2022-06

REDESIGNING THE COUNTER UNMANNED SYSTEMS ARCHITECTURE

Thiessen, Christian M.

Monterey, CA; Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

REDESIGNING THE COUNTER UNMANNED SYSTEMS ARCHITECTURE

by

Christian M. Thiessen

June 2022

Thesis Advisor:	Britta Hale
Co-Advisor:	Raymond R. Buettner Jr.
Second Readers:	Leo J. Blanken
	Douglas L. Van Bossuyt

THIS PAGE INTENTIONALLY LEFT BLANK

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

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2022	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
REDESIGNING THE COUNTER UNMANNED SYSTEMS ARCHITECTURE

5. FUNDING NUMBERS
QSE02

6. AUTHOR(S) Christian M. Thiessen

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)
DASN-OE, Washington, DC, 20310

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)

When the Islamic State used Unmanned Aerial Vehicles (UAV) to target coalition forces in 2014, the use of UAVs rapidly expanded, giving weak states and non-state actors an asymmetric advantage over their technologically superior foes. This asymmetry led the Department of Defense (DOD) and the Department of Homeland Security (DHS) to spend vast sums of money on counter-unmanned aircraft systems (C-UAS). Despite the market density, many C-UAS technologies use expensive, bulky, and high-power-consuming electronic attack methods for ground-to-air interdiction. This thesis outlines the current technology used for C-UAS and proposes a defense-in-depth framework using airborne C-UAS patrols outfitted with cyber-attack capabilities. Using aerial interdiction, this thesis develops a novel C-UAS device called the Detachable Drone Hijacker—a low-size, weight, and power C-UAS device designed to deliver cyber-attacks against commercial UAVs using the IEEE 802.11 wireless communication specification. The experimentation results show that the Detachable Drone Hijacker, which weighs 400 grams, consumes one Watt of power, and costs $250, can interdict adversarial UAVs with no unintended collateral damage. This thesis recommends that the DOD and DHS incorporates aerial interdiction to support its C-UAS defense-in-depth, using technologies similar to the Detachable Drone Hijacker.

14. SUBJECT TERMS
unmanned aircraft system, UAS, counter-unmanned aircraft systems, C-UAS, defense-in-depth, non-kinetic electronic warfare, electronic attack, broadband noise jamming, RF jammer, cyber-attacks, denial of service, DoS, energy consumption, low-SWaP, aerial interdiction, Department of Homeland Security, DHS

15. NUMBER OF PAGES
159

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.

REDESIGNING THE COUNTER UNMANNED SYSTEMS ARCHITECTURE

Christian M. Thiessen
Captain, United States Marine Corps
BS, San Diego State University, 2016

Submitted in partial fulfillment of the
requirements for the degrees of

MASTER OF SCIENCE IN INFORMATION WARFARE SYSTEMS ENGINEERING

and

MASTER OF SCIENCE IN APPLIED DESIGN FOR INNOVATION

from the

NAVAL POSTGRADUATE SCHOOL
June 2022

Approved by: Britta Hale
Advisor

Raymond R. Buettner Jr.
Co-Advisor

Leo J. Blanken
Second Reader

Douglas L. Van Bossuyt
Second Reader

Alex Bordetsky
Chair, Department of Information Sciences

Carter Malkasian
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

When the Islamic State used Unmanned Aerial Vehicles (UAV) to target coalition forces in 2014, the use of UAVs rapidly expanded, giving weak states and non-state actors an asymmetric advantage over their technologically superior foes. This asymmetry led the Department of Defense (DOD) and the Department of Homeland Security (DHS) to spend vast sums of money on counter-unmanned aircraft systems (C-UAS). Despite the market density, many C-UAS technologies use expensive, bulky, and high-power-consuming electronic attack methods for ground-to-air interdiction. This thesis outlines the current technology used for C-UAS and proposes a defense-in-depth framework using airborne C-UAS patrols outfitted with cyber-attack capabilities. Using aerial interdiction, this thesis develops a novel C-UAS device called the Detachable Drone Hijacker—a low-size, weight, and power C-UAS device designed to deliver cyber-attacks against commercial UAVs using the IEEE 802.11 wireless communication specification. The experimentation results show that the Detachable Drone Hijacker, which weighs 400 grams, consumes one Watt of power, and costs $250, can interdict adversarial UAVs with no unintended collateral damage. This thesis recommends that the DOD and DHS incorporates aerial interdiction to support its C-UAS defense-in-depth, using technologies similar to the Detachable Drone Hijacker.

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

List of Figures

List of Tables

List of Acronyms and Abbreviations

ACK	acknowledge
AJ	anti-jam
BBN	broadband noise
CAS	close air support
CLaWS	Compact Laser Weapons System
CONOPS	concept of operations
C-UAS	counter-unmanned aircraft systems
DDH	Detachable Drone Hijacker
DDoS	distributed denial of service
DoS	denial of service
DHS	Department of Homeland Security
DOD	Department of Defense
DSSS	direct sequence spread spectrum
EIRP	effective isotropically radiated power
EO/IR	electro-optical/infrared
EM	electromagnetic
ESSID	extended service set identifier
EW	electronic warfare
FHSS	frequency hopping spread spectrum

FPGA field programmable gate arrays

GCS ground control station

GNSS global navigation satellite system

GPU graphical processing units

GUI graphical user interface

IADS integrated air defense system

IED improvised explosive device

IEEE Institute of Electrical and Electronics Engineers

IoT Internet of Things

IP Internet protocol

ISIS Islamic State of Iraq and Syria

ISM Industrial, Scientific, and Medical

ISR intelligence, surveillance, and reconnaissance

JCS Joint Chiefs of Staff

JSR jam-to-signal ratio

KCI Key Compromise Impersonation

LPD low-probability of detection

LPI low-probability of intercept

LPE low-probability of exploitation

MAC media access control

MADIS Marine Air Defense Integrated System

MCWP Marine Corps warfighting publication

MITM man-in-the-middle

NBN narrow band noise

NIC network interface cards

OSI Open Systems Interconnection

OUI organizationally unique identifier

PBN partial band noise

RCS radar cross section

RF radio frequency

SAM surface-to-air missile

SDR software defined radios

SNR signal-to-noise ratio

sUAS small unmanned aircraft system

SWaP size, weight, and power

SYN synchronize

TCP Transmission Control Protocol

TLS Transport Layer Security

TTP tactics, techniques and procedures

UAS unmanned aircraft systems

UAV unmanned aerial vehicles

UDP user datagram protocol

USMC U.S. Marine Corps

VNC virtual network computing

WPA WiFi Protected Access

WWI World War I

Executive Summary

This work makes the case that the current U.S. framework for countering unmanned systems is insufficient because it lacks the robustness needed to thwart a multi-pronged attack from an adversarial group. Because of the technological limitations required to respond to high-flying UAVs, terrestrial surface-to-air missiles and other ground-based counter-unmanned aircraft system (C-UAS) technologies are flawed if used as stand-alone systems. Conversely, a networked squadron of UAVs designed for aerial interdiction, despite their own technological complications, presents a novel way to counter the adversarial UAVs.

This thesis begins by identifying the C-UAS technologies currently in use by the Department of Defense (DOD) and the Department of Homeland Security (DHS). Then, this thesis discusses the radio frequency (RF) jamming techniques used to disrupt digital communications links and the communication protocol vulnerabilities that can be exploited with cyber-attacks. Next, this thesis creates a theoretical framework for developing low-size, weight, and power (SWaP) cyber-attack devices that can be attached to a host-UAV. Using the knowledge gained from modern defensive operations and aerial interdiction, this thesis illustrates UAV-to-UAV interdiction through two hypothetical scenarios where a hydroelectric power facility is attacked by an insurgent group's unmanned systems.

Finally, this thesis conducted three separate experiments to develop a UAV-to-UAV interdiction capability called the *Detachable Drone Hijacker*. The *Detachable Drone Hijacker* was built from a Raspberry Pi 4 Model B, an Alfa AWUS036ACH wireless network card, and (2) 18650 Batteries and it was set up for remote access using a virtual network computing (VNC) connection [1]. Three commercial UAVs were chosen based on their use of the IEEE 802.11 wireless communication standards and the security afforded by their use of WPA2 encryption with a pre-shared key.

Experiment one consisted of field testing the *Detachable Drone Hijacker* during ground-to-air and air-to-air operations. Meanwhile, experiment two conducted benchtop testing of the *Detachable Drone Hijacker* in a sub-freezing environment and experiment three conducted thermography [2] tests of the *Detachable Drone Hijacker*. Deauthentication and Transmission Control Protocol (TCP)/Synchronize (SYN) flood attacks were chosen as

cyber-attack techniques. RF jamming and other electronic attack techniques methods were excluded because of the collateral damage to other systems operating in the 2.4GHz and 5GHz frequency bands. Additionally, the power consumption requirements for RF jamming were too high for consideration in this thesis.

To evaluate the efficacy of cyber-attacks against 802.11 WiFi UAVs, this thesis measured the following characteristics during each attack: the target's behavior, the distance between target and the *Detachable Drone Hijacker*, the power consumption associated with each attack method, and the thermal signature of the *Detachable Drone Hijacker*. After baseline testing, the preferred attack method proved to be the deauthentication attack targeting the Parrot Bebop [3] and the Skydio 2+ [4].

In the first experiment, despite a moderate amount of environmental clutter, the *Detachable Drone Hijacker* had no issues identifying and mitigating the threat posed by the target UAV from 250 meters away causing the target to expend additional battery power in hover mode. Next, the research team created a scenario where an adversarial UAV attacked a hydroelectric power facility. Beginning at 250 meters away from the *Detachable Drone Hijacker* and flying at 15 kilometers-per-hour and at changing elevations, once the attack was initiated, the target stopped in its place 80 meters from its intended destination. Initially, the target hovered in place and flew back to its launch point. Then, the UAV landed itself at the location where it last connected to its GCS—100 meters from the *Detachable Drone Hijacker*. Throughout testing, the *Detachable Drone Hijacker* proved effective in identifying and mitigating the targets without any interference to the host-UAV or surrounding environment.

The sub-zero temperature tests identified the need for better temperature sensors on the *Detachable Drone Hijacker* to ensure more accurate readings. However, even when exposed to sub-zero temperatures for thirty minutes, the *Detachable Drone Hijacker* severed the communication link of its target. For the *Detachable Drone Hijacker* to be used operationally, there will need to be a ruggedization process to ensure the device can operate in extreme-weather environments, which may increase the SWaP requirements.

In the thermography experiments, still images were taken using a FLIR A320 Tempscreen [5] and analyzed by the research team. Still images were taken from top-down, front, and bottom-up look angles of the *Detachable Drone Hijacker* before operational use, after five minutes of continuous operation, and five minutes after operation. The thermography

experiments show that after five minutes of operations, the temperature of the *Detachable Drone Hijacker* increases by only 3.3°C.

The experiments conducted proved to be very promising when integrating the *Detachable Drone Hijacker* onto another aerial platform. Not only did the research team prove that the system will work against WPA2 encrypted UAVs, but this research identified ways to grow the current prototype into a networked family of systems. The sub-zero experiments proved that the *Detachable Drone Hijacker* will operate sufficiently in multiple environments. From the baseline prototype development and aerial experiments, to the sub-zero and thermal testing, the *Detachable Drone Hijacker* is at a Technology Readiness Level Six. This Technology Readiness Level is an important milestone to develop a concept into a capability.

In its current form, the *Detachable Drone Hijacker* is meant to be a configurable "bolt-on" solution to be hosted on a variety of platforms. Depending on the host-UAV there could be issues with system integration. Specifically, the CPU versus ambient temperature differential during operational testing showed that depending on the specifications of the host-UAV, consideration should be given to the thermal characteristics when integrating on a host. Additionally, when running the cyber-attack, the VNC connection to the *Detachable Drone Hijacker* gets severed which denies the operator's ability to control the *Detachable Drone Hijacker* for troubleshooting purposes. This issue can be remedied by using the ethernet port on the *Detachable Drone Hijacker* with an embedded RF module to establish a separate connection back to the ground station. The research team conducted a baseline test of this functionality, with a Persistent Systems MPU5 [6] radio which is important for future system integration with other unmanned aircraft.

In summary, the C-UAS market remains nascent and ripe for disruption. High-performance computer modules are getting smaller and consuming less power, while increasing in capability. Companies developing C-UAS technologies should refocus their efforts on leveraging high-performance with low-SWaP to create less expensive, but more capable C-UAS devices. Additionally, the DOD and DHS should create requirements for designing low-SWaP cyber-attack systems for aerial C-UAS. This thesis and the experiments using the *Detachable Drone Hijacker* prove that it is possible to deliver an aerial cyber-attack against multiple UAVs with minimal effect on the host device. This framework is not meant to usurp the

current methodology but is meant to augment and increase the effectiveness of C-UAS technology to meet the needs of the operating environment. While this study focused on countering consumer drones to protect military bases and critical infrastructure, the past two European wars have shown that terrestrial short-range air-defenses are no match for high-flying UAVs with kinetic strike capabilities. Thus, there are many opportunities for future work to counter consumer and government UAVs, enhance doctrine, and design an aerial network of C-UAS devices.

List of References

[1] T. Richardson, Q. Stafford-Fraser, K. Wood, and A. Hopper, "Virtual network computing," *IEEE Internet Computing*, vol. 2, no. 1, pp. 33–38, 1998.

[2] M. Vollmer and K.-P. Mollmann, *Infrared Thermal Imaging*, 2nd ed. Weinheim, Germany: John Wiley & Sons, Ltd, 2017. Available: http://onlinelibrary.wiley.com/doi/10.1002/9783527693306

[3] Parrot, Inc. (2016). Parrot Bebop Drone User Guide. [Online]. Available: https://www.parrot.com/assets/s3fs-public/2021-09/bebop-drone_user-guide_uk_v.3.4.pdf

[4] Skydio, Inc. (2022). Skydio 2+. [Online]. Available: https://www.skydio.com/skydio-2-plus

[5] Fixed-Mount Thermal Camera for Skin Temperature Screening: FLIR A320 Tempscreen. (2020, Apr.). [Online]. Available: https://www.flir.com/products/flir-a320/

[6] Persistent Systems, LLC. (2021). MPU5, WR-5100 Specification Sheet. *PersistentSystems*. [Online]. Available: https://www.persistentsystems.com/site/wp-content/themes/persistensystems/pdf/mpu5/mpu5_spec_sheet.pdf

Acknowledgments

I want to begin by thanking my advisory team for challenging me and supporting me throughout the past year. The guidance and connections the team provided me has made this yearlong effort not only possible, but enjoyable. Dr. Leo Blanken and Dr. Ray Buettner opened a tremendous amount of doors for me and gave me the tools I needed to succeed. Additionally, Dr. Douglass Van Bossuyt provided invaluable support for crafting the narrative and developing the experiments contained in this thesis.

In particular, I would like to thank Dr. Britta Hale for her continued support, mentorship, and guidance. This thesis began with a conversation in San Diego in June 2021 and has manifested itself to a level I did not think was possible. Dr. Hale has been a true professional and has been remarkably influential not only in this thesis, but in the other work we have completed together—I cannot thank her enough.

While not an official member of my thesis advisory team, Dr. Kevin Jones provided me with access to his equipment and expertise in all things relating to unmanned systems. Dr. Jones, thank you, you brought this project to new heights.

I would also like to thank Daniel Lehnherr from the Graduate Writing Center who provided outstanding direction in crafting the words contained on the following pages.

Lastly, I would be remiss to forget my partner, Lydia Carnevale, who has been a bedrock of support through this process. Lydia, I could not have done this without you. Thank you for believing in me and for your unconditional love.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 1:
Introduction

Unmanned aerial vehicles (UAV), are not new to the modern battlefield. The U.S. used unmanned aircraft in the Vietnam War for intelligence, surveillance, and reconnaissance (ISR) during the Son Tay raid [1]. The first UAVs were built with mechanical gyros and stabilizers that allowed them to fly a pre-planned route and collect thousands of images during their flight [2]. Since then, unmanned aircraft have become integral not only for ISR missions, but also for delivering weaponry on the battlefield. They have expanded from the one-way devices used in Vietnam to integrated systems that can be remote controlled via satellite from anywhere in the world. While the term unmanned aircraft systems (UAS) is used somewhat interchangeably with UAV, the Department of Defense (DOD) defines an UAS as any device relating to the whole system, to include a remote ground control station (GCS), the UAV, and any sensor packages placed onboard the UAV [3]. The DOD also classifies UAS into the five groups seen in Figure 1.1 based upon their weight, operating altitude, and speed.

UA Category	Maximum Gross Takeoff Weight (lbs)	Normal Operating Altitude (ft)	Speed (KIAS)	Representative UAS
Group 1	0-20	< 1200 AGL	100 kts	WASP III, TACMAV RQ-14A/B, Buster, Nighthawk, RQ-11B, FPASS, RQ16A, Pointer, Aqua/Terra Puma
Group 2	21-55	< 3500 AGL	< 250	ScanEagle, Silver Fox, Aerosonde
Group 3	< 1320	< 18,000 MSL	< 250	RQ-7B Shadow, RQ-15 Neptune, XPV-1 Tern, XPV-2 Mako
Group 4	> 1320		Any Airspeed	MQ-5B Hunter, MQ-8B Fire Scout, MQ-1C Gray Eagle, MQ-1A/B/C Predator
Group 5	> 1320	> 18,000 MSL	Any Airspeed	MQ-9 Reaper, RQ-4 Global Hawk, RQ-4N Triton

Figure 1.1. JP 3-30 Unmanned Aircraft Systems Categorization Chart. Source: [3].

Groups 1-3 UAS, also known as small unmanned aircraft system (sUAS), pose a significant threat to the security of U.S. critical infrastructure. Primarily due to their operating frequencies, small radar cross section (RCS), low noise characteristics, and because they look similar to birds in flight, sUASs are difficult to detect and track using traditional air defense systems [4]. This has been well-documented within the last decade as sUASs give adversaries an asymmetric means of conducting ISR activities in addition to kinetic strike abilities.

Since the UAV threat emerged, the DOD and Department of Homeland Security (DHS) funded research into negating their ability to conduct ISR and strike missions. The use of kinetic (e.g., bullets and projectiles) and non-kinetic (e.g., radio frequency (RF) jamming, global navigation satellite system (GNSS) spoofing, and cyber-attack) UAV countermeasures have had wide-ranging effectiveness, legal implications, and collateral damage associated with their use.

This thesis explores the current measures used in countering UAVs and argues for a shift in the framework by which counter-unmanned aircraft systems (C-UAS) technology is devel-

oped. Through exploring potential non-kinetic C-UAS technologies, this thesis advocates for the use of low-size, weight, and power (SWaP) devices for aerial interdiction of adversarial UAVs. Specifically, these low-SWaP devices should use cyber-attack techniques that exploit the protocol vulnerabilities found in digital communications. Furthermore, we prototype a proof-of-concept device, termed the *Detachable Drone Hijacker (DDH)*, to show the feasibility of air-to-air cyber interdiction for C-UAS procurement. In developing a small, lightweight, and low-power device that can be easily attached to a friendly UAV, this thesis assesses viability considerations for using a friendly UAV enabled with a cyber-attack (and potentially detachable) payload to mitigate the threat posed by adversarial UAVs.

1.1 Thesis Motivation

In the past decade, UAV technology has proliferated on the 21st century battlefield, often giving non-state and weaker state actors an advantage over their more technologically sophisticated and numerically superior competitors. This was never more evident than in 2014 when the Islamic State of Iraq and Syria (ISIS) used consumer UAVs to surveil and target coalition forces during their seizure of Raqqa [5]. The terrorist group then leveraged their Facebook and Twitter presence to record and post jaw-dropping videos of their ambushes using sUAS retrofitted with grenades [6]. More recently, the Second Nagorno-Karabakh War fought between Armenia and Azerbaijan demonstrated the need for robust C-UAS plans while the numerically inferior Azeri military dismantled the Armenian army and destroyed over 350 armored vehicles [7] [8]. These two examples show how inexpensive technologies used in a sophisticated manner can eliminate an opponent's center of gravity.

Asymmetric warfare, also known as irregular, or guerrilla warfare, is conflict between a strong and weak combatant, where the weaker opponent engages in indirect or unconventional tactics instead of engaging in force-on-force pitched battles [9]. When done correctly, this gives the weak actor an advantage over the strong, as the weaker combatant is able to control the pace of the conflict by preying on a stronger opponent's critical vulnerability. Typically, irregular conflicts are characterized by the use of inferior and sometimes crude weaponry in conjunction with a sophisticated psychological operations campaign that seeks to garner support for their insurgent cause. In the case of ISIS, they waged an unconventional war against the numerically superior Iraqi and coalition forces to seize and occupy strate-

gically significant locations in Iraq and Syria. In part because ISIS leveraged commercial UAVs as a pseudo-air force, they were able to rapidly gain ground and easily defeat the coalition, despite the latter's strength in numbers.

In the Second Nagorno-Karabakh War, a mid-intensity conflict fought between Armenia and Azerbaijan, Azerbaijan used surveillance UAVs as forward observers to spot and record for their armed UAV attacks. In the Azeri capital of Baku, the Defense Ministry of Azerbaijan broadcast and reposted the footage of UAVs striking Armenian troops [10]. The Azeri usage of UAV footage for propaganda and manipulation of the information environment, scored easy victories over the Armenians in both the physical and information domains.

Ivan Arreguin-Toft's theory of asymmetric conflict from *How the Weak Win Wars* becomes useful in understanding conflicts where weak actors handily defeat stronger ones [9]. As seen in Figure 1.1, in symmetric conflicts, where both sides fight war in the same manner, the stronger opponent typically wins the battle of attrition. However, in a conflict where the weak actor employs an asymmetric or guerrilla strategy, a weaker opponent can overcome their technological and numerical inferiority if the stronger actor employs a direct strategy.

Table 1.1. Arreguin-Toft, Strategic Approach Model. Source: [9].

		Weak Actor Strategic Approach	
		Direct	Indirect
Strong Actor	Direct	Strong Wins	Weak Wins
Strategic Approach	Indirect	Weak Wins	Strong Wins

What Table 1.1 shows is that by engaging in a war of asymmetry, where an actor's interests and political vulnerability are inversely proportional, strong actors frequently lose opposite approach interactions [9]. Throughout his book, Arreguin-Toft takes a look at conventional attacks, barbarism, conventional defense, and guerrilla warfare as the conditions for success in strategy and counter-strategy. Through analyzing The Murid War (1830-1859), The Boer War (1899-1902), The Italo-Ethiopian War (1935-1940), The Vietnam War (1965-1973), and The Soviet-Afghan War (1979-1989), Arreguin-Toft finds that when there is an

asymmetry in strategic interaction, the weaker opponent has a higher probability of winning the conflict.

While Arreguin-Toft focuses on interactions at the strategic level of war, his model is useful in understanding how technologically inferior opponents are able to achieve battlefield success at the tactical level of war. The U.S. and its allies have seen this asymmetry over the past several years as nations like China, Russia, Iran, and North Korea have leveraged information technology to conduct ransomware and other attacks in cyberspace [11]. In the future, countries and state-sponsored militias may use solo UAVs or even networked UAV swarms to target strategic infrastructure or seek to assassinate political officials. Therefore, by understanding the nature of low- and mid-intensity conflicts where UAVs are used, the U.S. and its partners can recognize the asymmetric threat posed by these emerging technologies and develop a framework to defend their strategic infrastructure.

1.2 Lessons Learned from the ISIS Insurgency

In 2014, Twitter and Facebook feeds exploded with horrific videos of ISIS fighters ambushing coalition forces during fighting in the Syrian city of Raqqa [5]. Then in early 2017, ISIS again shocked western audiences with their sophisticated use UAVs retrofitted to drop grenades during the 2017 Battle for Mosul [6]. These videos gave a look into how terrorist groups could leverage emerging commercial technology to disrupt coalition operations [5]. As ISIS improved their ability to wage war with UAV technology, the west scrambled to find answers to this new threat [12].

Commercial UAVs may not be as sophisticated or as lethal as their military counterparts, but they do not have to be. Their lightweight and inexpensive nature gives insurgent groups the ability to procure their own air force at a fraction of the cost to conventional militaries, giving them a means of conducting aerial ISR and kinetic strike missions [13]. During the ISIS capture of the city of Mosul in Northern Iraq, small mortar shells with effective blast radii of 30-45 feet, killed and maimed countless Iraqi government troops, creating a panic that led to a rapid retraction of government forces [6]. At the outset, Pentagon officials believe that UAVs had minimal military significance and would not affect the Iraqi government's ability to stave off the ISIS invasion. However, this estimate proved untrue, and by 2017, coalition forces needed equipment to meet the threat posed by these sUAS [13].

Initially, the coalition forces repurposed older counter-improvised explosive device (IED) equipment, such as the MODI and CREW systems, that proved useful in jamming remote-controlled IEDs in Iraq and Afghanistan. However, as coalition forces gained ground throughout 2016 and 2017 to retake Mosul, ISIS stepped up their efforts by further weaponizing their UAVs as IEDs and exploding decoys [14]. This led the Pentagon to increase funding for the development and acquisition of UAV-detection and jamming equipment [15].

While the ISIS UAV operations in Fallujah, Raqqa, and Mosul had little tactical significance on the outset, the videos recorded during these operations proved useful for propaganda in the information war [13]. On 12 October 2016 in Erbil, two Peshmerga died and two French Special Forces soldiers were critically wounded after an ISIS UAV exploded near them after it was shot down [16]. This event marked the first Western military casualties from irregular UAV operations. Then in June 2017 near the Syria–Iraq border, US-led special forces were struck by a UAV-launched missile. These events were a sudden escalation from the typical ISIS assaults, and showed an increasing need to mitigate the threat posed by ISIS UAV attacks [17].

The ISIS insurgency created the market conditions by which the C-UAS ecosystem was born. By using commercial UAVs as an air force for ISR and close air support (CAS), ISIS fighters offset the technological superiority of Iraqi, Kurdish, and U.S. forces, achieving an asymmetric advantage over the coalition. Had ISIS fighters not used UAVs in their occupation of Mosul and Raqqa, the West would have largely ignored the disruption caused by sUAS proliferating on the battlefield, leading to a lack of maturity in the current C-UAS ecosystem.

Today, the ISIS case study serves as warning for how terrorist organizations can procure and weaponize consumer UAS technology to create asymmetric advantages, in both the physical and information domains, over its technologically superior opponent. ISIS surprised its enemies from the air by implementing widely available commercial technology with a sophisticated tactical understanding of the battlespace to create more favorable battlefield conditions [13]. The terrorist organization's adept usage of emerging technologies and social media led to an increase in their audience as their instructional YouTube videos showed beginners how to modify and weaponize commercial UAVs, leading to countless spin-off organizations that gave them more support worldwide [5].

1.3 Lessons Learned from the Nagorno-Karabakh War

In November 2020, Russian peacekeepers brokered a deal between Azerbaijan and Armenia to end the nearly six-week war between the neighboring nations. That mid-intensity conflict provides operational insights into the capabilities and doctrine needed for a future conflict between similarly armed adversaries that employ an asymmetric strategy of waging war [18]. Much like the lessons learned from the Arab-Israeli War of 1973, which led to the use of laser- and GPS-guided precision munitions in the U.S. engagement in Iraq during the First Gulf War, the Nagorno-Karabakh War provides useful insights into how a future conflict might play out where similarly armed adversaries use networked unmanned aircraft as CAS to execute Suppression of Enemy Air Defense missions, kinetic strikes, and ISR.

Figure 1.2. Map of Armenia-Azerbaijan Pre-Conflict. Source: [19]

Since 1994 when Armenians were victorious over Azerbaijan in the first Nagorno-Karabakh war, the Nagorno-Karabakh region shown in Figure 1.2 has been hotly contested. The loss of the Nagorno-Karabakh region led the Azeris to focus their efforts on developing an arsenal that asymmetrically countered the Armenian advantages in army size and equipment numbers [8]. By focusing on the acquisition of high-tech weaponry designed for battlefield superiority and training its military personnel in the implementation of their new equipment,

it is clear the Azeris enjoyed a qualitative advantage [20]. The conflict can be broken into four phases:

> In Phase 1 both sides inflicted mutual blows in a balanced fight with the Armenians destroying dozens of Azeri tanks and Armored Personnel Carriers while downing aircraft, UAV, and commando helicopters. Meanwhile, the Azeris used armed UAVs and loitering munitions to fight back but made little ground progress.
>
> Phase 2 saw Azeri UAVs, loitering munitions, and attack helicopters implemented for CAS missions to target Armenian ground forces, which enabled the Azeris to make significant gains on the ground.
>
> In Phase 3 Armenia launched inaccurate ballistic missiles towards Azerbaijan in frustration while the Azeris continued to use armed UAVs and loitering munitions for the attrition of Armenian tanks and artillery pieces, enabling the Azeri ground forces to make more gains south.
>
> In Phase 4 the Armenians fired rockets and missiles at Azerbaijan cities, while the Azeri army continued with its advances from the north and deep penetration to the southern edge of Nagorno-Karabakh along the Iranian border.

Figure 1.3. Map of Armenia-Azerbaijan Post-Conflict. Source: [18].

Ultimately, the Armenian use of rockets and missiles proved futile as the Azeris won out in the peace deal brokered by the Russian Federation. Armenia ceded a significant portion of the Nagorno-Karabakh region, as seen in Figure 1.3 [21].

The use of UAVs and loitering munitions to systematically neutralize any Armenian advantage is particularly interesting and relevant for study of future combats. Because Armenia's integrated air defense system (IADS) architecture was filled with outdated Soviet-era equipment, the Armenians found no success in combating Azeri UAVs which could fly higher than the Armenian IADS target capability [22]. This allowed the Azeris unfettered access to the skies where they could launch their UAVs to destroy military targets and unrecognized infrastructure in the contested zone. The CAS and ISR enabled by the Azeri UAVs gave them a cheap air force that could have devastating effects without ever having to send highly skilled and trained pilots into the air, increasing the survivability of their manned Su-24, Su-25 attack aircraft, and Mi-24 helicopter [23].

Using the Turkish built TB-2, a Group 4 unmanned vehicle that mirrors General Atomics' MQ-1 Predator, the Azeri military destroyed Armenian armament with impunity. The CAS provided by the TB-2s allowed ground troops to execute complicated suppression of enemy air defense missions to destroy dozens of Armenian surface-to-air missile (SAM) sites, including the once-exquisite SA-6, ZSU 23-4, and S-300. When the Armenian SAM threat was neutralized, the TB-2s moved on to destroy 130 artillery pieces, 245 tanks, and disrupt anti-tank guided missile teams [24].

Most surprising in the conflict was not just the use of UAVs by the Azeri military , but the extent to which their systems were integrated as a part of doctrine, training, and standard operating procedures. Integrating the TB-2 with its 24-hour loiter time, the Harpy-2, a loitering munition capable of a 6-hour flight time; and the Hermes-900, an ISR platform with a 36-hour time on station, alongside other Groups 1-5 UAVs enabled the Azeris to move through the kill-chain process and strike targets with precision beyond the forward line of troops.

The once vaunted Soviet S-300 is still an extremely capable SAM platform to destroy enemy aircraft. However, because the Armenian S-300 was meant for larger aircraft defense and not C-UAS missions, the platform has minimal effectiveness against smaller, unmanned aircraft with smaller radar cross-sections such as the TB-2. Once Azerbaijan targeted and destroyed the guidance stations, radars, and erector launchers of the S-300 [20], it easily exploited the gaps in the Armenian IADS architecture by using its large fleet of UAVs to destroy the vulnerable armor and heavy ground units.

The Baykratar TB-2, purpose built for ISR and armed attack missions, proved to be the most lethal UAV on the battlefield. With an 18,000- to 27,000-foot flight envelope, fully automatic flight controls, and autopilot systems it provides the ground control station with real-time image transmission and processing for a 24-hour loiter time [25]. Throughout the conflict, the TB-2 dominated the skies accounting for destruction of 16/24 2S1 self-propelled artillery pieces, 6/18 KS-19 anti-aircraft guns, 54/103 D-30 122mm howitzers, 45/74 D-20 152mm Howitzers, 16/21 9K33 Osa SAM, and 1/11 ZSU 23-4. In total, the TB2 alone accounted for the destruction, capture, or damage of 1708 pieces of equipment. If only accounting for the destruction rate, the TB-2 was responsible for destroying 63%, or 512 of 820 pieces from the Armenian order of battle [26]. Because the Armenian ground-

based IADS and electronic warfare (EW) systems failed to meet the needs of an unmanned conflict, they were forced to improvise and develop rudimentary thermal and RF signature management techniques that failed to stave off the TB-2 onslaught—ultimately proving futile.

