2022-09

A SYSTEMS ANALYSIS OF ENERGY USAGE AND EFFECTIVENESS OF A COUNTER-UNMANNED AERIAL SYSTEM USING A CYBER-ATTACK APPROACH

Lee, Chee Hoe

Monterey, CA; Naval Postgraduate School

http://hdl.handle.net/10945/71104

NAVAL
POSTGRADUATE
SCHOOL

MONTEREY, CALIFORNIA

THESIS

A SYSTEMS ANALYSIS OF ENERGY USAGE AND EFFECTIVENESS OF A COUNTER-UNMANNED AERIAL SYSTEM USING A CYBER-ATTACK APPROACH

by

Chee Hoe Lee

September 2022

Thesis Advisor:	Douglas L. Van Bossuyt
Co-Advisor:	Britta Hale

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

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

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

4. TITLE AND SUBTITLE A SYSTEMS ANALYSIS OF ENERGY USAGE AND EFFECTIVENESS OF A COUNTER-UNMANNED AERIAL SYSTEM USING A CYBER-ATTACK APPROACH	**5. FUNDING NUMBERS**
6. AUTHOR(S) Chee Hoe Lee	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

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

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

13. ABSTRACT (maximum 200 words)

Existing counter-unmanned aerial systems (C-UAS) rely heavily on radio frequency (RF) jamming techniques that require a large amount of energy. RF jamming results in undesirable consequences such as jamming nearby friendly devices as well as increasing the RF footprint of local operators. Current cybersecurity analysis of commercial-off-the shelf (COTS) UASs have revealed vulnerabilities that can be used to conduct C-UAS operations in the cyber domain via cyber-attacks that hijack device-specific communication links on narrow RF bands. This thesis validates the cyber-attack C-UAS (CyC-UAS) concept through reviewing recent C-UAS operational experimental scenarios and conducting analysis on the collected data. Then, a model of a defense facility is constructed to analyze and validate specific mission scenarios and several proposed concepts of operation. A comparison of the energy requirements between CyC-UAS and existing C-UAS techniques is performed to assess energy efficiency and trade-offs of different C-UAS approaches. The comparison of energy requirements between the CyC-UAS prototype and existing C-UAS RF jamming products shows CyC-UAS has significant energy savings while not affecting other telecommunication devices operating at the same frequencies. CyC-UAS is able to achieve the same mission by consuming much less energy and shows promise as a new, lower energy, and lower collateral damage approach to defending against UASs.

14. SUBJECT TERMS unmanned aerial system, counter-unmanned aerial system, cyber-attack, UAS, C-UAS	**15. NUMBER OF PAGES** 75
	16. PRICE CODE

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

THIS PAGE INTENTIONALLY LEFT BLANK

A SYSTEMS ANALYSIS OF ENERGY USAGE AND EFFECTIVENESS OF A COUNTER-UNMANNED AERIAL SYSTEM USING A CYBER-ATTACK APPROACH

Chee Hoe Lee
Major, Republic of Singapore Air Force
BE, Nanyang Technological University, 2012

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 2022

Approved by: Douglas L. Van Bossuyt
Advisor

Britta Hale
Co-Advisor

Oleg A. Yakimenko
Chair, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Existing counter-unmanned aerial systems (C-UAS) rely heavily on radio frequency (RF) jamming techniques that require a large amount of energy. RF jamming results in undesirable consequences such as jamming nearby friendly devices as well as increasing the RF footprint of local operators. Current cybersecurity analysis of commercial-off-the shelf (COTS) UASs have revealed vulnerabilities that can be used to conduct C-UAS operations in the cyber domain via cyber-attacks that hijack device-specific communication links on narrow RF bands. This thesis validates the cyber-attack C-UAS (CyC-UAS) concept through reviewing recent C-UAS operational experimental scenarios and conducting analysis on the collected data. Then, a model of a defense facility is constructed to analyze and validate specific mission scenarios and several proposed concepts of operation. A comparison of the energy requirements between CyC-UAS and existing C-UAS techniques is performed to assess energy efficiency and trade-offs of different C-UAS approaches. The comparison of energy requirements between the CyC-UAS prototype and existing C-UAS RF jamming products shows CyC-UAS has significant energy savings while not affecting other telecommunication devices operating at the same frequencies. CyC-UAS is able to achieve the same mission by consuming much less energy and shows promise as a new, lower energy, and lower collateral damage approach to defending against UASs.

