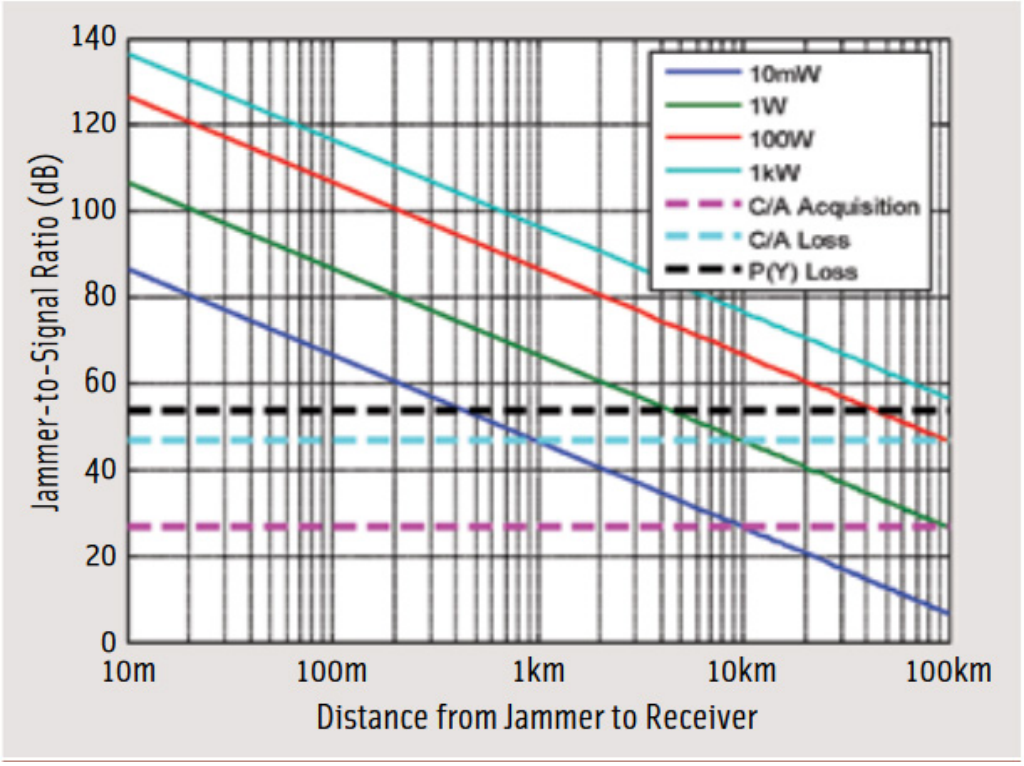


Figure 30. Effect of various jammer powers on GPS receivers. Source: Jones (2011).

C. ELECTRONIC ATTACK METHODOLOGY

The two basic tactics for jamming relate to the spatial location of the jammer in relation to the enemy and friendly units (Payne, 2006). Stand-off jamming is done by placing the jammer just outside of the range of enemy weapons systems to provide screening for friendly units. The significant advantage of this technique is that it protects the jamming unit from being engaged by the target. The major disadvantage is that it requires substantial power requirements to overcome attenuation and spreading loss. Stand-in jamming, also known as stand-forward jamming, is done by placing the jammer between the enemy and friendly units. This method is the most efficient in terms of power requirements but also is the most dangerous for the jamming unit since it would be within the range of enemy weapons.

Expendable EA systems can conduct the stand-forward jamming mission without the risk involved in placing a jamming unit within the enemy engagement zone. These

types of systems are employed when they can provide the advantage of either increased performance or reduced cost (Schleher, 1999). By reducing the distance between the jammer and the target, expendable EA systems allow for the deployment of multiple low-power transmitters with a lower cost than a single stand-off system.

1. Expendable GPS Jamming Devices

Although the disruption of GPS signals is illegal in the United States, there exist many different commercially available GPS jammers on the market. These devices are relatively cheap and are classified into one of three groups (Langley, 2012). Group one jammers are the smallest of the three and are small enough to plug into a car cigarette lighter. Group two devices have a rechargeable battery and an external antenna for portability. Group three jammers are similar in appearance to a cell phone and have internal antennas. All of these devices broadcast at frequencies with the intent to "block" PNT information, most commonly targeting the L1 signal but sometimes also the L2. A study of 18 commercially available GPS jammers found that the majority utilize a sweeping tone method to generate broadband RF interference with a bandwidth of 20 MHz (Langley, 2012). Figure 31 is a depiction of three common types of low-cost GPS jammers.

Figure 31. Three types of civilian GPS jammers. Source: Jammers.Store (2020).

2. Expendable GPS Spoofing Methods

GPS simulation devices have traditionally been more expensive and cumbersome on a hardware level. Replicating the desired signals needed to spoof a receiver requires a significant and complicated process that has been out of the reach of individuals lacking

technological expertise. Today, a GPS signal can be replicated easily with open source software and hardware, making the cost of GPS signal generation low and more sophisticated NAVWAR attacks easier to accomplish (Brown et al., 2012). This technology has been developed primarily for research and testing but could also be applied as an expendable EA system for NAVWAR-type attacks.

a. National Instruments LabView:

The National Instruments LabView GPS signal Simulation Toolkit is part of a group of applications built for navigation testing purposes (National Instruments, 2019). It uses an RF vector signal generator that is capable of creating a simulated GPS signal from up to 12 satellites. Figure 32 shows the user interface for this software.

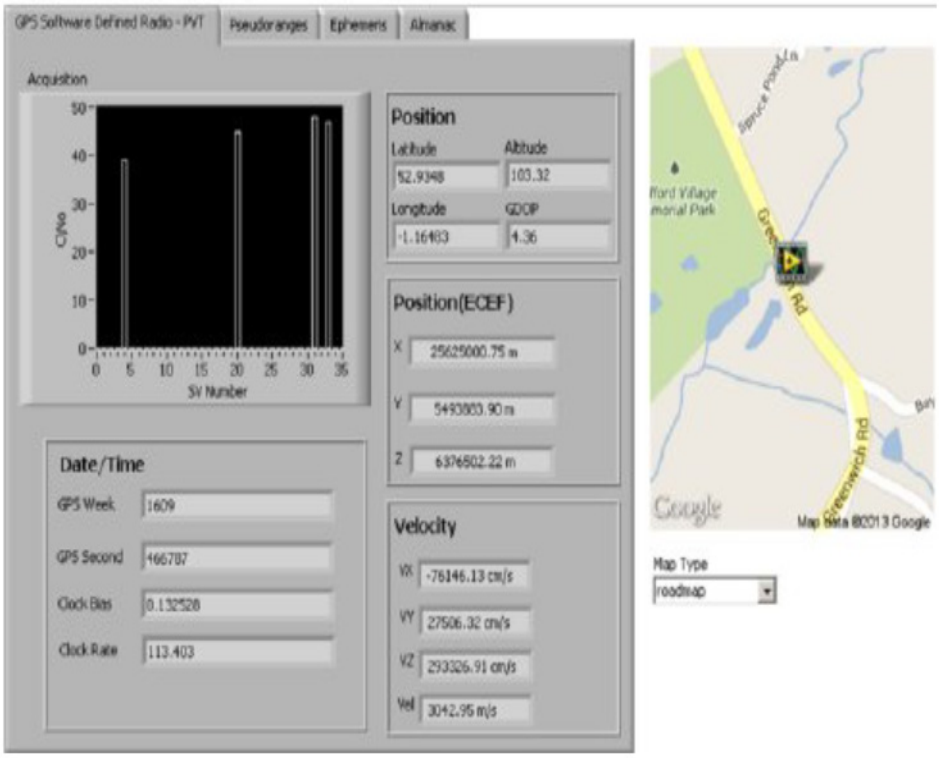


Figure 32. User interface for NI LabView GPS simulator. Source: Akopian and Soghogan (2013).

b. NAVSYS:

NAVSYS has developed several software add-ons to the MATLAB program that can provide signal and receiver tracking information (NAVSYS Corporation, 2019). The GNSS Signal Architect Simulator Software Tool is one specifically designed to simulate GPS or GLONASS signals for static or dynamic scenarios. Figure 33 is a depiction of the GNSS signal flowchart for the NAVSYS software.

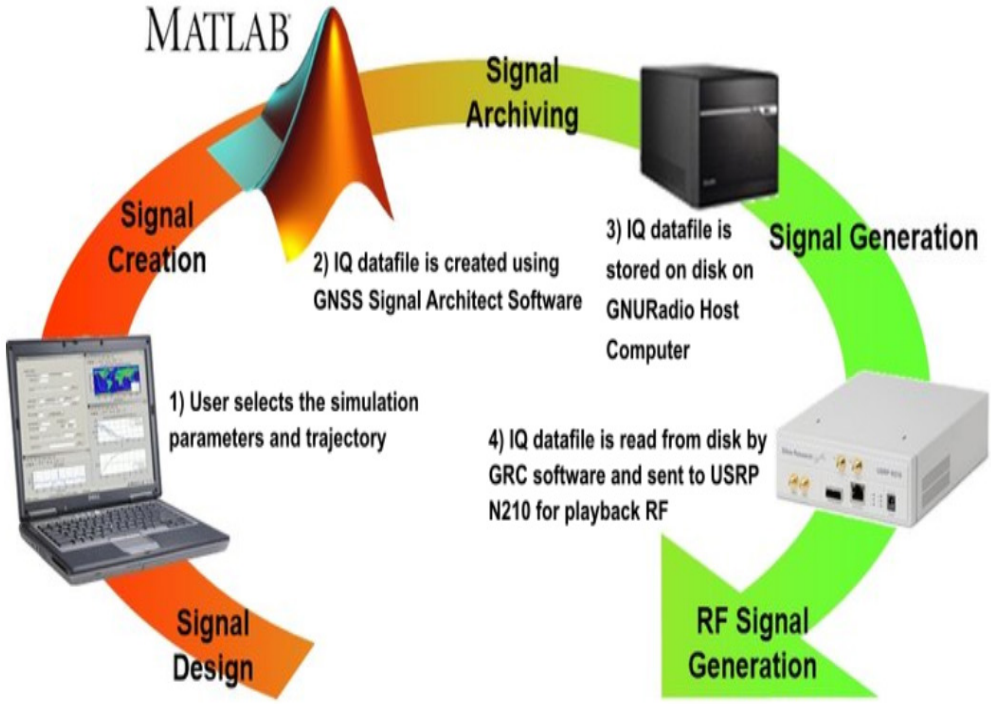


Figure 33. NAVSYS GNSS signal architect simulator flowchart. Source: Brown et al. (2012).

c. LabSat GNSS Simulator:

Developed by Racelogic, LabSat is a stand-alone navigation signal generator. It also can be used to record live GNSS data and replay it back when integrated with a GNSS scenario generation software called SatGen (Racelogic, 2019). This all-in-one hardware option costs $4,400. Figure 34 depicts the LabSat GNSS simulator.