The Nagorno-Karabakh War offers clear indications of how autonomous and unmanned systems impact the modern character of war. The Azeri integrated high-tech systems with sophisticated training to handily defeat their rival. The takeaways from this conflict mirror the lessons learned from the Arab-Israeli War in 1973 in preparation for the First Gulf War: airpower wins against large infantry and tank division, especially when there is no viable threat to said airpower [27]. First, close and deep air support was primarily provided by unmanned systems with high loiter times. Even though MQ-9 Reaper and MQ-1 Predator dominated the sky in the Global War on Terror in Iraq, Syria, and Afghanistan, the fact that a poor nation such as Azerbaijan can accomplish the same effect is remarkable. Lastly, the Nagorno-Karabakh War provides insight into thinking differently about key terrain, maneuver space and the implications for ground troop survivability and airpower, especially as unmanned systems continue to proliferate on the battlefield of the 21st century, while viable countermeasures lag behind [20].

Other technologies in the Nagorno-Karabakh War such as the Harop, known as the Harpy-2 and built by Israel Aerospace Industries, provide a useful look into how loitering munitions and UAVs can be networked into a constellation of unmanned systems that could be controlled autonomously. The Harpy can be ground, sea, or air launched with a six-hour loiter time and 2,000 kilometer range at an altitude of 15,000 feet. Despite its relatively slow speed at a maximum of 259 miles-per-hour, the Harpy-2 is only 8.2 feet in length and has an RCS of $<0.5m^2$ or -3.01 dBsm. The RCS on the Harpy-2 is so small that it compares to the RCS of the most high-end cruise missiles, rendering many of the current target identification methods inoperable. The onboard electro-optical/infrared (EO/IR) and RF sensors assist in target identification and two-way data-link control for striking high-value and high-payoff targets by crash landing [28]. Had Azerbaijan employed the Harpy more widely into the heart of Armenian territory, they could have caused an untold amount of destruction.

While the TB-2 and Harpy-2 are not the cheap commercial UAVs used by ISIS, the proliferation of low-cost UAVs gives an insight into how commercial and government UAV programs

can outpace the development of expensive C-UAS solutions [22]. The shear force laydown of Azerbaijan's highly capable unmanned vehicle suite shows that a country with a 2020 Gross Domestic Product of only $42.6 billion [29], can still possess elements of a top tier military at relatively low cost. The government and commercial unmanned systems market is continuing to grow rapidly, and eventually it will only take what amounts to a few lines of code with commercially available hardware to create a fully networked and interoperable constellation of unmanned systems that operate autonomously or semi-autonomously.

Ultimately, the diffusion of technology like UAVs and cyber-techniques gives way to a more lethal battlefield rife with precision guided munitions. Had the Armenian military integrated multiple layers of short-range air defense, old-fashioned anti-aircraft artillery, and modern EW, they may have been able to counter the modern aerial threat. Most importantly, had the Armenian military not focused on the pomp and circumstance of military affairs, the war's outcome may have been different [30]. The Nagorno-Karabakh War should be a reminder for western nations: invest heavily in the training and equipping of your military personnel, and you will reap the rewards. Failure to do so could lead to failure on the battlefield in a conflict with near-peer adversaries such as Russia or China, and even non-peer threats.

1.4 Counter Measure Preparation

Both the ISIS and Nagorno-Karabakh War highlight the need for effective countermeasures against unmanned combat air vehicles. Because of their low RCS, traditional integrated air defense measures are rendered essentially useless. Taking the lessons gleaned from Ivan Arreguin-Toft's theory of asymmetric warfare, it is evident that an inferior force can inflict great damage, and even win, against a numerically superior opponent. In a future conflict with China, Russia, North Korea, or Iran it is increasingly likely that the U.S. and its partners could fight a highly networked and integrated swarm of low-cost, unmanned vehicles. These swarms will be used to limit air power, deny sea power, and destroy armored personnel on the ground. However terrifying this reality may be, these autonomous systems all have inherent vulnerabilities leaving them susceptible to electronic jamming, spoofing, and cyber-hacking. It is here that this thesis explores the current state of C-UAS affairs, and where the U.S. should focus its efforts to rethink the way the DOD and DHS counter unmanned systems through the use of UAV-based devices for aerial interdiction. Clearly, middle-tier countries have learned from the Navy's concept of Network Centric Warfare [31],

it is time to harvest battlefield information found at the edges of western purview to learn new lessons in battlespace integration.

The most significant benefit of a UAV-based device is the maneuverability it provides for a defender. When biplanes were introduced to the battlefield in World War I (WWI) for intelligence gathering, there was a natural progression to weaponize the planes for close air support of ground troops, and dogfights to interdict an enemy's air assets. This gave defenders an offensive edge and the ability to push their defensive lines further ahead of what they could in the trenches. Additionally, when ground-based anti-aircraft artillery came into the mix, aircraft avoided the flak and projectiles by flying higher. So, the natural way to force aircraft to lower altitudes into a kill-zone was to use aerial interdiction patrols. The flexibility afforded by aircraft designed for air-combat extended the effectiveness of a defense and created a new type of warfare defined by maneuver and surprise, rather than stagnation like the trenches of WWI.

Thus, it is easy to extend this same natural progression to aerial combat with unmanned systems. With the right type of friendly UAVs on hand, an aerial interdiction patrol using low-SWaP payloads becomes reality. Instead of designing only general-purpose EW platforms like the Marine Air Defense Integrated System (MADIS), Sentry Tower, and Skytracker, the DOD and DHS can develop a suite of aerial interdiction platforms designed for purpose-built EW and cyber-attacks.

According to the Bard report, the only C-UAS device on the world market that uses a UAV-based EW-mitigation payload structure is the Leer-3 from JSC Concern Radio-Electronic Technologies [32]. JSC Concern is a subsidiary of Rostec, a state-owned Russian holding company that specializes in investing in defense and high-tech industries. This study indicates that a state-owned Russian company has the upper hand in aerial C-UAS technology, and may also have an upper-hand in the defense of their critical infrastructure. If the U.S. fails to build its own UAV-based EW and cyber-payloads, the country may not be unable to defend against an enemy's most dangerous course of action—a swarmed, multi-axis attack using UAVs hardened against RF scanning methods and EO/IR cameras.

1.5 Thesis Scope

Despite war's unchanging nature, technology continues to evolve in the coming decades, meaning that the individual characteristics of how wars are fought will change as well. Most notably, as information technology expands and autonomous systems proliferate on tomorrow's battlefield, the U.S. and its partners should adapt to the future of warfare. The intent of this thesis is to study the current suite of C-UAS technology and Joint Chiefs of Staff (JCS) doctrine in order to identify where improvements may be made. This will inform the shift in C-UAS strategy and the development of new products, such as that proposed in this thesis.

- Chapter 2 reviews the capabilities and limitations of C-UAS technology by analyzing where the current and future systems succeed or fall short in kill-chain processing. This will assist in identifying where the DOD and DHS could redesign their acquisition strategy for C-UAS technology. Additionally, this chapter looks at current C-UAS doctrine, tactics, techniques and procedures (TTP)s, and standard operating procedures to identify ways the DOD can improve its strategy for countering UAVs.

- Chapter 3 explores the non-kinetic RF mitigation measures used in jamming digital communications links. This technical discussion focuses on electromagnetic (EM) wave propagation, link budget analysis, the principles of low-probability of detection (LPD) and low-probability of intercept (LPI), spread spectrum communications, and RF jamming principles.

- Chapter 4 builds on the information contained within Chapter 3 and explore ways to exploit the communication protocol vulnerabilities onboard consumer UAVs. This chapter looks at the Open Systems Interconnection (OSI) model, its relation to digital communications, and how cyber-attack techniques might be developed to provide a precision attack against adversarial UAVs.

- Chapter 5 uses the Marine Corps' defense-in-depth model for defensive operations [33] to maintain an offensive mindset to limit an adversary's use of Group 1-3 unmanned systems [34]. This chapter also discusses the how combat aircraft are

used as aerial interdiction to defend critical infrastructure. Additionally, this chapter provides comparison charts to explore the current C-UAS architecture, what integrating airborne cyber-attack and EW devices could look like, as well as the pros and cons associated with the proposed architecture. Lastly, this chapter concludes with two hypothetical scenarios where an insurgent group attacks a hydroelectric power facility using a swarm of unmanned suicide UAVs.

- Chapter 6 outlines the experiment methodology, setup, and data collection methods used in Chapter 7 where a prototype of the *Detachable Drone Hijacker* was designed and built.

- Chapter 7 describes the experimentation process used to create a prototype of the concepts outlined in Chapter 5. The experiments conducted in this chapter deliver a denial of service (DoS) attack against an adversarial UAV, launched from the *Detachable Drone Hijacker*, which is attached to a friendly UAV.

- Chapter 8 concludes the thesis. There is a discussion of the proposed architecture in Chapter 5 as well as the experimentation from Chapter 7. This chapter concludes with the implications for future C-UAS system procurement and doctrinal development.

A December 2019 study by the Bard College Center for the Study of The Drone, identified 537 systems dedicated to countering unmanned aircraft [32]. While the countermeasures available have met the needs of the DOD and the DHS in the late 2010s and early 2020s, they will likely fail to hold up in a multi-pronged attack. Despite the market density, each system has technological, societal, and legal limitations associated with their use. Additionally, many of the fielded countermeasures are expensive and bulky, and only getting more so, making it difficult to procure and sustain enough C-UAS devices to cover all potential attack vectors. Meanwhile UAVs are getting cheaper, smaller, and increasingly more networked—leading to a future where the current systems may not hold up against a swarmed attack. This phenomena is playing out in real-time in the Ukraine's war with Russia, as Ukraine has leveraged UAVs to devastating effect. Namely, the one-million-dollar Bayraktar TB-2

has wreaked havoc on the Russian military, destroying over fifty-million-dollars of surface-to-air missiles in a single airstrike [35]. This makes it easy to foresee a scenario where an adversary uses a swarm of UAVs to conduct a multi-wave and multi-frequency attack on U.S. strategic infrastructure. The following chapter is devoted to outlining the current suite of C-UAS technology and in understanding that there has yet to be a definitive means of countering unmanned swarms, without drastic unintended consequences.

CHAPTER 2:
Current Counter Unmanned Systems Technology

The lessons learned from the ISIS insurgency and the Nagorno-Karabakh War show that many militaries, including the U.S. military, have gaps in their research, development, acquisition, and integration of C-UAS technology. This chapter is devoted to understanding the current technologies involved in the C-UAS processing chain, also known as the kill-chain. Additionally, there is an important, albeit brief, discussion on the current state of published C-UAS doctrine. By outlining the current C-UAS systems, this thesis looks to identify shortcomings and describe how the DOD and the DHS might improve the acquisition and implementation of C-UAS technology. Given the pace of technological development, the U.S. military and the DHS should update their doctrine, standard operating procedures, and tactics to meet the nascent threat posed by unmanned systems.

2.1 C-UAS Processing Chain and Kill-Chain Analysis

The DHS defines the full C-UAS kill-chain process in Figure 2.1, as the detection, tracking, identification, and mitigation of a UAV threat [36]. While different terminology exists between government and industry, each kill-chain describes the same process of moving from threat detection to mitigation.

Figure 2.1. Counter-Unmanned Aircraft System Kill-Chain. Source: [36].

From Figure 2.1, the technology used in the first three-quarters of the kill-chain are separate from the measures used for threat mitigation. The digital signal processing required for the detection, tracking, and identification of the threat is the most complex issue for C-UAS companies to tackle. This is due to the low-energy output of small unmanned systems in addition to the optical and physical characteristics that make Groups 1-3 UAVs appear as

small birds on many sensors. Several technology companies like CACI [37] and Anduril [38] have created fixed, ground-based platforms to meet the needs of the first three-quarters of the kill-chain by building target libraries to help in the digital signal processing and computer vision-based algorithms used in EO/IR sensors. However, the downside to many of the current C-UAS systems are the costs for deployment, maintenance, and calibration, as well as the power consumption requirements and the potential for collateral damage to surrounding electronic systems [39].

It should be noted that the accuracy and effectiveness of non-kinetic C-UAS technologies are susceptible to system degradation in adverse weather conditions [39]. Kinetic systems such a nets, explosives, and projectiles are more weather-proof than the non-kinetic systems, in general. This is due to the way electromagnetic waves propagate in general, and when subject to rain, fog, or adverse terrain, EM wave propagation is severely hampered [40].

Other characteristics of C-UAS technology that should be noted include the use of directional antennas like phased arrays that increase the gain and directivity of a system by focusing the EM waves [41]. Phased arrays are typically the antenna of choice for many ground-based radar and RF detection systems because they have an increased detection range that can operate below the noise floor [40]. Phased arrays are chosen over omnidirectional antennas and dipoles as these older antenna types have significant attenuation losses and fail to meet the needs of coherent reception at higher frequencies.

As the digital communication revolution has expanded, so too have the modulation techniques for LPD, LPI, and low-probability of exploitation (LPE) communication [42]. For commercial and government UAVs, the remote control link between the GCS and the UAV is modulated using spread spectrum digital communication techniques such as frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS) [39]. Lastly, each system is at risk to counter-countermeasures which is discussed at the end of this chapter.

2.2 Capabilities and Limitations of Detect, Track, and Identify Technologies

2.2.1 Radio Frequency Sensors

For the purposes of this thesis and the experimentation that follows in Chapter 7, the RF scanning method is the most important sensor system to understand. An in-depth understanding of digital communications is covered in further detail in Chapter 3. Understanding the fundamentals of EM wave propagation is critical to understanding how UAVs communicate and to know which countermeasures exist to mitigate these threats.

Capabilities:

RF sensors scan the most common frequency bands used by for communications between an UAV and its GCS. Typically, these are set to scan the 433 MHz, 915 MHz, 2.4 GHz, and 5.8 GHz frequency bands [43]. Similar to modern radar systems, RF sensors use field programmable gate arrays (FPGA) and graphical processing units (GPU) hardware to allow for software defined signal processing, thus eliminating the need for a human in the loop [44].

Limitations:

There are two primary issues with RF scanning. First, the frequency bands used in UAV communications are wide and because many of them employ FHSS techniques, determining the sub-band a UAV transmits on requires detailed of the UAV's communication protocol [45]. Second, because there is a lot of environmental noise from other devices in the four main frequency bands used in UAS communications, discerning signals of interest is resource intensive [45]. For example, a wireless router operates using the 2.4 and 5.8 GHz Industrial, Scientific, and Medical (ISM) frequency bands. Since these routers are ubiquitous in densely populated areas, it is difficult to discern between an adversarial communication link and normal traffic due to the surrounding RF clutter.

2.2.2 Radar Sensors

Capabilities:
Radar sensors are among the most capable sensors used in detecting and tracking unmanned systems. These sensors use radio frequency pulses to detect and track an unmanned vehicle's RCS [40]. Modern radar systems are built with advanced computer chips such as FPGAs and GPUs allowing the radar systems to become software defined. This allows each system to employ digital signal processing algorithms that both classify UAVs based on size and distinguish UAVs from birds.

Limitations:
Using radar sensors to detect, track, and identify sUASs is one of the most difficult problems for radar engineers to solve. The RCS of a target is used to describe a target's scattering properties in decibel square meters, similar to how an antenna's gain, or directivity, is calculated [40]. Radar is primarily limited by the target's size, the characteristics of the radar system and its components, as well as the viewing angle from which the radar sees the target [46]. Due to the size of sUAS, they have much smaller cross sections than manned aircraft, making it more difficult to distinguish them from environmental clutter when compared to traditional air defense radar [47].

2.2.3 Electro-Optical and Infrared Cameras

Capabilities:
EO/IR cameras are typically also employed with a computer-vision algorithm that enables the onboard computer to detect, track, and identify a UAV based on its visual and/or heat signature [48]. These cameras can be used separately but are typically employed together. Depending on the sophistication of the algorithm used with the EO/IR cameras, they can be very useful in detecting, identifying, and tracking small RCS threats like UAVs and snipers [48].

Limitations:
EO/IR cameras face several limitations. First, because of the computer-vision algorithms, FPGAs, and GPUs, EO/IR cameras are expensive to build, manufacture, and maintain [48].

Second, the technology necessitates large amounts of power, leading to their implementation as terrestrial platforms—an easier target for adversaries. Lastly, the autonomous or semi-autonomous use of computer-vision algorithms are reliant upon accurate data points while training the algorithm. If the algorithm is trained with inaccurate or forged data [49], the computer fails to discern adversarial UAVs from friendly UAVs or even birds [50].

2.2.4 Acoustic Sensors

Capabilities:
Acoustic sensors are used to detect UAVs based on the motor's distinct sound [50]. For target classification, these systems passively listen for specific reverberations and match the detected signals to a library of known sounds [51]. When multiple acoustic sensors are used at dispersed distances, the probability of detection vastly increases [52].

Limitations:
Because of the surrounding environmental noise, acoustic sensors have a limited detection range and are not very effective in densely populated environments or during periods of high wind [50] [51].

2.2.5 Combined sensors

Capabilities:
Combining multiple sensors allows for a robust countermeasure system rather than one lone device. This is evident with Anduril's Sentry Towers [38] and CACI's Skytracker, [37] which combine radar, RF, and EO/IR sensors. For good reason, these systems have been procured by the DHS and DOD for border and infrastructure security against unmanned systems.

Limitations:
Sensor combination is inhibited by the chosen technology used in the C-UAS system. While CACI and Anduril have deployed their sensors in multiple theaters, there are inherent limitations in their designs that are primarily due to adverse weather conditions [39].

Additionally, combining different systems makes them less mobile and expeditionary, which leads to the bulky and expensive towers. In 2019, the Marine Corps formalized a program of record for an expeditionary ground-based platform with their MADIS, a mobile EW platform capable of moving on semi-improved surfaces [53].

2.3 Capabilities and Limitations of Non-Kinetic Mitigation Measures

Non-kinetic mitigation measures, also known as the less-than-lethal or soft-kill measures, are the actions taken to degrade, deny, or disrupt an adversary's capability without physical destruction. Soft-kill measures are usually temporary and are delivered through EW or cyber-missions. The two primary methods to target UAVs are through RF jamming or GNSS spoofing—both of which have been around for decades. Laser, directed energy, and high-powered microwave weapons are emerging technologies that defense contractors are exploring as precision mitigation measures [54].

2.3.1 RF Jamming

Capabilities:

RF jamming is designed to sever the communication link between an UAV and its GCS by injecting large amounts of electromagnetic energy, referred to as noise, into a receiving antenna [55]. Uplink jamming disrupts the receiving antenna of the target UAV, while downlink jamming interferes with the receiving antenna of the GCS [56]. Uplink and downlink jamming can be accomplished by two types of jammers: stand-off and stand-in. Stand-off jammers are devices located amongst friendly forces. Typically they are large terrestrial or aerial sites (e.g., the MADIS [53] and EA-18G [57]) that consume copious amounts of power to overcome the free-space path loss associated with their use [58]. Stand-in jammers are within the weapons engagement zone of their targets (unlike stand-off jammers), but can have an outsize impact by significantly reducing the power requirements for signal disruption [59] [60]. Historically, RF jamming has been the most common C-UAS mitigation technique and both stand-off and stand-in jammers can be seen in Figure 2.2.

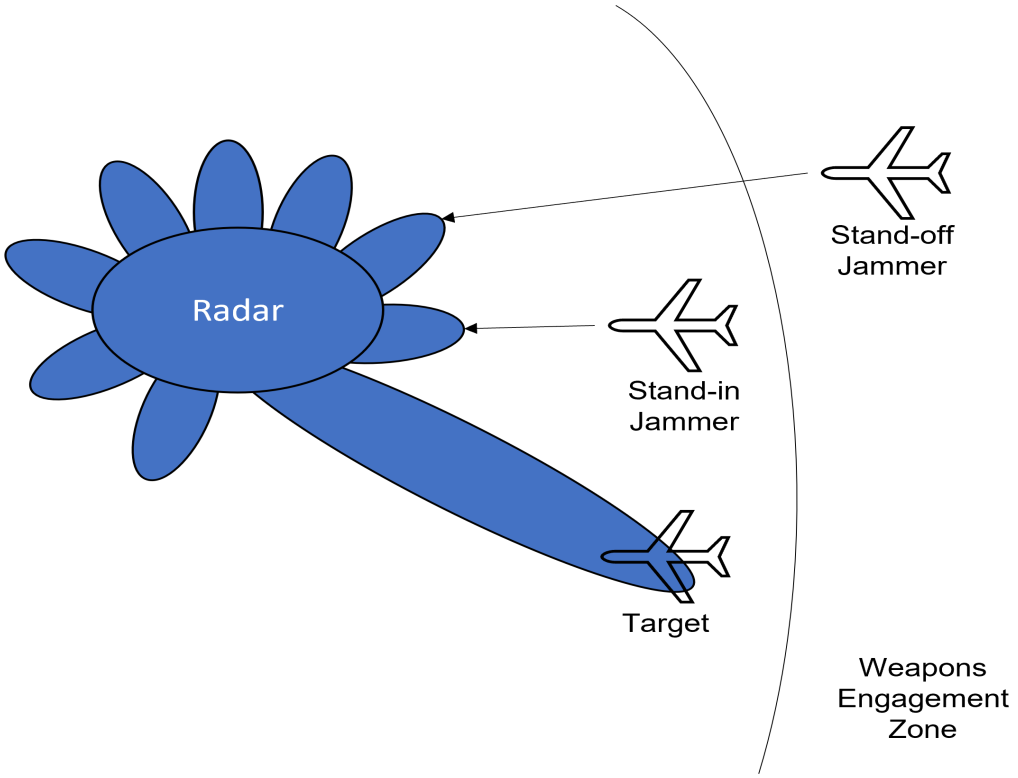

Figure 2.2. Stand-off and Stand-in Jamming Attack Geometry, Adapted From: [60].

Limitations:

RF jamming is limited by terrain, weather, equipment cost, and potential disruption of friendly and civilian devices [39]. Terrain in the operational environment affect an RF jammer by causing increased signal attenuation from power lines, trees, and buildings. Adverse weather, such as rain, fog, and ice, also negatively affect the ways in which RF waves propagate [61]. Particularly in the 1-300 GHz ranges, where most commercial UAVs operate, these weather phenomena tend to exacerbate the attenuation issues from multiple users operating in the same frequency band. RF jamming techniques is covered in further detail in Chapter 4, but each technique is also limited by the type of UAV an intruder is using [55] and collateral damage considerations for surrounding communications devices. Many modern devices are hardened against rudimentary RF jamming techniques, which has led to new jamming techniques which require high-power consumption, thus increasing

the complexity and cost of the C-UAS device.

2.3.2 GNSS Jamming

Capabilities:
GNSS jamming uses the same principles as RF jamming to disrupt the link between a UAV and its navigational satellite [62]. This ultimately leads to a denial of service for the UAV operator and may trigger the device to execute an alternate course of action, such as returning to home. As with RF jamming, GNSS jamming can be accomplished through uplink or downlink jamming. Because the frequency bands of commercial devices operate on the known frequencies, GNSS jamming can be accomplished fairly easily to overpower the communications link between a target and its ground station [62].

Limitations:
The primary limitation of GNSS jamming is the increased collateral damage to friendly satellites or other systems operating in the same GNSS sub-band [62]. Additionally, even if a GNSS link is severed on a fixed-wing craft, the device continues to glide despite losing guidance. Finally, UAVs, who mask their operating frequencies may not be affected by GNSS jamming.

2.3.3 GNSS Spoofing

Capabilities:
GNSS spoofing is the most common cyber-attack method used in C-UAS technology. It is similar to jamming, except that it allows an attacker to impersonate and take control of the UAV by feeding it false communications or navigation links [63]. Spoofing GNSS grid locations is fairly easy to accomplish if the device is using commercial frequencies to send fake signals to the target. One of the most common types of GNSS spoofing is known as a Carry-Off Attack, in which an adversary synchronizes its receiver with the target, then gradually increases the power of its counterfeit signal to draw the target away from its legitimate GCS to a pre-designated location of the attackers choosing [64]. Recently, Russia

has implemented GNSS spoof attacks in Syria to cause target devices to land in an area of their choosing or just disrupt normal operations [65].

Limitations:
GNSS spoofing is limited by the same loss functions associated with RF and GNSS jamming, requiring extensive consideration for uplink and downlink spoofing [63]. Additionally, this attack method relies on knowledge of the operating frequencies of the target device. Many commercial UAVs do not have spoofing protections. Typically, this can lead to a positive countering outcome; however, if done from a friendly-UAV, GNSS spoofing can interrupt the navigation of the friendly-UAV itself. Additionally, if the UAV is a military target, an ample amount of intelligence must be gathered to reverse engineer the UAV's signal characteristics—especially if it uses a protected GNSS signal [66]. Lastly, with the rise in spoofing of commercial and government systems, many unmanned devices are moving to FHSS-based modulation schemes in addition to increasing the data authentication standards for devices using GNSS navigation methods. FHSS communications make it more difficult to implement a spoofing attack as the attacker must hop onto the correct channel and follow the hop rate to inject malformed packets that contain the rogue GNSS information [63].

2.3.4 Laser Dazzling

Capabilities:
Laser dazzling uses a high-intensity laser beam to blind the camera system on a UAV [67]. The Marine Corps, as well as the Army, have both begun procuring the Compact Laser Weapons System (CLaWS), for use as a ground-based laser system that can integrate with the MADIS and the Stryker vehicles [68]. By blinding the camera system of an adversarial UAV, laser systems have the potential to disrupt an adversary's ability to accurately control their UAV for its assigned mission.

Limitations:
Lasers are primarily limited by the beam strength required to reach the UAV and saturate its camera system. This is a difficult feat for a human operator to do from the ground because of interference and beam scattering [67]. This would require having at least some knowledge

of the camera's look angle to best target the adversarial UAV. Additionally, lasers are susceptible to environmental conditions like rain, fog, dust, buildings and windows which can cause beam scattering, reflection, and refraction—all of which lead to a reduction in mitigation effectiveness. Laser systems consume significant amounts of power [69] [68], which necessitate their use on the ground and further accelerates the aforementioned environmental and signal scattering issues. Finally, laser systems require a lot of coordination for their operational use. From [70], the CLaWS "requires approval from the Office of the Secretary of Defense, as it involves various factors such as legal reviews, concepts of employment, rules of engagement, tactics, potential collateral damage and human effects, proposed public affairs guidance and other relevant information."

2.3.5 High Power Microwave/Directed Energy

Capabilities:
Directed energy weapons focus large amounts of high intensity microwave energy at a target UAV to disable the aircraft's electronic systems [71]. These systems can be very effect against single, or multiple, devices with precision. Additionally, several of these directed energy weapons from Epirus are being integrated with the Army's Stryker vehicle, a General Dynamics-led contract [72].

Limitations:
Directed energy weapons suffer from the same limitations as laser weapons in that they are affected by rain, clouds, fog, dust, or buildings that can cause beam divergence, refraction, or reflection, reducing beam's ability to mitigate UAS threat [71]. These systems also require large amounts of power, are very expensive, and are not expeditionary.

2.4 Capabilities and Limitations of Kinetic Mitigation Measures

Kinetic mitigation measures, also known as hard-kill measures, seek to degrade an adversary's use of, or permanently destroy, a target [32]. In the C-UAS fight, hard-kill measures employ nets, projectiles, or collision UAVs. By-and-large, the current suite of kinetic mitigation measures fail to adequate address the problem posed by adversarial UAS. During

the initial stages of the ISIS UAV operations, coalition forces responded by shooting the UAVs out of the sky with light- and medium-machine guns, before employing the counter-IED equipment from Iraq and Afghanistan [5]. Since the initial measures were taken, the C-UAS community responded with myriad techniques to combat the threat—each having significant physical or legal limitations. For example, the use of kinetic mitigation measures such as explosives and projectiles can harm innocent civilians or damage surrounding infrastructure. This creates a number of problems for employment in the U.S. and abroad.

2.4.1 Nets

Capabilities:
Nets can be launched aerially via a host-UAV or from the ground to entangle a target UAV or its rotors. The usage of nets lessens the collateral damage when compared to other kinetic countermeasures [73].

Limitations:
Nets are constrained by their effective range, target speed, and number of rounds—all of which contribute to a fairly low success rate [73]. Recently, sUAS companies like Skydio and DJI have begun employing collision avoidance software to prevent their devices from running into terrestrial structures like trees and buildings. The collision avoidance technology has also proven to be effective in preventing a device from net capture as Skydio's deep learning system uses 45 megapixels of visual sensing for 360-degree coverage that gives the UAV a safe flight that is mapped to fulfill a pilot's commands or its pre-planned route [74].

2.4.2 Projectiles and Munitions

Capabilities:
Projectiles and munitions are typically employed from either the ground or the air using regular or special ammunition to mitigate an adversarial UAV [75]. Shotguns provide a close-range weapon system that can be very effective at neutralizing threats within 50-meters in all weather conditions [32].

Limitations:
Projectiles and munitions are limited by the operator's proficiency with the weapon system and the weapon's max effective range [32]. For shotguns, this remains around 50 meters, but for machine guns, the max range can be over 1800 meters. Additionally, there are significant collateral damage, liability, and legal concerns with using projectiles to mitigate UAVs – especially in urban areas [75].

2.4.3 Collision UAVs

Capabilities:
Collision UAVs are designed for mid-air interception of a target [32]. They mitigate a threat by using ramming their frame against a target UAV. These systems typically have reinforced structure and are very maneuverable.

Limitations:
Doing this with a human in the loop is extremely difficult to accomplish given the maneuverability of sUAS. Doing so autonomously like Anduril's product, Anvil, is also challenging because the computer vision algorithm must maintain a track of an adversarial UAV while ramming the adversary out of the sky [76]. While Anduril has demonstrated that the Anvil works in some experimental settings, reliably predicting the behavior and movement of an autonomous UAV to intercept it with a flying battering ram is improbable to work in a realistic conflict due to the degree of precision on contingent factors involved.

2.5 C-UAS Platform Types

2.5.1 Ground-Based, Fixed Systems

Capabilities:
Ground-based, fixed C-UAS sites are typically employed aboard military bases, secure facilities, and other strategic points of interest. Because they are operating with access to shore power, they have the most robust suite of countermeasures available on the market [32]. Ground-based, fixed platforms also employ a multi-layered approach to their UAS

countermeasures, integrating all (or most) sensor types with several mitigation methods. Lastly, these systems can have an autonomous mode that allows the platform to move through all aspects of the kill-chain with a human-on-the loop, human-in-the-loop, or human-out-of-the-loop.

Limitations:
These ground-based platforms require large amounts of shore power to operate the various sensor packages onboard [32]. Additionally, because they are located in static positions, they become big and easy targets for adversaries to attack or sabotage—and an effective attack against the centralized system leaves a lack of defense layers. Lastly, these systems are expensive to acquire and sustain throughout the product life cycle.

2.5.2 Ground-Based, Mobile Systems

Capabilities:
Ground-based, mobile platforms are C-UAS technologies mounted on vehicles and operated while moving [32]. Depending on the vehicle they are transported, they can be very capable in austere environments by carrying a modest amount of power and sustainment before needing to return to base for rest and refit.

Limitations:
Ground-based, mobile C-UAS systems like the MADIS have several glaring limitations [53]. First off, they are human operated which requires extensive operator training on the system to ensure that the proper attack methods are used. Between operating the vehicle, the detection sensors, and the threat mitigation systems onboard, the MADIS is a manpower intensive vehicle that requires operators to go through an extensive amount of system training. Second, because they are general-purpose EW systems, the ground-based mobile systems require significant amounts of power that have a large RF signature. This power consumption means that the ground-based, mobile C-UAS cannot act as a persistent sensor unless there is a logistics resupply hub for the operators to tie into.