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

THIS PAGE INTENTIONALLY LEFT BLANK

List of Figures

THIS PAGE INTENTIONALLY LEFT BLANK

List of Tables

THIS PAGE INTENTIONALLY LEFT BLANK

List of Acronyms and Abbreviations

AO	Area of Operation
C-UAS	Counter-Unmanned Aerial System
CyC-UAS	C-UAS Cyber-Attack Technique
CONOPS	Concept of Operations
COTS	commercial-off-the-shelf
C2	Command and Control
DoD	Department of Defense
DoS	Denial-Of-Service
EMP	Directional Electromagnetic Pulse
EO/IR	Electro-Optical and Infrared
FHSS	Frequency-Hopping-Spread Spectrum
GCS	Ground-Control-Station
GNSS	Global Navigation Satellite System
ISIS	Islamic State
LAN	Local Area Network
MAC	Media Access Control
MGTOW	Max Gross Take-Off Weight
OSI	Open Systems Interconnection Radio-
RCS	Cross-Section

RF	Radio Frequency
TCP	Transmission Control Protocol
TTPs	Tactics, Techniques and Procedures
UAS	Unmanned Aerial System
UDP	User Datagram Protocol
WiFi	Wireless Fidelity

Executive Summary

The intent of the thesis is to verify the concept of the application of cyber-attacks in the counter-unmanned aerial system (C-UAS) domain. The conduct of the literature reviews to understand the existing development on C-UAS Cyber-Attack Technique (CyC-UAS) suggested that commercial UAS that operates in the Wireless Fidelity (WiFi) frequency band (2.4 GHz and 5GHz) is extremely vulnerable to C-UAS attacks, since the operating frequency is known. In the context of CyC-UAS, the cyberattack scheme attempts to manipulate or tamper the information flowing within the OSI model with the intent to deny the use of communication network. The Denial of Service (DoS) technique that aims to suspend or to interrupt the use of a communication network was accomplished by "flooding" the communication network with data packets such that the network became 'overwhelmed.'

One of the DoS techniques, the "Deauthentication Attack" method that made used of the knowledge of the MAC address to perform C-UAS operation over the wireless network was intensively discussed in this thesis. This includes the construct of a CyC-UAS prototype that comprises a micro-controller (with transceiver integrated within) and a WiFi antenna to carry a set of experiments to validate the effectiveness of the "Deauthentication Attack" technique applied on commercial drones that operates in the 2.4GHz and 5GHz WiFi frequency bands. The results of the experiments revealed the (1) physical behavior of the adversary drone upon a successful C-UAS attack, (2) the range limitations of the CyC-UAS as well as (3) the transmission power and energy requirement for the CyC-UAS. This information was essential for the development of the CyC-UAS simulation model.

Given the system description and physical behavior of the CyC-UAS, two feasible Concept of Operations (CONOP) schemes namely, "Defensive deployment" and "Aggressive deployment" were proposed and elaborated for discussion. In the "Defensive deployment" schemes, the function of the CyC-UAS is to defense against provocative adversary drone of a stationary or a mobile infrastructure. In the "Aggressive deployment" schemes, the CyC-UAS achieved the ability to maneuver in order so as to take on the aggressive role in the attempt to seek and mitigate potential adversary drone.

A simulation model to mimic the proposed CONOPS on "Defensive deployment" of the

CyC-UAS was made. The simulation model was model upon the information attained from the experiments and the physical responses gathered based on the "Deauthentication" cyber-attack technique. To simulate the responsiveness of the CyC-UAS based on a SWARM attack, the group of adversary drones would be represented by a salvo in the simulation. The result from the simulation runs provides an estimation of the performance and the power and energy requirements for the CyC-UAS.