Figure 34. LabSat GNSS simulator. Source: Racelogic Ltd (2019).

d. CLAW GPS Simulator:

A product of Jackson labs, the CLAW GPS Simulator, is a self-contained navigation signal generator that can produce full satellite constellation scenarios. Additionally, it has the capability of producing RF signals with CW, sweep, or noise functions to replicate the effects of jamming on communications equipment. (Jackson Labs Technologies, Inc., 2017) As the most affordable self-contained simulator, it costs $3000 and is roughly the size of a cell phone. Figure 35 is a depiction of this GPS simulation device.

Figure 35. CLAW GPS Simulator. Source: Jackson Labs Technologies Inc. (2017).

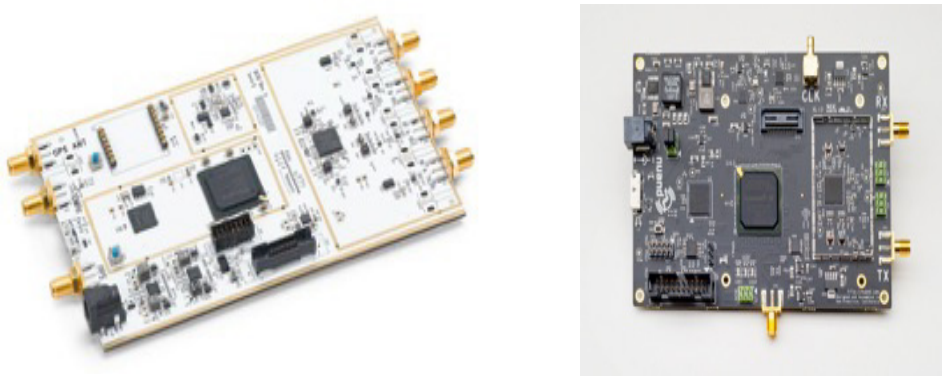
e. Open Source Software

The generation of a simulated GPS signal is now readily available with free open source code. GPS-SDR-SIM is a computer code that was initially developed under a Massachusetts Institute of Technology (MIT) license by Takuji Ebinuma. When a desired latitude and longitude are imputed into this program, it creates five minutes of a simulated GPS signal that replicates the satellite signals for the specific location. It has become highly popular with users of the game Pokemon Go, in which players must physically go to precise GPS coordinates to interact with virtual characters (Gartenberg, 2016). With little effort and the aid of software like GPS-SDR-SIM, players can cheat the game by spoofing their location on their cell phone.

f. Software-Defined Radios

Open-source software such as GPS-SDR-SIM utilize a software-defined radio (SDR) as the primary hardware component for GPS signal transmission. As its name states, an SDR is a radio communication system that has components implemented by software rather than hardware. In traditionally designed devices, specially built circuits are used to emit RF energy over a relatively narrow frequency range with a limited modulation type. In contrast, an SDR can be programmed to transmit or receive frequencies over a much broader range.

There are many different types of SDRs that have a range of capabilities and prices. Those types of devices that can transmit RF energy are characterized as either full- or half-duplex. Full-duplex SDRs are capable of simultaneously sending and receiving radio transmissions. Half-duplex SDRs can send and receive transmissions but not at the same time. At the higher end of this spectrum is the full-duplex capable Universal Software Radio Peripheral (USRP), which is available for approximately $13,000. (National Instruments, 2020). The mid-range full-duplex device is the BLADERF made by Nuand and costs roughly $1,000 (Nuand, 2020). Figure 36 depicts these two SDRs.



From left to right, USRP (National Instruments, 2020), BLADERF (Nuand, 2020).

Figure 36. Two examples of SDRs.

One of the most popular of these SDR devices is the HackRF-One. The HackRF-One is a half-duplex SDR that was designed by wireless security researcher Michael Ossmann. Roughly the size of a cell phone, it is capable of transmitting and receiving radio signals from 1 MHz to 6 GHz at a rate of 20 million samples per second and can be purchased for less than $300 as of February 2020 (Great Scott Gadgets, 2016). Figure 37 is an image of the HackRF-One.

Figure 37. HackRF-One SDR. Source: Great Scott Gadgets (2016).

The programming of the SDR to generate specific frequencies can be accomplished by using free open source software such as GNU Radio Companion. As a front-end graphical interface to GNU Radio, this program is a signal development toolkit that provides easy to use signal processing blocks to design flow graphs for a variety of specific communications functions. These flow graphs are then written in Python and C++ applications for a computer to either receive or transmit data into digital streams through the SDR hardware. Figure 38 depicts an example flow graph from the graphical user interface (GUI) called GNU radio companion. The picture shows signal source with specified frequency and waveform generated by the program and fed into the "osmocom sink," which in this case is the connected SDR. In this flowgraph, a Gaussian noise source is generated at the GPS L1 frequency of 1575.42 MHz and a bandwidth of 20 MHz. The settings for the RF and IF gain in the osmocom sink block are used to set the desired power emitted from the device. In the example, the values chosen are those which produce the maximum radiated power for the HackRF-One. The device can also be supplemented with an amplifier or have the signal fed into an antenna to produce a higher ERP.

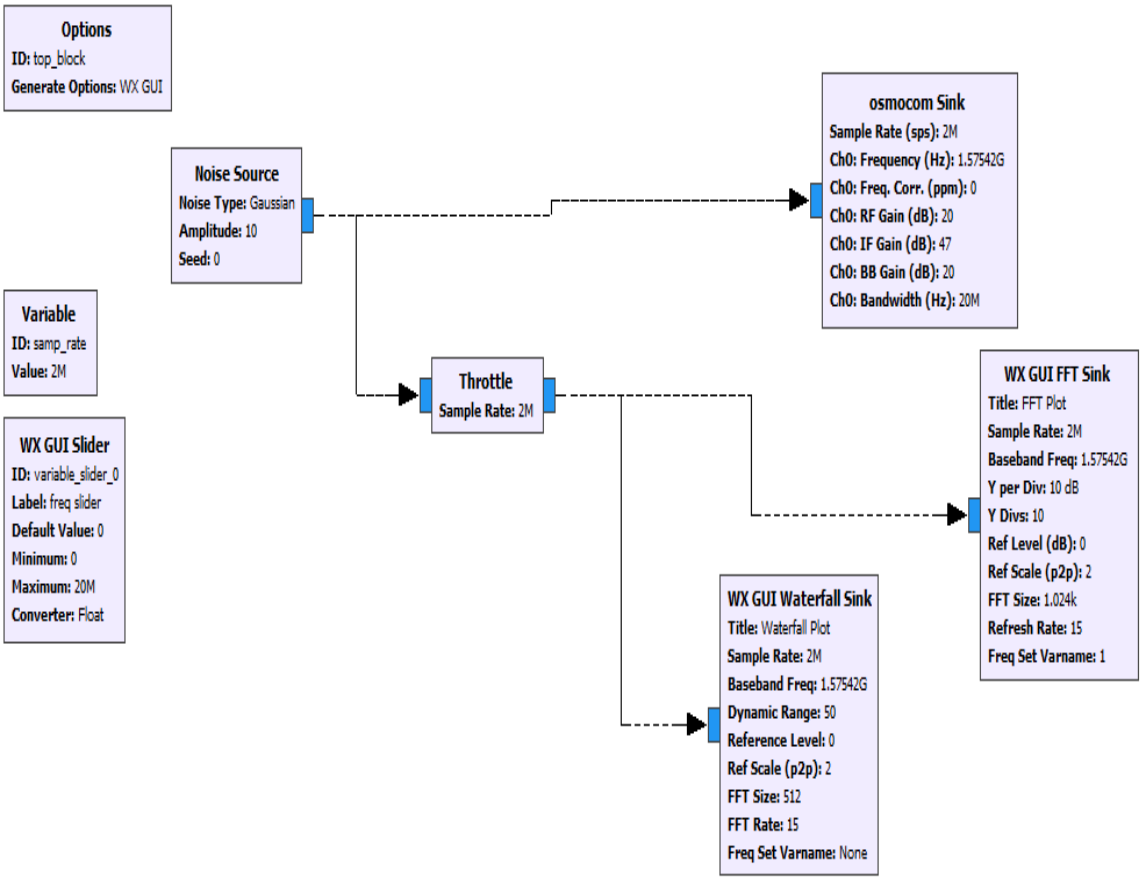


Figure 38. Jamming signal flowgraph from GNU radio companion

A visualization of the signal is done through the addition of the fast Fourier transform (FFT) and frequency (WX) sink blocks. A “throttle” bock is added before these two blocks of the flowchart to limit the number of samples taken and reduce the load on the computer. Figure 39 is the visualization of this signal generated by the HackRF-One with a waterfall display on top and the FFT on the bottom. From the FFT plot it is apparent that the output power of the HackRF-One at this frequency is approximately -15dBm. If connected to an omnidirectional antenna, this radiated power would result in a GPS denial area with a radius of roughly 400 meters.