2.5.3 Handheld Systems

Capabilities:

Handheld systems are operated by a single, or team of, individuals by hand. The Dedrone DroneDefender is a good example of a lightweight handheld system that resembles a small arms weapon with a highly directional antennas [77]. These devices are offered at a lower cost than the fixed, mobile, or UAV-based devices. The low power and portability of these systems gives another advantage over their larger counterparts; handheld systems can jam an entire frequency band with minimal collateral damage to friendly communications because of highly directional antennas and signal attenuation over longer distances. Because omnidirectional antennas propagate their signal in all directions, handheld C-UAS devices that use directional antennas can limit the collateral damage they inflict by pointing their signal in the direction of the intended target.

Limitations:

Due to their portability, they have a lower power setting than the larger mobile and fixed ground systems. This low power allows them to operate on 1 or 2 frequency bands and the lack of a library requires them to jam the whole band—typically the 2.4 or 5 GHz bands [32]. Additionally, even though they use directional antennas, if there are other devices located behind the target, there may be unintended collateral damage to civilian or friendly communications. In urban environments communication signals are regularly degraded due to buildings, trees, and power lines, which increase signal attenuation and make handheld systems less effective at longer ranges. Finally, even though they are more portable than their mobile or fixed counterparts, handheld systems are still bulky and unwieldy; Dedrone's DroneDefender weighs 15.8 lbs [77], making it an unwieldy piece of gear for soldiers to carry for a sustained period of time.

2.5.4 UAV-based

Capabilities:

The biggest benefit of an UAV-based (aerial) device is the maneuverability it provides for a defender [32]. By giving forward depth in the battlespace, a defender can deliver a payload at greater distances than handheld or ground-based systems [59]. With enough UAVs on hand,

UAV-based countermeasures can act as aerial security patrols that mimic the interdiction patrols ground units use in defensive operations. This concept is discussed in further detail in Chapter 5, and serves as the basis for experimentation in Chapter 7.

Limitations:
Similar to the limitations of a handheld device, the UAV-based C-UAS systems have a smaller payload size that operates on lower power settings to increase their sustainability. Because they cannot be sustained indefinitely, they must have a built-in hand-off connection between a ground station, which increases the complexity in the system. In aircraft design, these are known as SWaP considerations, which govern the systems and location of the systems placed on an aircraft [32].

2.6 Countering the Current C-UAS Technologies

The primary platforms employed by the DOD and DHS against adversarial UAVs are ground-based devices. Currently, CACI's CORIAN, Anduril's Sentry Towers, Lockheed Martin and Sierra Nevada Corporation's MADIS, as well as Dedrone's DroneDefender are the most prominent programs of record for both departments. While all four systems are capable in their own right, the costs and system designs limit their effectiveness against a coordinated adversarial attack.

To counter a ground-based, fixed system such as CACI's CORIAN and Anduril's Sentry Tower, an adversary could simply identify the towers visually or in the EM spectrum through direction finding methods. Because of the high power output of these systems, finding them in the EM spectrum would be relatively easy. With no ability to displace, the tower is vulnerable to a multitude of attacks; sabotage, EW, or a kinetic strikes would be the most likely methods an adversary could take.

Despite the platform's mobility, conducting a kinetic or EW strike against a mobile, ground system like the MADIS would be similar to the attack on a ground-based, fixed platform. Knowing that the MADIS is constrained to semi-improved roadways, an attacker could target the MADIS during a convoy operation with roadside IEDs, small arms, or a variety of ambush tactics.

With Dedrone's handheld DroneDefender there are several ways to limit its effectiveness. First, because the device uses a directional antenna, it only works against a UAS if the DroneDefender is pointed at its target. Additionally, because the device weighs nearly 16 pounds and is carried and operated by a soldier, if the soldier is not pointing the device in the target's direction for enough time, does not produce a high enough jam-to-signal ratio (JSR) to overcome the signal between the target and its GCS [78]. Additionally, because they are man-portable, they are unable to be used in an automated fashion. Therefore, when the DroneDefender is being used, it is constrained by the proficiency of its operator, the proximity of the operator to the target with relation to the target's GCS, and the inherent technical limitations of the system.

2.7 Current DOD Strategy, Doctrine, and TTPs

In the past decade, UAVs have made an outsized impact on the battlefield. Outside of special operations forces, the U.S. military has limited experience in fighting against adversaries using UAVs. In advance of a large-scale conflict strategy, doctrine and TTPs should be updated to better inform the conventional military's use of UAV countermeasures. Appendix 1 presents a more thorough explanation of C-UAS strategy, doctrine, and TTPs and is omitted from this section due to Controlled Unclassified Information.

2.8 Conclusion

To date, there remains an lack of sufficient C-UAS strategy, doctrine, or TTPs to address the threat UAVs pose to military installations and critical infrastructure. As outlined in this chapter, different C-UAS devices offer different capabilities as well as suffer different limitations. The energy required to sustain terrestrial systems is not sustainable under a multi-wave attack. If broadband RF jamming is used in urban areas, the potential for collateral damage is extremely high. Furthermore, countering a UAV swarm with the current suite of C-UAS weapons is not adequate; bullets travel farther than intended and RF jamming can shut down other communications for miles. Thus, to create a robust system that is capable of denying an adversary's use of UAVs and potentially future swarms, various C-UAS devices must be combined into a coherent defensive, layered system. In the next chapter, we take a closer look at RF mitigation techniques through EW and jamming.

CHAPTER 3:
C-UAS RF Mitigation Techniques

The following sections explore the principles of electromagnetic wave propagation, discuss link analysis, and provide an overview of methods to degrade the RF link between two devices. The main takeaway is that digital communications when bits of data are encoded onto RF waveforms, which requires the digital modification of analog waveforms [42]. Understanding modulation techniques allows engineers to analyze power spectral density plots and demodulate target signals. Given the requisite background in digital signal processing, the reverse engineer then decrypts the contents of each data packet or interferes with the communications between hosts. These concepts are important to grasp in order to understand the RF jamming techniques outlined later in this chapter, which informs the scenarios in Chapter 5.

3.1 Principles of Electromagnetic Wave Propagation

Digital communications are carried out through the modulation and encoding of bit streams between hosts [42]. In the past, analog communications were wholly dependent upon the hardware components built onto a device. However, over the past few decades electrical engineers, computer scientists, and others have vastly expanded the world's capacity to transmit data through the use of digital modulation techniques on software defined radios (SDR). The implementation and growth of SDRs has led to the ubiquity of telecommunications in modern countries because of the modularity afforded by changing a software program within a device. The commercialization of consumer- and micro-electronics has made SDRs less expensive for engineers to design radios for amplitude modulation communications, barrage jamming, or the remote injection of malware into a target device [79]. With this in mind, it is important to have an understanding of how EM waves propagate between hosts, as the information contained within messages can be captured by attackers, demodulated, and then decrypted to reveal useful information to an attacker.

3.2 Communications Link Analysis

The link between two communication systems encompasses the entire path, from the information source, through the encoding and modulation steps, into the transmitter and channel, up to the receiving source, and back through the signal processing steps until the communication link is terminated at the receiving information sink [41]. "Link budget" refers to the one-way link analysis of a signal. In determining the link budget, the engineer gains useful information about signal power, noise power, free space path loss, as well as environmental losses. By analyzing the link between systems, an error probability can be established to learn about the system's design, performance, and ability to communicate with other devices [42]. When dealing with spread spectrum signals that may operate beneath the noise floor, detection and interception of wireless traffic becomes very difficult because each communicating device operates on low-power settings that make it hard to distinguish between noise and a signal of interest [42].

3.2.1 Link Budget

When evaluating system performance, the most important variable to quantify is the signal-to-noise ratio (SNR). This is because a receiver must be able to detect signals in the presence of noise within an acceptable error probability. In order to evaluate the SNR of a system, there are several key pieces of information to be evaluated. Figure 3.1 shows the one-way transmission of an RF signal and the potential losses associated with that transmission.

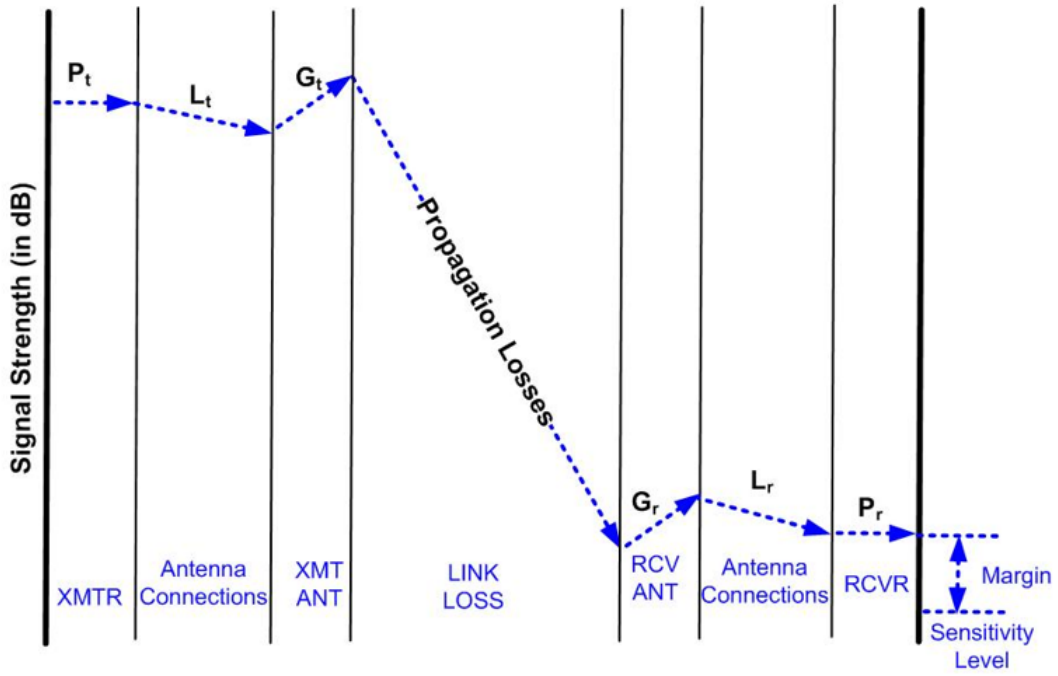

Figure 3.1. One-Way Communications Link. Source: [80].

The simplified one-way transmission shown in Figure 3.1 helps visualize the components in the Friis Equation, which is a mathematical formula for link budget analysis that is useful to identify the necessary received power of a communication device. The Friis' equation forms the basis for communication analysis and assumes a clear line-of-sight path with no secondary wave interference or reflections [42]. The equation also assumes that both the transmitting and receiving antennas are perfectly aimed towards one another to maximize gain and that both antennas are identically polarized [41].

Friis Equation: Linear Format

The linear format of the Friis equation (Equation 3.1) in [41] proves useful in link analysis.

$$P_r = \frac{EIRPG_r}{L_s L_p} \tag{3.1}$$

$$L_p = \frac{(4\pi R)^2}{\lambda^2} \tag{3.2}$$

$$EIRP = P_t G_t \tag{3.3}$$

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

where $EIRP$ is the effective isotropically radiated power, G_r is the gain of the receiving antenna, L_s are the system losses, L_p are the path losses, R is the distance between the receiving and transmitting antennae, λ is the wavelength associated with a given carrier frequency, P_t is the amount of transmit power, G_t is the gain of the transmitting antenna, c is the speed of light measured at 3 x 10^8 (m/s), and f is the carrier frequency measured in hertz [41].

The effective isotropically radiated power (EIRP) from Equation 3.3, is the amount of power emitted from an isotropic antenna to obtain the same power density in the direction of the antenna pattern peak which is calculated by multiplying the gain of the transmitting antenna by the net power from a connected transmitter [41].

Path loss, or L_p from Equation 3.2, is the power lost as the propagating wave front attenuates over a given distance, R, between the transmit and receive terminals [41]. The path loss is the most significant loss to account for and can prevent wireless communications from reaching their intended destination.

System losses, L_s, are important to note because telecommunication systems are imperfect, which leads to power losses from noise within the system [41]. The system noise occurs due to modulation distortions, mismatches between the transmitter and its antenna, or noise amplifications. More often than not, these losses are ignored when analyzing the full system; however, inducing excess system power loss is an important technique in disrupting communication systems.

Antenna gain, G_t or G_r, is the focused antenna output in a given direction where the beam has a maximum value relative to an isotropically radiated source [41]. In [41], the generalized equation for antenna gain is calculated by Equation 3.5:

$$G = \frac{4\pi A_{eff}}{\lambda^2} \tag{3.5}$$

$$A_{eff} = \epsilon A_p$$

where A_{eff} is the antenna's effective area, which is determined by ϵ, the antenna's aperture efficiency and A_p, the area of the antenna.

3.2.2 Received Signal Power and Noise Power

As mentioned in the previous subsection, determining the SNR power ratio at the receiving antenna is critical to the reception of telecommunications. This is given in [42] by Equation 3.7:

$$SNR = \frac{P_r}{P_n} = \frac{P_t G_t G_r}{L_p L_s} = \frac{EIRP G_r}{k T_s B_n L_p L_s} \tag{3.7}$$

where B_n is the receiver bandwidth, T_s is the system equivalent noise temperature, and k is Boltzmann's constant, $1.38x10^{-23}$ (J/K).

When analyzing digital communications it is essential to understand the received signal's power spectral density and its relation to the average energy per bit and the noise power spectral density. From [42], this information can be found by:

$$P_r = \frac{E_b}{T_b} = E_b R_b$$

$$P_n = N_0 B$$

where T_b is the bit duration in seconds and R_b is the bit rate in hertz.

Substituting P_r and P_n into Equation 3.7 yields Equation 3.10:

$$SNR = \frac{P_r}{P_n} = \frac{E_b R_b}{N_0 B} = \frac{EIRP B_r}{L_p k T_s B} = \frac{P_r}{N_0} = \frac{EIRP G_r}{L_p k T_s} \tag{3.10}$$

Communication engineers design communication devices to be optimized for reliable communications. In government systems, this includes the addition of sidelobe filters so that an attacker can only target the main beam of the receiving antenna, making it more difficult to jam [41]. However, with many commercial systems, engineers are seeking to optimize reliability at a reduced cost to increase the profit margin associated with manufacturing at scale. Given this understanding of communications link analysis, would-be attackers can more easily disrupt the RF link between antennas through a variety of jamming techniques. By taking into consideration the antenna size, transmit power, and carrier frequency with relation to environmental and system noise considerations, Equations 3.1, 3.7, and 3.10 inform the engineer to design a communications system that ensures reception. By understanding the variables within the Friis and the SNR equations, engineers can interpret how an influx of power will increase the likelihood of communication reception. Additionally, these equations allow engineers to analyze the negative effects of a system's temperature on the entire system. Finally, and most importantly, this type of analysis is important for engineers to design an antenna that fits the needs (in terms of type, size, and polarization) of the entire system. For example, a transmitting antenna that is right-hand polarized antenna will not be able to communicate with a receiving antenna that is left-hand polarized because of the difference in phase between the communicating devices. Additionally, a transmitting omnidirectional antenna can propagate in all directions around a fixed axis, but because omnidirectional antennas are inefficient, they require an excess of input power to maximize the received signal strength.

3.3 Jamming the RF Links

Currently, the current primary means of attacking the RF link of a communication system is done by jamming the signal between a transmitting and receiving antenna. RF jammers use a variety of strategies to generate high levels of noise and disrupt the link between an unmanned vehicle and its control station [58]. However, as many modern communications schemes employ LPI, LPD, and LPE modulation techniques [42], modern RF jamming equipment requires high-power output in addition to knowledge of the specific frequencies that an unmanned system is using to "hop" on. When it comes to UAVs that do not emit RF energy by connecting to a GCS, it is nearly impossible to use RF jamming as a mitigation technique. Thus, from this point forward, we will focus on the mitigation techniques for

UAVs that maintain some form of RF connection with its GCS. Given this, broadband noise (BBN), partial band noise (PBN), sweep, pulse, follower, and smart noise jamming are currently the most important techniques to understand when disrupting modern digital communications [58].

When using noise jamming techniques, a jammer modulates a carrier signal with a random noise waveform to interrupt the communication of an intended target [58]. The jamming signal's bandwidth can be as wide as the entire spectrum used by the target, or as narrow as a single channel.

Another jamming technique, *BBN jamming*, spreads Gaussian noise across the full width of the target's anticipated frequency spectrum [58]. For example, if a UAV and its GCS communicate on the 2.4 GHz frequency band, then a BBN jammer would place Gaussian noise across the 2.4-2.5 GHz frequencies, requiring 100 MHz of bandwidth. This technique is useful against all communications by physically locating the jammer between an adversary's communication links to overwhelm the legitimate communication with Gaussian noise. BBN jamming differs from the other techniques in this respect, as it is more focused on overwhelming an entire frequency band, instead of providing targeted disruption of a signal of interest. To mitigate fratricide, directional antennas are needed to avoid interference with friendly communications in the same frequency band [41]. Additionally, since broadband jamming raises background noise levels, it degrades the synchronization and tracking processes of the targeted communication scheme. The primary limitation with BBN jamming is its inefficient use of power, large system size, and the likelihood to inflict unintentional collateral damage to adjacent communication systems [58].

A *PBN jammer* uses noise-producing energy to disrupt multiple channels used by the target in a given frequency band [58]. PBN jamming differs from BBN jamming because it does not require channels to be adjacent to one another to disrupt the signal of interest. On the other hand, a *narrow band noise (NBN) jammer* focuses all of its noise energy across the width of a single channel [58].

Tone jamming is similar to NBN, but it uses one or more jammer tones placed strategically within the spectrum to disrupt a signal [58]. Single-tone jamming, also referred to as spot jamming, happens when the carrier wave is modulated to disrupt very narrow targets that do not change channels, such as on-off keying telegraphy [58]. Single-tone jammers can

be useful against DSSS systems to overcome the receiver's processing gain, thus causing adverse ramifications when signals are recombined within the communicating device [81]. When the jammer power is fixed, more power can be placed in a single tone, increasing the probability of overcoming processing gain. Multiple-tone jamming seeks the disruption of multiple channels at specific or randomly placed frequencies while comb jamming (another tone-jamming type technique) disrupts consecutive channels [58].

Sweep jamming is similar to broadband and partial-band jamming in that it uses a relatively narrow signal with an arbitrary bandwidth that is swept, or scanned, across the target's operating frequency band [58]. Because the signal is swept, this jamming technique can disrupt a wide frequency range in a short period of time. The sweep jammer can accomplish this by using low power and bandwidth requirements in comparison to BBN jamming. By using a designated bandwidth, the sweep jammer can degrade entire sets of hop frequencies where a PBN would be ineffective because of its fixed status [58]. Timing is the most important limitation in sweep jamming because the sweeping must be fast enough to ensure the whole band is covered in a sufficiently short period of time or the signal's frequency hops will occur at a time in which no signal is present [58]. However, sweep jamming cannot be so fast that it fails to adequately jam the fraction of the signal required [58].

A *pulse jam* is similar to PBN jamming but is predicated upon the time a jammer is used instead of being in a continuous-use state. While this leads to roughly the same effectiveness as PBN, pulse jamming has a lower average power consumption [58].

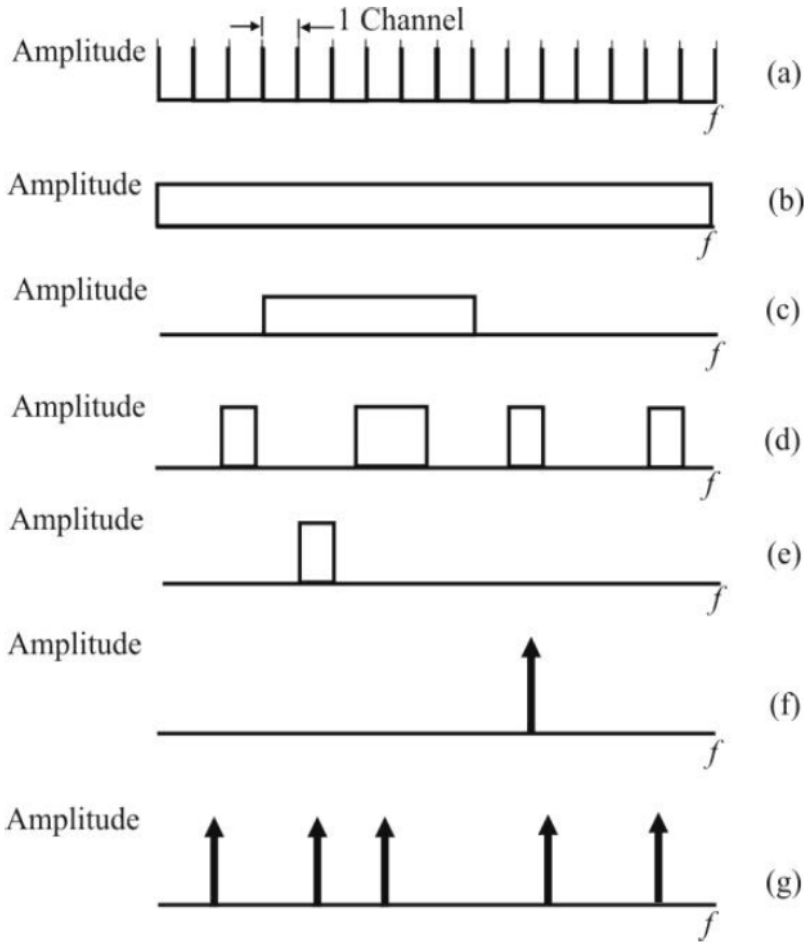

Figure 3.2. Noise Jamming Strategies: (a) single channel full-band jam; (b) full-band jam BBN; (c) contiguous PBN; (d) noncontiguous PBN; (e) NBN; (f) single-tone jam; (g) multi-tone jam. Source: [58].

Follower jamming attempts to locate the frequency to which the frequency-hopping transmitter moved, identify the target frequency of interest, and jam at the new frequency [58]. This is also referred to as responsive, repeater, or repeat-back jamming and is primarily constrained by the target's signal timing due to signal processing, wave propagation, and hopping speed.

Follower jamming with NBN places a noise waveform in the channel to hinder the receiver's ability to properly detect the tone, while follower tone jamming enhances the intended

receiver's ability to properly detect the signal just as it does for NBN jamming [58]. Noncoherent frequency shift keying receivers measure the energy from the channel filters for signal detection, thus adding additional energy at the correct frequency increases likelihood of detection.

FHSS jamming is best accomplished through the use of a follower jammer where only a portion of each dwell is jammed, meaning the jammer has to ascertain the newly detected energy and determine if it is the correct signal to jam.

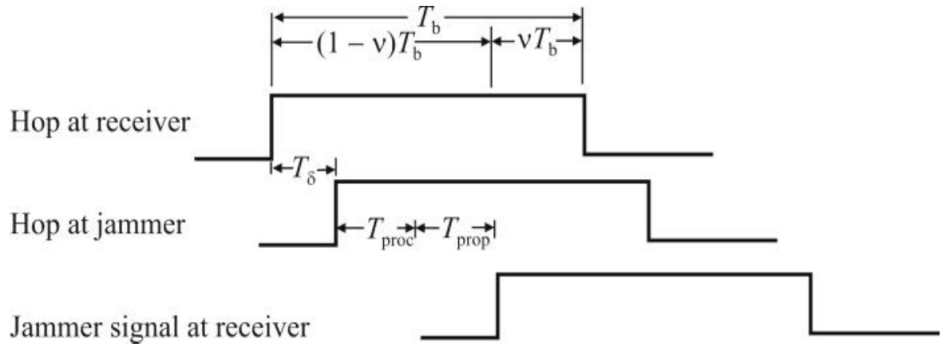

Figure 3.3. Frequency Hopping Follower Jamming. Source: [58].

Protocol aware or smart jamming disrupts digitized signals selected based on an algorithmic library [82]. While similar to follower jamming, protocol aware jamming requires more target information. Additionally, a protocol aware jammer is more capable in that it can predict the next frequency the target will hop to, therefore disrupting the signal continuously. This requires extensive synchronization and knowledge about the target signal to track the timing and phase of the transmitted signal. The major limitation with protocol aware jamming is that the time acquisition must be known to determine the signal used for communications [58].

3.3.1 Jamming Considerations

The goal of jamming a communications signal is to deny a reliable connection between two hosts using the minimum-required equipment, power, and antenna [58]. Thus, when designing communication systems, engineers seek to create jam-resistant waveforms to

"force a jammer to expend its resources over a wide-frequency band, for a maximum amount of time, and from a diversity of sites" [42].

In modern digital communications, anti-jam (AJ) communications seek to vary the frequencies used, time hop, and use narrow-beam antennas to put a jammer at a disadvantage compared to the communicator. These AJ techniques are used in frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS) modulation schemes. This is due to the notion that the intelligibility of information transfer can be sufficiently degraded by only jamming 30% of a voice transmission [78]. In AJ systems, an unmodulated carrier signal is centered on the transmitting frequency and then modulated with one (or more) tone signals, or modulated with a varying-bandwidth noise signal. These tones are placed based on prior knowledge of the target to prevent signal reception by raising the SNR [58].

When using a friendly UAV to jam an adversary's UAV, a Two-Ray Propagation JSR is useful in understanding the relationship between antenna height to find the optimal JSR due to ground reflections. In Two-Ray Propagation, it is assumed that both the receiver and transmitter are affected by ground reflections [58]. The JSR in Equation 3.11 has a linear correlation with the ratio of the jammer antenna's gain with respect to the target's transmitting antenna. Additionally, there is a linear relationship between the power ratio of the jammer in comparison to the transmitting device. This is expected, as the jammer power increases, that the targeted receiving antenna will be unable to communicate with its normal device. Additionally, from Equation 3.11, as the height of the jammer increases, the power requirements of the jammer to maintain the same JSR go down. This is because of ground reflections that are amplified when the height ratio is in favor of the jamming antenna. From [58], the JSR for Two-Ray Propagation can be found by:

$$\text{JSR} = \zeta = \frac{J_t G_{jr} G_{rj}}{S_t G_{tr} G_{rt}} \left(\frac{h_j}{h_t}\right)^2 \left(\frac{D_{tr}}{D_{jr}}\right)^4 \tag{3.11}$$

where J_t is the received jammer power, G_{jr} is the gain of the jamming antenna in the direction of the target's receive antenna, G_{rj} is the gain of the target's receive antenna in the direction of the jamming antenna, S_t is the target's signal power, G_{tr} is the gain of the transmit antenna in the direction of the receiver, G_{rt} is the gain of the receive antenna in the direction of the transmitter, $\frac{h_j}{h_t}$ is the height ratio of the jamming antenna and the target's

transmitting antenna, D_{tr} is the distance between the target's transmitting and receiving antenna, and D_{jr} is the distance between the jammer and the receiving antenna.

3.3.2 Spread Spectrum as Anti-Jam Techniques

Spread spectrum communication techniques transform a data signal to occupy a much larger bandwidth than the minimum bandwidth required to transmit a signal [42]. Spread spectrum techniques typically use a known-pseudonoise, or pseudorandom, spreading code shared between networked nodes, making interception difficult. The original data is then recovered by a receiver and synchronized using the spreading code, then compiled into the original data packet. The two most common spread spectrum techniques are DSSS and FHSS, which lower the probability of signal detection and interception, yielding higher security and privacy. The AJ properties of DSSS and FHSS signals force jammers to distribute their power over a wider bandwidth, which in turn increases system resilience by decreasing fading and increasing resolution range [42].

A DSSS device, uses a carrier wave modulated with a data signal, combined with a wideband spreading signal to send larger amounts of data between systems than a traditional narrow-band signal [42]. The spreading signals in DSSS techniques contain accumulated data that correlates to specific code sequences to ensure reception between the two communicating devices.

While similar in that they decrease the power required for reception and spread the signal over a given frequency band, FHSS devices occupy a given transmission channel for an allocated amount of time before moving to the next channel [42]. This allows each communication channel to be used by multiple devices and permits the FHSS signal to hop in a pseudorandom sequence with its receiving device.

Compared to other signaling methods DSSS and FHSS offer no error performance advantage against thermal noise [42]. On the other hand, they also have no disadvantage either, making them an attractive option for multiple access systems like WiFi routers and Bluetooth. Both DSSS and FHSS techniques shown in Figure 3.4 allow for the detection of signals that have a power spectral density below the noise floor, giving them the LPD, LPI, and LPE properties previously discussed [42].

DSSS is typically used in wireless links such as Internet of Things (IoT) devices and Institute of Electrical and Electronics Engineers (IEEE) 802.11 schemes while FHSS is used in wireless links where LPD and AJ properties are more desirable [83]. As Figure 3.4 shows, identifying and jamming a DSSS signal is easier to accomplish than for a FHSS signal [84].

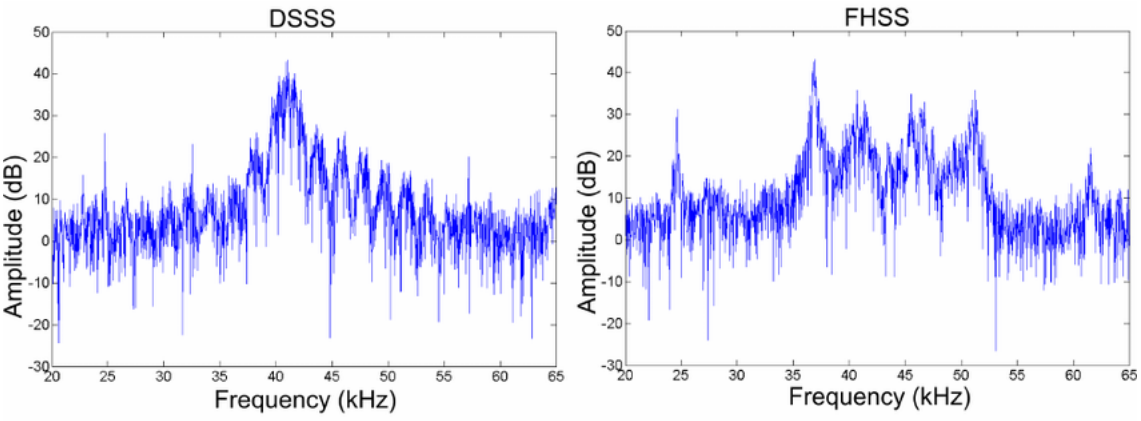

Figure 3.4. DSSS versus FHSS Plots. Source: [84].

From Figure 3.4, the DSSS plot shows a large amplitude spike around 42kHz whereas the FHSS has four distinct amplitude spikes at 36, 42, 46, and 52 kHz. Without transforming this information into the time domain, it appears that the FHSS signal is four separate devices transmitting instantaneous signals as opposed to one signal that is hopping between frequency channels. With this in mind, targeting a DSSS signal easier than a FHSS signal due to the lower probability of detection of the FHSS signal. Additionally, because IEEE 802.11 standards use the DSSS modulation technique [84], it is easier to target these types of devices even if they are difficult to find. This is discussed in Chapter 7 where the proof of concept targets 802.11 communication links between a UAV and its GCS.

While the jamming of DSSS signals is easier than FHSS signals, it is by no means trivial. Figure 3.5 shows the spreading codes used in DSSS which make single tone jamming obsolete. These spreading codes then necessitate a broadband noise jam, causing the EW engineer to design a system that requires large power consumption to overcome the target's received power [42].

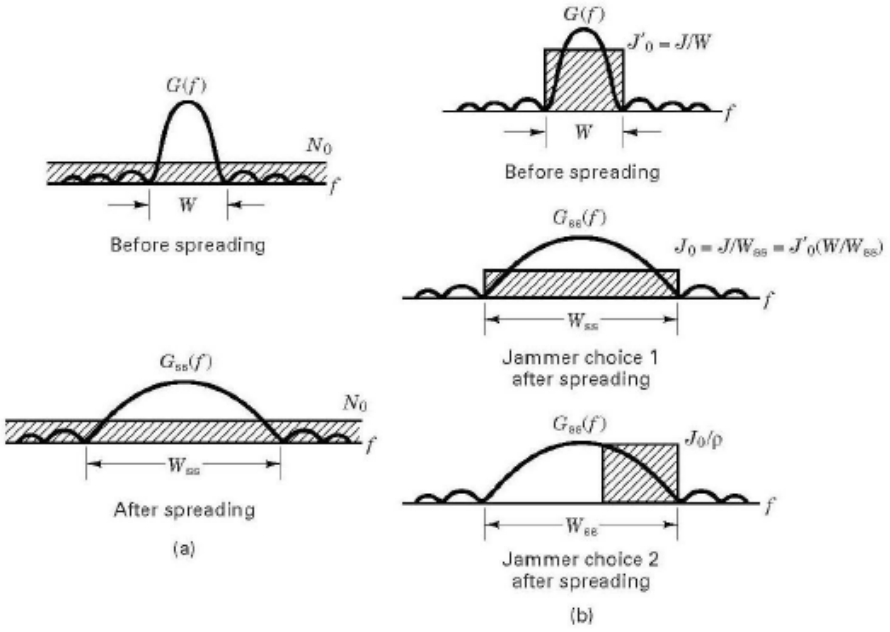

Figure 3.5. DSSS Jammer Plot. Source: [42].