Energy efficiency analysis of the CyC-UAS was achieved through the comparison of energy consumption between CyC-UAS and other popular existing C-UAS technique such as the RF jamming method. From the comparison between the CyC-UAS prototype and the EAGLE108 shows that CyC-UAS achieve significant energy saving as compared to conventional RF jamming method.

Acknowledgments

The completion of the thesis would not have been possible without the strong support and assistance rendered by the following individuals. First and foremost, I would like to thank my thesis advisor, Dr. Douglas Van Bossuyt, who had dedicated his precious time in providing me with guidance weekly to ensure that my work meets the intent of the thesis's objectives. To my co-advisor, Dr. Britta Hale, I would like to thank her for providing me with useful suggestions to enhance my thesis proposal.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 1: Introduction

The use of Unmanned Aerial Systems (UASs) has proliferated rapidly across the military and commercial domains. The ease of access to small Commercial-Off-The Shelf (COTS) UAS through the commercial market has given malicious entities (such as terrorist groups) the ability to use UAS to conduct malicious activities. This includes the use of UAS to gain unauthorized access into military installations to conduct malicious activities such as spying, to sabotage specific High-Value-Targets, or to cause physical harm to soldiers deployed within the vicinity. To guard against unauthorized UAS intrusion, several Counter-Unmanned Aerial System (C-UAS) techniques have been developed and deployed.

Currently, the Department of Defense (DoD) utilizes C-UAS mechanisms such as Radio Frequency (RF) jamming, laser, or device destruction methods against adversarial UAS. RF jamming via energy bursts and laser mechanisms requires enormous amounts of energy, which necessarily affects usage for expeditionary forces or in energy constrained environments. Furthermore, undesirable consequences such as jamming of nearby friendly devices, increased RF footprint for local operators, and unintentional loss or destruction of the adversarial UAS may occur. This paradigm contradicts well-established Tactics, Techniques and Procedures (TTPs) for defense of DoD's installations and bases.

In contrast, cyber security analyses of low cost UAS have pointed to many vulnerabilities ripe for exploitation that would provide a C-UAS with both energy improvements and scalpel-edge accuracy in defense mechanisms, such as through cyber-attack hijacking the adversarial UAS or forms of jamming that utilize the device-specific communication link frequency instead of broad-spectrum RF energy bursts and therefore have highly controlled effects on the adversarial UAS.

This thesis aims to validate the concept of C-UAS Cyber-Attack Technique (CyC-UAS) for the conduct of C-UAS operation. This includes (1) an investigation of the effectiveness and efficiency of using CyC-UAS on commercial drones as well as (2) developing an understanding of the energy requirements during CyC-UAS operations. This thesis provides DoD with justification to continue with the research and development effort to maximize the potential of CyC-UAS so as to reduce the reliance on other conventional C-UAS techniques that have high energy requirements.

The research in this thesis encompasses five phases. Phase One surveys existing literature to identify threats that arise from the use of UAS. In Phase Two, a literature review is conducted on existing available C-UASs to determine its (1) Concept of Operations (CONOPS), (2) Capabilities and limitations, and (3) Specifications. In Phase Three, a literature review is conducted on the current development of C-UAS with the use of cyber-attack techniques with specific focus on energy consumption and effectiveness. The results attained from recent CyC-UAS experiments are also be reviewed to capture the physical behavior of the system during attack. In Phase Four, a simulation model of a defense facility is constructed to help analyze and validate specific mission scenarios of interest and the proposed concept. In the final phase (Phase Five), comparison of the energy requirements between CyC-UAS and existing C-UAS techniques are performed to assess the energy efficiency of CyC-UAS. Lastly, this thesis concludes with a discussion of the results and broad conclusions, recommendations, and future work.

This thesis adopts the “manuscript option” and has the following structure: Chapter 1 provides broad context and objective of the thesis; Chapter 2 presents a journal manuscript submitted to MDPI *Drones* for peer review; and Chapter 3 provides a summary of the research and the recommended future work that is of interest of the thesis topic.