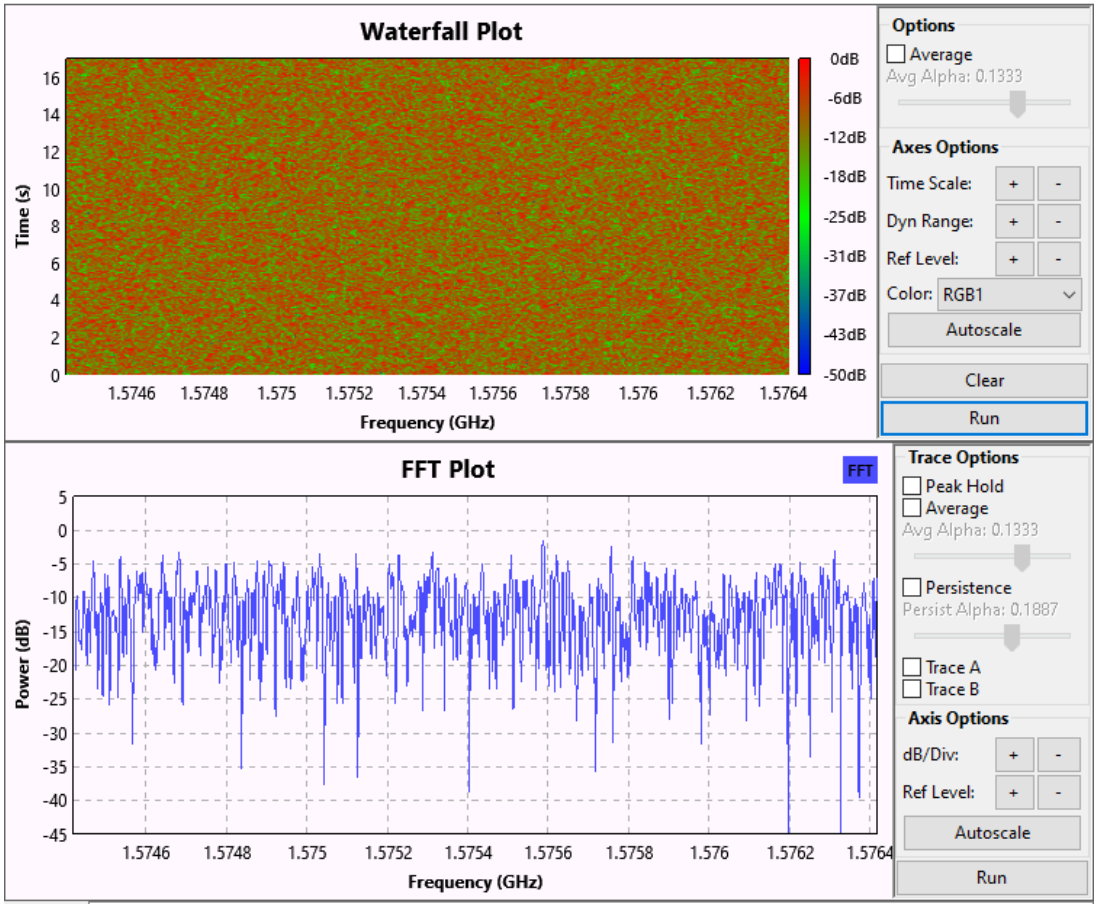


Figure 39. GNU Radio plot of the jamming signal

3. Prior Work on SDRs for Signal Jamming and Spoofing against UAS

a. UAS Jamming with SDR

A 2017 master's thesis done at the Tallinn University of Technology in Finland by Karel Parlin investigated the effects of jamming spread spectrum communications used in UAVs with a BladeRF SDR. In this thesis, barrage, tone, sweep, and protocol-aware jamming techniques were compared by their relative power requirements. A protocol-aware jammer was found to be the most efficient; however, it required prior knowledge of the type of UAV it would be implemented against (Parlin, 2017). Similar work done by Martins DaSilva in 2017 demonstrated the feasibility of an RF jammer on an SDR platform using open-source software. This experiment proved that an interference signal with a

cosine waveform required the highest power to jam GPS signals while additive white gaussian noise or AWGN needed the lowest (Martins DaSilva, 2017).

b. UAS Spoofing with SDR

The versatility of the SDR platform as a UAS spoofing tool has been explored by several different studies. In 2018 a spoofing apparatus was developed from a BladeRF SDR and open-source software. The research done by Horton and Ranganthan proved that with limited resources, an Android smartphone and a DJI Matrice 100 quadcopter could easily be spoofed. Of note, the GPS location signal of the quadcopter was spoofed in less time than the phone since the quadcopter uses GPS alone for positioning and not cellular data networks and Wi-Fi (Horton and Ranganthan, 2018). Another study conducted in 2019 by Yuniati, Ulvan, and Hasim, proved the feasibility of using a HackRF-One SDR to effectively take over a drone mid-flight by analyzing and demodulating the intercepted signal commands from a ground station controller (Yuniati et al., 2019). Similarly, experiments have shown that with a HackRF-One SDR, it is possible to take control of a UAV through the input of spoofed navigation signals. In 2014, a study at the University of Texas by Kerns, Shepard, Bhatti, and Humphries proved this by altering a UAV's perception of its location and a time-reference receiver's perception of the current time. By changing the perceived location of the device, it could be "steered" in a specific direction by generating a spoofed signal in the direction opposite of the desired motion. This allowed for the spoofed signal to force a UAV to follow a false trajectory unknowingly (Kerns et al., 2014).

c. Portable SDR Signal Generator

An SDR must be attached to a computer in order to process the code required for the generation or reception of signals. The wireless attack lunch box or WALB overcomes the lack of portability with a desktop computer by connecting it to a small single-board computer called a Raspberry Pi and an external power supply (Crecentvenus, 2019). This configuration creates an SDR-based portable signal jammer that can fit in a lunch box. The plans for developing the WALB is freely available on the software sharing site GitHub. A rotary encoder that has been programmed into the system also allows the user to switch

between frequencies or attack mode. With free spoofing software like GPS-SDR-SIM and minimal training, this expendable EA system can be created for less than $400. Figure 40 is an image of the WALB.

Figure 40. WALB. Source: Crecentvenus (2019).

D. CHAPTER SUMMARY

The opening case study of the capture of the RQ-170 demonstrates that reliance on GPS for PNT data is a significant vulnerability of UASs operating in autonomous modes. Therefore, it is likely that NAVWAR techniques like GPS signal jamming and spoofing can be an effective C-UAS strategy to be used against SUAS swarms. The most cost-effective method of producing a navigation interference signal is through an SDR with open-source software. Recent studies show that the use of this technique against UAVs is effective. Still, there have been no attempts to develop a system like the WALB to be employed explicitly as an artillery-delivered expendable jammer against SUASs.

THIS PAGE INTENTIONALLY LEFT BLANK

V. ARTILLERY SHELL DESIGN AND SIMULATION

This chapter defines the requirements for a C-UAS artillery shell utilizing the NAVWAR concept. For simplicity, the desired effects are defined against a swarm of micro-sized UAVs utilizing the civilian L1 GPS band for navigation. The transmission power needed for the disruption of the signal is calculated, along with the antenna parameters and the rate of fall for a base ejecting payload. Simulations using the RF propagation tool CloudRF are then used as a means to visualize the effective engagement area of the weapon at different altitudes.

A. SYSTEM DESIGN PARAMETERS

The design of an expendable EA system is determined by the delivery vehicle, payload, and deployment requirements (Schleher, 1999). This expendable system will be delivered via a projectile launched from a howitzer. The C-UAS artillery shell will be similar to other cargo holding 155 mm projectiles that utilize a base ejecting design. The "kill mechanism" for the UAV targets will be programmed into the shell before firing through an internal computer, which can be programmed to generate the desired waveforms. It is the intent that this signal generator would be capable of transmitting either jamming or spoofing signals depending on the programmed setting. For simplicity, the signal generator will be referred to as the "jammer" throughout this section.

1. Delivery Vehicle

The projectile is loaded into the howitzer along with a separately loaded propellant canister. The computed firing data determines the propellant charge to be loaded as well as the deflection and elevation for the howitzer tube. A struck primer initiates the explosive sequence that propels the projectile on a ballistic arc to its pre-determined coordinates and altitude. When the projectile has reached a specific point in its trajectory, a timed fuse initiates the charge that will eject a submunition consisting of a signal generator and parachute. The three major components of the projectile are depicted in Figure 41, and a representation of the firing sequence is shown in Figure 42.

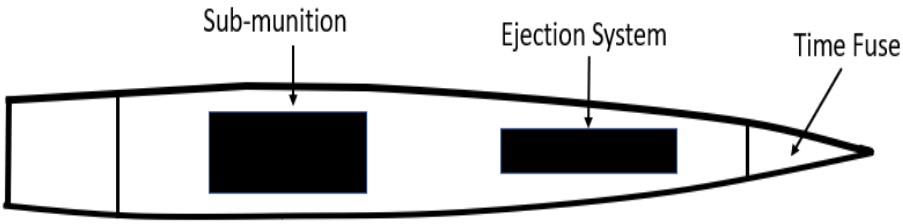


Figure 41. Proposed C-UAS artillery projectile components

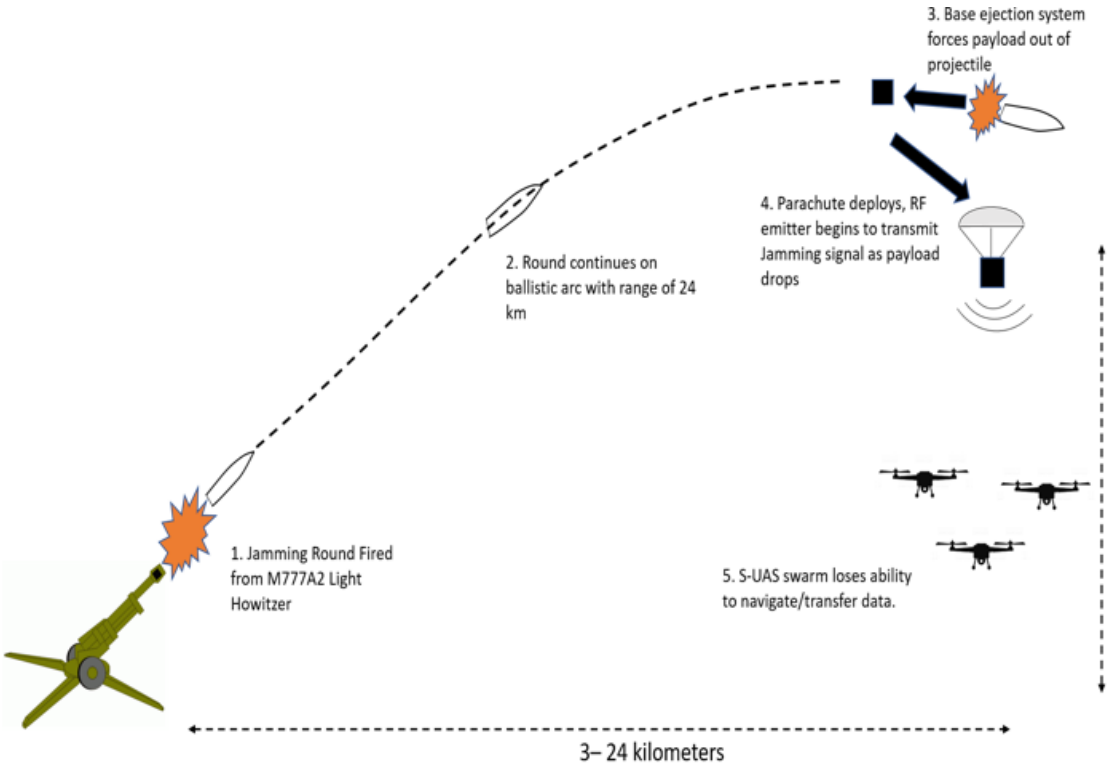


Figure 42. Firing sequence of C-UAS projectile

2. Payload

The payload is comprised of three major components required for the propagation of the jamming signal. These are a parachute, a signal generator, and an antenna. The signal generator requires a power source that supports an internal computer and SDR. Once activated by its ejection from the shell, the SDR then feeds the signal into an antenna to

deliver the electromagnetic effects while the parachute creates drag to reduce the payload's rate of fall. Figure 43 is a diagram showing the interaction between the components of the signal jammer.