3.4 Conclusion

Due to the clutter in the ISM bands where most commercial UAV communications occur, RF detection and mitigation are very complicated problems to solve. The LPD, LPI, and LPE characteristics of FHSS and DSSS signals allow the signals to hide amongst the background clutter, making it more difficult for attackers to identify and disrupt signals of interest [42]. Engineers and EW system designers can develop more effective mitigation measures by understanding RF communications, the link budget equation, and the fundamentals of jamming. This understanding is foundational to the attack methods outlined in the example scenarios in Chapter 5.

It should be reiterated that, regardless of which RF jamming technique is used, the necessity of significant power increases the physical parameters of a system. This has a deleterious effect on the form, fit, and function of a modular payload that could be used as a bolt-on solution to other systems. In addition to the issues with SWaP tradeoffs, RF jamming also has negative effects on the sensors packages integrated on board its host aircraft. Because

of the collateral damage and SWaP considerations, integrating RF jamming on manned and unmanned aircraft is an incredibly difficult process [85]. While spread spectrum techniques do offer higher security and privacy to users because of lower power requirements that make them more difficult to detect, there is still a need for data encryption and authentication to ensure that digital signals reach their intended recipients [86]. It is here where we turn our attention to the use of cyber-attack techniques for opportunities to disrupt adversarial UAVs.

Throughout this chapter, power requirements were addressed repeatedly in the Friis equation, the SNR equation, and the JSR equation. A major component of each of these equations is the power required for interception of communications between end-devices. When using electronic attack methods such as RF jamming, the calculus becomes a matter of overpowering the signal strength between two users. Notably, this type of link budget analysis is absent when discussing cyber-attack techniques. This is because cyber-attacks exploit the communication protocol vulnerabilities, instead of trying to overpower the received signal of a targeted device. While the link budget is still a factor when delivering a remote cyber-attack, it is only important insofar as an attacker can send one packet containing malicious data to its intended target.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 4:
Cyber-Attacks as C-UAS Mitigation Techniques

Over the past thirty years information and consumer technology has massively impacted the lives of people worldwide. Simultaneous to the development of new information systems, hackers and nefarious actors have sought to steal, manipulate, and exploit the data transmitted between devices. In some instances, hacking led to the creation of solutions that are both more capable and more secure. In other cases, nefarious actors broke into target systems to wreak havoc, gain online credibility, or make themselves rich and famous. In the mid- to late-2000s, hacktivist groups like Anonymous sought to impose their will on Visa and Mastercard by carrying out distributed denial of service (DDoS) attacks in response to those companies banning transactions between the WikiLeaks website and its users [87]. More recently, both state and non-state groups have turned to ransomware attacks to steal and encrypt data with the hopes of collecting massive ransom payments from their targets [11] [88].

UAVs operate using the same principles of digital communications as terrestrial information systems, making them vulnerable to the some of the same cyber-attacks carried out in the past three decades. To begin this chapter, Section 4.1 discusses the OSI Model and how it enables the transmission of digital information. Then, Section 4.2 covers the most applicable cyber-attacks to target UAVs. While there are technical limitations to each cyber-attack technique, this approach takes more of a scalpel's edge approach when compared to RF jamming. Cyber-attack vectors typically require less power because they have *a priori* knowledge of an information system. Second, cyber-attacks lower the risk of collateral damage to surrounding infrastructure. Finally, because there are lower SWaP requirements in comparison to RF jamming, cyber-attacks can be easily delivered via a friendly UAV.

4.1 Open Systems Interconnection Model

The OSI Model shown in Figure 4.1 is a seven-layer model that represents how information is transmitted between digital communication devices. The seven components are the application, presentation, session, transport, network, data link, and physical layers [89]. While layers 5-7 are tightly coupled and grouped together, it is important to separate each layer be-

cause of how communication protocols affect the packaging, transmission, and presentation of information.

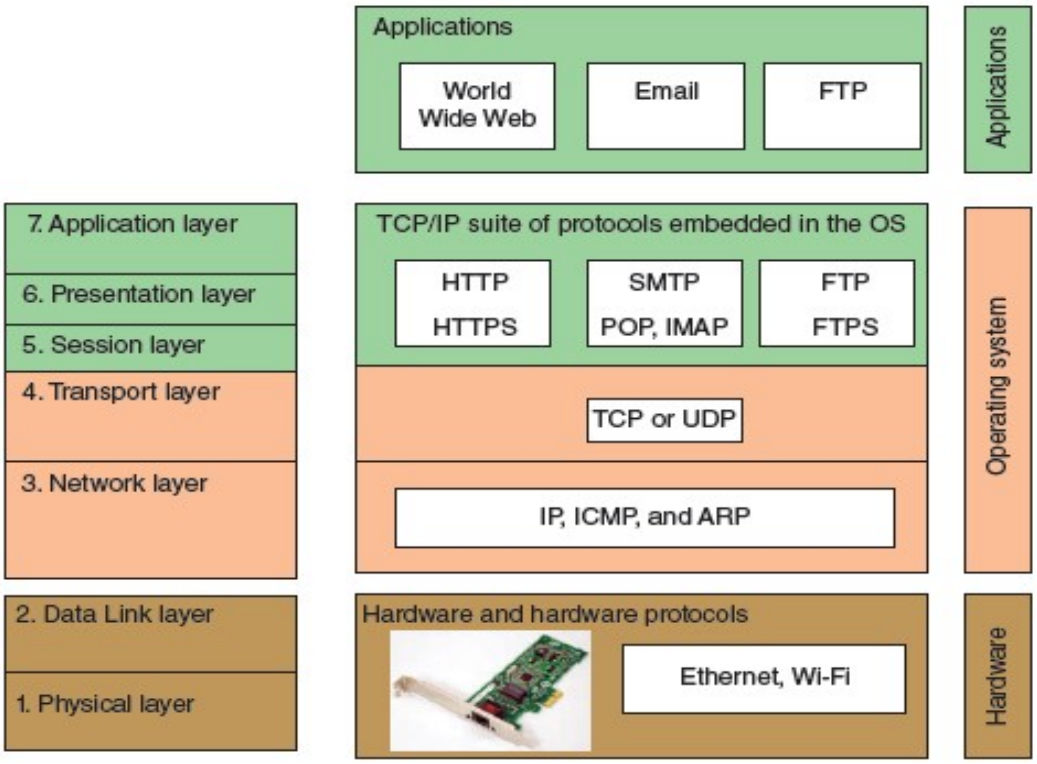

Figure 4.1. Seven-Layer OSI Model. Source: [90].

To introduce the seven layers of the OSI model it is helpful to use the analogy of sending a letter through the mail service and road system, with each layer governed by a different set of protocols [90]. Beginning with a user writing a business letter, the sender then drops their letter off at a post office box. From there, the post office sorts and processes the mail to send to a delivery truck, where the driver adheres to local traffic laws. Once reaching their destination, the driver drops the letter off at the receiving person's mailbox.

As it relates to the OSI model, the actions where the sender writes, packages, and drops the letter in the mailbox correspond to layers 5, 6, and 7 [90] of the OSI model. The infrastructure required by the road network, post office, and delivery drivers are layers 1-4 are considered to be a part of the telecommunications stack, where RF communications intersects with digital modulation. The system finally terminates when the recipient reads,

opens, and processes the contents of the letter, where layers 5, 6, and 7 remain the same layers as when the letter was sent; this time, in reverse order. Lastly, protocols refer to the standard operating procedures for a given action. For example, a business letter is written in accordance with specific rules, also known as a protocol.

4.1.1 Layer 7: Application Layer

The Application Layer is the interface where data passes through two (or more) applications or utility programs on different computers [90]. This includes the application programs that provide web browsers and web servers using Hypertext Transfer Protocol and Hypertext Transfer Protocol Secure, as well as the utility programs that provide system services like Simple Network Management Protocol [90].

4.1.2 Layer 6: Presentation Layer

The Presentation Layer displays data in a manner that the receiving application can interpret [90]. When sending an email, this takes the form of compression, encryption, and translation of an email sent between hosts [89].

4.1.3 Layer 5: Session Layer

The Session Layer receives raw data without division or concatenation to provide the presentation layer with organized data for multiple sessions [89]. The layer 5 protocols establish and maintain a session connection between hosts [90].

4.1.4 Layer 4: Transport Layer

The Transport Layer transfers Application Layer payloads by using control information to encapsulate data packets to send data to a specific port on a receiving machine [90]. The two primary Transport Layer protocols are Transmission Control Protocol (TCP) and user datagram protocol (UDP), both of which compress packets into a transmissible size. For TCP these compressed messages are called segments, while UDP divides messages into datagrams.

TCP is referred to as a connection-oriented protocol because it uses a “three-way” handshake to guarantee message delivery between hosts [90]. The initiating client sends a synchronize

(SYN) packet to the receiving device, which follows up with a SYN/acknowledge (ACK) packet to correlate and confirm receipt of the connection. Finally, the initiating client sends a final ACK packet to their intended recipient to confirm and establish a true connection. If at any point the handshake is broken, the transmitting host receives information stating that the desired message was not delivered [91].

Meanwhile, UDP is considered a connectionless protocol that does not guarantee delivery the same way that TCP does. UDP is typically used for broadcasting information or monitoring network traffic and is faster at transmitting data than TCP [90]. Figure 4.2 shows a visual representation of the TCP handshake method and the UDP connectionless broadcast.

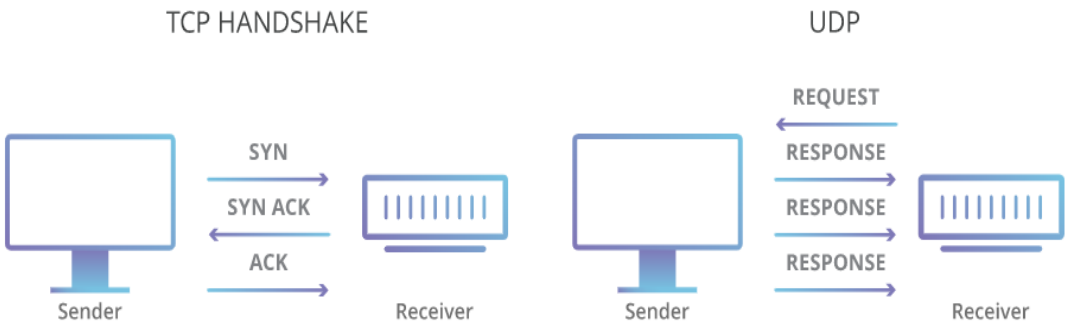

Figure 4.2. TCP versus UDP Communications. Source: [92].

The TCP protocol is more reliable than the UDP protocol because of its connection guarantee for information transmission. However, it is slower than UDP and if an attacker can disrupt an element of the TCP handshake, they can carry out a DoS attack. Both TCP and UDP flood attacks were used by the hacktivist group Anonymous in the 2010 DDoS attacks [87].

4.1.5 Layer 3: Network Layer

The Network Layer transfers messages between nodes by determining the physical path a message takes until reaching its destination host [90]. It is also known as the Internet Layer, and the most common protocol used is Internet protocol (IP), which makes a packet by adding a header to the segment or datagram. This header identifies the transmitting node and receiving host by an IP address, unique to each node on a network [90].

IP is supported by other protocols like Internet Control Message Protocol and Address Resolution Protocol, which help the transmitted packet find its way to its destination [90]. Adding the network layer header makes the packet larger, and if it is too large for transportation, the protocol breaks the packet into fragments. The fragmentation process is not lossless, which may lead to a receiving host not recovering all of the transmitted data [90].

4.1.6 Layer 2: Data Link Layer

The Data Link Layer adds its own control information in a header at the beginning of a packet and in a trailer at the end of a packet. This transforms the data packet from the Network Layer into a frame which contains the hardware media access control (MAC) address of the transmitting and receiving network interface cards (NIC) [90]. A MAC address, also referred to as an extended service set identifier (ESSID) or a hardware address, are unique device identifiers that can only be found within nodes on the local network [90].

Most MAC addresses are required to register with the IEEE organizationally unique identifier (OUI) public database [93]. This forms the basis for the experimentation covered in Chapter 7, as this public information provides would-be attackers with an easy method to automate the identification and attack of a wireless access point. MAC addresses are also easily spoofed, allowing attackers to mask their identity. For the purposes of experimentation in Chapter 7, the data link connection between a target UAV and its GCS is targeted.

4.1.7 Layer 1: Physical Layer

The Physical Layer represents the interaction at the bit level from which an information system sends streams of "0s" and "1s" via a wired or wireless transmission to its destination [90]. It is here where the OSI model then interacts with EM waves that propagate between receiving and destination sources. This interaction is where the RF jamming techniques discussed in Chapter 3 seek to disrupt the communication flow between information systems.

4.2 Attacking the OSI Model

Now that a baseline understanding of the OSI Model is established, there are several noteworthy cyber-attacks for eavesdropping, intercepting, or interrupting the data between a

UAV and its GCS. It is much simpler to carry out attacks on UAVs using IEEE 802.11 wireless schemes than on UAVs using FHSS modulation schemes. This is because IEEE 802.11 WiFi communication uses a DSSS technique [94], allowing for the easy targeting of layer 2 MAC addresses, while FHSS eavesdropping spreads the signal out over a larger frequency range with a hopping sequence to match. Thus, even if eavesdropping is successful, creating a FHSS transmitting device to successfully inject malicious packets of information at the correct hop speed and with the right information is a highly complex problem. However, given the requisite information by reverse engineering a signal of interest, the following attacks are possible as singular or combined options against a target UAS.

4.2.1 Man-in-the-Middle Attacks

A man-in-the-middle (MITM) occurs when an adversary intercepts the communication between two communicating devices and, by various means, is able to successfully impersonate one device to the other, ultimately giving the attacker access to the transferred data between end-users [95]. Also known as an adversary-in-the-middle attack, this attack compromises the integrity and confidentiality of a given security scheme without notifying the server or the client. By subverting entity authentication controls and intercepting the communications, an attacker can subsequently alter and manipulate the information transmission between devices at their discretion—including hijacking a target or spoofing GNSS navigation [96]. Thus, a MITM compromises the confidentiality, integrity, and availability between two communicating devices through impersonating, location-based, or communication channel techniques [95].

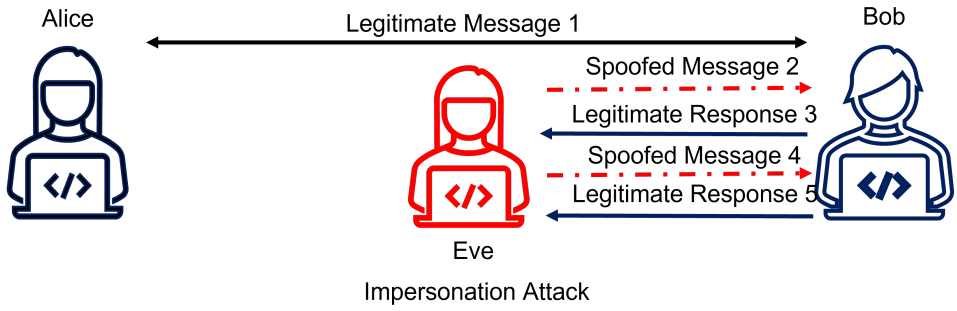

Figure 4.3. Impersonation (Spoof) Attack with a Man-in-the-Middle. Adapted From: [95].

Understanding methods to achieve a MITM is essential to grasping the attacks laid out in the framework established in Chapter 5. According to the Common Attack Pattern Enumeration and Classification community, a cyber-attack resource operated by the government-contracted MITRE Corporation, a MITM has the following prerequisites: two components must be communicating with each other with insufficient encryption or data authentication for an attacker to identify and eavesdrop on the communication exchange with or without the target's knowledge. Alternatively, there is a lack of sufficient mutual authentication between the targets giving way to attacker interposition. From this point, an attacker can subsequently manipulate the actions of its target [96]. As seen in Figure 4.3, a MITM is reliant upon the exploitation of protocol or system vulnerabilities, which makes a MITM more of an end state instead of a cyber-attack. In this figure, Eve is the MITM seeking to intercept the network traffic between Alice and Bob. Once Eve is able to establish a network connection between her targets, she then carries out a variety of attacks, including the hijacking and spoofing of network traffic.

4.2.2 DDoS Attacks

While much different from a MITM, protocol attacks such as UDP and TCP/SYN Flood attacks can be an integral part of achieving a desirous end state for the attacker. Both the UDP and TCP/SYN Flood are examples of DoS attacks that are more effective when multiple, distributed systems are used, creating a DDoS attack [97]. Figure 4.4 shows a DDoS attack using computers and other networked IoT devices to create a surreptitious botnet that prevents normal communications from occurring as planned [98].

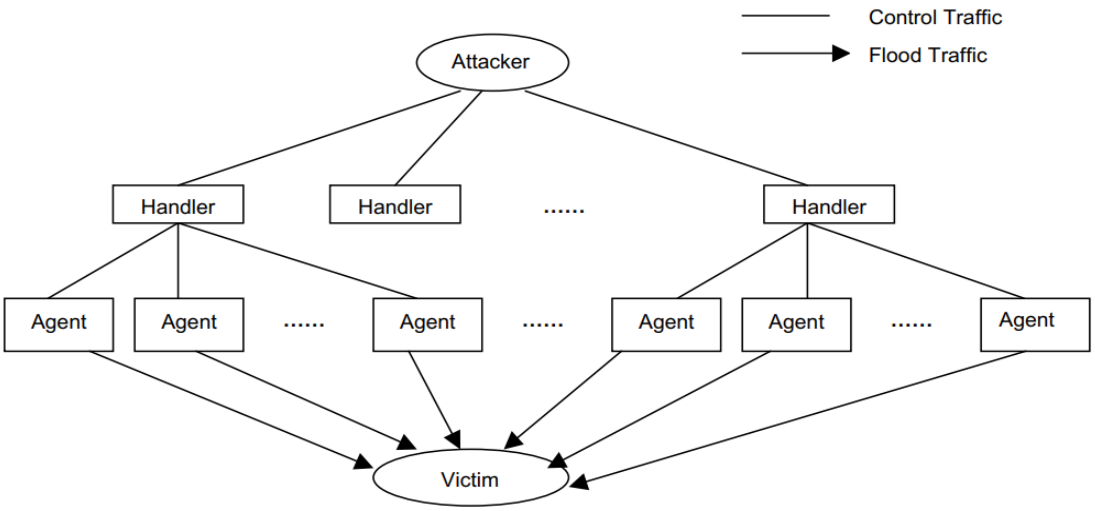

Figure 4.4. Architecture of DDoS Attacks. Source: [97].

Both flood attacks are easy to carry out using open source tools like Low-Orbit Ion Cannon or hping3 to flood a target server with TCP or UDP packets to disrupt the service connection [99]. The DDoS attack is particularly sinister if implemented properly as this type of attack is unpreventable and can only be mitigated through firewall strengthening and filtering protections [97].

4.2.3 UDP Flood Attack

In February 1996, the CERT Coordination Center at Carnegie Mellon University "received reports of programs that launch DoS attacks by creating a 'UDP' packet storm either on a system or between two systems" [100]. This is known as a UDP Flood attack that degrades the host performance by increasing packet congestion. This attack is also accompanied by IP spoofing, and because the UDP protocol is connectionless, an attacker can send out broadcast packets to congest and deny service to all hosts on the network [100]. While a DoS attack can be devastating, this type of attack by itself does not allow an attacker to gain additional access to a target system.

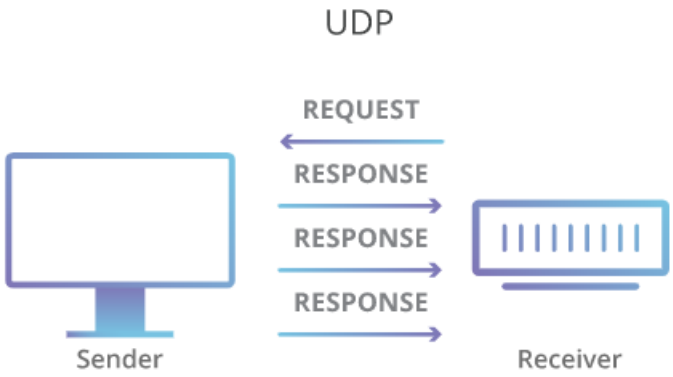

Figure 4.5. UDP Communications. Source: [92].

UDP Flood attacks can deliberately target and disrupt local firewalls because the UDP protocol has built-in resistance to local firewall protections [100]. Therefore, the only meaningful way to stop this type of DDoS attack is through dedicated DDoS protection built into the application and transport layer protocols.

4.2.4 TCP/SYN Flood Attack

In September 1996, the CERT Coordination Center at Carnegie Mellon University issued another CERT Advisory regarding TCP/SYN Flood and IP spoofing attacks [101]. This advisory described an attack method that exploits the three-way handshake in the TCP connection process outlined in Section 4.1.4, which is displayed in Figure 4.6.

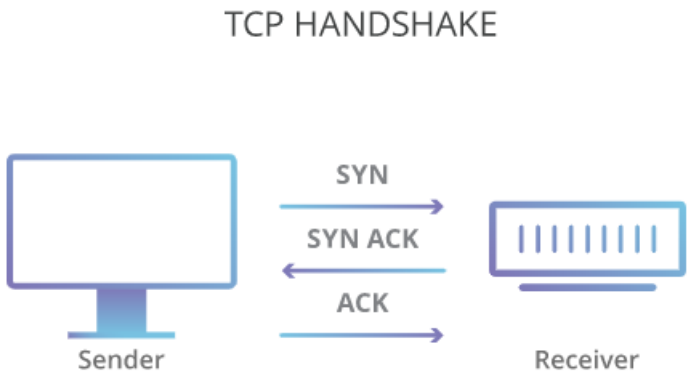

Figure 4.6. TCP Three-Way Handshake. Source: [92].

A TCP Flood attack works by exploiting the open "SYN-ACK" connection between a client and a server before the "ACK" message is received by the server. Because the server's data structure is of finite size, sending an overflow of partially-open connections with a spoofed IP address denies the connection between the original client and the victim server [101]. Ultimately, a TCP Flood attack results in a DoS, where the service itself is unharmed, but the ability to provide the service is impaired by exhausting memory, crashing the system, or rendering it inoperable.

This attack is significant because any device that is connected to the internet is vulnerable to this type of attack, making it difficult for the victim to accept any new network connections. Because the IP address is spoofed, the network continues forwarding packets based on its destination address unless input source filtering is enabled, which is only a temporary fix in reducing IP spoofed packets.

4.2.5 Deauthentication Attack

A layer two deauthentication attack exploits behavior in 802.11-based wireless access points to prevent legitimate users from accessing a network [102]. A deauthentication attack is very adaptive, as an attacker can elect to limit an individual client's access or deny service to an entire channel. To prevent a target from hopping to a new channel, an attacker can simultaneously scan adjacent channels to deny service continually.

A deauthentication attack can be delivered by placing a wireless NIC in monitor or promiscuous mode so an attacker can view the network traffic between a user and a wireless access point by correlating the MAC hardware addresses associated with each device [103]. The MAC addresses of layer two devices are easily scanned via the public IEEE OUI database where attackers can scan for specific targets [93]. From [102], Figure 4.7 shows a graphical depiction of the deauthentication attack where an attacker only has to generate one packet for every six exchanged between a client and access point.

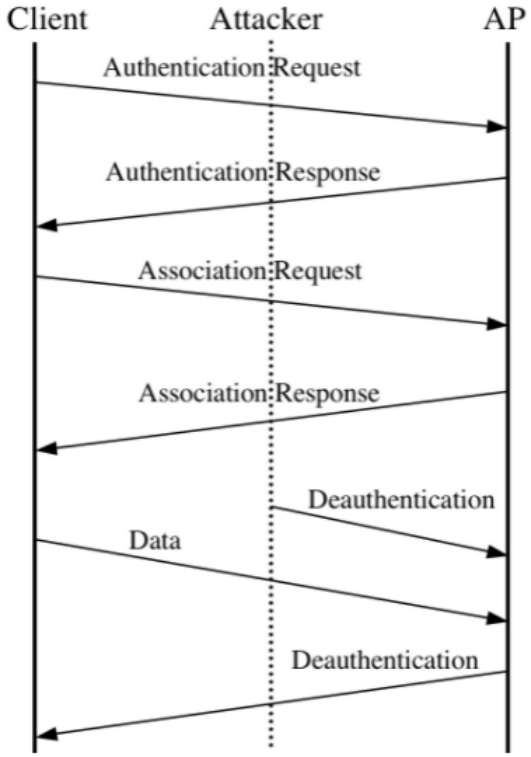

Figure 4.7. Deauthentication Attack. Source: [102].

Regardless of network encryption such as Wired Equivalency Protocol, WiFi Protected Access (WPA), WPA2, or even WPA3, an attacker can deliver a DoS attack by simply sending deauthentication frames between a target access point and its legitimate clients [102]. This type of attack is especially useful in capturing the WPA handshake between access points and clients for offline dictionary attacks used in gaining access to a target system [103]. The deauthentication attack is useful in energy conservation but is limited in that it is only effective against targets using MAC protocols—such as wireless access points.

4.2.6 Reflection Attack

A reflection attack occurs when an adversary reflects a message to the sender by impersonating the receiving host [104] which can lead to a DoS or an impersonation attack. For example, if Alice and Bob are communicating with one another, and Eve is the MITM, Eve would impersonate Bob and send the reflected message that originated with Alice back to

Alice.

The mutual authentication standards found in [104] established a distinguishing identifier between users. However, there are no requirement for UAV manufacturers to comply with the standardization process from the International Organization for Standardization. Additionally, the work from [105] shows that despite yielding integrity and authenticity, the mutual authentication standard does not yield privacy for communicating users. Thus, to successfully carry out a reflection attack, an attacker must have first-hand knowledge of the protocol, the most vulnerable part of which is when a client initiates the handshake rather than a server [106].

4.2.7 Replay Attack

As seen in Figure 4.8, a replay attack occurs when network traffic is captured between hosts and then retransmitted back to either host. By retransmitting the captured information, an attacker can use the authenticated traffic to produce undesired effects or gain unauthorized access [107].

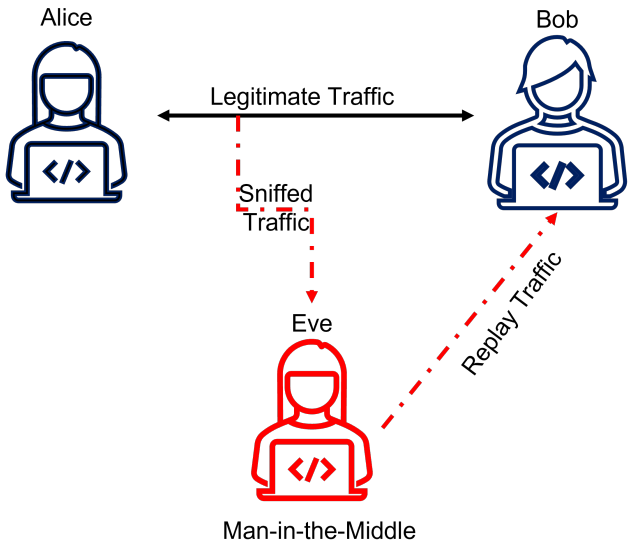

Figure 4.8. MITM Replay Attack.

These attacks can be especially useful when an attacker is able to impersonate a legitimate user, thus gaining access to the network and issuing commands to the target client.

4.2.8 Key Compromise Impersonation Attack

A Key Compromise Impersonation (KCI) attack occurs when an attacker compromises e.g. a client secret key and then uses that information to impersonate connections back towards the client for further exploitation [108]. While most of the literature on these attacks focuses on compromising Transport Layer Security (TLS), a KCI attack may be useful for a C-UAS device. This is because a KCI attack targets the cipher weaknesses in authenticated key agreement protocols, which in turn allows the attacker to conduct further MITM attacks to block connection, connect to the victim server illegitimately, or issue malicious code to the victim [109]. If an attacker can compromise the authentication key established between a UAV and its GCS, the attacker can then impersonate the GCS [108]. This type of attack would target the keys on the UAV, as opposed to the keys on the GCS, which is more of a concern than compromising the GCS key.

4.2.9 GNSS Spoofing

GNSS spoofing is an attack method where a spoofer generates a counterfeit signal for each authentic signal received to distort the relative true location of a target in favor of a counterfeit location that is more favorable for the spoofer [66]. In order for an attacker to sufficiently exert control of a target device via GNSS spoofing, the attacker must capture the GNSS signal of interest dynamically or through *a priori* knowledge. There are two primary methods of capturing GNSS signals for spoofing attacks: overt and covert capture.

Overt Capture

Overt capture involves GNSS jamming of the authentic signal followed by the injection of a new reacquisition signal. In this type of capture, the attacker does not conceal its attempted subjugation, and experiments have shown that a power differential, η of 10 dB is sufficient in overwhelming the authentic signal, P_a in favor of the spoofer's signal, P_s [66]. As described in [66], Equation 4.1 yields:

$$\eta = \frac{P_s}{P_a} \tag{4.1}$$

where η is the spoofer power advantage, P_a is the power of the authentic signal, and P_s is the power of the spoofing signal.

Covert Capture

Covert capture differs from overt capture in that it seeks to avoid the anti-spoof blockers a target may have and remaining undetected throughout the spoofing process. This is done through evading the target's JSR monitors, as well as evading the frequency unlock monitoring of a GNSS receiver [66]. Covert capture is a more effective spoofing technique than overt capture as it bypasses the target system's internal blockers without alerting the target that it is receiving counterfeit GNSS signals. However, covert capture is a highly complex process and difficult to implement.

4.3 Conclusion

In sum, the attack types outlined in this chapter provide a baseline for researching future attack vectors against adversarial UAVs. To make this a fully realized effort, there needs to be a library of attack vectors designed to mitigate the threat posed by commercial UAVs and integrated with a menu of options within a graphical user interface (GUI). This fully-automated GUI would give the operator monitoring the system a common operating picture of local threats and actions taken. While this was only lightly touched on in the discussion on deauthentication attacks, cyber-attacks notably consume less power than the BBN jamming techniques mentioned in Chapter 3 [110]. This is because each cyber-attack focuses on protocol vulnerabilities within the OSI model instead of trying to overwhelm the received signal during an RF jamming attack. While each attack covered exploits a different (sometimes overlapping) protocol vulnerability than the others, and some can be patched easily, many UAV manufacturing companies continue to design and build UAVs with known vulnerabilities. This is in part due to the lack of concern for data privacy and security by consumers because the typical commercial user wants an efficient product at a low price point. To conclude, this chapter gives a variety of attack considerations for escalation of force procedures in protecting strategic infrastructure.

CHAPTER 5:
Redesigning the Counter Unmanned Systems Architecture

Now that an understanding of C-UAS technology is established, this chapter builds upon the knowledge gained from the previous two chapters to form a new framework to augment and enhance the current C-UAS systems. As previously discussed, the most capable of the C-UAS technologies on the market are the static ground systems like the CACI Skytracker [37] and the Anduril Sentry Tower [38], as well as the mobile MADIS [53]. While all three systems have had operational successes, like the MADIS in a 2019 engagement in the Straits of Hormuz, [111], these "watch-tower" type systems indicate that the acquisition of C-UAS technology remains incomplete. This is because each system, while capable in its own right, has significant disadvantages when facing more than one UAV threat. The doctrine that was outlined in Chapter 2 proves that there is a lack of robust systems and procedures in place to handle a multi-axis and multi-wave attack against adversarial unmanned system. Thus, both the DOD and DHS should invest in the design, procurement, and integration of a constellation of unmanned systems to serve as aerial security patrols. The adoption of these stand-in devices will give commanders increased force protection measures beyond the high-performing yet extremely vulnerable sentry towers.