CHAPTER 2:
Manuscript Submission

2.1 A Systems Analysis of Energy Usage and Effectiveness of a Counter-Unmanned Aerial System Using a Cyber-Attack Approach

A version of this chapter was submitted in June 2022 to the MDPI journal *Drones* as: C.H. Lee, C. Thiessen, D. L. Van Bossuyt, and B Hale, “A Systems Analysis of Energy Usage and Effectiveness of a Counter-Unmanned Aerial System Using a Cyber-Attack Approach.” The submission has been accepted and published by MDPI journal *Drones* in August 2022.

2.2 Introduction

Current Counter-Unmanned Aerial Systems (C-UAS) used against smaller Unmanned Aerial Systems (UAS) rely largely on radio frequency (RF) jamming and Denial-Of-Service (DoS) against adversarial UAS [1]. C-UAS used on installations, for example, realize this via RF jamming or communication link jamming. However, this paradigm not only contradicts well-established Tactics, Techniques and Procedures (TTPs) for defense of installations and bases, but also under-utilizes potential cyber-attack C-UAS (CyC-UAS) measures [2], [3].

In addition, current UAS defense mechanisms rely heavily on DoS (either jamming, laser, or device destruction) [4]. RF Jamming via energy bursts and laser mechanisms requires enormous amounts of energy, which necessarily affects usage for expeditionary forces or in energy constrained environments [5]. Furthermore, undesirable consequences such as jamming of nearby friendly devices, increased RF footprint for local operators, and unintentional loss/destruction of the adversary UAS may occur [6], [7].

In contrast, cybersecurity analysis of low cost UAS have pointed to many vulnerabilities ripe for exploitation that would provide a C-UAS with both energy improvements and scalpel-edge accuracy in defense mechanisms, such as through cyber-attack hijacking the adversary UAS or forms of jamming that utilize the device-specific communication link frequency band instead of broad-spectrum RF energy bursts and therefore have highly controlled effects [2], [8], [9].

In recent studies, the application of cyber-attacks in the C-UAS domain have indicated both energy improvements and scalpel-edge accuracy in defense mechanisms [10], such as through cyber-attacks to hijack adversary UAS, or in the form of jamming that utilize device-specific communication link frequencies instead of broad band jamming and therefore achieve highly controlled effects on the malign device [2].

Techniques used to employ existing C-UAS by the military, state governments, federal agencies, and private companies consume high levels of energy during operation. Certain C-UAS techniques such as frequency jamming may not always be suitable in an environment where operating machines utilize RF transmission for communication such as a military airbase, a major sporting event, or anywhere in a crowded urban area [11]. The US Navy, Department of Defense (DoD), civilian airports, sporting venues, wildland firefighters, and other facilities and users that may be targets of adversarial UAS may benefit from the research presented in this paper.

This paper performs comparisons of the energy consumption of existing C-UAS versus a proposed CyC-UAS. Further, this research analyzes the effectiveness of CyC-UAS versus existing C-UAS approaches. Through the attainment of energy readings extracted from the conduct of physical experiments with a CyC-UAS prototype [10], as well as the comparison of energy consumption between existing C-UAS method and CyC-UAS, the results indicate that CyC-UAS can significantly reduce C-UAS energy consumption and can serve as a useful portion of a broader C-UAS defense strategy for many types of installations and expeditionary situations.

The remainder of this paper contains the following: Section 2 surveys existing literature to identify threats that arise from the use of UAS to motivate the need for C-UAS. Section 3 presents a literature review of existing available C-UAS to determine (1) Concept of

Operations (CONOPS), (2) capabilities and limitation and (3) specifications. Section 4 presents a literature review and study of current developments of CyC-UAS with specific focus on energy consumption and effectiveness, and reviews a recent CyC-UAS experiment. Then, an analysis of data collected in several experimental scenarios for the conduct of CyC-UAS operations where data on the physical behavior of the CyC-UAS system and adversarial UAS are documented. In Section 5, a simulation model of a defense facility is constructed to analyze and validate specific mission scenarios of interest and proposed CyC-UAS CONOPS. In Section 6, comparison of the energy requirements between CyC-UAS and existing C-UAS technique are performed to assess the energy efficiency of CyC-UAS. Finally, the paper concludes in Section 7 with a discussion of the results and broad conclusions, recommendations, and future work.