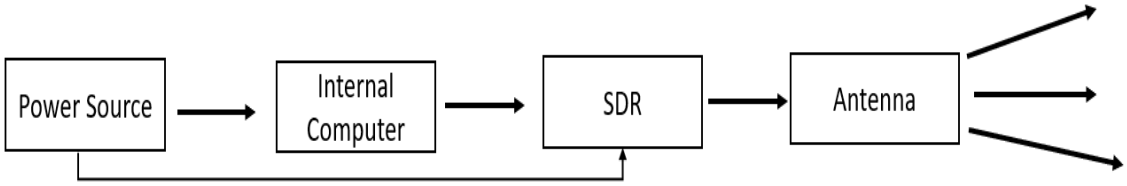


Figure 43. Signal jammer components of proposed C-UAS projectile

3. Deployment Requirements

It is the overall intent for the C-UAS artillery shell to interfere with the navigation links that a UAS relies on. In the context of this research, the target in question will be a group of micro-sized quadcopters operating as a swarm of three or more devices utilizing the GPS L1 band for PNT information. In this case, the introduction of RF interference at this frequency with the intent to jam or spoof the navigation link would theoretically result in the loss of control of the UAVs.

a. Engagement Area

A single shell's jamming effects are limited to approximately a one kilometer square region on the earth's surface. This is done to limit electromagnetic fratricide against friendly troops or aircraft that could also be utilizing the GPS navigation signal, but can be adjusted based on mission requirements. The beamwidth required for this area coverage will be measured at the half-power or -3 dB point of the primary radiation lobe and can be calculated to give a specified gain for the payload antenna. Figure 44 is a depiction of the jamming payload against a swarm of three SUASs.

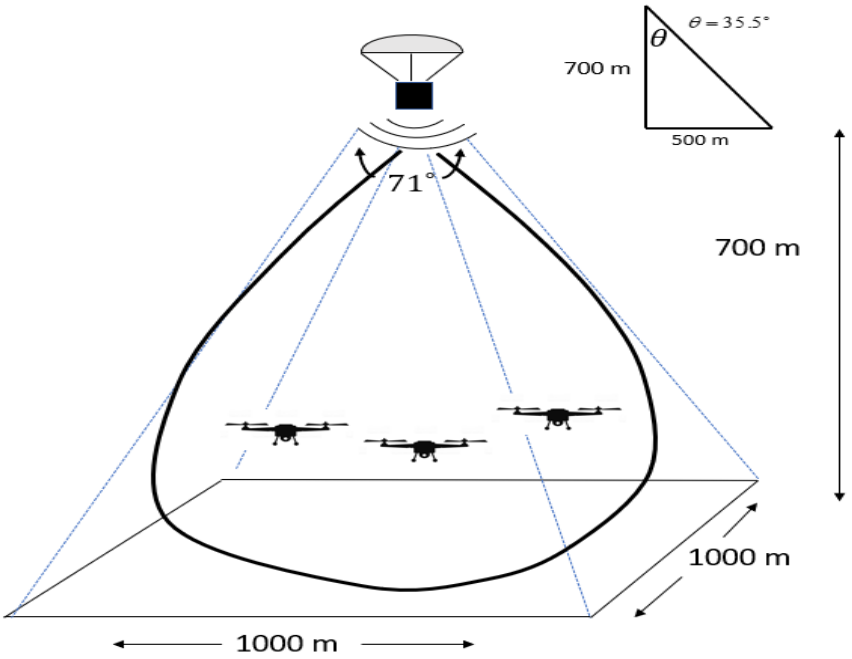


Figure 44. Maximum desired beamwidth of the jammer

After the payload is ejected, it transmits the interference signal with an initial altitude of 700 meters. This value will ensure that the device is activated at a height above the altitude limitation of a micro-UAS. From Figure 44, the desired beamwidth formed by both the elevation (ϕ) and azimuth (θ) angles of the GPS denial area is 71°. According to Naval Air Systems Command, the antenna's ground footprint can be estimated to be a rectangular area, although, in reality, it would be more of an ellipse. Using their equation, the desired gain, G, can be found by dividing the area of a sphere from the area of the antenna radiation pattern as seen in the below equation.

$$G = \frac{4\pi r^2}{r^2 \sin\theta \sin\phi} = \frac{4\pi}{\sin\theta \sin\phi}$$

This can be further simplified to:

$$G = \frac{41,253}{BW_\phi \times BW_\theta}$$

The constant in this equation represents the number of square degrees that can be placed in an ideal sphere. Solving results in a gain of 8.18 or approximately 9 dB.

b. Antenna Design

Many different types of antennas could provide the gain necessary to produce the desired UAS denial area. The physical limitations of the C-UAS artillery shell, as well as the characteristics of the target signal, guide suitable options. The shell can be seen as a cylinder that has a diameter of 0.155 meters and a total length of approximately 0.59 meters. This gives a volume of less than $0.011\,m^3$ to be used for all components necessary for the antenna, its jamming payload, and the ejection mechanism.

Additionally, GPS signals have a specified polarization, and navigation receivers are designed to match this to detect the signal. To address these constraints, this thesis will focus on utilizing an axial-helix antenna that can be built into the circular shell casing. This particular type of antenna resembles a cork-screw and produces radiation along the axis of its orientation. The benefits of this design allow for the generation of right-hand circular polarized (RHCP) waves that match the polarization of the GPS signal and ensure their reception by the UAVs. Additionally, this type of antenna is simple to construct and easily conformed to the shape of the C-UAS shell. Figure 45 depicts the basic components of an axial helix antenna.

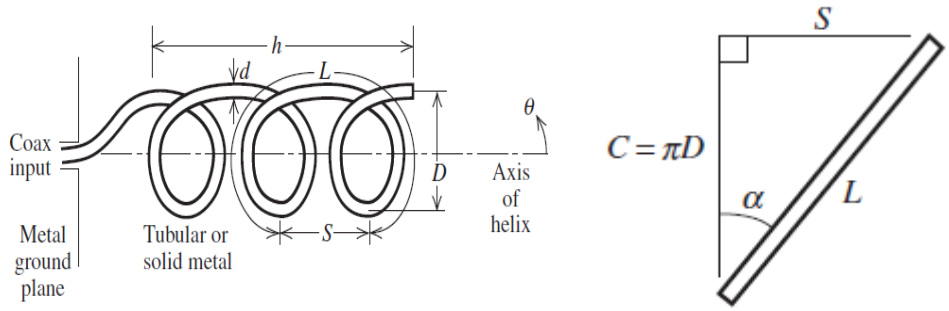


Figure 45. Axial helix antenna geometry. Source: Stutzman and Thiel (2011).

The following variables define the parameters of the helix antenna:

D = Diameter of helix (between centers of coil material)

C = Circumference of the helix $C = \pi D$

S = Vertical separation between turns for the helix antenna S=C/4

N = Number of turns

h = Total height of the antenna H= NS

L = Length of one coil turn $L = \sqrt{C^2 + S^2}$

α = Pitch angle (controls how far the antenna grows along its axis with each turn)

The circumference of the helix antenna is designed to be roughly the same size as the wavelength of the propagating signal. Using the wavelength of the GPS signal, 0.19 meters, as the circumference will result in an antenna diameter of $D = .19 / \pi$ or 60.5 mm, which would easily fit into the payload for the C-UAS shell. Using these dimensions, the operating bandwidth is determined by Stutzman and Thiele by the inequality:

$$\frac{3\lambda}{4} \leq C \leq \frac{4\lambda}{3}$$

This gives the operational range for the antenna between 2103.807 to 1183.547 MHz, which covers both the GPS L1 and L2 frequency bands.

Joseph Bevlacqua is an engineer who has a Ph.D. in antennas and a wide range of experience in their design and applications. On his website www.antenna-theory.com, he argues that the following equation can approximate the gain of a helix antenna.

$$G = \frac{6.2C^2NS}{\lambda^3}$$

Using the predetermined gain of 8.18, a circumference, C, of 0.19 m, and a vertical separation of S=C/4 = 47.5 mm, the required number of turns, N, can now be solved. In this case, N would be 5.27 or approximately 5 turns. The overall height of the antenna, h, can now be found by multiplying the vertical separation between the turns, S, by N to give

a total height of 237 millimeters or 9.33 inches. It is of note that reducing the number of turns or the vertical spacing between them will have the effect of reducing the antenna's gain and therefore increasing the beamwidth.

Axial helix antennas also require a ground plane to serve as a reflecting surface to direct radio waves in a particular direction. This is done by attaching a circular conducting disk with a diameter of at least $\frac{3}{4}\lambda$ or 142.5 mm. A depiction of the antenna with the described parameters is displayed in Figure 46. The antenna is configured to be in the -Z direction to simulate its orientation when suspended from a parachute and radiating towards the surface of the earth.

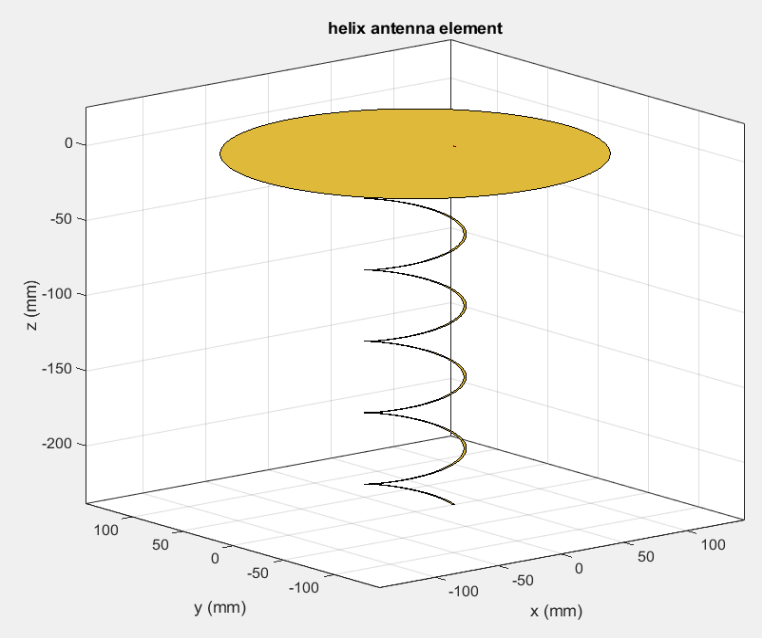


Figure 46. Z-axis helical antenna design with five turns

Figure 47 is a three-dimensional depiction of the theoretical radiation pattern for the antenna. The color scheme on the right corresponds to the relative gain of the antenna radiation field.