What is being proposed in this chapter is a novel approach to enhance current practices used in defense-in-depth and air-to-air combat operations. In historical warfare revolutions, technology has created an opportunity space for new procedures, techniques, and tactics to take hold. Whether this was the biplane in WWI [112], anti-ship cruise missiles in the Yom Kippur War [113] [114], or precision-guided munitions during Operation Desert Storm [115], technology has been the first innovation while organizational and tactical implementation has followed closely thereafter. By borrowing from the lessons learned in modern defensive operations and air-to-air combat, this chapter focuses not on innovative technology, but instead revises the current tactics used in countering unmanned systems and outlines a unique way of approaching the problem. Rather than the aerial battles that have captivated audiences for over a century, the dogfights of the next century will be defined by shooting bits of information and electromagnetic waves instead of rockets and missiles.

The following sections detail a strategy to use friendly UAVs in C-UAS combat. Instead of the kinetic-kill options that many are developing, these devices are designed to carry soft-kill electronic warfare and cyber-payloads. For the following framework to work in its designed capacity, airborne C-UAS must exist solely to destroy other aircraft. As with fighter aircraft development, increasing the requirements to create a generalized EW UAV will dilute an aerial C-UAS' ability to effectively combat adversarial UAVs and UAV swarms [116]. This chapter begins with a discussion on defense-in-depth tactics used by the U.S. Marine Corps (USMC), then provides an overview of aerial interdiction, before identifying the pros and cons of current technology. Finally, this chapter concludes with two hypothetical scenarios of an attack on a hydroelectric power facility to illustrate the concepts contained herein. The first scenario illustrates the defense of a hydroelectric power facility using the current watch tower C-UAS technology. The second scenario includes the addition of the *Detachable Drone Hijacker* as a new C-UAS weapon for the security team to utilize in the defense of the hydroelectric power facility.

5.1 Defense in Depth

Marine Corps warfighting publication (MCWP) 3-01, Offensive and Defensive Tactics defines a defensive operation as "an operation conducted to defeat an enemy attack, gain time, economize forces, and develop conditions favorable to offensive or stability operations" [117]. Defensive operations create the conditions that allow a friendly force to recover and regain operational initiative by denying an enemy's access to vital areas or by eroding an enemy's ability to concentrate firepower in an attack. While there are myriad defensive positions to analyze, they are all designed to defend in depth using a main engagement area (e.g., a main battle area), a support area, and a security area where forward positioned patrols gather information and interdict the enemy. In the example shown in Figure 5.1, the defenders are using the perimeter defense to give 360-degree coverage of a vital asset, which in the case of C-UAS would be a military base or installation [117].

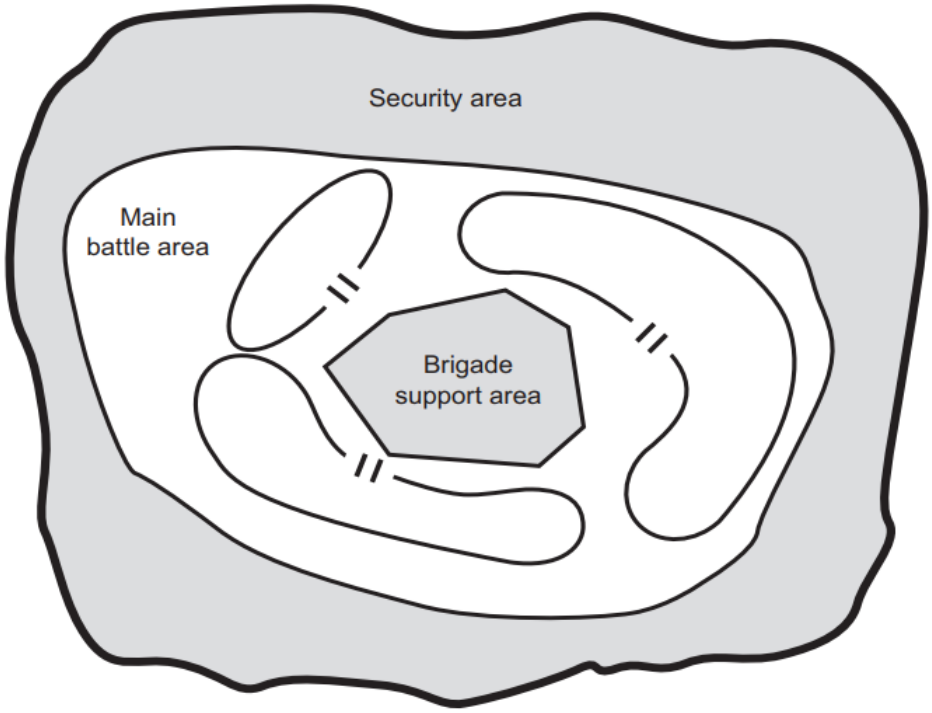

Figure 5.1. Sample Perimeter Defense. Source: [117].

Defensive operations are characterized by maneuver, preparation, flexibility, mutual support, and surprise to disrupt an adversary's attack momentum [117]. In a defense-in-depth scenario, this is achieved by engaging the enemy at the earliest opportunity with security forces as well as moving reserve and fire support units to positions of advantage [118]. This gives the defense a buffer against an attacker's main thrust, ensuring that the attacker commits their forces in piecemeal fashion and preventing the attacker from massing firepower where they intend.

In the context of defending infrastructure against adversarial UAVs, the goal of the defense is to maintain normal operations without interruption or degradation from an attack. Given that most bases and critical infrastructure in the continental U.S. have defined physical perimeters with restricted operating zones for aircraft, the main engagement area in the C-UAS fight becomes a matter of procedure based on standard operating procedures and terrain restrictions [119]. In defensive operations, this engagement area development establishes control measures and trigger lines to outline specific weapons and actions to be taken

given a set of circumstances [117]. These escalation of force procedures are well-defined for human incursions into a military facility, yet they remain immature in the C-UAS fight.

In the planning process for carrying out defense-in-depth, the Marine Corps teaches its officers seven steps of engagement area development. One of the first actions taken is to gain depth in the battle space by launching security patrols to interdict would-be attackers [117]. These security patrols are designed to increase the situational awareness of the ground force commander and are given with several guiding principles: observe, report, and protect against enemy infiltration or ambush [120]. This may, or may not, require a security patrol to engage the enemy kinetically, making the patrol essential for the successful execution of a ground commander's mission.

This begs the question, why is there not a similar outlined process for defending U.S. bases and infrastructure against adversarial UAVs? The author contends that this is because there has yet to be a serious multi-wave attack using only unmanned systems. The current method for defending military installations and critical infrastructure from UAV incursions mirrors the static defense of medieval forts and castles rather than the maneuverable defenses of the 21st century. In a medieval defense scenario, there is a wall that is designed to be impenetrable, watch towers to cover entry points, and indirect fires that cover the obstacles in front of the fort. However, as with medieval fortresses, if one portion of the wall or gate comes down, the enemy can flood through that access point and inflict massive amounts of damage. In the context of C-UAS, watch towers are quite literally named "Sentry Towers," like the Anduril product [38], and yet they are usually the sole defensive measure against an adversarial UAS attack. While these tower systems are the most capable defensive systems, if an intruder slips through, escalation of force procedures dictate the use of shotguns or battering ram UAVs [76]. This lack of depth leaves defenders solely reliant on the use of the electronic attack methods contained within the watch tower, but if those fail to eliminate each threat, an adversary can easily gain access to its intended target. As a metaphor for defensive operations, this is more akin to opening fire with crew-served weapons instead of beginning an engagement with security patrols and harassing fires. Ultimately, the lack of defensive layers allows an attacker increased mobility to target the defender's most lethal assets.

With an understanding of the current systems and how they match, or do not match, custom-

ary planning guidance, the DOD and DHS should incorporate the concept of aerial security patrols into the C-UAS framework. To fully realize this, friendly unmanned platforms can be terrestrially or aerially deployed to act as patrols, giving installations a forward presence to assist in the full gamut of C-UAS kill-chain actions. Because many of the kill-chain functions can be offloaded to the main sentry tower, these devices are adequately modular and customizable to meet the form, fit, and function of the host device. To assist in this conceptualization, it is important to look at the evolution of aerial combat to incorporate the types of attacks outlined in the previous two chapters.

5.2 Air-to-Air Combat

Given that UAVs operate using digital communications, such devices can be exploited by the same cyber-attacks that terrestrial systems experience [121]. Aerial C-UAS devices would also be a natural extension of ground-based capabilities—yet instead of a singular, centralized system in one location, aerial C-UAS can patrol further afield and be a mobile guardian for any centralized component, whether system or operational unit. This mimics precisely the lessons learned in defensive warfare, where interdiction patrols and observation posts gain depth in the battlespace [117], ultimately giving commanders increased security and situational awareness.

The first offensive use of aircraft was swiftly followed by investigation into counter methods. When the first anti-aircraft weapons materialized in 1910, they were fixed ground-to-air systems—not unlike the current watchtower systems today. The rudimentary biplane aircraft were used for reconnaissance and intelligence gathering missions, dropping hand grenades on enemy trenches, and destroying enemy aircraft. Air-to-air combat or dogfighting, as it is commonly referred to, finds its origins in WWI as the newly developed airplane proliferated on European battlefields [122].

By 1914, technological maturation had reached a point of air-to-air combat [112]. LtCol "Billy" Bishop, the most decorated British Royal Air Force ace, stated “the most important thing in fighting was shooting, next the various tactics in coming into a fight, and last of all flying ability itself” [116]. Aerial gunnery has evolved since the days of LtCol Bishop, and the need for shooting as rapidly as possible has gone by the wayside. Instead modern fighter pilots are mathematicians responsible for solving numerous geometry problems

to accurately engage an enemy with guns, rockets, or missiles [116]. Figure 5.2 shows this attack geometry, which only gets more complicated as pilots have more targets to engage [116].

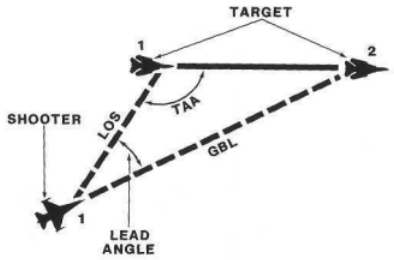

Figure 5.2. Shooter to Target Geometry. Source: [116].

The attack geometry problem can be simplified when using soft-kill techniques because soft-kill techniques are reliant upon the antennas through which the electromagnetic waves propagate. This flexibility allows soft-kill devices to be in a variety of modes, configured for stand-in or stand-off attacks. An omnidirectional antenna would allow a stand-in device to exist in the middle of its targets and propagate an attack in all directions [59]. While this would require the stand-in device to be closer to its targets than to a device using a high-gain, directional antenna, it would be more effective against lower-end designed devices. On the other hand, a high-gain, directional antenna would be more effective against a target UAV that suppresses its side lobes by overwhelming the main beam of the target's signal [41]. Both of these configurations would reduce the fratricide and collateral damage associated with kinetic kill methods.

Another advantage to soft-kill over hard-kill techniques stems from the concept of a beaten zone. As defined by [123], the beaten zone is the impact area where a projectile reaches its destination and is dependent upon the cone of fire from the weapon system used. For a machine gun, the cone of fire is fixed and can only be widened by adding more bullets and physically moving the weapon platform. Conversely, a fixed position jammer can have a steerable and wide cone of fire that can be electronically adjusted, leading to a beaten zone that is more precise than a machine gun's [41]. Figure 5.3 gives a visual representation of a machine gun's cone of fire and beaten zone, which has the ability to inflict collateral damage on unwitting targets—especially when an aircraft is involved.

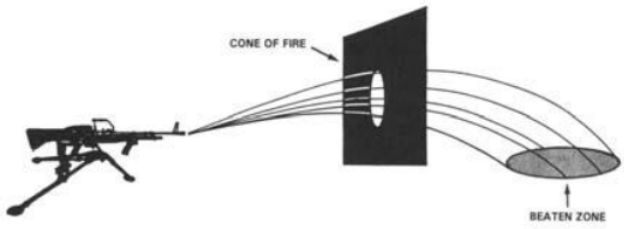

Figure 5.3. Machine Gun Beaten Zone. Source: [123].

Using kinetic kill methods for C-UAS may inflict damage to friendly units or bystanders, while aerial EW or cyber-attack platform would not. This type of aerial C-UAS device would be constrained by the device's power which causes the signal to attenuate to a level where it would not affect friendly systems. Another advantage of the aerial C-UAS device is range extension to mitigate threats beyond that of the ground watch towers.

5.3 Comparison Charts

Considering the notion of defending in depth and air-to-air combat, the following section shows several comparison charts to visually depict the concepts outlined up to this point. Specifically, the conceptualization of C-UAS technology in terms of ground-to-air and air-to-air systems. Table 5.1 depicts the most common C-UAS systems and looks to the future at the emerging ground-to-air devices that are in the acquisition pipeline. This table also proposes aerial C-UAS using the EW and cyber-attack vectors described in Chapters 3 and 4.

Table 5.1. Current and Future C-UAS Mitigation Measures.

	Current C-UAS	Future C-UAS
Ground to Air	MADIS Compact Laser Weapon UAVDefender CACI CORIAN Anduril Sentry Tower Shotguns	MADIS/FWS Inter-Networked Systems mmWave Directed Energy
Air to Air	Nets Anduril's Anvil Explosives	Autonomous Stand-in Hijackers Cryptographic Protocol Attacks DDoS Attacks Stand-in GNSS Jammers Stand-in RF Jammers

Of note are the emerging ground-to-air technologies such as mmWave directed-energy weapons and high-powered lasers that will be integral in the MADIS/Future Weapon System [124]. Most importantly, the C-UAS systems of the future will likely incorporate data fusion capabilities to combine all aspects of the kill-chain within a networked web of devices. Table 5.2 represents the pros and cons associated with the current ground and air C-UAS devices.

Table 5.2. Pros versus Cons of Current C-UAS Mitigation Measures.

	Current Systems	Current C-UAS Pros	Current C-UAS Cons
Ground to Air	MADIS	Mobility	High-Power Consumption
	Compact Laser Weapon	Small Form Factor	Easily Disrupted
	UAVDefender	Handheld	BBN Jamming Only
	CACI CORIAN	Purpose-Built for commercial UAVs	Fixed Position
	Anduril Sentry Tower	Exquisite AI Backbone	Expensive
	Shotguns	Close-Range	Potential Fratricide
Air to Air	Nets	Capture Target	Short-Range
	Anduril's Anvil	Kinetic Kill w/o Fratricide	Extensive Flight Path Metrics
	Explosives	Target Destruction	Damages Friendly Device

The main problems with the current suite of C-UAS technology are the high power requirements, system size, and cost per unit. Additionally, many of these systems, like projectiles, explosives, and BBN jamming, have a considerable fratricide risk associated with their use. The main takeaway from the current systems listed in Table 5.2 is this: all of the current systems are meant to serve as general purpose C-UAS platforms and none of them provide a low-SWaP capability that is modular enough for placement on a friendly UAV.

However, the good news is this: innovation and competition continues to excel in this domain as many new systems are being built and integrated into the existing architecture [32]. Table 5.3 shows a pros and cons list of the future ground-to-air countermeasures in the acquisition cycle in addition to the proposed air-to-air capabilities outlined in Chapters 3 and 4.

Table 5.3. Pros versus Cons of Future C-UAS Mitigation Measures.

	Future Systems	Future C-UAS Pros	Future C-UAS Cons
Ground to Air	AFRL NINJA	Reliability, Fully Funded	Bulky
	MADIS/FWS	Mobility	High-Power Consumption
	Inter-Networked Systems	Small Form Factor	Easily Disrupted
	mmWave Directed Energy	Handheld	BBN Jamming Only
Air to Air	Autonomous Stand-in Hijackers	Usurp Control of Target	Requires Target Reverse Engineering
	Cryptographic Protocol Attacks	Precision	Requires Target Profile
	DDoS Attacks	Effective Against Swarms	Spreading Complexity
	Stand-in GNSS Jammers	Easier to Implement	Attack Profile Modification
	Stand-in RF Jammers	Close Proximity to Target	Potential Communication Fratricide

By taking a defense-in-depth approach, aerial C-UAS devices give the DOD and the DHS a stand-in hacking and jamming capability that mitigates fratricide with minimal power consumption. Specifically, the cyber-attack vectors can be seen as a scalpel's edge capability that specifically targets only threat devices. The downside to this approach is the need to reverse engineer a device to identify vulnerabilities to carry out the attacks covered in Chapter 4. On the other hand, there are the GNSS and RF jammers, which require a less intense reverse engineering process unless the development of a protocol aware jamming system is desired.

5.4 Example Scenario One

In the not-so-distant future, the U.S. might face an attack performed solely by unmanned systems. This attack may be carried out against a military installation, a hydroelectric power facility, or even an aircraft carrier transiting through a strait. Despite the focus on force protection in the post-9/11 years, each one of these locations remains vulnerable to an airborne swarm attack. The attacker in each instance could be a lone wolf, a radicalized insurgent group, or even a state-sponsored proxy. Consider the following scenarios in the defense of a hydroelectric power facility on the Pacific west coast as the target.

Begin Scenario:

At the hydroelectric power facility, a security guard receives a warning notification from the northeast C-UAS tower's radar sensor that there is a 95% chance a UAV swarm is moving at 20 miles-per-hour towards the tower. A few seconds later, the guard receives another notification indicating a new swarm of 10 UAVs are flying at 25 miles-per-hour[1] directly at the southwest tower, located on the dam's primary entry way. At the guard's disposal are the ground-based barrage jammers to target threats in the 2.4 and 5 GHz frequency bands. The guard's display shows a heterogeneous swarm operating on the 2.4 GHz band. Due to the swarms' rapid speed and multi-directional attack, the guard chooses to barrage jam the entire 2.4 GHz band using the northeast and south tower's omnidirectional antenna suites.

The jamming effect causes the UAVs to act as if they have hit an invisible wall—some collide with one another and others stop in place to hover. At this point several more UAVs self-land. Meanwhile, back at the command center near the southwest tower, the security guard receives an updated situation report from the heads-up display, showing the targeted UAVs returning to their point of origin, making it appear as though the attack has been thwarted. As the watch towers are reset, and the guard begins to send a situation report outlining the attack, the tracking system identifies another UAV swarm approaching the southwest tower. This time there are 50 UAVs operating on the 5 GHz band and rapidly approaching at nearly 30 miles-per-hour. Because the C-UAS system is resetting, the guard is unable to restart the barrage jam, and the new UAV swarm delivers shape charge after shape charge to the walls of the dam, causing explosions along the dam's center. As the guard contacts local authorities to inform the need for evacuation, the dam bursts, and tens of thousands of tons of water pour out.

The dam finally disintegrates and power immediately goes out in the nearby metropolitan city as well as significant parts of the surrounding region, because of their reliance on the power generated by the dam. Airplanes trying to land in the city airport lose connection with the air traffic control station and while the ground crews work to get the backup generators operational, many flights are diverted. The larger aircraft can make it to other airports, but the smaller planes with dwindling fuel supplies are required to find open clearings for emergency landings in the heavily wooded areas surrounding the dam.

[1]Data-sheet for Intel Drone Light Shows states current max-speed up to 17 m/s (38 mph) [125]

After the attack, large-scale physical infrastructure damage is identified, including roads, power grids, buildings, and the dam itself. The loss of power disrupted businesses, transport, and security systems. Moreover, back-up generator functionality does not cover the months needed to restabilize power and the years needed to rebuild the dam to its original state. The attacks led to countless power grid blackouts and interruptions to normal services, not to mention the loss of hundreds of lives and tens of billions of dollars in infrastructure damage. In comparison, the entire attack was carried with little more than twenty thousand dollars of equipment and minimal training for the operators.

5.5 Example Scenario Two

In the ensuing scenario, the same attack is revisited, but the C-UAS protections at the dam are enhanced with a security patrol of UAVs armed with the *Detachable Drone Hijacker*, a drone hijacking device meant to enhance the C-UAS systems used at the power facility. The security team at the dam developed a concept of operations (CONOPS) in the event the dam came under attack as seen in Figure 5.4.

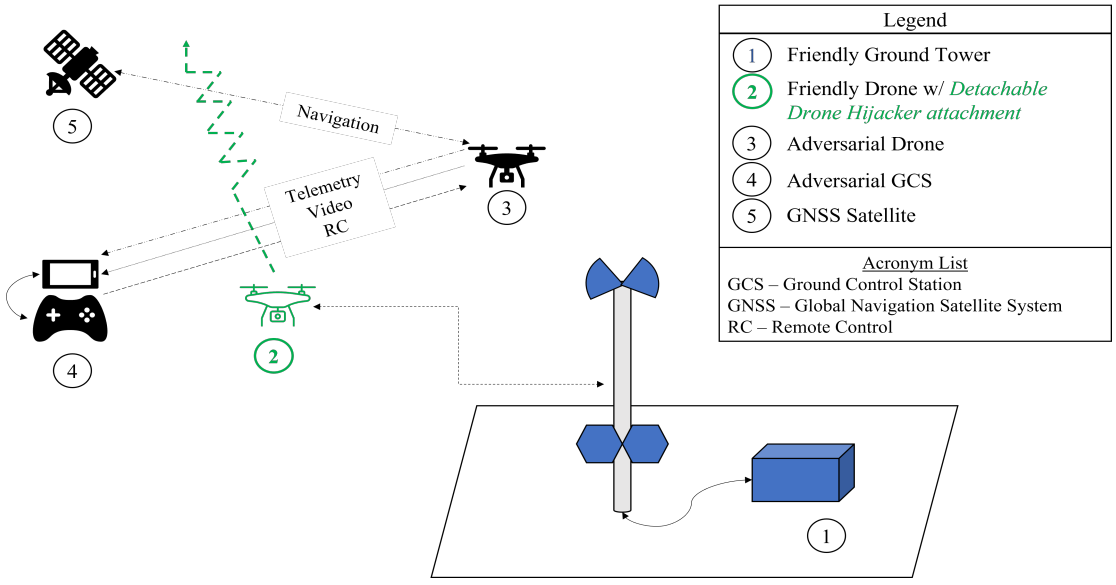

Figure 5.4. Detachable Drone Hijacker CONOPS.

Begin Scenario:

At the hydroelectric power facility, each C-UAS watch tower is reconfigured with a new type of UAV security patrol outfitted with the *Detachable Drone Hijacker*, termed by the security guards as the "Alphas." This upgrade is significant as the Alphas deploy forward of the watch towers on a patrol schedule and the security patrols can receive mid-flight updates from the towers to guide their attack methods. Additionally, given their small form-factor and low-power consumption, the Alphas can patrol for an hour a piece, giving the watch officers a persistent presence to augment the sentry towers.

While on watch, the security guard receives a notification from the northeast tower's radar sensor that there is a 95% probability of an inbound UAV swarm moving at 20 miles-per-hour. A few seconds later, the guard receives another notification, this time a swarm of 10 UAVs are flying at 25 miles-per-hour directly at the southwest tower located on the dam's primary entry way. The guard's display shows a heterogeneous swarm operating on the 2.4 GHz band. Due to the swarm's rapid speed and multi-directional attack, the security guard deploys the Alphas to counter the approaching swarm with mid-air interdiction. The guard still reserves the capability to jam the entire 2.4 GHz frequency band using the omnidirectional antennas of the watch towers as backup.

The Alphas begin to issue UDP packets and deauthentication frames to counter the UAV swarms. As with the centralized system, the two swarms act as if they have hit an invisible wall and a few drop out of the sky, while others stop in place and hover. Several more UAVs begin returning to their point of origin and self-land.

Meanwhile, back at the command center, the guard receives situation updates from the heads-up display showing the effects of the attack. As the guard is about to send in the situation update to higher headquarters, the tracking system identifies another UAV swarm approaching the southwest tower. The guard sends updated instructions to the Alphas before activating the jamming system, sending RF noise out of the tower's omnidirectional antennas to barrage jam the entire 5GHz frequency band. The new UAV swarm stops, and the Alphas take a forward position to preemptively mitigate any new incoming threats. In the ensuing 10 minutes, a ground team captures five suspects on all-terrain vehicles carrying large briefcases filled with small UAVs and explosives.

5.6 Conclusion

In the second scenario, the security team effectively countered the adversarial UAV swarm by incorporating friendly UAVs capable of delivering cyber-attacks. The maneuverability afforded by the use of the "Alphas" directly enhanced the security team's ability to defend in depth.

Ultimately, if the DOD and the DHS fail to adopt a new framework in their approach to C-UAS development, the U.S. may experience some of the same heartache suffered by the Armenians in the Nagorno-Karabakh War. With such techniques, it is likely that weak states and non-state actors will achieve asymmetric advantages over their technologically superior foes. In 2020, Baykar sold over $360 million of Bayraktar TB-2s to the world market [126]. Considering their battlefield and propaganda successes in the past two European conflicts, the company's market share is likely to increase.

While the two scenarios in this chapter did not talk about government-procured weapon systems like the TB-2, the lessons learned from the ISIS insurgency show that low-cost devices can have an outsized impact on non-standard military targets. It is no longer science fiction to believe that a modestly funded insurgent group can build a network of UAVs, attach satchel charges or C4, and use them as kamikaze swarms to attack U.S. infrastructure. To counter this, the DOD and DHS can develop airborne C-UAS tools to operate as stand-in, forward security patrols to prevent the destruction from this type of event. The following chapters take the framework outlined up to this point and describe the experiment methodology to go from concept to capability.

CHAPTER 6:
Experiment Methodology

6.1 Introduction

This chapter outlines the experiment methodology to take an operational concept such as aerial C-UAS patrols and turn it into a capability. The experimentation conducted for this thesis sought to use commercial equipment and open-source software to build a low-SWaP payload called the *Detachable Drone Hijacker*. The *Detachable Drone Hijacker* can be easily attached to a friendly UAV to a friendly UAV to identify, track, target, and deny an adversary's use of a WiFi UAV.

Prior to the building the *Detachable Drone Hijacker*, the research team conducted a feasibility assessment to determine which hardware and software would be required. Then, the thesis team carried out three primary experiments to test and evaluate the concept of UAV-to-UAV interdiction using targeted cyber-attacks. Experiment One was an operational assessment of the effectiveness and power consumption of the *Detachable Drone Hijacker* at various ranges and elevation differentials. Experiment Two was a benchtop test designed to measure the survivability of the *Detachable Drone Hijacker* in sub-freezing temperatures. The final experiment, Experiment Three, measured the *Detachable Drone Hijacker's* thermal signature before, during, and after operation.

The purpose of the experiments conducted in Chapter 7 were to evaluate the effectiveness, power consumption, and thermal signature of using cyber-attacks to counter commercial UAVs using the IEEE 802.11 wireless communication schemes. Three commercial UAVs were chosen based on their use of the IEEE 802.11 wireless communication standards—the Parrot ARDrone 2.0 [127], Parrot Bebop [128], and Skydio 2+ [129]. The Parrot Bebop and the Skydio 2+ were secured with WPA2 and a pre-shared key. The Parrot ARDrone 2.0 could not be secured with WPA2.

Several attack vectors were identified based on the neutralization methods presented in Chapters 3 and 4. For experimentation purposes, this thesis uses deauthentication and TCP/SYN Flood attacks while the RF electronic attack methods outlined in Chapter 3

were excluded. The RF mitigation measures were omitted because of potential collateral damage to other systems operating in the 2.4GHz and 5GHz ISM bands. Additionally, these experiments focused low-SWaP mitigation techniques. Therefore, the large power consumption requirements associated with barrage jamming were outside the scope of this thesis.

To evaluate the efficacy of such attacks against 802.11 UAVs, this thesis measured the following characteristics: target behavior, distance between target and *Detachable Drone Hijacker*, power consumption associated with each attack method, and thermal signature.

6.2 Research Questions

As mentioned previously, the payload built for these experiments is referred to as the *Detachable Drone Hijacker*.

1. How might we create a stand-in C-UAS device that can be "bolted on" to a friendly UAV?
2. What type of attack methods would be the most effective using such a device?
3. Will a micro computer, wireless NIC, and a low power source have sufficient power and range to carry out DoS attacks against an intruding UAV?
4. At what ranges will the *Detachable Drone Hijacker* fail?
5. What is the power consumption associated with the DoS attacks used?
6. Will the *Detachable Drone Hijacker* work in below freezing temperatures?
7. What is the thermal signature associated with the *Detachable Drone Hijacker*?

6.3 Experiment Setup

The initial baseline testing used a laptop, an Alfa AWUS036ACH wireless NIC, a Parrot ARDrone 2.0, and software developed by the author to answer Research Questions 1, 2, and 3. During baseline testing, the primary outputs were the creation of software and logging scripts to automate the attack and record results. These can be found at: https://github.com/c-thie1958/Thesis.git. The software and logging scripts were especially important to create a repeatable process that allowed for easy data analysis.

6.3.1 Experiment One (Operational Field Testing) Setup

Experiment One consisted of field testing of the *Detachable Drone Hijacker* to simulate an operational use case to defend critical infrastructure against an adversarial UAV incursion. The *Detachable Drone Hijacker* was designed using the schematic in Figure 6.1 and used the following hardware:

- (1) Raspberry Pi 4.0 Model B, with 4GB of Random Access Memory [130], used as the computer from which to control the experiments.
- (1) SanDisk Extreme 64 Gigabyte Micro-SD Card used to store the Raspbian Operating System [131] and the software developed.
- (1) Raspberry Pi Sense HAT Version 1.0 [132] used for recording environmental characteristics.
- (1) MakerHawk Raspberry Pi UPS Power Supply used as a power bank for the Raspberry Pi.
- (2) 18650 Rechargeable Batteries used to provide 5V of power to the Raspberry Pi.
- (1) Alfa AWUS036ACH WiFi NIC [133] used as the radio from which to identify and target WiFi UAVs.

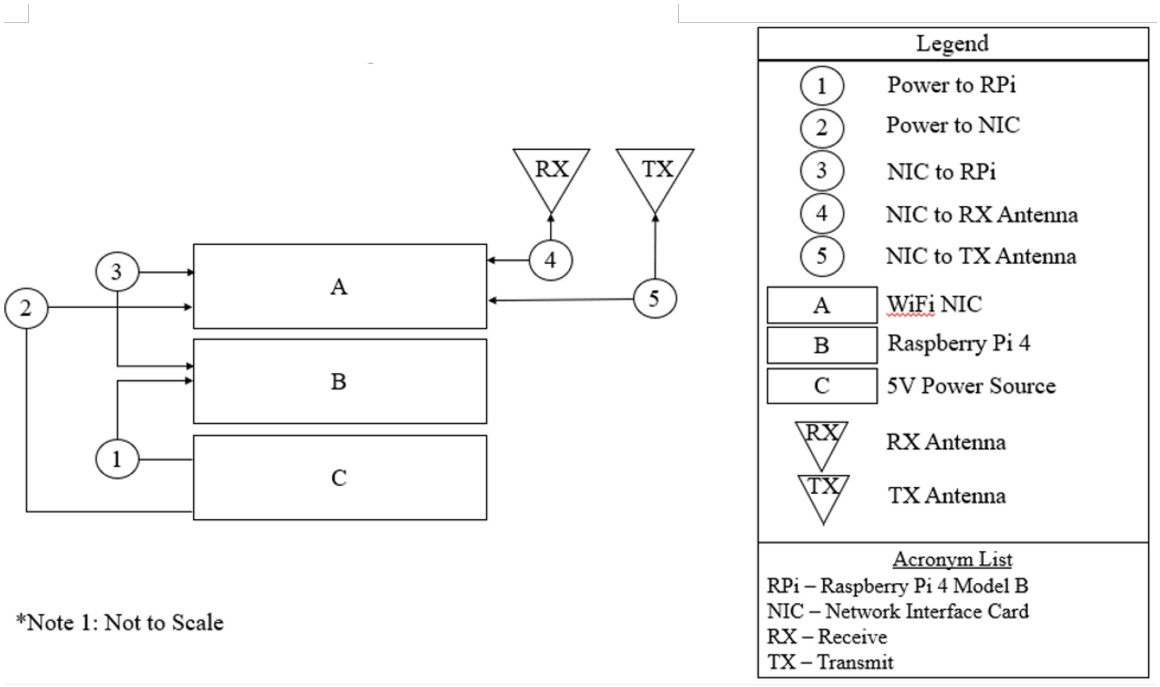

Figure 6.1. *Detachable Drone Hijacker* Schematic.