2.3 UAS Threat Analysis and Vulnerability Assessment

The use of UAS in the military domain has produced enormous advantages and benefits in military operations [12]. Such military operations include electronic warfare attacks, precision strikes, intelligence, surveillance, and reconnaissance (ISR) missions, and resupply missions [13], [14]. The effectiveness of UAS was proven and validated during military operations such as Operation Iraqi Freedom and Operation Enduring Freedom [15], [16], and more recently, the military conflict between Ukraine and Russia [17]. In the commercial domain, the use of UAS to fulfill recreational or leisure purposes such as imaging and video capturing for social events has further expanded into businesses across different industries. Businesses have integrated the use of UAS to transform daily tasks [18]. For example, some insurance companies have adopted UAS to perform inspection of damaged assets for claims, and in the farming industry farmers use UAS to monitor crops in the field to achieve labor savings [19], [20]. The commercial sector within the United States has been investing heavily in UAS development over the years, due in part to the positive economic growth in UAS-related patents. A study conducted by Mckinsey & Company suggests that by 2026, the usage and investment in UAS in the commercial sector will reap a profit between US$31 billion and US$46 billion [21]. The upward trends suggested that the utility of UAS will continue to gain popularity among consumers and that the use of UAS for industrial and defense applications will continue to expand and grow.

2.3.1 Malicious Use of UAS

On the other hand, with the ease of access to small Commercial Off-The-Shelf (COTS) UAS through the commercial market, organized crime and terrorist groups have started to adopt UAS to conduct malicious activities [22]. These activities include the illegal intrusion of UAS into restricted infrastructure such as the civil airport facilities with the intent of disrupting the services and operations. For example, the Gatwick Airport situated in London largely stopped flight operations between 19 and 21 December 2018 due to a deliberate UAS attack that affected about 140,000 passengers, with about 1,000 flights diverted or cancelled [23]. Terrorist groups such as the Islamic State (ISIS) were found to be using weaponized UAS on the battlefield in Iraq and elsewhere [24]. Many of the UAS that ISIS and other terror organizations have employed are weaponized COTS UAS where explosives or munitions have been attached to an otherwise consumer-grade UAS [25]. These malicious attacks coupled with the rapid growth of UAS in the commercial and military domains pose significant challenges and concerns to safety and security within the civil and military domains [26].

2.3.2 Classification of UAS

Different classes of UAS are grouped based on the designed "Max Gross Take-Off Weight (MGTOW)", "Maximum Operating Altitude", and "Top Speed" as shown in Table 2.1. Typical COTS UAS that are readily available for procurement in the commercial market are relatively smaller in size and lighter in weight, and often falls under the Group 1 category.

Table 2.1. UAS Groupings Based on Weight, Operating Altitude, and Top Speed. Source: [27]

UAS Group	Weight Range (lbs.) MGTOW	Nominal Operating Altitude	Speed (knots)	Representation UAS
Group 1	0-20	<1200 Above Ground Level (AGL)	100	Raven (RQ-11), WASP DJI Phantom, Solo, Typhoon H, Ghostdrone 2.0
Group 2	21-55	<3500 AGL	<250	ScanEagle
Group 3	<1320	<Flight Level (FL) 180	<250	Shadow (RQ-7B) Tier II/STUAS
Group 4	>1320	<Flight Level (FL) 180	Any	Fire Scout (MQ-8B, RQ-8B), Predator (MQ-1A/B), Sky Warrior ERMP (MQ-1C)
Group 5	>1320	>FL 180	Any	Reaper (MQ-9A), Global Hawk (RQ-4), BAMS (RQ-4N)