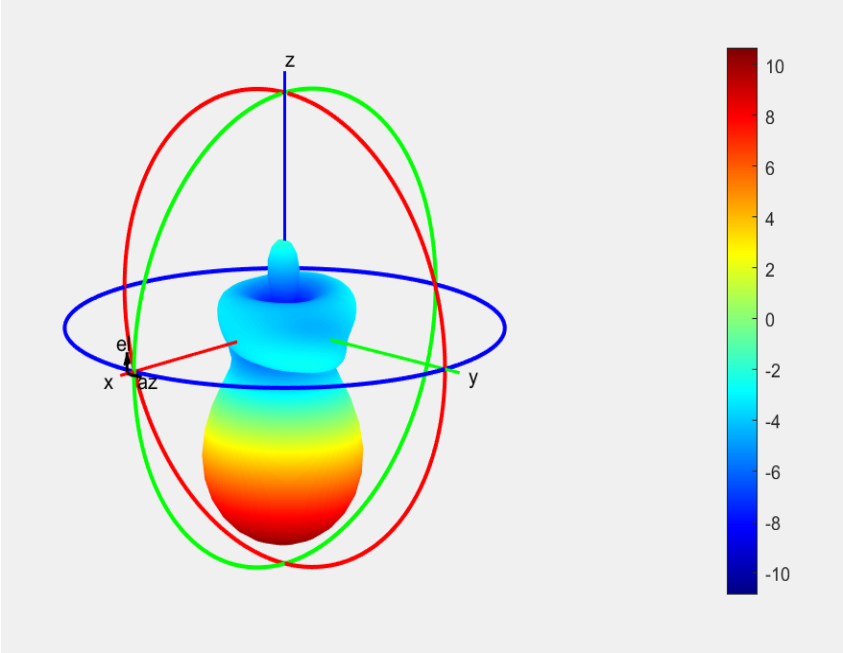


Figure 47. The three-dimensional radiation pattern for five turn axial helix antenna

c. Required Transmission Power

The transmission power required is directly related to the desired J/S. This thesis will focus on determining the power requirements for either causing a loss of GPS signal or the denial of GPS reception. As previously established in Chapter IV, a J/S of 47 would cause a GPS receiver to lose its PNT lock, and a value of 27 would prevent its reception. Additionally, it was determined in Chapter II that the signal strength required for GPS C/A code reception is approximately -160 dBW.

Figure 48 is a depiction of the jamming relationship between the artillery-delivered expendable jammer and the GPS signal against a single UAV receiver. The effect against any number of UAVs operating in a swarm configuration would be identical as long as they fall within the beamwidth of the jammer. In this diagram, the variables d_j and d_s represent the relative distances of the jammer and GPS signal from the UAV. Since the jamming transmitter is within line-of-sight of the UAV receiver, the values of the gain of the receiver in the direction of the jammer and the gain of the receiver can be negated.

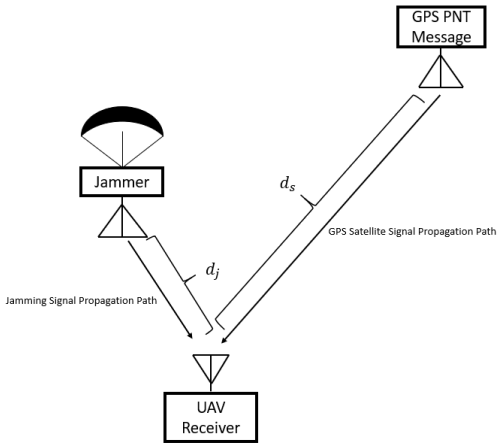


Figure 48. Jamming diagram. Adapted from Adamy (2000).

The required jamming signal power, S_j, at a specific UAV receiver for each of these scenarios can be found by adding the specified J/R to the GPS signal strength. This concept is shown in the following equation:

$$S_j = -160dBW + J/R$$

This equation gives us the values of -113 dBW for navigation signal loss and -133 dBW for navigation signal denial. For this research, the artillery jammer will be designed so that it provides sufficient power from its maximum altitude to cause a swarm of SUAS to lose its navigation lock. Using this performance metric, the jamming to signal strength ratio equation can be simplified by the below equation in order to determine the required transmission power of the jamming payload.

$$47dBw = ERP_j - 160dBw - L_j$$

To solve this equation, the losses due to attenuation for the jamming signal, (L_j), must first be found. This is computed from the following equation.

$$L_j = 32.44 + 20\log(d_j) + 20\log(f)$$

To ensure the effectiveness of the weapon, this scenario assumes that the target UAVs are at the maximum range from the C-UAS payload. Using an initial distance of d_s = 700 meters from the jamming transmitter to the SUAS receiver and a frequency of 1575.43 MHz, the interference signal attenuates 93.28 dBW. By then solving for the effective radiated power of the jammer, it is found that an ERP of -19.7 dBW or 10.65 milliwatts (mW) would be sufficient to cause a UAS to lose its GPS C/A lock from this distance.

Finally, using the equation $ERP_j = P_j + G_j$ with the established ERP of -19.7 dBW and the desired gain, G_j, of 9 dB, the power required for the jammer to transmit, P_r, is determined to be -28.7 dBW or 1.3 mW.

d. Decent Rate

The duration and effective engagement area for RF interference effects is limited by the rate of descent of the parachute-jammer assembly. In his book *Parachute Recovery Systems: Design Manual*, Theo Knacke describes the variables that determine this rate of fall for a circular parachute. He argues that to achieve a steady descent rate V_e, an equilibrium is necessary between the drag of the parachute and the load, D_T, and the weight of the load and the parachute assembly, W_T (Knacke, 1992). In other words, this is accomplished when $D_T = W_T$. Figure 49 is a depiction of these forces.

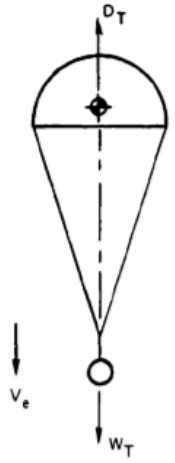


Figure 49. Forces acting on a parachute in steady descent. Source: Knacke (1992).

Knacke states that the equation for the steady-state velocity of descent is found by solving the equation:

$$v_e \simeq \sqrt{\frac{2W_T}{S \cdot C_D \cdot \rho}}$$

In this equation,

v_e = payload descent rate (meters/second)

W_T = mass of the parachute and load (lbs)

C_D = parachute drag coefficient (0.8 for solid round parachute)

S = parachute surface area (ft^2)

p = air density (slugs/ft^3)

To mimic the effects of the illumination shell in the current military inventory, an initial height of burst will be 700 meters. Additionally, the standard rate of fall for an illumination shell is approximately 5 meters/second. This rate allows for approximately 140 seconds of effects over the target area in optimal weather conditions. This research will assume that

the mass and parachute surface area of the C-UAS shell is similar, and therefore the descent rate will be identical. Figure 50 shows the theoretical ground coverage area of such a C-UAS shell as a function of time using a decent rate of 5 meters per second and an initial height of 700 meters above ground level (AGL).

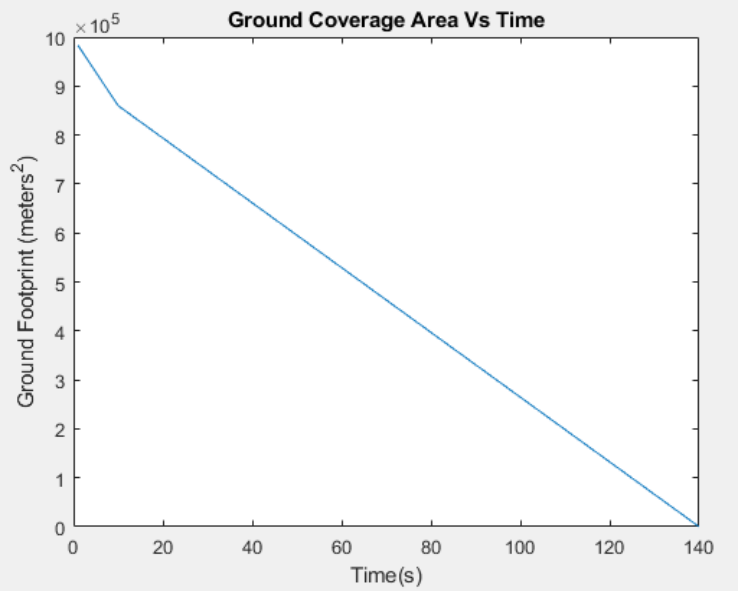


Figure 50. Ground area coverage versus time

Figure 51 is a depiction of the J/R for a stationary target within the main beam of the antenna as a function of time. Due to the nature of RF propagation in free space, this is an exponential relationship. For simplicity, this simulation is done assuming that the target SUAS swarm is stationary and relatively close to the surface. In reality, the swarm would be at any altitude from 0 to 700 meters AGL and have a specific velocity.

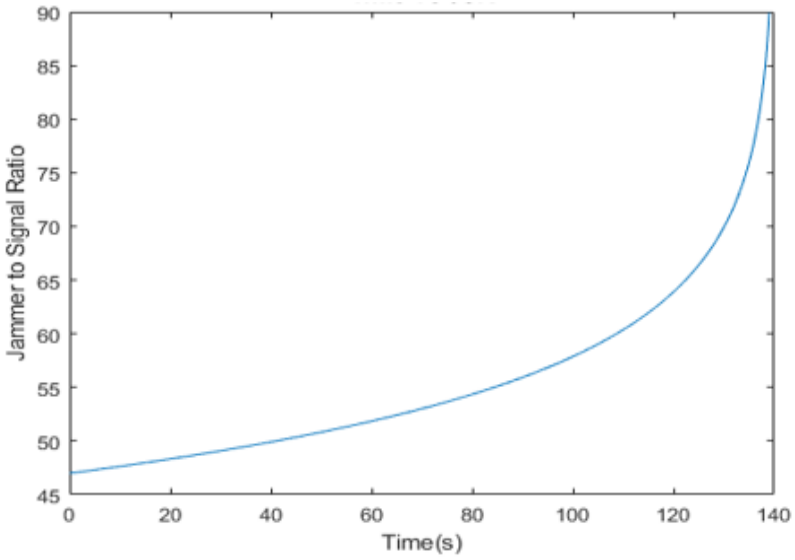


Figure 51. J/R as a function of time for a C-UAS shell

B. ARTILLERY-DELIVERED JAMMING SIMULATION

CloudRF is an RF propagation modeling tool that was developed by Alex Farrant, who is a former telecommunications specialist for the Royal Marines (Farrant, 2019). By specifying antenna and receiver parameters, it is possible with this software to design and test coverage areas for signal reception. An added interface with the Google Earth application gives the user the ability to visualize the signal models and how they are impacted by surrounding terrain. For this research, this tool is used to create a contour map of the jamming signal strength delivered by the artillery shell payload at different elevations along its descent.