The final prototype was then fully assembled as seen in Figure 6.2. Upon assembly, the research team attached the UM25C USB multimeter [134] to take voltage, current, and power consumption readings during ground-to-air testing.

Figure 6.2. *Detachable Drone Hijacker* Prototype.

Once the *Detachable Drone Hijacker* prototype was assembled, it was then attached to a host UAV called the AquaQuad [135]. The AquaQuad is a larger Group 1 UAS with a configurable payload compartment as seen in Figures 6.3 and 6.4. Figure 6.3 shows the AquaQuad configured for maritime launch and flight, while Figure 6.4 shows the AquaQuad reconfigured for use with the *Detachable Drone Hijacker*.

Figure 6.3. The AquaQuad.

Figure 6.4. *Detachable Drone Hijacker* attached to its host - The AquaQuad.

All tests in Experiment One were carried out in accordance with the experiment diagram shown in Figure 6.5. Notably, this diagram proved helpful in visualizing how the research team would control for certain variables such as the distance from the *Detachable Drone Hijacker* to the UAV target , attack method (e.g., deauthentication or TCP/SYN Flood), and the elevation of the *Detachable Drone Hijacker* and the UAV target.

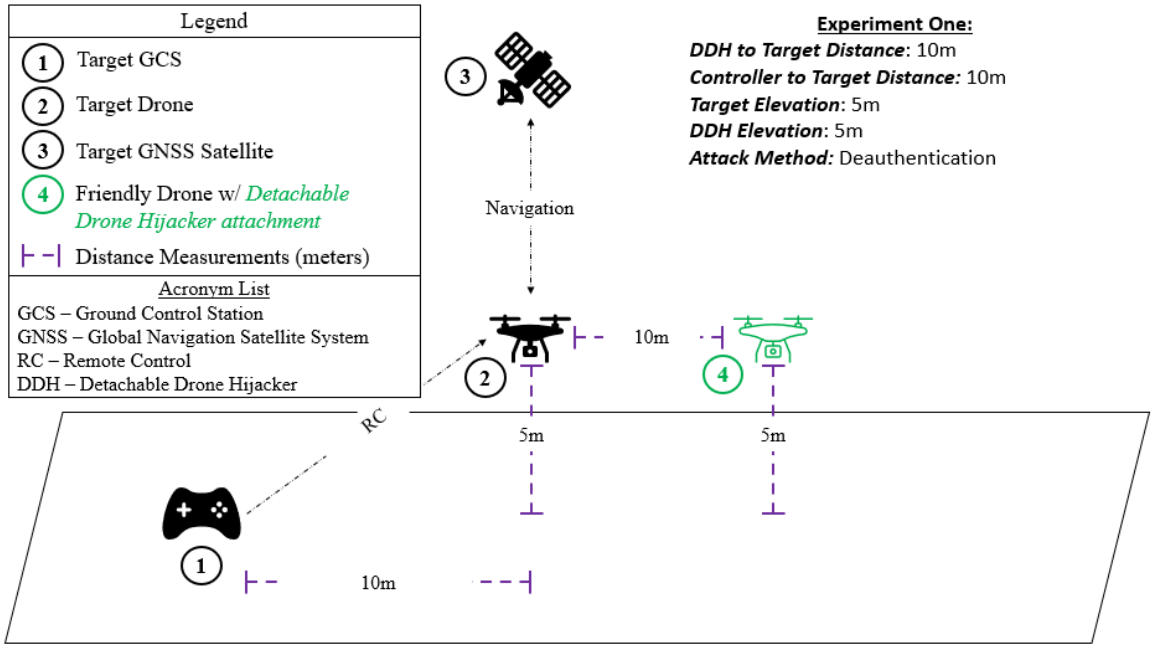

Figure 6.5. Experiment One Set-up: Operational Field Testing.

Then, quantifiable data was collected and organized in accordance with Table 6.1 to measure the target UAV's behavior once attacked, the environmental conditions (such as humidity percentage, ambient temperature, and CPU temperature), power consumption, and thermal signature associated with each attack method. The measured results will be given in Chapter 7.

Table 6.1. Experiment One Data Collection Table.

Target		**Average Power Consumption (W)**	
Target Behavior		**Minimum Power Consumption (W)**	
GCS Behavior		**Maximum Power Consumption (W)**	
DDH to Target Distance (m)		**Average CPU Temperature (°C)**	
GCS to Target Distance (m)		**Minimum CPU Temperature (°C)**	
Target Elevation (m)		**Maximum CPU Temperature (°C)**	
DDH Elevation (m)		**Average Ambient Temperature (°C)**	
Humidity (%)		**Minimum Ambient Temperature (°C)**	
		Maximum Ambient Temperature (°C)	

6.3.2 Experiment Two (Sub-Freezing Temperature Testing) Setup

Within the past several years the U.S. has pivoted its national security interests from the Global War on Terrorism to a renewed focus on Great Power Competition and Strategic Deterrence with Russia and China. While much of the Navy and Marine Corps' interests have focused on the South and East China Seas, the Russians have steadily built up a military presence in the Arctic Circle [136]. As climate change continues to have an out-sized impact on the melting of polar icecaps, the Navy will have to deal with the challenges associated with transits through the northern straits. With this in mind, it is important to adapt C-UAS systems to operate in a multitude of environments. From this background, the research team decided to simulate future operating environments where the *Detachable Drone Hijacker* might be employed. Experiment Two was designed to simulate an environment where the *Detachable Drone Hijacker* is used during naval exercises in the Baltic Sea during the winter months, where average temperatures remain sub-zero for months on end.

Due to lab and equipment constraints, the *Detachable Drone Hijacker* was removed from the AquaQuad. Experiment Two sought to determine if the *Detachable Drone Hijacker*

would remain operational in a sub-freezing environment as shown in Figure 6.6. Two tests were designed to mimic a scenario in which the *Detachable Drone Hijacker* moves in, and out, of a controlled temperature environment, as it would onboard a ship in a sub-freezing environment.

Figure 6.6. Experiment Two Set-up: Sub-Freezing Temperature Testing.

The first test held the *Detachable Drone Hijacker* at room temperature for five days and then brought it into sub-freezing temperatures for operations. The second test left the *Detachable Drone Hijacker* in a sub-freezing environment for 30 minutes and the third test left the *Detachable Drone Hijacker* in a sub-freezing environment for 60 minutes. With these controls in mind, quantifiable data was recorded and consolidated into a table similar to Table 6.2. This helped the research team understand the correlation between device functionality, CPU temperature, and ambient temperature.

Table 6.2. Experiment Two Data Collection Table.

Target		**Average CPU Temperature (°C)**	
Target Behavior		**Average Ambient Temperature (°C)**	
GCS Behavior		**Average Humidity (%)**	
H to Target Distance (m)		**CPU Temp (°C)**	
GCS to Target Distance (m)		**Minimum Ambient Temp (°C)**	
Target Elevation (m)		**Maximum CPU Temp (°C)**	
DDH Elevation (m)		**Maximum Ambient Temp (°C)**	

6.3.3 Experiment Three (Thermography Testing) Setup

Thermal image testing, also known as thermography, is applied in the research and development of new technologies in many different industries [137]. Whether it be nondestructive testing, condition monitoring, or reducing energy costs, the field of thermography has rapidly expanded alongside other information technologies throughout the past three decades . As it pertains to the development of aircraft and the systems which they employ, thermography is used to study propulsion systems, propellers, and is most useful when conducting SWaP analysis in aircraft payload development [137]. This type of experimentation is especially important when the testing viability of EW systems that are employed onboard aircraft.

To carry out the thermography testing in Experiment Three, the research team used the following hardware and software systems for measurement:

- (1) FLIR A320 Tempscreen
- (1) Dell Inspiron Laptop
- (1) *Detachable Drone Hijacker* Prototype
- (1) FLIR CamTools 4.0.0 Software

The FLIR A320 Tempscreen is a thermal camera that is primarily used for temperature

deviation detection [138]. The mobility of the camera makes it easy to employ almost anywhere for persistent monitoring of personnel, equipment, and infrastructure. The FLIR A320 was selected due to its ease of use, image quality, and accessibility to the research team. Of note, the FLIR camera has a temperature accuracy of "+/-2°C or +/-2% of [the] reading", [138].

Figure 6.7 shows the setup for Experiment Three. It should be noted that both the experiment table and the cardboard backdrop act as EM energy blockers, preventing any unnecessary fading, reflection, or other interference with the experiment.

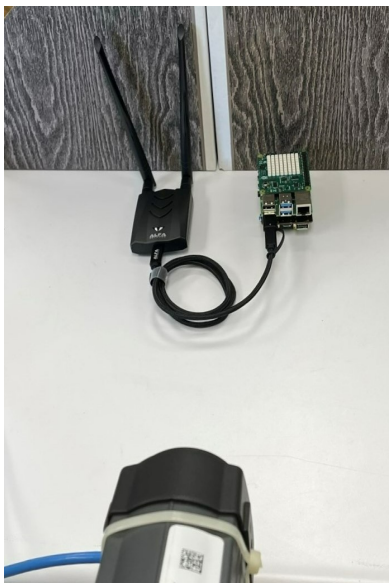

Figure 6.7. Experiment Three Set-up: Thermography Testing.

The FLIR A320 Thermascreen camera enabled the research team to take static infrared images while noting the average temperatures associated with color transitions in the camera's software. This data was aggregated and recorded into a table similar to Table 6.3 for further analysis.

Table 6.3. Experiment Three Data Collection Table.

Camera Look Angle	Power State	Test Mode	Color Code	Color Temperature (°C)
Top		Pre-Operational	White/Yellow	
Top		Pre-Operational	Orange/Red	
Top		Pre-Operational	Light Blue	
Top		Pre-Operational	Dark Blue	
Front		Pre-Operational	White/Yellow	
Front		Pre-Operational	Orange/Red	
Front		Pre-Operational	Light Blue	
Front		Pre-Operational	Dark Blue	
Bottom		Pre-Operational	White/Yellow	
Bottom		Pre-Operational	Orange/Red	
Bottom		Pre-Operational	Light Blue	
Bottom		Pre-Operational	Dark Blue	

6.4 Conclusion

As mentioned, the overarching objective was to determine the most effective manner of conducting a cyber-attack against a target UAV from a payload hosted on a friendly UAV. This chapter describes the testing methodology, while results will be presented in the next chapter.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 7:
Experiment Results and Discussion

To prove the viability of the air-to-air C-UAS concepts outlined in Chapter 5, the research team carried out three main experiments. The primary goal was to create a payload that was small enough to be attached to a friendly host UAV without significant integration with the host's ship power or performance degradation. The *Detachable Drone Hijacker* is a $250 prototype weighing 400 grams designed to identify, target, and mitigate specified UAVs using the IEEE 802.11 wireless standards.

The three experiments outlined herein specifically target consumer UAVs operating on IEEE 802.11 WiFi channels. Before the experiments were conducted, baseline testing was needed to establish the viability of a cyber-attack against a UAV using WiFi communications. The UAV chosen was the Parrot ARDrone2.0, but because the UAV's software was outdated, it could not be flown while recording data. Thus, the ARDrone2.0 was only useful for initial testing and was omitted from the research findings.

After initial bench-top testing verified system functionality, Experiment One consisted of field testing the *Detachable Drone Hijacker* to mimic realistic conditions during ground-to-air, and air-to-air, operations. In Experiment Two, the research team sought to understand system performance of the *Detachable Drone Hijacker* in sub-freezing conditions. Finally, the thermography tests conducted in Experiment Three sought to understand the thermal characteristics associated with system operation before, during, and after use. Whether they be manned, or unmanned platforms, gathering thermographic data is especially important when integrating new payloads on existing aircraft.

7.1 Experiment One: Field Testing the *Detachable Drone Hijacker*

7.1.1 Introduction

The following tests sought to test the operational employment of the *Detachable Drone Hijacker* on the ground and in the air.

7.1.2 Objectives

Experiment One was carried out to simulate the operational employment of the *Detachable Drone Hijacker* while attached to a host device to counter a WiFi UAVs. The following proof of concept experiments were designed to:

- Determine effectiveness against the Parrot Bebop and Skydio 2+
- Test DoS attacks in the form of TCP/SYN Flood and deauthentication attacks
- Minimize power requirements for attacks
- Understand prototype limitations and SWaP requirements

7.1.3 Execution

During initial testing, the TCP/SYN Flood attacks showed promise. However, when there are no established IP address gateways between the UAV target, its GCS, and the *Detachable Drone Hijacker*, TCP/SYN Flood attacks became untenable and less effective. More importantly, the main goal of testing was to reduce the amount of power required for each attack. And in this case, a DoS attack like the TCP/SYN flood is less computationally efficient than a deauthentication attack. For those reasons, the research team decided to omit the field testing of the TCP/SYN flood attacks. Thus, the preferred attack method proved to be the deauthentication DoS attack against the Parrot Bebop and the Skydio 2+.

Ground-to-Air Testing

During the first phase of field testing, the research team conducted seven ground-to-air tests targeting the Parrot Bebop. These tests evaluated the *Detachable Drone Hijacker's* ability to carry out its deauthentication attack with ground interference from trees, buildings, and power lines.

Figure 6.5 gives a visual representation of the static experiments conducted at ranges of 10, 100, 250, and 400 meters between the *Detachable Drone Hijacker* and its target. These tests were conducted using the Parrot Bebop 2 as a target. This is because the Skydio 2+ was not yet available for use by the research team. The final test was a moving test in which the target drone flew towards the *Detachable UAV Hijacker* at varying heights and speeds to simulate an adversarial UAV attacking critical infrastructure. During the final air-to-air tests, the research team used the Parrot Bebop 2 and the Skydio 2+ as adversarial UAVs.

Power consumption, maximum effective range, CPU temperature, ambient temperature, and target behavior were all measured during Day One testing.

Air-to-Air Testing

During the second phase of field experimentation, the research team conducted two air-to-air tests targeting the Parrot Bebop and the Skydio 2+. During air-to-air testing, the AquaQuad moved at various ranges from its ground control station at 40 meters of elevation while the elevation and range of the target UAVs was varied to simulate UAV-versus-UAV combat. The air-to-air tests measured CPU temperature, ambient temperature, and target behavior on of the air-to-air tests. Power consumption tests using the UM25C multimeter were omitted given the consistent results from prior experiments and the need to reduce payload weight. Additionally, max effective range tests were omitted due to facility constraints where the maximum distance between the *Detachable Drone Hijacker* and its target was 100m.

7.1.4 Results and Discussion

Ground-to-Air Testing

Tables 7.1, 7.2, and 7.3 depict the ground-to-air test results. To eliminate unnecessary clutter, the data from tests 1-4 are located in Appendix A.1. Of note, the power consumption associated with each test remained consistent, averaging approximately 1 Watt during all attacks.

Table 7.1. Ground-to-Air Field Test Five: Static Deauthentication Attack (250m - Different Elevation).

Target	Parrot Bebop	**Average Power Consumption (W)**	1.1
Target Behavior	Hovers then lands	**Minimum Power Consumption (W)**	0.92
GCS Behavior	Disconnected/No Control	**Maximum Power Consumption (W)**	1.1
DDH to Target Distance (m)	250	**Average CPU Temperature (°C)**	29.3
GCS to Target Distance (m)	10	**Minimum CPU Temperature (°C)**	27.3
Target Elevation (m)	10	**Maximum CPU Temperature (°C)**	33.1
DDH Elevation (m)	5	**Average Ambient Temperature (°C)**	16.0
Humidity (%)	48.6	**Minimum Ambient Temperature (°C)**	15.3
		Maximum Ambient Temperature (°C)	17.2

Despite a moderate amount of environmental clutter, the results from Test Five showed that the maximum effective range of the *Detachable Drone Hijacker* operated in ground-to-air mode is 250 meters. The *Detachable Drone Hijacker* had no issues identifying its target UAV and mitigating the threat using the deauthentication attack. Once the link was severed between the Bebop and the GCS, the UAV hovered, burning extra battery power to overcome the drag coefficient from vertical takeoff and the computational power needed to reconnect to its GCS. Lastly, the internal logging showed an 18.3°C differential between the ambient temperature and the CPU temperature. This is important to note when attaching the *Detachable Drone Hijacker* onto a host-UAV where excess heat can cause malfunctions to normal operations.

Table 7.2. Ground-to-Air Field Test Six: Static Deauthentication Attack (400m - Different Elevation).

Target	Parrot Bebop	**Average Power Consumption (W)**	1.1
Target Behavior	No Effect	**Minimum Power Consumption (W)**	0.92
GCS Behavior	No Effect	**Maximum Power Consumption (W)**	1.1
DDH to Target Distance (m)	400	**Average CPU Temperature (°C)**	35.1
GCS to Target Distance (m)	10	**Minimum CPU Temperature (°C)**	28.7
Target Elevation (m)	30	**Maximum CPU Temperature (°C)**	38.5
DDH Elevation (m)	5	**Average Ambient Temperature (°C)**	17.9
Humidity (%)	50.6	**Minimum Ambient Temperature (°C)**	16.5
		Maximum Ambient Temperature (°C)	19.7

In Test Six, the research team attempted to extend the range of target identification to 400m. However, due to environment clutter associated with power lines, buildings, trees, and free space path loss, the *Detachable Drone Hijacker* was unable to identify the target. The CPU and ambient temperature differential in this test showed a 13.3°C delta, which is more favorable than the previous test. This is likely because of an increase in wind, which may have caused the CPU to cool faster than in previous tests.

Table 7.3. Ground-to-Air Field Test Seven: Moving Deauthentication Attack (250-100m - Different Elevation).

Target	Parrot Bebop	**Average Power Consumption (W)**	1.1
Target Behavior	Return to last known connection point	**Minimum Power Consumption (W)**	0.93
GCS Behavior	Disconnected/No Control	**Maximum Power Consumption (W)**	1.1
DDH to Target Distance (m)	100-250	**Average CPU Temperature (°C)**	34.6
GCS to Target Distance (m)	N/A	**Minimum CPU Temperature (°C)**	30.7
Target Elevation (m)	10-20	**Maximum CPU Temperature (°C)**	38.5
DDH Elevation (m)	5	**Average Ambient Temperature (°C)**	19.5
Humidity (%)	43.6	**Minimum Ambient Temperature (°C)**	19.0
		Maximum Ambient Temperature (°C)	20.0

In Test Seven, the research team created a scenario by which a target UAV attacked a building. Beginning at 250 meters and flying at 15 kilometers-per-hour at changing elevations towards the *Detachable Drone Hijacker*, the enemy UAV stopped in its place 80m from its intended destination. The *Detachable Drone Hijacker* ran its automated attack process that begins with a scan of potential UAV targets in the area. Then, once a target is identified, it immediately hops to the same WiFi channel the target is operating on. Once the *Detachable Drone Hijacker* has successfully hopped to the target's channel, it immediately begins sending deauthentication frames to sever the connection between the adversarial UAV and its GCS. This entire process—from scanning for targets, to threat mitigation—occurs in a matter of less than 10 seconds. The attack process can be sped up by enabling the scanning functions of the *Detachable Drone Hijacker* to operate continuously, which reduces the attack timeline to less than a second.

Once attacked, the adversarial UAV begins hovering in place. Then it flew back to its launch point and finally it landed at the location where it last connected to its GCS—100m from its intended target. This movement, disconnection, and extra hovering made the target UAVs battery drain from 99% to 5% in an attack that lasted two minutes. Lastly, the differential between CPU operating temperature and ambient temperature was approximately 15°C.

Air-to-Air Testing

During air-to-air testing, the *Detachable Drone Hijacker* to a host aircraft called the AquaQuad. Tables 7.4 and 7.5, as well as Figures 7.1 and 7.2 show the results from the air-to-air moving tests targeting a Parrot Bebop and Skydio 2+.

Table 7.4. Air-to-Air Test One: Parrot Bebop.

Target	Parrot Bebop	**Average CPU Temperature (°C)**	32.4
Target Behavior	Return to last known connection point	**Minimum CPU Temperature (°C)**	20.4
GCS Behavior	Disconnected/No Control	**Maximum CPU Temperature (°C)**	38.5
DDH to Target Distance (m)	Varied	**Average Ambient Temperature (°C)**	17.6
GCS to Target Distance (m)	Varied	**Minimum Ambient Temperature (°C)**	13.9
Target Elevation (m)	10-30	**Maximum Ambient Temperature (°C)**	20.6
DDH Elevation (m)	40	**Humidity (%)**	36.7

Table 7.5. Air-to-Air Test Two: Skydio 2+.

Target	Skydio 2+	**Average CPU Temperature (°C)**	27.6
Target Behavior	Return to last known connection point	**Minimum CPU Temperature (°C)**	16.5
GCS Behavior	Disconnected/No Control	**Maximum CPU Temperature (°C)**	31.6
DDH to Target Distance (m)	Varied	**Average Ambient Temperature (°C)**	18.9
GCS to Target Distance (m)	Varied	**Minimum Ambient Temperature (°C)**	13.4
Target Elevation (m)	10-30	**Maximum Ambient Temperature (°C)**	48.3
DDH Elevation (m)	40	**Humidity (%)**	34.7

As one can see in the previous two tables, the *Detachable Drone Hijacker* proved effective in identifying, targeting, and mitigating threats at various distances and elevations while maintaining a low average temperature difference between the CPU and the ambient temperature. When attacked, both the Parrot Bebop and the Skydio 2+ returned back to their last known connection point, ultimately landing, while the GCS had no control or connection. While it only takes one deauthentication frame to initially disrupt the connection between the targeted UAV and its GCS, the *Detachable Drone Hijacker* is programmed to send 15

deauthentication frames, with 128 packets for each frame, to sever the link for enough time to cause the target UAVs to self-land. Because each UAV has different software functionality, actions a given UAV takes when the connection between a UAV and its GCS is disrupted also differ. In the case of these experiments, both the Parrot Bebop and the Skydio 2+ were preprogrammed to return to home after 15 seconds of disruption. Therefore, the connection only needed to be severed for 15 seconds to cause the drone to return to its point of origin.

The *Detachable Drone Hijacker* can easily be reprogrammed to send continuous deauthentication messages to the targeted UAV. As in the ground-to-air tests, the battery of target UAVs suffered a great deal from extensive hovering and processing power trying to reestablish connection. The Bebop's battery drained from 87% to 21%, while the battery of the Skydio 2+ proved more efficient with a battery that decreased from 85% to 71%.

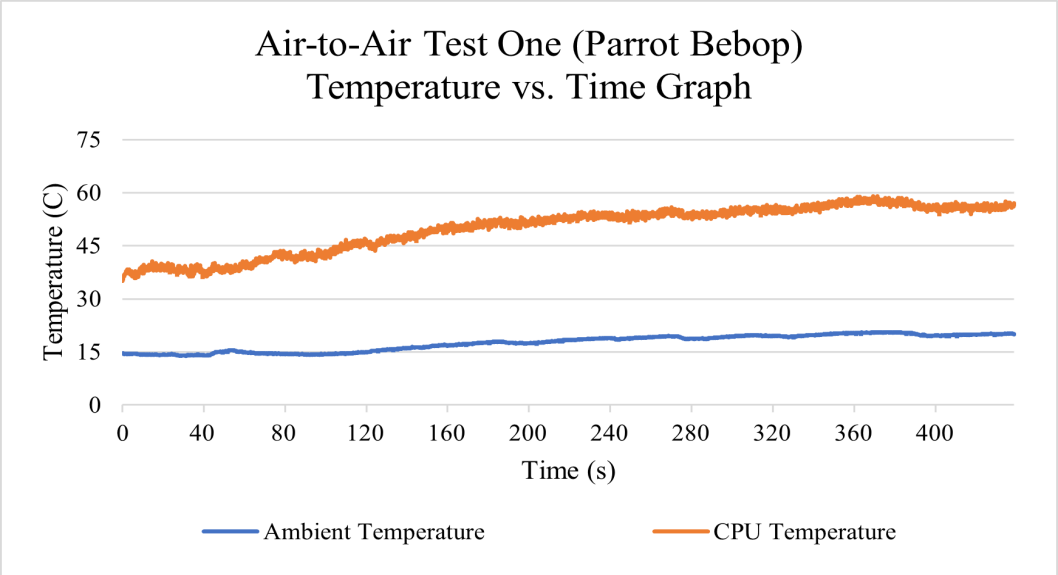

Figure 7.1. Air-to-Air Test One: Difference between the Ambient and CPU Temperature (Parrot Bebop Target).

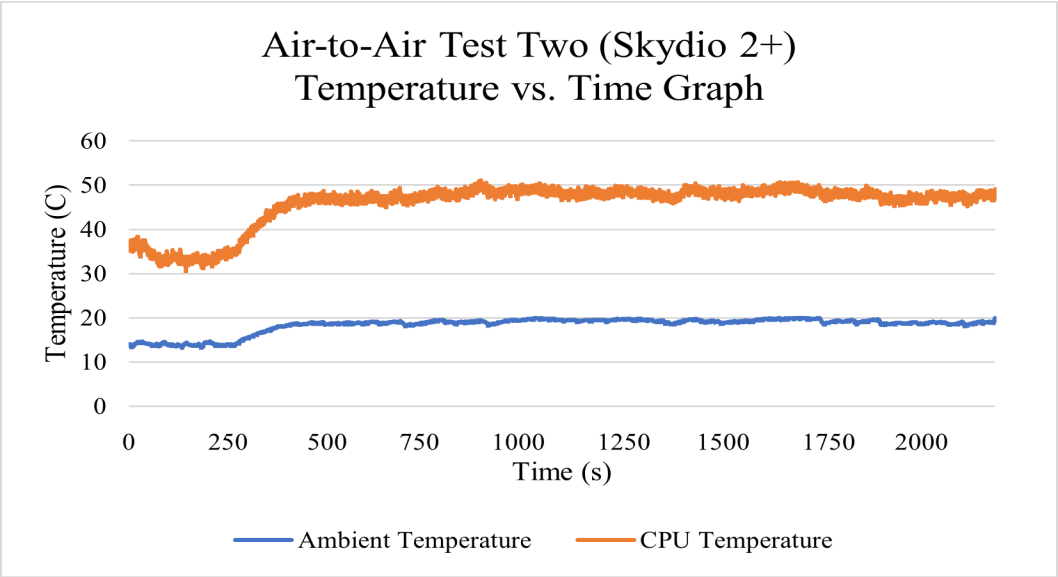

Figure 7.2. Air-to-Air Test Two: Difference between the Ambient and CPU Temperature (Skydio 2+ Target).

Both Figure 7.1 and Figure 7.2 highlight the ambient and CPU temperature changes to learn more about the thermal properties associated with attaching the *Detachable Drone Hijacker* to a host aircraft. Given the average results listed in the previous two tables, it was necessary to graph this differential over time. During the Parrot Bebop attack there was an average delta between the CPU and ambient temperature of 15°C while during the attack on the Skydio 2+, the average difference was 10°C. This is a noteworthy difference in precision between measurements because there are no differences in processes on the DDH when attacking the Parrot Bebop or the Skydio 2+. Therefore, future experiments should incorporate higher quality sensors than the Raspberry Pi SenseHat to gain more accurate insights into the temperature effects of running the deauthentication attack using the *Detachable Drone Hijacker*.

7.1.5 Conclusion

In its current form, the *Detachable Drone Hijacker* is meant to be a configurable "bolt-on" solution to be carried on a variety of platforms. Depending on the host system, there could be issues with system integration. Specifically, the average temperature difference of 15°C

and 10°C from the CPU versus ambient temperature results during air-to-air operations may cause problems when integrating on certain host aircraft. This excess heat could cause unintentional short circuits or fires onboard the host-UAV if it is not appropriately equipped. Additionally, when using the deauthentication attack, the remote connection to the *Detachable Drone Hijacker* is severed so there are no processes interfering with scanning for potential UAV targets. Therefore, the operator of the *Detachable Drone Hijacker* does not have any control of the device for troubleshooting purposes. This issue can be remedied by integrating the Ethernet port on the Raspberry Pi with an embedded module to establish a separate connection back to the ground station. The research team conducted a baseline test of this functionality with a Persistent Systems MPU5 [139] wave relay radio. This function testing is important for future research in system integration with other unmanned aircraft in Chapter 8.

The preceding tests associated with Experiment One proved to be very promising as it pertains to the development of a future operational capability. Not only did the research team show that the system works against WPA2 encrypted targets, but this research showed that it is possible to deliver cyber-attacks to target an adversarial UAV from a friendly-UAV with no disruption to the surrounding environment. Additionally, the functions test using the Persistent Systems MPU5 identified ways to grow the current prototype into a networked family of systems.

7.2 Experiment Two: Static Sub-Freezing Temperature Testing

7.2.1 Introduction

Experiment Two sought to simulate, in a restricted environment, an operational environment where the *Detachable Drone Hijacker* is employed on a ship deployed in the Arctic. Test One simulates storage inside the skin of a ship and employment in a sub-freezing environment. Then, Test Two simulated persistent operation in a sub-freezing environment for thirty minutes, while Test Three simulated persistent operations for 60 minutes. These bench-top tests are meant to inform future experiments in an alpine or arctic environment. This type of testing proves integral in the system design and engineering process used for low-rate initial production.

7.2.2 Objectives

Experiment Two seeks to understand the following information:

- The *Detachable Drone Hijacker* functionality in sub-freezing temperatures.
- The thermal characteristics associated with sub-freezing temperatures.
- Any system limitations or degradation in sub-freezing temperatures.

7.2.3 Execution

To prevent frozen condensation interrupting any system operations during the sub-freezing tests, the *Detachable Drone Hijacker* was placed inside a one-gallon Ziploc bag with ten silicon desiccate packets for five days to absorb any system or environmental moisture. Because of environmental and range constraints, these static tests were carried out with the *Detachable Drone Hijacker* located inside of a commercial freezer. Thus, the target UAV could not be flown, which limited the research team's ability to observe the target's behavior in a sub-freezing environment. However, the GCS behavior was observed, and given the consistency of results from previous tests, it is safe to assume that the target UAV would hover in place and return to its point of origin after a preset time, in the event of a successful attack. The proceeding tests seek to measure the ambient temperature, CPU temperature, average humidity, and the ground control station's behavior once the attack occurs.

Sub-Zero Test One: Room Temperature to Sub-Zero Temperature

In sub-zero test one, the research team sought to simulate an operational use-case where the *Detachable Drone Hijacker* would be held in a temperature controlled environment and then employed in a sub-freezing environment. Due to freezer size constraints that limit the range of electromagnetic wave propagation, the *Detachable Drone Hijacker* was employed inside of a closed freezer that was located five meters away from its target, which was outside of the freezer. Test one initially stored the *Detachable Drone Hijacker* in a room temperature environment, then placed the *Detachable Drone Hijacker* in a freezer, with the door shut, for two minutes prior to attacking the target UAV from within the closed freezer. This attack was controlled by the ground station outside of the freezer.

Sub-Zero Test Two: Thirty Minutes of Sub-Zero Temperature

In sub-zero test two, the research team sought to simulate an operational use-case where the *Detachable Drone Hijacker* is powered on in an alpine or arctic environment. Much like test one, the freezer's size and doors constrained the range of electromagnetic wave propagation; thus, the *Detachable Drone Hijacker* was employed inside of a freezer, at a distance of five meters from its target, which was located outside of the freezer. The *Detachable Drone Hijacker* was placed in the closed freezer for 30 minutes prior to launching an attack against the target. Much like the first attack, the freezer door was shut and was the only physical obstacle between the *Detachable Drone Hijacker* and the target.

Sub-Zero Test Three: Sixty Minutes of Sub-Zero Temperature

In sub-zero test three, the research team extended the operational use-case where the *Detachable Drone Hijacker* is consistently powered on in an alpine or arctic environment for 60 minutes. All other controls from the previous sub-zero tests remained constant.

7.2.4 Results and Discussion

During this experiment the pre-set temperature of the commercial freezer used was −13.9°C. However, the results tables shows numbers vastly different from the operating temperature. That is likely due to the Raspberry Pi's heat radiation which disrupts the SenseHat's temperature sensors which causes an elevated ambient temperature output. Additionally, it is possible that the SenseHat temperature sensors are damaged, giving faulty data. However,

given the consistent range of data it is more likely to be thermal interference from the Raspberry Pi's normal operation than a significant degradation to the SenseHat sensors.

Table 7.6 and Figure 7.3 show the results from the first round of tests. As can be seen in Table 7.6, the target behavior could not be observed because both devices were indoors, but the *Detachable Drone Hijacker* was still able to sever the link of between the target UAV and its GCS. Therefore, in an operational environment, the target UAV would hover and return to its point of origin, just as it did during the field tests conducted in Experiment One.

Table 7.6. Sub-Zero Test One: Room Temperature to Sub-Zero Temperature.

Target	Parrot Bebop	**Average CPU Temperature (°C)**	54.1
Target Behavior	Could not be observed	**Average Ambient Temperature (°C)**	33.1
GCS Behavior	Disconnected/No Control	**Average Humidity (%)**	15.7
DDH to Target Distance (m)	5	**CPU Temp (°C)**	50.6
GCS to Target Distance (m)	0	**Minimum Ambient Temp (°C)**	31.3
Target Elevation (m)	0	**Maximum CPU Temp (°C)**	57.0
DDH Elevation (m)	0	**Maximum Ambient Temp (°C)**	35.2

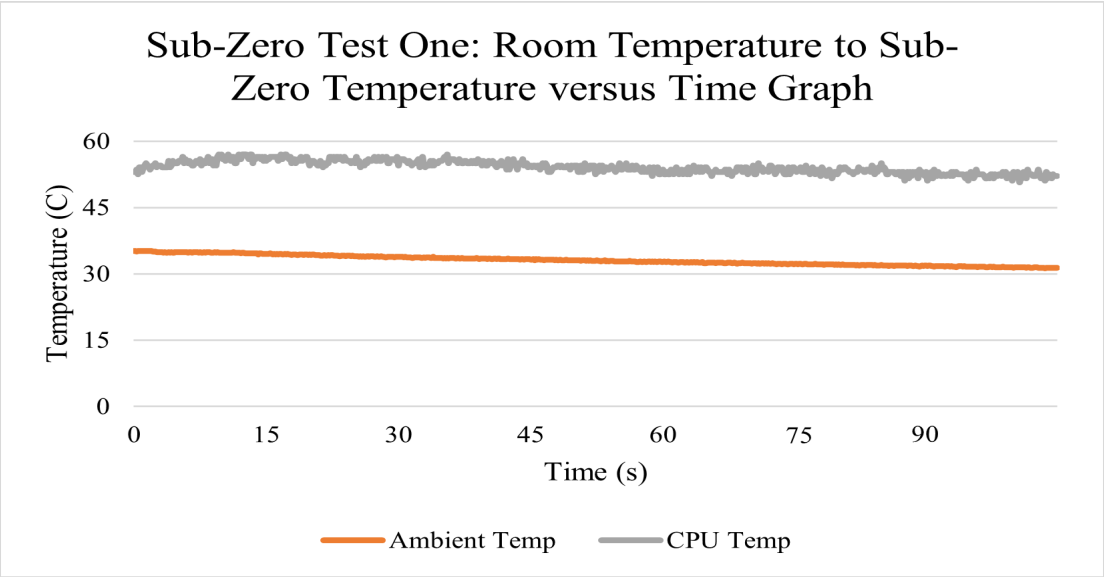

Figure 7.3. Sub-Zero Test One: Room Temperature to Sub-Zero Graph.

Table 7.7 and Figure 7.4 show the results from the second round of tests in a sub-freezing environment. This test sought to emulate a scenario when the *Detachable Drone Hijacker* is attached to a host UAV during operations for an extended period of time. As Table 7.7 shows, operations were not degraded, and the *Detachable Drone Hijacker* successfully severed the link between the target and its GCS.

Table 7.7. Sub-Zero Test Two: Thirty Minutes of Sub-Zero Temperature

Target	Parrot Bebop	**Average CPU Temperature (°C)**	37.5
Target Behavior	Could not be observed	**Average Ambient Temperature (°C)**	16.2
GCS Behavior	Disconnected/No Control	**Average Humidity (%)**	15.7
DDH to Target Distance (m)	5	**CPU Temp (°C)**	34.1
GCS to Target Distance (m)	0	**Minimum Ambient Temp (°C)**	16.1
Target Elevation (m)	0	**Maximum CPU Temp (°C)**	40.4
DDH Elevation (m)	0	**Maximum Ambient Temp (°C)**	16.4

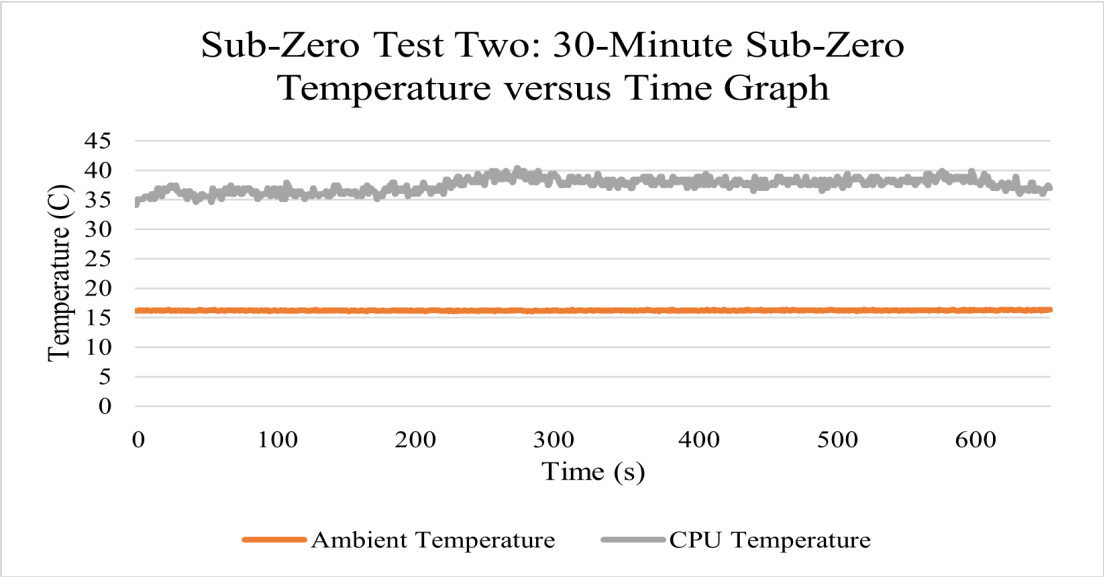

Figure 7.4. Sub-Zero Test Two: 30-Minute Sub-Zero Temperature Graph.

Table 7.8 and Figure 7.5 represent the third sub-zero test conducted. In this test, the *Detachable Drone Hijacker* was left in the freezer for sixty-minutes to simulate an operation where the device was powered continuously in a sub-freezing environment. This could be an operational use-case in the Baltics as before, or during winter operations in the Pacific Northwest. It is here where the *Detachable Drone Hijacker* failed to sufficiently sever the link between the target and its GCS. The *Detachable Drone Hijacker* had no problem identifying its target, but it could not switch to the correct channel to send the deauthentication frames to its target. This is most likely due to sluggish operations that occur in extreme cold temperatures. In an operational environment, the *Detachable Drone Hijacker* would need to have a protective case to ensure that moisture and other cold weather-related issues do not hamper operations.

Table 7.8. Sub-Zero Test Three: Sixty Minutes of Sub-Zero Temperature.

Target	Parrot Bebop	**Average CPU Temperature (°C)**	35.4
Target Behavior	Could not be observed	**Average Ambient Temperature (°C)**	13.7
GCS Behavior	Detection Only	**Average Humidity (%)**	18.3
DDH to Target Distance (m)	5	**CPU Temp (°C)**	33.5
GCS to Target Distance (m)	0	**Minimum Ambient Temp (°C)**	13.5
Target Elevation (m)	0	**Maximum CPU Temp (°C)**	37.7
DDH Elevation (m)	0	**Maximum Ambient Temp (°C)**	13.6

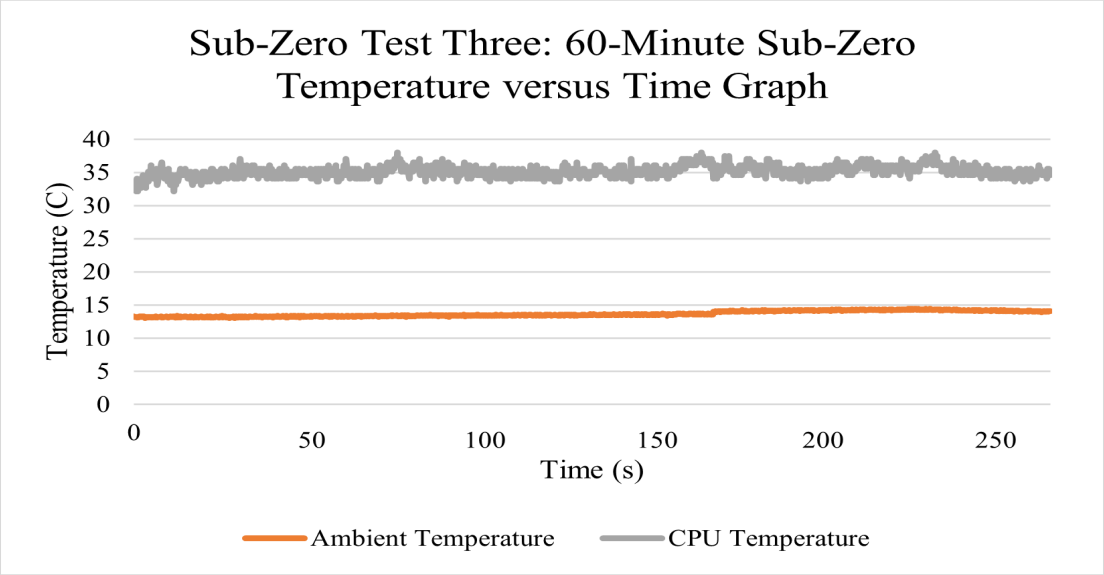

Figure 7.5. Sub-Zero Test Three: 60-Minute Sub-Zero Temperature Graph.

7.2.5 Conclusion

All-in-all, the sub-zero temperature tests were useful in identifying the capabilities and limitations of the *Detachable Drone Hijacker* for cold weather environments. Additionally, these tests helped the research team identify future work for operational use in Arctic or alpine environments. First, the research team identified the need for better temperature

sensors on board to ensure more accurate readings. The SenseHat specifications listed an accuracy of 2°C within 0-65°C range. At the testing temperature of -13.9°C, this likely caused malfunctions with the SenseHat. On the other hand, there were promising results when exposing the *Detachable Drone Hijacker* to continuous cold-weather for 30 minutes. For the *Detachable Drone Hijacker* to be used operationally, it will need to be ruggedized to operate in extreme-weather environments. This may increase the SWaP of the *Detachable Drone Hijacker* (if no further optimizations are made) which could limit compatible UAVs for future testing. In sum, further system design and testing should take place to meet a requirement for operations in a cold- or wet-weather environment.

7.3 Experiment Three: Static Thermal Testing

7.3.1 Introduction

Experiment Three consisted of thermal image testing of the *Detachable Drone Hijacker* prototype before, during, and after operations.

7.3.2 Objectives

The goal of Experiment Three was to measure the thermal signature associated with the *Detachable Drone Hijacker* and determine the tradeoffs that may be associated with the use of a lightweight, low power consuming C-UAS prototype. Ultimately, this information will help future researchers test and evaluate the viability of the cyber-attack methods outlined in Experiment One.

7.3.3 Execution

Throughout this experiment, still images were taken (one meter away from the *Detachable Drone Hijacker*) and analyzed by the research team. It was desirable to get separate measurements at different angles to best determine the temperature associated with each phase of operation. Thus, still images were taken from top-down, front, and bottom-up angles before, during, and after system operation.

7.3.4 Results and Discussion

Table 7.9 shows the temperature catalogues of the *Detachable Drone Hijacker* before operations. These still images show a system that stores and radiates thermal energy even when not operational. While not pertinent for this thesis, if further production of this device occurs, determining the thermal signature of the *Detachable Drone Hijacker* at farther distances as this would be important for units who require low-signature for their operations.

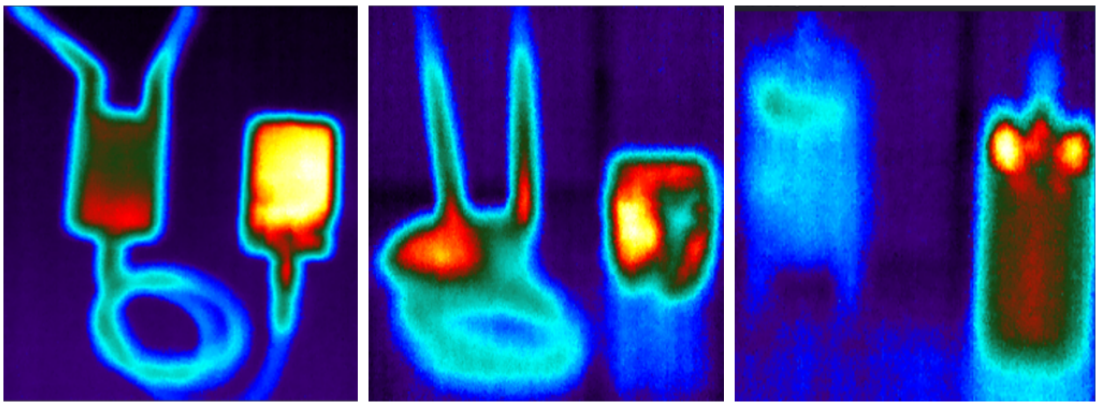

Figure 7.6. Thermal Test One: Mode OFF, Pre-Operations.

Table 7.9. Thermal Test One Results: Mode OFF, Pre-Operations.

Camera Look Angle	Power State	Test Mode	Color Code	Color Temperature (°C)
Top	OFF	Pre-Operations	White/Yellow	26.6
Top	OFF	Pre-Operations	Orange/Red	24.6
Top	OFF	Pre-Operations	Light Blue	22.5
Top	OFF	Pre-Operations	Dark Blue	20.5
Front	OFF	Pre-Operations	White/Yellow	21.7
Front	OFF	Pre-Operations	Orange/Red	21.3
Front	OFF	Pre-Operations	Light Blue	20.6
Front	OFF	Pre-Operations	Dark Blue	19.7
Bottom	OFF	Pre-Operations	White/Yellow	22.3
Bottom	OFF	Pre-Operations	Orange/Red	21.5
Bottom	OFF	Pre-Operations	Light Blue	20.5
Bottom	OFF	Pre-Operations	Dark Blue	19.5

Table 7.10 shows that after five minutes of operations, the temperature of the *Detachable Drone Hijacker* increases by only 3.3°C. This is extremely promising given the need to

integrate the *Detachable Drone Hijacker* onto another aerial platform. This varies significantly from the in-flight temperature measurements for several reasons. First, it is possible that this disparity comes from the SenseHat on the Raspberry Pi, which possibly gave faulty temperature measurements. This temperature disparity may also be due to the fact that the FLIR A320 is primarily meant for surface monitoring of systems, not CPU monitoring like the SenseHat and the internal monitors on the Raspberry Pi.

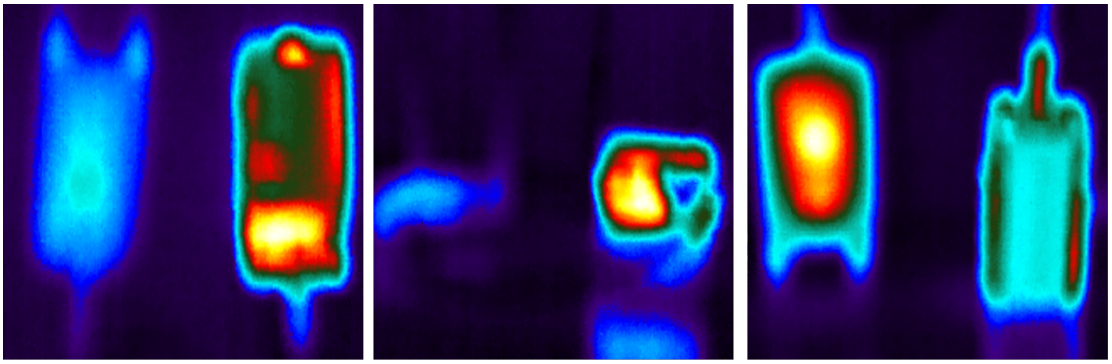

Figure 7.7. Thermal Test Two: Mode ON, During Operations (5 Minutes Active).

Table 7.10. Thermal Test Two Results: Mode ON, 5 Minutes Active.

Camera Look Angle	Power State	Test Mode	Color Code	Color Temperature (°C)
Top	ON	During Operation (5 Minutes Active)	White/Yellow	29.8
Top	ON	During Operation (5 Minutes Active)	Orange/Red	27.7
Top	ON	During Operation (5 Minutes Active)	Light Blue	23.7
Top	ON	During Operation (5 Minutes Active)	Dark Blue	20.2
Front	ON	During Operation (5 Minutes Active)	White/Yellow	30.3
Front	ON	During Operation (5 Minutes Active)	Orange/Red	27.3
Front	ON	During Operation (5 Minutes Active)	Light Blue	22.5
Front	ON	During Operation (5 Minutes Active)	Dark Blue	19.7
Bottom	ON	During Operation (5 Minutes Active)	White/Yellow	30.5
Bottom	ON	During Operation (5 Minutes Active)	Orange/Red	27.3
Bottom	ON	During Operation (5 Minutes Active)	Light Blue	23.8
Bottom	ON	During Operation (5 Minutes Active)	Dark Blue	20.2

Table 7.11 shows that after only five minutes of cool down time, the *Detachable Drone Hijacker* returns to its pre-operational temperature. This is important as the system cannot continue to expend excess heat after use or else there may be deleterious effects to the host-UAV.

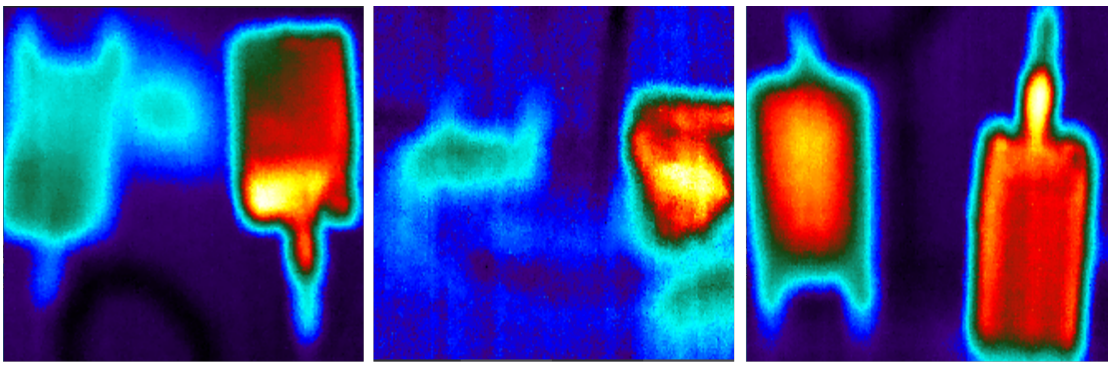

Figure 7.8. Thermal Test Three: Mode OFF, Post-Operations.

Table 7.11. Thermal Test Three Results: Mode OFF, 5 Minutes Post-Operations.

Camera Look Angle	Power State	Test Mode	Color Code	Color Temperature (°C)
Top	OFF	5-Minutes Post Operations	White/Yellow	25.2
Top	OFF	5-Minutes Post Operations	Orange/Red	24.2
Top	OFF	5-Minutes Post Operations	Light Blue	21.9
Top	OFF	5-Minutes Post Operations	Dark Blue	20.3
Front	OFF	5-Minutes Post Operations	White/Yellow	22.2
Front	OFF	5-Minutes Post Operations	Orange/Red	21.4
Front	OFF	5-Minutes Post Operations	Light Blue	20.4
Front	OFF	5-Minutes Post Operations	Dark Blue	20.1
Bottom	OFF	5-Minutes Post Operations	White/Yellow	23.8
Bottom	OFF	5-Minutes Post Operations	Orange/Red	23.1
Bottom	OFF	5-Minutes Post Operations	Light Blue	21.7
Bottom	OFF	5-Minutes Post Operations	Dark Blue	20.2

7.3.5 Conclusion

In sum, the results from the thermal camera tests differed greatly from those carried out in Experiment One and Experiment Two. This variation could be from sensor placement or inaccuracies in the SenseHat or from inaccuracies in the FLIR A320. However, the documentation provided for the FLIR A320 is more substantial than the documentation available for the SenseHat which seems to suggest that validation data from the former may be more substantial than the latter. However, for low-rate initial production and system development, further thermal characteristic testing should be carried out. Lastly, depending on host-device integration specifications, if there is a concern over heat properties, it is recommended to build a cool-down mechanism for the *Detachable Drone Hijacker*.

7.4 Conclusion

As the three preceding experiments show, it is possible to create a system that are personalized to create a decentralized web of devices that can identify, track, target, and mitigate unwanted UAVs. The framework established in Chapter 5 and results from this chapter are not meant to replace the current systems, but instead to augment and enhance them.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 8:
Conclusion

This thesis makes the case that the current U.S. framework for countering unmanned systems is insufficient because it lacks the robustness needed to thwart a multi-pronged attack from an adversarial group. This was evidenced in the ISIS drone program [5], the Nagorno-Karabakh conflict [7], and now in Russia's war on the Ukraine [35]. UAVs give less technologically advanced combatants the ability to fight asymmetrically against their foes and achieve outsized tactical and strategic victories. In the case of Russia's war on Ukraine, a single $1 million dollar UAV destroyed Russian surface-to-air missiles valued at over $50 million dollars—the exact equipment that was supposed to protect their convoys from aircraft in the first place [35]. The primary use of centralized, terrestrial equipment is flawed in its assumptions that it will be able to mitigate a threat entering into its engagement area. This is because a ground-based C-UAS device has to overcome the myriad technological limitations to respond to high-flying UAVs. Conversely, a networked squadron of UAVs designed for aerial interdiction with devices such as the *Detachable Drone Hijacker* present a novel way to counter the UAV threats.

The three experiments carried out in Chapter 7 serve as the basis for future experimentation of the aerial C-UAS concept using the *Detachable Drone Hijacker*. While the 802.11 WiFi drone targets are not the most capable, these experiments prove that it is possible to develop a family of low-SWaP devices that can be networked under a common GUI and application.

The field testing was promising and showed that the concept is viable, while the sub-zero tests proved that the *Detachable Drone Hijacker* can be employed in multiple operating environments. With an average temperature increase of only 3.3 degrees Celsius, the thermal signature experiments also proved that when integrated onboard another aircraft, the *Detachable Drone Hijacker* has minimal effect to the host device.

Notably, the experiments conducted in Chapter 7 show that by using only commercial technology, it is possible to build a C-UAS device designed for aerial interdiction. From the baseline prototype development and aerial experiments to the sub-zero and thermal testing, the *Detachable Drone Hijacker* can move toward development of a concept into a capability.

8.1 Future Work

As described in Chapter 2, the C-UAS field is experiencing an incredible amount of competition that will only continue to grow as new threats enter the battlefield. Therefore, there are many options for future work in developing low-SWaP payloads like the *Detachable Drone Hijacker*. Of note, future researchers may be interested to:

- measure the maximum effective range of the *Detachable Drone Hijacker* during air-to-air operations.
- measure the time between scanning, picking up a target, and mitigation of target. This should be built into the logging processes in future experiments.
- investigate the viability of a GNSS spoofing capability without adversely affecting the host UAV.
- investigate and develop a target library for signals used by the DJI family of drones. These devices use communication protocols that are more complex than those investigated in this thesis. The commanding lead from DJI in the consumer drone market place must be taken into consideration.
- investigate and develop a target library for the do-it-yourself drones that use FHSS modulated signals for communications between a GCS and the UAV. Anyone can buy the flight control motors, a mini-computer, and the RF or GNSS modules to create a customized UAV that flies via GNSS waypoints or fails to emit traditional RF energy for command and control.
- study the effects of EM interference from the *Detachable Drone Hijacker* on any other onboard systems. One of the main problems in the road to the widespread adoption of this system is the potential for interference with other processes onboard a host-UAV. This should be further investigated using the ScanEagle drone as a host.
- integrate each C-UAS into a networked family of systems that are accessible for users through a single application. This includes the integration with the existing systems in the acquisition process like the MADIS [53], Sentry Tower [38], and Skytracker [37].
- conduct a business acquisition use-case to determine the customers in the DOD, DHS, and civilian sectors (such as police stations, stadium security, or port authorities).
- study, analyze, and make recommendations to update current C-UAS doctrine, standard operating procedures, and TTPs. As mentioned in the appendix to Chapter 2, the current doctrine and joint-force TTPs must be updated to meet this threat.

- investigate the viability for development and integration of target libraries for use with a high-performance computer like the NVIDIA Jetson TX2 [140]. The TX2 is used in many sensor modules for its compute power; it is more reliable and has a higher performance rating than the RaspberryPi 4 used in this thesis.
- analyze the RF and thermal signatures of C-UAS technologies currently in use by the DOD and DHS.

8.2 Concluding Remarks

In summary, the C-UAS market remains nascent and ripe for disruption. High-performance computer modules are getting smaller and consuming less power while increasing in capability. Companies developing C-UAS technologies should refocus their efforts on harnessing high-performance with low-SWaP to create less expensive, but more capable C-UAS devices. This thesis and the experiments using the *Detachable Drone Hijacker* prove that it is possible to deliver an aerial cyber-attack against multiple UAVs with minimal effect on the host device. This framework is not meant to usurp the current methodology, but is meant to augment and increase the effectiveness of C-UAS technology to meet the needs of the operating environment. While this study focused on countering consumer drones to protect military bases and strategic infrastructure, the past two European wars have shown that terrestrial short-range air-defenses are no match for high-flying UAVs with kinetic strike capabilities. Thus, there are many opportunities for future work in this space to target both consumer and government UAVs alike.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX: Experiment One: Operational Field Testing Results

A.1 Results Tables from Ground-to-Air Field Testing

Table A.1. Ground-to-Air Field Test One: Static Deauthentication Attack (10m - Different Elevation).

Target	Parrot Bebop	**Average Power Consumption (W)**	0.678
Target Behavior	Hovers then lands	**Minimum Power Consumption (W)**	0.00
GCS Behavior	Disconnected/No Control	**Maximum Power Consumption (W)**	75.0
DDH to Target Distance (m)	10	**Average CPU Temperature (°C)**	44.1
GCS to Target Distance (m)	10	**Minimum CPU Temperature (°C)**	39.4
Target Elevation (m)	10	**Maximum CPU Temperature (°C)**	47.2
DDH Elevation (m)	5	**Average Ambient Temperature (°C)**	28.8
Humidity (%)	31.5	**Minimum Ambient Temperature (°C)**	28.3
		Maximum Ambient Temperature (°C)	29.2

Table A.2. Ground-to-Air Field Test Two: Static Deauthentication Attack (10m - Same Elevation).

Target	Parrot Bebop	**Average Power Consumption (W)**	1.11
Target Behavior	Hovers then lands	**Minimum Power Consumption (W)**	0.002
GCS Behavior	Disconnected/No Control	**Maximum Power Consumption (W)**	1.54
DDH to Target Distance (m)	10	**Average CPU Temperature (°C)**	33.5
GCS to Target Distance (m)	10	**Minimum CPU Temperature (°C)**	30.2
Target Elevation (m)	5	**Maximum CPU Temperature (°C)**	36.5
DDH Elevation (m)	5	**Average Ambient Temperature (°C)**	18.0
Humidity (%)	45.8	**Minimum Ambient Temperature (°C)**	17.8
		Maximum Ambient Temperature (°C)	18.2

Table A.3. Ground-to-Air Field Test Three: Static Deauthentication Attack (100m - Different Elevation).

Target	Parrot Bebop	**Average Power Consumption (W)**	1.11
Target Behavior	Hovers then lands	**Minimum Power Consumption (W)**	1.03
GCS Behavior	Disconnected/No Control	**Maximum Power Consumption (W)**	1.44
DDH to Target Distance (m)	100	**Average CPU Temperature (°C)**	32.7
GCS to Target Distance (m)	10	**Minimum CPU Temperature (°C)**	30.7
Target Elevation (m)	30	**Maximum CPU Temperature (°C)**	35.1
DDH Elevation (m)	5	**Average Ambient Temperature (°C)**	17.6
Humidity (%)	45.6	**Minimum Ambient Temperature (°C)**	17.1
		Maximum Ambient Temperature (°C)	18.2

Table A.4. Ground-to-Air Field Test Four: Static Deauthentication Attack (200m - Different Elevation).

Target	Parrot Bebop	**Average Power Consumption (W)**	1.10
Target Behavior	Hovers then lands	**Minimum Power Consumption (W)**	1.03
GCS Behavior	Disconnected/No Control	**Maximum Power Consumption (W)**	1.44
DDH to Target Distance (m)	400	**Average CPU Temperature (°C)**	30.6
GCS to Target Distance (m)	10	**Minimum CPU Temperature (°C)**	27.3
Target Elevation (m)	30	**Maximum CPU Temperature (°C)**	33.1
DDH Elevation (m)	5	**Average Ambient Temperature (°C)**	15.7
Humidity (%)	49.7	**Minimum Ambient Temperature (°C)**	15.1
		Maximum Ambient Temperature (°C)	16.1

Table A.5. Ground-to-Air Field Test Five: Static Deauthentication Attack (250m - Different Elevation.)

Target	Parrot Bebop	**Average Power Consumption (W)**	1.08
Target Behavior	Hovers then lands	**Minimum Power Consumption (W)**	0.923
GCS Behavior	Disconnected/No Control	**Maximum Power Consumption (W)**	1.11
DDH to Target Distance (m)	250	**Average CPU Temperature (°C)**	29.3
GCS to Target Distance (m)	10	**Minimum CPU Temperature (°C)**	27.3
Target Elevation (m)	10	**Maximum CPU Temperature (°C)**	33.1
DDH Elevation (m)	5	**Average Ambient Temperature (°C)**	16.0
Humidity (%)	48.6	**Minimum Ambient Temperature (°C)**	15.3
		Maximum Ambient Temperature (°C)	17.2

Table A.6. Ground-to-Air Field Test Six: Static Deauthentication Attack (400m - Different Elevation).

Target	Parrot Bebop	**Average Power Consumption (W)**	1.08
Target Behavior	No Effect	**Minimum Power Consumption (W)**	0.915
GCS Behavior	No Effect	**Maximum Power Consumption (W)**	1.11
DDH to Target Distance (m)	400	**Average CPU Temperature (°C)**	35.1
GCS to Target Distance (m)	10	**Minimum CPU Temperature (°C)**	28.7
Target Elevation (m)	30	**Maximum CPU Temperature (°C)**	38.5
DDH Elevation (m)	5	**Average Ambient Temperature (°C)**	17.9
Humidity (%)	50.6	**Minimum Ambient Temperature (°C)**	16.5
		Maximum Ambient Temperature (°C)	19.7

Table A.7. Ground-to-Air Field Test Seven: Moving Deauthentication Attack (250-100m - Different Elevation).

Target	Parrot Bebop	**Average Power Consumption (W)**	1.08
Target Behavior	Return to last known connection point	**Minimum Power Consumption (W)**	0.927
GCS Behavior	Disconnected/No Control	**Maximum Power Consumption (W)**	1.11
DDH to Target Distance (m)	100-250	**Average CPU Temperature (°C)**	34.6
GCS to Target Distance (m)	N/A	**Minimum CPU Temperature (°C)**	30.7
Target Elevation (m)	10-20	**Maximum CPU Temperature (°C)**	38.5
DDH Elevation (m)	5	**Average Ambient Temperature (°C)**	19.5
Humidity (%)	43.6	**Minimum Ambient Temperature (°C)**	19.0
		Maximum Ambient Temperature (°C)	20.0

List of References

[1] J. Gargus, *The Son Tay Raid: American POWs in Vietnam Were Not Forgotten* (Williams-Ford Texas A&M University military history series). College Station, TX: Texas A & M University Press, 2010. Available: https://books.google.com/books?id=n21jHFfHxiMC

[2] R. C. Hall, "Reconnaissance drones: Their first use in the Cold War," *Air Power History*, vol. 61, no. 3, pp. 20–27, 2014. Available: http://www.jstor.org/stable/26276490

[3] Joint Chiefs of Staff, "Joint Publication 3-30: Joint Air Operations," July 2019.