Figures 52, 53, and 54 models the signal strength density for the parachute delivered jammer over a relatively flat surface and optimal atmospheric conditions. The rainbow scale on the left correlates colors to the signal strength in decibel-milliwatts (dBm) received by a notional target on the surface directly below the transmitter. Red indicates a more robust signal, while blue indicates a weaker signal. The overlays measure the effective area that would receive signal strengths corresponding to a J/S of 47 (-83 dBm) and 27 (-103 dBm), respectively. These distances were measured at jammer altitudes of 700, 350, and

100 meters. These measurements correspond to times of 0, 70, and 120 seconds, respectively, after the jammer has begun transmitting.

As predicted, the effective jamming coverage area decreases as the jammer descends towards the surface. At the initial altitude of 700 meters, the area impacted by the higher J/S is a circle with a radius of 1,090 meters, and the entire GPS denial zone has a radius of approximately 4,960 meters. Midway through the descent of the jammer, the GPS lock loss radius reduces to 870 meters, and the GPS denial zone is now 3,300 meters. Even at 100 meters AGL, the signal strength is still powerful enough to create a GPS lock loss area of 600 meters and a denial zone of 1,784 meters. It is important to note that these values would change due to different atmospheric conditions and ground terrain that would contribute to the attenuation of the signal.

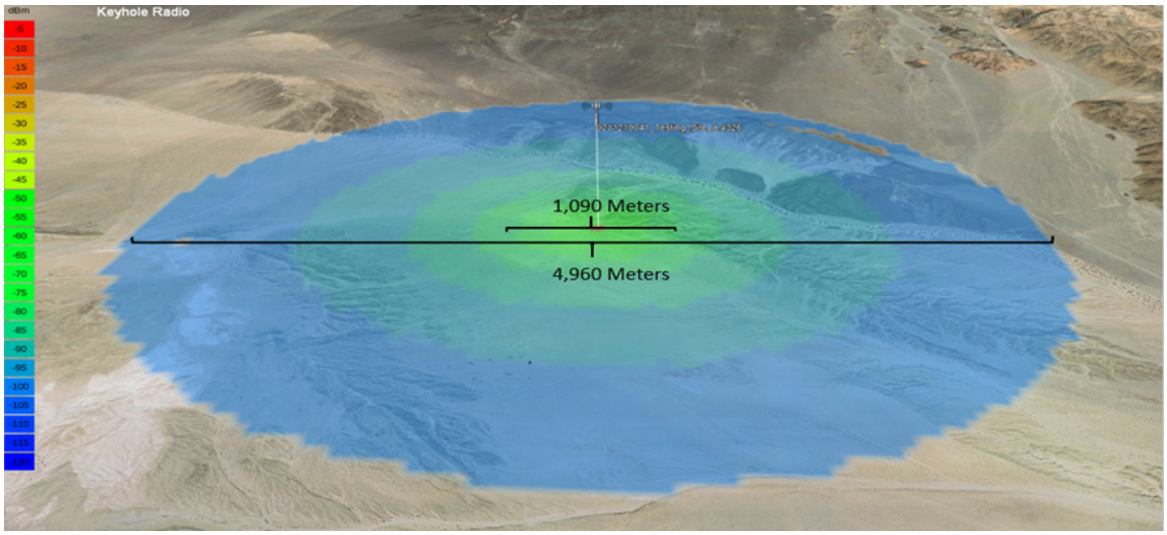


Figure 52. 700-meter AGL signal strength density

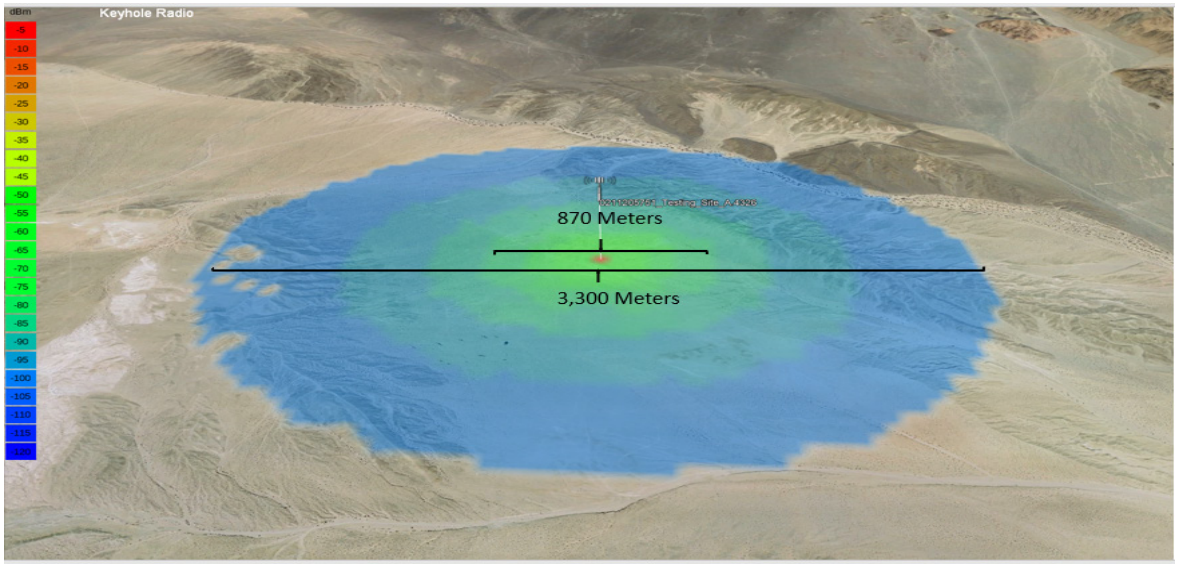


Figure 53. 350-meter AGL signal strength density

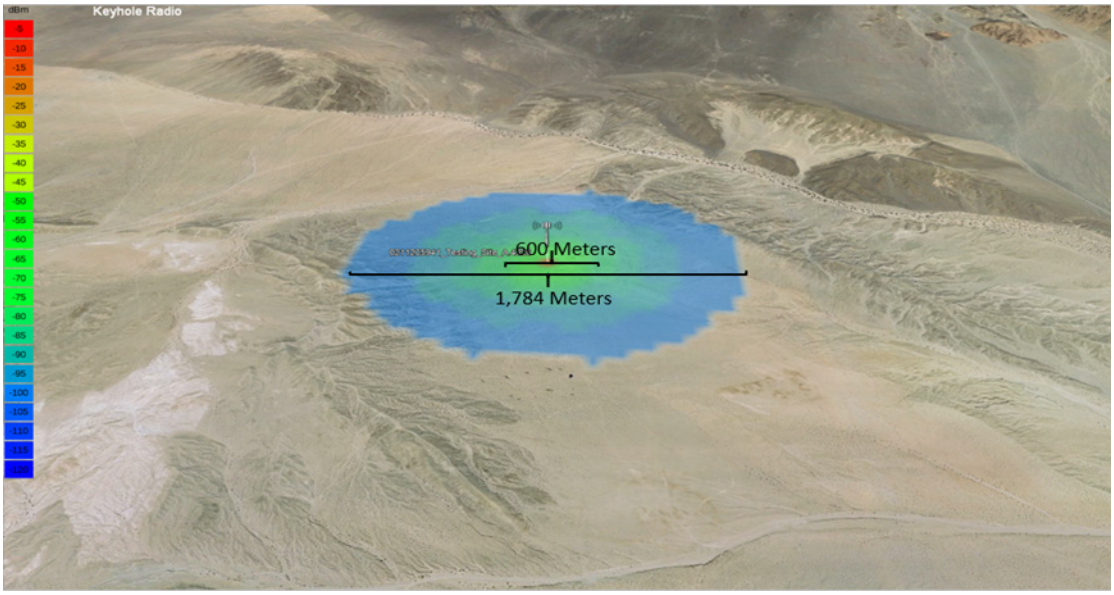


Figure 54. 100-meter AGL signal strength density

C. CHAPTER CONCLUSION

The essential design elements for this invention are relatively straightforward and are easily constructed using existing components of other types of base ejecting projectiles. The jamming payload itself is not a novel concept. However, it is the author's opinion that the tailoring a portable SDR to create a parachute deployed C-UAS device is. By identifying a specific frequency to target, the performance requirements of the jammer is easily computed since J/S ratios are well known, and the propagation of the signals will obey the laws of physics. Of note, the calculations presented in this chapter do not encompass the specifics for the internal signal losses incurred within the entire system. Still, they do describe the total power that must be transmitted through the antenna to disrupt a GPS signal. Furthermore, the CloudRF simulations prove that it is feasible to develop this projectile that can execute a NAVWAR effect within a designated time and space window.

VI. CONCLUSIONS AND RECOMMENDATIONS

SUAS swarms are not an immediate threat to our ground forces, but the pace of the technological advancements of these devices clearly shows that they may be a threat int he future. To be prepared for this emerging threat the USMC and the DOD must invest in the development of an indirect fire capability like the one presented in this thesis. Such a system would augment currently fielded systems to build a more robust defense-in-depth that can engage swarms at greater distances and before they can deliver harmful effects.

The integration of multiple systems is needed for a C-UAS defense-in-depth that is part of an overarching air-defense strategy. For the USMC, this strategy is currently comprised of ground-based, vehicle-mounted, and handheld C-UAS systems. Adding an additional defensive layer with effects provided by cannon artillery is a concept that extends this concept beyond the range of current systems without line-of-sight limitations. Furthermore, the ground-based air defense is a mission that can easily be adopted by the USMC field artillery and is a natural progression of its evolution in support of combat operations.

It is feasible to develop a C-UAS artillery shell that can be integrated into current fire support procedures. This can be done using an existing concept for cargo-carrying projectiles that can deliver effects into hostile environments that are outside of the range of conventional munitions. By modifying the projectile's cargo to hold an expendable jammer and parachute, the effects can be non-kinetic, to promote drone recovery and be limited to the desired engagement area for a set duration.

The shell design in Chapter V targets the UAS navigation signal as its primary target. The antenna parameters and transmission power required for an aerial delivered jamming payload were developed to show how the NAVWAR concept could be applied to a C-UAS shell. This was done due to the prior research which highlighted the vulnerabilities of UAS that rely on GNSS frequencies for autonomous modes of operation. In theory, the jamming payload of the shell could be tailored to any frequency by using the versatility of an SDR. The transmission power and antenna characteristics could easily be

altered to match the desired target command and control frequency or data channels if desired.