[4] B. Wilson, S. Tierney, B. Toland, R. Burns, C. Steiner, C. Adams, M. Nixon, R. Khan, M. Ziegler, J. Osburg, and I. Chang, *Small Unmanned Aerial System Adversary Capabilities*. Santa Monica, CA: RAND Corporation, 2020. Available: https://www.rand.org/pubs/research_reports/RR3023.html

[5] A. Almohammad and A. Speckhard, "ISIS Drones: Evolution, Leadership, Bases, Operations and Logistics," International Center for the Study of Violent Extremism, Tech. Rep., May 2017. Available: https://www.icsve.org/isis-drones-evolution-leadership-bases-operations-and-logistics/

[6] J. Warrick, "Use of weaponized drones by ISIS spurs terrorism fears," *Washington Post*, Feb. 2017. Available: https://www.washingtonpost.com/world/national-security/use-of-weaponized-drones-by-isis-spurs-terrorism-fears/2017/02/21/9d83d51e-f382-11e6-8d72-263470bf0401_story.html

[7] S. Sukhankin, "The Second Karabakh War: Lessons and Implications for Russia (Part One)," *Eurasia Daily Monitor*, vol. 18, no. 2, Jan. 2021. Available: https://jamestown.org/program/the-second-karabakh-war-lessons-and-implications-for-russia-part-one/

[8] S. Sukhankin, "The Second Karabakh War: Lessons and Implications for Russia (Part Two)," *Eurasia Daily Monitor*, vol. 18, no. 7, Jan. 2021. Available: https://jamestown.org/program/the-second-karabakh-war-lessons-and-implications-for-russia-part-two/

[9] I. Arreguin-Toft, *How the Weak Win Wars: A Theory of Asymmetric Conflict* (Cambridge Studies in International Relations). New York: Cambridge University Press, 2005, no. 99.

[10] R. Dixon, "Azerbaijan's drones owned the battlefield in Nagorno-Karabakh — and showed future of warfare," *Washington Post*, Nov. 2020. Available: https://www.washingtonpost.com/world/europe/nagorno-karabkah-drones-azerbaijan-aremenia/2020/11/11/441bcbd2-193d-11eb-8bda-814ca56e138b_story.html

[11] Official Alerts & Statements - CISA: Stop Ransomware. *cisa.gov*. [Online]. Available: https://www.cisa.gov/stopransomware/official-alerts-statements-cisa

[12] A. Beccaro, "Modern Irregular Warfare: The ISIS Case Study," *Small Wars & Insurgencies*, vol. 29, no. 2, pp. 207–228, Mar. 2018, publisher: Routledge _eprint: https://doi.org/10.1080/09592318.2018.1433469. Available: https://doi.org/10.1080/09592318.2018.1433469

[13] D. Rassler, "The Islamic State and Drones: Supply, Scale, and Future Threats," Combating Terrorism Center at West Point, West Point, NY, Tech. Rep., July 2018. Available: https://ctc.usma.edu/wp-content/uploads/2018/07/Islamic-State-and-Drones-Release-Version.pdf

[14] B. Watson. (2017, Jan.). The Drones of ISIS. *Defense One*. [Online]. Available: https://www.defenseone.com/technology/2017/01/drones-isis/134542/

[15] M. S. Schmidt and E. Schmitt, "Pentagon Confronts a New Threat From ISIS: Exploding Drones," *The New York Times*, Oct. 2016. Available: https://www.nytimes.com/2016/10/12/world/middleeast/iraq-drones-isis.html

[16] Reuters Staff, "Islamic State drone kills two Kurdish fighters, wounds two French soldiers," *Reuters*, Oct. 2016. Available: https://www.reuters.com/article/us-france-iraq-iraq-idUSKCN12B2QI

[17] A. Plaw and E. Santoro, "Reaping the Whirlwind: Drones Flown by Non-state Actors Now Pose a Lethal Threat," *The Jamestown Foundation: Terrorism Monitor*, vol. 15, no. 17, Sep. 2017. Available: https://jamestown.org/program/reaping-the-whirlwind-drones-flown-by-non-state-actors-now-pose-a-lethal-threat/

[18] "Armenia-Azerbaijan: Why did Nagorno-Karabakh spark a conflict?" *BBC News*, Nov. 2020. Available: https://www.bbc.com/news/world-europe-54324772

[19] I. Tharoor, "The war in the Caucasus could turn into a regional calamity," *Washington Post*, Oct. 2020. Available: https://www.washingtonpost.com/world/2020/10/05/azerbaijan-armenia-clash-turkey-russia/

[20] M. Kofman. (2020, Dec.). A Look at the Military Lessons of the Nagorno-Karabakh Conflict | Russia Matters. *Russia Matters - Analysis*. [Online]. Available: https://www.russiamatters.org/analysis/look-military-lessons-nagorno-karabakh-conflict

[21] Y. Ramati, "Military Lessons: Armenia-Azerbaijan Conflict," Dec. 2020. Available: https://www.miryaminstitute.org/commentary-blog/military-lessons-armenia-azerbaijan-conflict

[22] S. Shaikh and W. Rumbaugh, "The Air and Missile War in Nagorno-Karabakh: Lessons for the Future of Strike and Defense," Center for Strategic and International Studies, Washington D.C., Analysis, Dec. 2020. Available: https://www.csis.org/analysis/air-and-missile-war-nagorno-karabakh-lessons-future-strike-and-defense

[23] C. Kasapoglu, "'Dronization' Period in Turkish Warfare Approach: Azerbaijan Carried Turkey's SİHA Concepts in the Middle East to the Caucasus," Center for Economics and Foreign Policy Studies, Istanbul, Turkey, Tech. Rep., Sep. 2020. Available: https://edam.org.tr/turk-harp-yaklasiminda-dronizasyon-donemi-azerbaycan-turkiyenin-orta-dogudaki-siha-konseptlerini-kafkasyaya-tasidi/

[24] S. Mitzer and J. Oliemans. (2021, Jan.). Aftermath: Lessons of the Nagorno-Karabakh War Are Paraded through the Streets of Baku. *Oryx Blog*. [Online]. Available: https://www.oryxspioenkop.com/2021/01/aftermath-lessons-of-nagorno-karabakh.html

[25] Bayraktar TB-2. [Online].

[26] S. Mitzer and J. Oliemans. (2020, Sep.). The Fight For Nagorno-Karabakh: Documenting Losses On The Sides Of Armenia And Azerbaijan. *Oryx Blog*. [Online]. Available: https://www.oryxspioenkop.com/2020/09/the-fight-for-nagorno-karabakh.html

[27] M. Kofman and L. Nersisyan. (2020, Oct.). The Second Nagorno-Karabakh War, Two Weeks In. *War on the Rocks*. [Online]. Available: http://warontherocks.com/2020/10/the-second-nagorno-karabakh-war-two-weeks-in/

[28] Loitering munitions: HAROP - Electro-Optically guided attack weapon. *Israeli Aerospace Industries*. [Online]. Available: https://www.iai.co.il/p/harop

[29] "Report for Selected Countries and Subjects: October 2021," International Monetary Fund, Tech. Rep., Oct. 2021. Available: https://www.imf.org/en/Publications/WEO/weo-database/2021/October/weo-report

[30] B. Ho, "The Second Nagorno-Karabakh War: Takeaways for Singapore's Ground-Based Air Defense," *Journal of Indo-Pacific Affairs, Air University Press*, Aug. 2021. Available: https://www.airuniversity.af.edu/JIPA/Display/Article/2743721/the-second-nagorno-karabakh-war-takeaways-for-singapores-ground-based-air-defen/#sdendnote16anc

[31] R. B. Urcosta, "Drones in the Nagorno-Karabakh," *Small Wars Journal*, Oct. 2020. Available: https://smallwarsjournal.com/jrnl/art/drones-nagorno-karabakh#_edn20

[32] A. H. Michel, "Counter-Drone Systems, 2nd Edition," Center for the Study of the Drone, Bard College, Annandale-on-Hudson, NY, Tech. Rep., Dec. 2019. Available: https://dronecenter.bard.edu/files/2019/12/CSD-CUAS-2nd-Edition-Web.pdf

[33] Training and Doctrine Command, "Army Training Publication 3-21.8 The Infantry Platoon and Squad," Aug. 2016. Available: https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN13842_ATP%203-21x8%20FINAL%20WEB%20INCL%20C1.pdf

[34] Marine Corps Tactics and Operations Group, "Marine Corps Reference Publication (MCRP) 3-10A.1, Infantry Battalion Operations," July 2020.

[35] B. Perrigo, "Ukraine's Secret Weapon Against Russia: Turkish Drones," *Time*, Mar. 2022. Available: https://time.com/6153197/ukraine-russia-turkish-drones-bayraktar/

[36] B. Patel and D. Rizer, "Counter-Unmanned Aircraft Systems Technology Guide," National Urban Security Technology Laboratory, U.S. Department of Homeland Security Science and Technology Directorate, Washington D.C., Tech. Rep. CUAS-T-G-1, Sep. 2019. Available: https://www.dhs.gov/sites/default/files/publications/c-uas-tech-guide_final_28feb2020.pdf

[37] SkyTracker Technology Suite. *caci.com*. [Online]. Available: https://www.caci.com/skytracker-technology-suite

[38] Anduril - Our Work. [Online]. Available: https://www.anduril.com/work

[39] J. Wang, Y. Liu, and H. Song, "Counter-Unmanned Aircraft System(s) C-UAS: State of the Art, Challenges, and Future Trends," *IEEE Aerospace and Electronic Systems Magazine*, vol. 36, no. 3, pp. 4–29, 2021.

[40] M. I. Skolnik, *Introduction to Radar Systems*, 2nd ed. Singapore: McGraw-Hill, Inc., 1981.

[41] W. L. Stutzman and G. A. Thiele, *Antenna Theory and Design*, 3rd ed. United States of America: John Wiley & Sons, Inc., 2013.

[42] B. Sklar, *Digital Communications: Fundamentals and Applications*, 2nd ed. Upper Saddle River, NJ: Prentic Hall Professional Technical Reference, 2001.

[43] P. Hell, M. Mezei, and P. J. Varga, "Drone communications analysis," in *2017 IEEE 15th International Symposium on Applied Machine Intelligence and Informatics (SAMI)*, 2017, pp. 000 213–000 216.

[44] D. Mototolea and C. Stolk, "Detection and Localization of Small Drones Using Commercial Off-the-Shelf FPGA Based Software Defined Radio Systems," *2018 International Conference on Communications (COMM)*, pp. 465–470, 2018.

[45] H. Zhang, C. Cao, L. Xu, and T. A. Gulliver, "A UAV detection algorithm based on an artificial neural network," *IEEE Access*, vol. 6, pp. 24 720–24 728, 2018.

[46] C.-C. Tsai, C.-T. Chiang, and W.-J. Liao, "Radar cross section measurement of unmanned aerial vehicles," in *2016 IEEE International Workshop on Electromagnetics: Applications and Student Innovation Competition (iWEM)*, 2016, pp. 1–3.

[47] J. Farlik, M. Kratky, J. Casar, and V. Stary, "Radar cross section and detection of small unmanned aerial vehicles," in *2016 17th International Conference on Mechatronics - Mechatronika (ME)*, 2016, pp. 1–7.

[48] M. Laurenzis, F. Christnacher, A. Matwyschuk, S. Schertzer, and S. Hengy, "Electro-optical detection probability of optical devices determined by bidirectional laser retro-reflection cross section," in *Radar Sensor Technology XIX; and Active and Passive Signatures VI*, G. C. Gilbreath, C. T. Hawley, K. I. Ranney, and A. Doerry, Eds., International Society for Optics and Photonics. SPIE, 2015, vol. 9461, pp. 502 – 509. Available: https://doi.org/10.1117/12.2175858

[49] F. Liang, W. G. Hatcher, W. Liao, W. Gao, and W. Yu, "Machine learning for security and the internet of things: The good, the bad, and the ugly," *IEEE Access*, vol. 7, pp. 158 126–158 147, 2019.

[50] F. Christnacher, S. Hengy, M. Laurenzis, A. Matwyschuk, P. Naz, S. Schertzer, and G. Schmitt, "Optical and acoustical UAV detection," in *Electro-Optical Remote Sensing X*, G. Kamerman and O. Steinvall, Eds., International Society for Optics and Photonics. SPIE, 2016, vol. 9988, pp. 83 – 95. Available: https://doi.org/10.1117/12.2240752

[51] J. Kim, C. Park, J. Ahn, Y. Ko, J. Park, and J. C. Gallagher, "Real-time UAV sound detection and analysis system," *2017 IEEE Sensors Applications Symposium (SAS)*, pp. 1–5, 2017.

[52] A. Sedunov, H. Salloum, A. Sutin, N. Sedunov, and S. Tsyuryupa, "UAV passive acoustic detection," in *2018 IEEE International Symposium on Technologies for Homeland Security (HST)*, 2018, pp. 1–6.

[53] B. Barrett, "The Marines' New Drone-Killer Aces Its First Test," *Wired*, July 2019, section: tags. Available: https://www.wired.com/story/iran-drone-marines-energy-weapon-lmadis/

[54] Northrup Grumman. (2020, July). Defining Possible Against Unmanned Aerial Systems. *Counter Unmanned Aerial Systems C-UAS*. [Online]. Available: https://www.northropgrumman.com/what-we-do/land/counter-unmanned-aerial-systems-c-uas

[55] K. Pärlin, M. M. Alam, and Y. L. Moullec, "Jamming of UAV remote control systems using software defined radio," *2018 International Conference on Military Communications and Information Systems (ICMCIS)*, pp. 1–6, 2018.

[56] M. Lichtman, R. P. Jover, M. Labib, R. Rao, V. Marojevic, and J. H. Reed, "LTE/LTE-A jamming, spoofing, and sniffing: Threat assessment and mitigation," *IEEE Communications Magazine*, vol. 54, no. 4, pp. 54–61, 2016.

[57] D. Kindley, "EA 18G Growler Aircraft," US Navy, Program Executive Officer (PMA265) Patuxent River United States, Tech. Rep., 2015.

[58] R. Poisel, *Modern Communication Jamming Principles and Techniques*, 2nd ed. Norwood, MA: Artech House, Inc., 2011.

[59] K. Brown, S. Drake, K. Mason, A. Piotrowski, and L. Swierkowski, "A distributed stand-in EW hunter-killer system," in *2007 10th International Conference on Information Fusion*, 2007, pp. 1–8.

[60] P. Thangasamy and T. Tesfay, "Effectiveness Evaluation for VHF Radar Jammer," *International Research Journal of Engineering and Technology*, vol. 03, pp. 76–83, 12 2016.

[61] R. Crane, "Fundamental limitations caused by RF propagation," *Proceedings of the IEEE*, vol. 69, no. 2, pp. 196–209, 1981.

[62] H. Rausch, "Jamming commercial satellite communications during wartime an empirical study," in *Fourth IEEE International Workshop on Information Assurance (IWIA'06)*, 2006, pp. 8 pp.–118.

[63] M. L. Psiaki and T. E. Humphreys, "GNSS Spoofing and Detection," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258–1270, 2016.

[64] Common Attack Pattern Enumeration and Classification (CAPEC), "CAPEC-628: Carry-Off GPS Attack," The MITRE Corporation, CAPEC Report CAPEC-628, Oct. 2021. Available: https://capec.mitre.org/data/definitions/628.html

[65] C. Kube. (2018, Apr.). Russia is jamming American drones in Syria, officials say. *NBC News*. [Online]. Available: https://www.nbcnews.com/news/military/russia-has-figured-out-how-jam-u-s-drones-syria-n863931

[66] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *Journal of Field Robotics*, vol. 31, no. 4, pp. 617–636, 2014. Available: https://onlinelibrary-wiley-com.libproxy.nps.edu/doi/abs/10.1002/rob.21513

[67] Boeing. (2015, Aug.). Silent Strike: Boeing's Compact Laser Weapons System tracks and disables UAVs. *Boeing Features & Multimedia: Defense*. [Online]. Available: https://www.boeing.com/features/2015/08/bds-compact-laser-08-15.page

[68] J. R. Hoehn and K. M. Sayler, "Department of Defense Counter-Unmanned Aircraft Systems," Congressional Research Service, Washington D.C., Congressional Report IF11426, June 2021. Available: https://sgp.fas.org/crs/weapons/IF11426.pdf

[69] T. Weise, M. Jung, D. Langhans, and M. Gowin, "Overview of directed energy weapon developments," in *2004 12th Symposium on Electromagnetic Launch Technology*, 2004, pp. 483–489.

[70] A. Calingo. (2019, June). Marine Corps at the forefront for ground-based lasers. *Marines.mil*. [Online]. Available: https://www.marines.mil/News/News-Display/Article/1880583/marine-corps-at-the-forefront-for-ground-based-lasers/

[71] A. V. Gomozov, D. V. Gretskih, V. A. Katrich, and M. V. Nesterenko, "Functional neutralization of small-size UAVs by focused electromagnetic radiation," in *2017 XXIInd International Seminar/Workshop on Direct and Inverse Problems of Electromagnetic and Acoustic Wave Theory (DIPED)*, 2017, pp. 187–189.

[72] A. Paleja. (2021, Oct.). General Dynamics' Stryker Will Counter Drone Swarms With a Microwave Weapon. *Interesting Engineering*. [Online]. Available: https://interestingengineering.com/general-dynamics-stryker-will-counter-drone-swarms-with-a-microwave-weapon

[73] M. Goodrich. (2016, Jan.). Drone Catcher: "Robotic Falcon" can Capture, Retrieve Renegade Drones. *Michigan Technological University*. [Online]. Available: https://www.mtu.edu/news/2016/01/drone-catcher-robotic-falcon-can-capture-retrieve-renegade-drones.html

[74] C. McGraw. Skydio Capability Statement Datasheet. [Online]. Available: https://pages.skydio.com/rs/784-TUF-591/images/capability-statement-datasheet-defense-pg.pdf

[75] S. H. Brooks, C. Jacobus, C. G. Kohestani, J. A. Stikar, and E. J. Faye, "Counter unmanned aircraft systems market survey (uur)," Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), Tech. Rep., 2019.

[76] Anduril - Anvil. [Online]. Available: https://www.anduril.com/hardware/anvil/

[77] Data Sheet - DroneDefender Counter-UAS Device. [Online]. Available: https://gdmissionsystems.com/-/media/General-Dynamics/Ground-Systems/PDF/Counter-UAS---Dedrone/DroneDefender-DataSheet.ashx?la=en&hash=516300C425D3CDA5C69CBAD29C1886EEFD9EA54A

[78] R. Poisel, *Introduction to Communication Electronic Warfare Systems*, 2nd ed. Norwood, MA: Artech House, Inc., 2008. Available: http://pws.npru.ac.th/sartthong/data/files/Introduction%20to%20Communication%20Electronic%20Warfare%20Systems.pdf

[79] T. Ulversoy, "Software defined radio: Challenges and opportunities," *IEEE Communications Surveys Tutorials*, vol. 12, no. 4, pp. 531–550, 2010.

[80] T. E. Smith, "EO3602 Antennas and Electromagnetic Propagation - Link Analysis," Feb. 2021.

[81] P. Martinelli, E. Cianca, M. De Sanctis, L. Di Paolo, A. Pisano, and L. Simone, "Robustness of satellite telecommand links to jamming attacks," in *2012 IEEE First AESS European Conference on Satellite Telecommunications (ESTEL)*, 2012, pp. 1–6.

[82] B. Kaplan, I. Kahraman, A. Görçin, H. A. Çırpan, and A. R. Ekti, "Measurement based fhss–type drone controller detection at 2.4ghz: An stft approach," in *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, 2020, pp. 1–6.

[83] "IEEE Standard for Information Technology - Telecommunications and information exchange between systems - local and metropolitan networks - specific requirements - part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher Speed Physical Layer (PHY) Extension in the 2.4 GHz band," pp. 1–96, 2000.

[84] L. Segers, J. Tiete, A. Braeken, and A. Touhafi, "Ultrasonic multiple-access ranging system using spread spectrum and mems technology for indoor localization," *Sensors (Basel, Switzerland)*, vol. 14, pp. 3172–3187, 02 2014.

[85] C. Johnston, "Technical challenges for small UAV payloads," *Electronic Military and Defense. Accessed May*, vol. 24, p. 2016, 2012.

[86] M. Song and T. Allison, "Frequency hopping pattern recognition algorithms for wireless sensor networks," in *PDCS*, 2005.

[87] P. Olson, *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency*. New York: Little, Brown, 2012. Available: https://books.google.com/books?id=ncGVPtoZPHcC

[88] I. Kara and M. Aydos, "The rise of ransomware: Forensic analysis for windows based ransomware attacks," *Expert Systems with Applications*, vol. 190, p. 116198, Mar. 2022. Available: https://linkinghub.elsevier.com/retrieve/pii/S0957417421015141

[89] M. M. Alani, "OSI Model," in *Guide to OSI and TCP/IP Models*. Cham: Springer International Publishing, 2014, pp. 5–17. Available: https://doi.org/10.1007/978-3-319-05152-9_2

[90] J. West, J. Andrews, and T. Dean, *Network+ Guide to Networks*, 8th ed. Boston, MA: Cengage Learning, 2019.

[91] J. Postel, "RFC: 793 - Transmission Control Protocol," *DARPA Internet Program Protocol Specification*, Sep. 1981. Available: https://www.hjp.at/doc/rfc/rfc793.html

[92] What is User Datagram Protocol (UDP/IP)? (2022). *Cloudflare, Inc.* [Online]. Available: https://www.cloudflare.com/learning/ddos/glossary/user-datagram-protocol-udp/

[93] OUI/MA-L Database. (2021, Nov.). [Online]. Available: http://standards-oui.ieee.org/oui/oui.txt

[94] T. S. Rappaport, *Wireless communications : principles and practice*, 2nd ed. (Prentice Hall communications engineering and emerging technologies series). Upper Saddle River, N.J: Prentice Hall PTR, 2002.

[95] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," *IEEE Communications Surveys Tutorials*, vol. 18, no. 3, pp. 2027–2051, 2016.

[96] Common Attack Pattern Enumeration and Classification (CAPEC), "CAPEC-94: Adversary in the Middle (AiTM)," The MITRE Corporation, CAPEC Report CAPEC-94, Oct. 2021. Available: https://capec.mitre.org/data/definitions/94.html

[97] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art," *Computer Networks*, vol. 44, no. 5, pp. 643–666, 2004. Available: https://www.sciencedirect.com/science/article/pii/S1389128603004250

[98] J. Mirkovic and P. Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," *SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 2, p. 39–53, apr 2004. Available: https://doi.org/10.1145/997150.997156

[99] What is a distributed denial-of-service (DDoS) attack? (2022). *Cloudflare, Inc.* [Online]. Available: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

[100] C. Division, "CA-1996-01: UDP Port Denial-of-Service Attack," Carnegie Mellon University Software Engineering Institute, Pittsburgh, PA, CERT Advisory REV-03.18.2016.0, Sep. 1997. Available: https://resources.sei.cmu.edu/asset_files/WhitePaper/1996_019_001_496172.pdf#page=123

[101] C. Division, "CA-1996-21: TCP SYN Flooding and IP Spoofing Attacks," Carnegie Mellon University Software Engineering Institute, Pittsburgh, PA, CERT Advisory REV-03.18.2016.0, Nov. 2000. Available: https://resources.sei.cmu.edu/asset_files/WhitePaper/1996_019_001_496172.pdf#page=123

[102] J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," in *12th USENIX Security Symposium*. Washington D.C.: USENIX Association, May 2003. Available: https://www.usenix.org/legacy/events/sec03/tech/full_papers/bellardo/bellardo_html/

[103] Aircrack-ng. [Online]. Available: https://www.aircrack-ng.org/

[104] ISO, "Information technology - security techniques - entity authentication - part 2: Mechanisms using symmetric encipherment algorithms," International Organization for Standardization, Geneva, Switzerland, ISO ISO/IEC 9798-2:2008, 2008. Available: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/05/50522.html

[105] B. J. Hale and C. A. Boyd, *Computationally Analyzing the ISO 9798-2.4 Authentication Protocol*. Springer Publishing Company.

[106] Common Attack Pattern Enumeration and Classification (CAPEC), "CAPEC-90: Reflection Attack in Authentication Protocol," The MITRE Corporation, CAPEC Report CAPEC-90, Oct. 2021. Available: https://capec.mitre.org/data/definitions/90.html

[107] CNSS Secretariat, "Committee on National Security Systems (CNSS) Glossary," National Security Agency, Fort Meade, MD, Tech. Rep. 4009, Apr. 2015. Available: https://www.cnss.gov/CNSS/openDoc.cfm?Ge7MJmksKl21+Kh3E6YwGw==

[108] S. Blake-Wilson, D. Johnson, and A. Menezes, "Key agreement protocols and their security analysis," in *Lecture notes in computer science*. New York NY: Springer-Verlag, 1997, pp. 30–45.

[109] C. Hlauschek, M. Gruber, F. Fankhauser, and C. Schanes, "Prying open pandora's box: KCI attacks against TLS," in *9th USENIX Workshop on Offensive Technologies (WOOT 15)*. Washington, D.C.: USENIX Association, Aug. 2015. Available: https://www.usenix.org/conference/woot15/workshop-program/presentation/hlauschek

[110] E. Bout, V. Loscri, and A. Gallais, "Energy and distance evaluation for jamming attacks in wireless networks," in *2020 IEEE/ACM 24th International Symposium on Distributed Simulation and Real Time Applications (DS-RT)*, 2020, pp. 1–5.

[111] S. LaGrone. (2019, July). Marines Took Out Iranian Drone for the Cost of a Tank of Gas. *USNI News*. [Online]. Available: https://news.usni.org/2019/07/19/marines-took-out-iranian-drone-for-the-cost-of-a-tank-of-gas. Section: Budget Industry.

[112] N. Franks, *Dog Fight: Aerial Tactics of the Aces of World War I*. London: Greenhill Books, 2003.

[113] C. H. Heller. (2019, Feb.). The Impact of Insignificance: Naval Developments from the Yom Kippur War. *CIMSEC - History*. [Online]. Available: https://cimsec.org/the-impact-of-insignificance-naval-developments-from-the-yom-kippur-war/

[114] Missile Defense Project. (2017, Sep.). Harpoon. *Missile Threat, Center for Strategic and International Studies*. [Online]. Available: https://missilethreat.csis.org/missile/harpoon/

[115] M. W. Browne, "Invention That Shaped the Gulf War: the Laser-Guided Bomb," *The New York Times*, Feb. 1991. Available: https://www.nytimes.com/1991/02/26/science/invention-that-shaped-the-gulf-war-the-laser-guided-bomb.html

[116] R. L. Shaw, *Fighter Combat: Tactics and Maneuvering*, 5th ed. Annapolis, MD: Naval Institute Press, 1987.

[117] U. M. Corps, "Marine Corps Warfighting Publication 3-01: Offensive and Defensive Tactics," Sep. 2019.

[118] U. M. Corps, "Marine Corps Warfighting Publication 3-1: Ground Combat Operations," Nov. 2002.

[119] "Multi-Service Tactics, Techniques, and Procedures for Air and Missile Defense," Mar. 2019. Available: https://armypubs.army.mil/epubs/DR_pubs/DR_d/ARN15491-ATP_3-01.15-000-WEB-1.pdf

[120] U. M. Corps, "Marine Corps Warfighting Publication 3-11.3: Scouting and Patrolling," Apr. 2000.

[121] M. R. Manesh and N. Kaabouch, “Cyber Attacks on Unmanned Aerial System Networks: Detection, Countermeasure, and Future Research Directions,” *Computers & Security*, vol. 85, 2019.

[122] N. Franks, *Dog Fight: Aerial Tactics of the Aces of World War I*. London: Greenhill Books, 2003.

[123] U.S. Marine Corps. (1996, Sep.). MCWP 3-15.1 Machine Guns and Machine Gun Gunnery. [Online]. Available: https://www.marines.mil/Portals/1/MCWP%203-15.1.pdf

[124] Missile Defense Advocacy Alliance. (2020, July). Marine Air Defense Integrated System (MADIS) – Missile Defense Advocacy Alliance. *Missile Defense Advocacy Alliance: U.S. - Air Defense, Intercept*. [Online]. Available: https://missiledefenseadvocacy.org/defense-systems/marine-air-defense-integrated-system-madis/

[125] Intel. (2021). Intel Drone Light Show Premium Fact Sheet. [Online]. Available: https://inteldronelightshows.com/wp-content/uploads/sites/3/2021/01/Intel-Drone-Light-Show-Premium-Fact-Sheet-23112020.pdf

[126] BaykarTech. (2021, Nov.). Bayraktar TB2 successfully completes 400 thousand flight hours. *Baykar Defence*. [Online]. Available: https://www.baykartech.com/en/press/bayraktar-tb2-400-thousand-hours/

[127] Parrot, Inc. (2013). AR.Drone2.0 User Guide. [Online]. Available: https://www.parrot.com/assets/s3fs-public/2021-09/ar.drone2_user-guide_uk.pdf

[128] Parrot, Inc. (2016). Parrot Bebop Drone User Guide. [Online]. Available: https://www.parrot.com/assets/s3fs-public/2021-09/bebop-drone_user-guide_uk_v.3.4.pdf

[129] Skydio, Inc. (2022). Skydio 2+. [Online]. Available: https://www.skydio.com/skydio-2-plus

[130] Raspberry Pi Trading Ltd. (2021, Jan.). Raspberry Pi 4 Computer Model B. [Online]. Available: https://datasheets.raspberrypi.com/rpi4/raspberry-pi-4-product-brief.pdf

[131] W. Harrington, *Learning Raspbian*. Packt Publishing Ltd, 2015.

[132] Micro Center. (2022). Raspberry Pi Sense HAT. *Micro Center: Computers & Electronics*. [Online]. Available: https://www.microcenter.com/product/453920/raspberry-pi-sense-hat

[133] ALFA AWUS Product List. *ALFA Network Inc.* [Online]. Available: https://www.alfa.com.tw/search?q=awus*&type=product

[134] "UM25/UM25C Instructions for USB Tester with Full Colour Display," Sep. 2019.

[135] V. Dobrokhodov, K. Jones, C. Dillard, and I. Kaminer, "Aqua-Quad - solar powered, long endurance, hybrid mobile vehicle for persistent surface and underwater reconnaissance, part II - onboard intelligence," in *OCEANS 2016 MTS/IEEE Monterey*, 2016, pp. 1–9.

[136] E. Rumer, R. Sokolsky, and P. Stronski. (2021, Mar.). Russia in the Arctic—A Critical Examination. [Online]. Available: https://carnegieendowment.org/2021/03/29/russia-in-arctic-critical-examination-pub-84181

[137] M. Vollmer and K.-P. Mollmann, *Infrared Thermal Imaging*, 2nd ed. Weinheim, Germany: John Wiley & Sons, Ltd, 2017. Available: http://onlinelibrary.wiley.com/doi/10.1002/9783527693306

[138] Fixed-Mount Thermal Camera for Skin Temperature Screening: FLIR A320 Tempscreen. (2020, Apr.). [Online]. Available: https://www.flir.com/products/flir-a320/

[139] Persistent Systems, LLC. (2021). MPU5, WR-5100 Specification Sheet. *PersistentSystems*. [Online]. Available: https://www.persistentsystems.com/site/wp-content/themes/persistensystems/pdf/mpu5/mpu5_spec_sheet.pdf

[140] NVIDIA Jetson TX2: High Performance AI at the Edge. (2022). *NVIDIA*. [Online]. Available: https://www.nvidia.com/en-us/autonomous-machines/embedded-systems/jetson-tx2/

THIS PAGE INTENTIONALLY LEFT BLANK

Initial Distribution List

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California