The work in this thesis is only a small part of the research required to build an indirect fire weapon with the capabilities to disrupt drone swarms. The future work needed to develop this concept fully can be separated into the categories of prototype development, testing, and employment considerations.

Physical testing of a prototype payload like the one described in Chapter IV is necessary in order to refine the data and find the optimal jamming power densities and rate of fall for the payload. This could be done first in a laboratory setting against a tethered UAV with the jamming transmitter power set to a level to simulate various distances. The time it takes for the UAV to lose its GPS signal or detect the spoofing signal at different power levels would be measured. This data would provide more detailed information to influence the desired rate of fall for the payload.

Testing this system against a swarm of SUASs would then be necessary to determine the effects of GPS signal disruption against multiple devices operating in close proximity. Dropping the prototype parachute and payload assembly from a set height over a swarm would confirm the laboratory results and provide a better understanding of the swarm response. This can be done with swarms operating with different types of command and control architectures. Additional testing could be done to demonstrate the effectiveness of varying spoofing tactics against SUAS swarms. Another potential strategy could be the firing of multiple rounds that would transmit spoofed coordinates designed to trick a SUAS swarm into a specific area. This technique would trap the swarm in a designated area away from ground troops, perhaps even back over adversary forces, where they would circle until their batteries are exhausted.

This weapon system also requires more research concerning its tactical employment. Similar to kinetic weapons, the deconfliction of the effects would be a primary concern to avoid the spillage of the jamming footprint into an adjacent battlespace without prior coordination. The authority for influencing the EM spectrum would also need to be reconsidered. To maximize the responsiveness of this kind of weapon, the approval

for EM spectrum jamming must be established at the proper level to facilitate timely effects on the target.

The application of the artillery C-UAS shell in a combat environment would also need to be researched in terms of how it would be employed as part of an integrated fire support plan. Forward observers would need to be trained on the detection and identification of SUAS to include the use of new sensors that monitor the EM spectrum. Furthermore, the method of attack would need to be adjusted by these observers to ensure that the effects cover the required area and are sufficient to stop a swarm.

These shells could be applied in support of defensive or offensive operations, and techniques, tactics, and procedures (TTPs) would need to be established to support different phases of operations. The integrated air-defense strategy that was outlined in Chapter II is a reactive employment method to facilitate force protection. Offensively, these shells could also be used to shape the battlefield prior to an assault proactively. Options could include the creation of SUAS denial zones by seeding key areas with jamming shells or launching such shells over enemy positions to prevent an initial launch.

In conclusion, this thesis has identified the way forward to proactively integrate a low-cost counter to SUAS swarms into the USMC and other services. The development of this C-UAS shell is based on existing technologies with proven effectiveness. Furthermore, it leverages an existing platform for its delivery that has an established role within the fire support framework and a pre-existing support structure. The role of artillery in combat will not change, but the threat faced by our maneuver elements continues to evolve. It is imperative that this novel solution to the SUAS swarming tactics be implemented or else USMC units are likely to be limited to engaging the SUAS swarm threat at a reduced range and an unnecessary level of risk.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Adamy, D. (2000). *EW 101*. Norwood: Artech House.

Akopian, D., & Soghoyan, A. (2013). A LabVIEW-based fast prototyping software defined GPS receiver platform. *2013 IEEE Global Conference on Signal and Information Processing*, 1230–1233. Retrieved from https://doi.org/10.1109/GlobalSIP.2013.6737130

Berger, D. (2019). *38th Commandant's planning guidance*. Retrieved from https://www.hqmc.marines.mil/Portals/142/Docs/%2038th%20Commandant%27s%20Planning%20Guidance_2019.pdf?ver=2019-07-16-200152-700

Bevelacqua, J. (n.d). *Helix antenna*. Antenna-Theory. Retrieved from http://www.antenna-theory.com/antennas/travelling/helix.php

Brown, A., Redd, J., & Hutton, M. (2012). Simulating GPS signals: It doesn't have to be expensive. *GPS World*. Retrieved from https://www.gpsworld.com/simulating-gps-signals/

Bailey, J. (2004). *Field artillery and firepower*. Naval Institute Press.

Battelle Memorial Institute. (2019). *Battelle DroneDefender® counter-UAS device*. Retrieved December 11, 2019, from https://www.battelle.org/government-offerings/national-security/payloads-platforms-controls/counter-UAS-technologies/dronedefender

Baxter, L. J. (1998). Meeting the future: State of the field artillery 1998. *Field Artillery.* ProQuest.

Campion, M., Ranganathan, P., & Faruque, S. (2019). UAV swarm communication and control architectures: A review. *Journal of Unmanned Vehicle Systems*, *7*(2), 93–106. Retrieved from https://doi.org/10.1139/juvs-2018-0009

Chung, H., Clement, M., Day, M., Jones, K., Davis, D., Jones, M. (2016). Live-fly, large-scale field experimentation for large numbers of fixed-wing UAVs. Calhoun.

Crescentvenus. (2020). *Crescentvenus/WALB*. Github. Retrieved from https://github.com/crescentvenus/WALB

Dean, C.E. (1997). *Resupply projectile* (U.S. Patent No. 5,684,267). U.S. Patent and Trademark Office. Retrieved from https://patents.google.com/patent/US5684267A/en?q=resupply+projectile&inventor=dean&scholar

Department of the Army. (1994). *Army ammunition data sheets* (TM 43–001-28) Retrieved from https://bulletpicker.com/pdf/TM%2043-0001-28,%20Artillery%20Ammunition.pdf#page=326

Department of the Army. (2008). *Commander's appreciation and campaign design*. (TraDoc Pamphlet, 525–5-500). Retrieved from http://indianstrategicknowledgeonline.com/web/p525-5-500.pdf

Department of the Army. (2014). Howitzer, medium, towed: 155–mm, M777 (NSN 1025–01–445–0991). (TM 9–1095-215-10).

Department of Defense (2018). *Positioning, navigation, and timing (PNT) and navigation warfare (NAVWAR).* (DOD Instruction 4650.8). Retrieved from https://fas.org/irp/doddir/dod/i4650_08.pdf

Department of Defense. (2011). *Unmanned aircraft system airspace integration plan*. Washington, DC. Retrieved from https://www.hsdl.org/?abstract&did=723337

Department of Homeland Security. (2019) *Counter-unmanned aircraft systems technology guide*. National Security Technical Laboratory. Retrieved from https://www.dhs.gov/publication/st-c-uas-technology-guide

DJI. (2020). *Phantom 4 Pro specs.* DJI. Retrieved February 25, 2020, from https://www.dji.com/phantom-4-pro

Dozier, K., & Baldor, L. C. (2011). Iran shows off lost U.S. Drone capture a setback for surveillance of nuclear program. *Pittsburgh Post – Gazette.* Retrieved from https://www.post-gazette.com/news/world/2011/12/09/Iran-shows-off-lost-U-S-drone/stories/201112090157

Ettus Research. (2020). *Ettus Research: Products.* Retrieved February 24, 2020, from https://www.ettus.com/products/.

Farrant, A. (2019). *CloudRF API.* [Computer Software]. Farrant Counseling Ltd.

Frieden, D., & Bender, G. (1985). *Principles of naval weapons systems*. Annapolis, MD: Naval Institute Press.

Friis, H. (1946). A note on a simple transmission formula. *Proceedings of the IRE, 34(5), 254–256*. Retrieved from https://doi.org/10.1109/JRPROC.1946.234568

Gartenberg, C. (2016, July 28). This Pokémon Go GPS hack is the most impressive yet. *The Verge*. Retrieved from https://www.theverge.com/circuitbreaker/2016/7/28/12311290/pokemon-go-cheat-gps-signal-spoofing.

GISGeography. (2016). *Trilateration vs triangulation – How GPS receivers work*. GISgeography. Retrieved February 24, 2020 from https://gisgeography.com/trilateration-triangulation-gps/

Godson, R., & Wirtz, J. (2000). Strategic denial and deception. *International Journal of Intelligence and Counter Intelligence*, Volume 13, Number 4. Retrieved from https://calhoun.nps.edu/bitstream/handle/10945/43266/Wirtz_Strategic_Denial_and_Deception2013-11-20.pdf?sequence=1&isAllowed=y

Great Scott Gadgets. (2016). *HackRF.* Great Scott Gadgets. Retrieved January 14, 2020, from https://greatscottgadgets.com/hackrf/

Halliday, D., Resnick, R. & Walker, J. (2014) *Fundamentals of physics* (10th ed.). John Wiley & Sons, Inc.

Hambling, D. (2018). Swarm of drones attacks airbase. *New Scientist*. Retrieved from https://doi.org/10.1016/S0262-4079(18)30110-6

Herring, T. (2014). *Lecture 7* [Class notes for 12.540 Principles of the global positioning system]. Geodesy and Geodynamics Department, Massachusetts Institute of Technology. http://geoweb.mit.edu/~tah/12.540/

Hindle, P. (2018). Drone detection and counter measures take the world stage. *Microwave Journal*, 6–18. ProQuest.

Horton, E., & Ranganathan, P. (2018). Development of a GPS spoofing apparatus to attack a DJI Matrice 100 Quadcopter. *The Journal of Global Positioning Systems*, *16*(1), 9. Retrieved from https://doi.org/10.1186/s41445-018-0018-3

Imperial War Museums. (2020). *Shell message 7.5 cm trench mortar.* IWM Collections. Retrieved from https://www.iwm.org.uk/collections/item/object/30023685

Jackson Labs. (n.d) *CLAW simulator spec sheet*. Retrieved January 16, 2020, from http://www.jackson-labs.com/assets/uploads/main/CLAW_Simulator_specsheet.pdf

Joint Air Power Competence Centre. (2010). *Strategic concept of employment for unmanned aircraft systems in NATO.* Retrieved from https://www.japcc.org/portfolio/strategic-concept-of-employment-for-unmanned-aircraft-systems-in-nato/

Joint Chiefs of Staff. (2010). *Department of defense dictionary of military and associated terms*. Retrieved from http://www.dtic.mil/docs/citations/ADA536504

Joint Chiefs of Staff. (2012). *Electronic warfare*. (JP 3-13.1). Retrieved from https://info.publicintelligence.net/JCS-EW.pdf

Joint Chiefs of Staff. (2014). *Joint airspace control*. (JP-3-52). Retrieved from https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_52.pdf

Joint Chiefs of Staff. (2018). *Space operations.* (JP 3-14). Retrieved from https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_14.pdf

Jones, M. (2011). The civilian battlefield. Protecting GNSS receivers from interference and jamming. *Inside GNSS.* Retrieved from https://insidegnss.com/auto/marapr11-Jones.pdf

Freedberg, S. (2015). Russian drone threat: Army seeks Ukraine lessons. *Breaking Defense*. Retrieved from https://breakingdefense.com/2015/10/russian-drone-threat-army-seeks-ukraine-lessons/

Kerns, A., Shepard, D., Bhatti, J., & Humphreys, T. (2014). Unmanned aircraft capture and control via GPS spoofing. *Journal of Field Robotics*, *31*(4), 617–636. https://doi.org/10.1002/rob.21513

Kinard, J. (2007). *Artillery: An illustrated history of its impact*. Santa Barbara, CA: ABC-CLIO.

Knacke, T. (1992). *Parachute recovery systems: Design manual* (1st ed.). Santa Barbara, CA: Para Pub.

Knowles, J., & Swedeen, H. (2019). Technology survey: A sampling of counter-UAS systems. *Journal of Electronic Defense*, *42*(5). ProQuest.

LaGrone, S. (2018). Marines forward-deploy portable drone-killing system. *USNI News* Retrieved February 21, 2020, from https://news.usni.org/2018/06/04/marines-forward-deploy-portable-drone-killing-system.

Lele, A., & Mishra, A. (2009). Aerial terrorism and the threat from unmanned aerial vehicles. *Journal of Defense Studies*. Retrieved from https://idsa.in/system/files/jds_3_3_alele_amishra.pdf

Martins DaSilva, D.A. (2017). *GPS jamming and spoofing using software defined radio* [Doctoral Dissertation, University Institute of Lisbon]. Retrieved from https://repositorio.iscte-iul.pt/handle/10071/15244

McFarland, M. (2017). Slaughterbots film shows potential horrors of killer drones. *CNN Business*. Retrieved from https://money.cnn.com/2017/11/14/technology/autonomous-weapons-ban-ai/index.html

Mena. (2019). Al Azhar condemns drone attack on Saudi oil pumping stations. *Egypt Today*. Retrieved from https://www.egypttoday.com/Article/1/70424/Al-Azhar-condemns-drone-attack-on-Saudi-oil-pumping-stations

Mitch, R., Dougherty, R., Psiaki, M., Powell, S., O'Hanlon, B., Bhatti, J., & Humphreys, T. (2012). Know your enemy: signal characteristics of civil GPS jammers. *GPS World*, *23*(1), 64–71.

National Instruments (2019). *GPS receiver testing.* Retrieved from https://www.ni.com/en-us/innovations/white-papers/08/gps-receiver-testing.html

Naval Air Systems Command & Naval Warfare Center Weapons Division, (1993). *EW and radar systems engineering handbook*. (NAWCWPNS TS 92–78). Information and Electronic Warfare Directorate.

Newell, M. (2011). Three new munitions from picatinny light up the night sky for warfighters. *USAASC*. Retrieved December 9, 2019, from https://asc.army.mil/web/three-new-munitions-from-picatinny-light-up-night-sky-for-warfighter

Nuand LLC. (2020). *BladeRF.* Retrieved February 24, 2020 from https://www.nuand.com/bladerf-1/

Palik, M., & Nagy, M. (2019). *Brief history of UAV development*. Retrieved from https://doi.org/10.32560/rk.2019.1.13

Palmer, T., & Geis, J. (2017). Defeating small civilian unmanned aerial systems to maintain air superiority. *Air & Space Power Journal*, *31*(2), 102–118. ProQuest.

Parkinson, B., Spilker, J., Axelrad, P., & Enge, P. (1996). *The global positioning system theory and applications. Volume I*. American Institute of Aeronautics and Astronautics.

Parlin, K. (2017). *Jamming of spread spectrum communications used in UAV remote control systems.* [Master's thesis, Tallinn University of Technology]. https://pdfs.semanticscholar.org/0dc9/6b76366bcee1029f67a44d858b5c68315c92.pdf

Parsons, J. (2019, February 18) Terrifying Russian suicide drone is the "Kalashnikov of the skies." *Metro News*. Retrieved January 14, 2020, from https://metro.co.uk/2019/02/18/terrifying-russian-suicide-drone-kalashnikov-skies-8653466/

Payne, C. M. (Ed.). (2006). *Principles of naval weapon systems*. Naval Institute Press.

Phone Jammer. (2020). *Portable jammer.* Jammers.Store. Retrieved February 20, 2020, from https://jammers.store/portable-jammer-c-18.html?lg=g

Pomerleau, M. (2017). In drones, ISIS has its own tactical air force. *C4ISRNET*. Retrieved from https://www.c4isrnet.com/digital-show-dailies/modern-day-marine/2017/09/21/in-drones-isis-has-its-own-tactical-air-force/

Racelogic Ltd. (2019.). *The LabSat product range.* Retrieved February 24, 2020, from https://www.labsat.co.uk/index.php/en/

Rawnsley, A. (2011). Iran's alleged drone hack: Tough, but possible. *Wired*. Retrieved from https://www.wired.com/2011/12/iran-drone-hack-gps/

Requested Decreases Disapproved. (1995). *Defense Daily*. ProQuest.

Rohde and Shwarz GmbH & Co KG. (2015). *Protecting the sky: Signal monitoring of radio controlled civilian unmanned aerial vehicles and possible countermeasures* (Report number 10.2015-V02.00) Retrieved from http://www.rohde-schwarz-usa.com/rs/324-UVH-477/images/Drone_Monitoring_Whitepaper.pdf

Richardson, D. (1998). GPS in the shadows of NAVWAR. *Armada International*, *22*(4), 22–26. ProQuest.

Rochus, W. (2000). *UAV data-links: Tasks, types, technologies and examples*. Retrieved from http://www.dtic.mil/docs/citations/ADP010757

Russel, J.R. (2019). *CUAS security performance metrics and requirements* [Presentation]. Counter-UAS USA, Arlington, VA.

Sathyamoorthy, D., Muhammad, M., Bakthir, N., Abdul, S., Shafii, S., Ismail, A., … Yusoff, M. (2012). Evaluation of global positioning system (GPS) performance during simplistic GPS spoofing attacks. *In Defence S&T Technical Bulletin, 5, 99–113*. ProQuest.

Samel-90 PLC.(2020). *Artillery jammers*. Retrieved February 29, 2020, from https://www.samel90.com/en/products/category/jammer-solutions-military-equipment-surveillance-systems/artillery-jammers

Schleher, D. (1999). *Electronic warfare in the information age*. Boston: Artech House.

Schwartz, M. (2011). Iran hacked GPS signals to capture U.S. drone. *InformationWeek Online*. ProQuest.

Shepard, D., Bhatti, J., & Humphreys, T. (2012). Drone hack: spoofing attack demonstration on a civilian unmanned aerial vehicle. *GPS World*, *23*(8), 30–33.

Sims, A. (2018). The rising drone threat from terrorists. *Georgetown Journal of International Affairs*, *19*(1), 97–107. Retrieved from https://doi.org/10.1353/gia.2018.0012

Slavin, E. (2017). Pentagon unveils Perdix micro-drone swarm. *TCA Regional News: Chicago*. ProQuest.

Sly, L. (2019, February 23). The Kalashnikov assault rifle changed the world. Now there's a Kalashnikov drone. *The Washington Post.* Retrieved from https://www.washingtonpost.com/world/2019/02/23/kalashnikov-assault-rifle-changed-world-now-theres-kalashnikov-kamikaze-drone/

Smith, S. (2018). Venezuela detains six after failed drone attack on president. *The Globe and Mail*. ProQuest.

Stanley, W., & Jeffords, J. (2006). *Electronic communications: Principles and systems*. Thomson Delmar Learning.

Stiles, J. (2017). Drone wars are coming. *United States Naval Institute. Proceedings*, *143*(7), 44–47. ProQuest.

Stutzman, W., & Thiele, G. (2013). *Antenna theory and design* (3rd ed.). New York: J. Wiley.

Swanbeck, D. (2018). [Light Marine air-ground integrated defense system (LMADIS)]. Defense Visual Information Distribution Service. Retrieved from https://www.dvidshub.net/image/4912157/realistic-urban-training-ace-support

Taylor, R. R., Bendowski, M. A., & McFeaters, R. C. (1997). *Demonstrated delivery/employment systems for unattended ground sensors.* Retrieved from https://doi.org/10.1117/12.280651

Tippenhauer, N., Pöpper, C., Rasmussen, K., & Capkun, S. (2011). On the requirements for successful GPS spoofing attacks. *Proceedings of the 18th ACM Conference on Computer and Communications Security*, 75–86. Retrieved from https://doi.org/10.1145/2046707.2046719

U.S. Government Accountability Office. (2018). Small unmanned aircraft systems. (GAO-18-110). Retrieved from https://www.gao.gov/products/gao-18-110

U.S. Marine Corps. (2016). *Tactics, techniques, and procedures for the field artillery manual cannon gunnery* (MCRP 3–10E.4). Retrieved from https://www.marines.mil/portals/1/Publications/MCRP%203-10E.4%20Formerly%20MCWP%203-16.4.pdf?ver=2017-09-26-101122-060

U.S. Marine Corps. (2018a). *Unmanned aircraft systems operations*. (MCRP 3–20.5) Retrieved from https://www.marines.mil/Portals/1/Publications/MCRP%203-20.5.pdf?ver=2018-11-15-090158-420

U.S. Marine Corps. (2018b) *Antiair warfare* (MCTP 3-20C). Retrieved from https://www.marines.mil/portals/1/Publications/MCTP%203-20C%20GN.pdf?ver=2019-01-31-114859-677

U.S. Marine Corps. (2018c). *Artillery operations* (MCTP 3-10E). Retrieved from https://www.marines.mil/Portals/1/Publications/MCTP%203-10E%20GN.pdf?ver=2020-02-12-115230-233

U.S. Marine Corps PEO LS. (2019). *Program executive officer land systems advanced technology investment plan update 2019*. Retrieved February 20, 2020, from https://www.marcorsyscom.marines.mil/Portals/105/PELandSystem/ATIP/2019_ATIP.pdf

Valavanis, K., & Vachtsevanos, G. (2015). *Handbook of unmanned aerial vehicles*. Springer Netherlands. Retrieved from https://doi.org/10.1007/978-90-481-9707-1

Wang K., Chen S. and Pan A. (2015). Time and position spoofing with open source projects. *BlackHat Europe 2015*. Semantic Scholar.

Yuniati,Y., Ulvan, A., & Hasim, S. (2019). Signal analysis of remote control (RC) UAV used software defined radio (SDR) HackRF One. Semantic Scholar.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California