2.3.3 Existing UAS Capabilities – Payload-Enabled

A typical UAS is equipped with a camera to enable a UAS operator with situational awareness of the UAS's surroundings and environment [28]. Depending on the payload weight limit (determined in part by the MGTOW) of the UAS, the UAS can carry a payload to meet a desired operational outcome. The different types of payload configurations can be classified into three distinct classifications, namely (1) non-sensing, (2) sensing, and (3) counter measure payload [29]. For (1) with adversarial UASs, these payloads can comprise homemade explosives, biological, and radiological weapons (e.g., Chemical, Biological, Radiological and Explosives (CBRE)). For (2), these type of payloads enable live video feeds for the purpose of surveillance and intelligence gathering or precision strikes on a specific target. Lastly on (3), these types of payloads enable the disruption of telecommunication devices through RF jamming and similar. The list of payload-enabled capabilities is summarized in Table 2.2. While the development of payload capabilities is usually developed based on good intentions and for legitimate uses, malicious entities may utilize these capabilities to conduct malicious UAS activities against the public.

Table 2.2. Types of UAS Payload-Enabled Capabilities. Source: [29]

Type	Capabilities
Non-Sensing Payload	
Payload Release	The payload is carried to a certain altitude and is released upon hovering above the target.
Kamikaze	Both the payload and UAS crash into the target.
Sensing Payload	
Electro-Optic	Imagery and video recording functions to support ISR operations.
Light Detection and Ranging	The pulsing of a laser that enables distance measurements.
Countermeasure Payload	
RF Jammer	The payload overloads sensor and RF control inputs which causes disruption to operations.
Spoofers	The spoofing capability payload disrupts navigational or command and control receiver systems, such as those that rely on Global Navigation Satellite System (GNSS), for instance.

2.3.4 Emerging UAS Threats – Swarm Capabilities

The concept of a swarm in the context of UAS operations comprises a group of UAS working as a system, collaborating, and communicating with each other to achieve the desired mission objective [30]. In addition, swarm technology adopts an automation architecture to achieve self-maneuvers so as to assist the UAS operator in controlling multiple UAS to achieve a common goal [31]. The integration of micro-UAS coupled with the concept of a swarm poses challenges to existing C-UAS measures [32]. This is due to the small Radio-Cross-Section (RCS) of micro-UAS where detection at large distances with existing radar would be challenging [32]. While the concept of swarms for UAS is still in the testing and development phase [33], it is essential to assess the effectiveness of existing C-UAS techniques and emerging C-UAS technique such as the CyC-UAS concept in anticipation of the emerging threats posed by a swarm of UAS.

One of the main threats to installations today is small COTS UAS (Groups 1 and 2), as these UAS are often easily accessible in the commercial market, inexpensive, and are difficult to detect and neutralized [34]. A near future threat is swarms of COTS UAS used to target strategic and critical infrastructure.

The threats impose by UAS were defined and discussed in this section. To gain insight on the impact on the threats, various capabilities were also discussed.

2.4 Literature Review of Existing C-UAS Techniques

As discussed in Section 2, the infiltration of adversary UAS into restricted areas to perform malicious activities may cause severe consequences or threaten the interests of a facility. For this reason, it is critical to develop effective methods to deter any potential intrusion into restricted areas by adversarial UAS. Since the early 2000s, the need for C-UAS capabilities has been defined and developed through the adoption of engineering techniques to derive feasible solutions. This section seeks to (1) introduce the C-UAS processing chain (also known as the kill-chain) operating in a defined area, (2) provide a broad overview of the main existing C-UAS techniques and their capability trade-offs, and (3) introduce the need for a Command and Control (C2) system within C-UAS networks to enhance C-UAS operation.

2.4.1 C-UAS Processing Chain and Techniques

The C-UAS processing chain encompasses the following phases as shown in Figure 2.1. These phases include the need to ‘Detect’, ‘Locate/Track’, ‘classify/identify’ and then to ‘Mitigate’ [29], [35]. At the initial phase, the C-UAS must be capable of performing detection and provide the location of the adversary UAS. While the location of the UAS is being ‘tracked’, the C-UAS attempts to identify and classify the unknown UAS such that ‘Mitigation’ actions could be taken against the adversary UAS. These mitigating actions may include the use of ‘Kinetic’ and/or ‘Non-Kinetic’ techniques to prevent the adversary UAS from performing any malicious activities within the protected area. To achieve the various C-UAS functions at the different phases, several engineering solutions have been adopted.

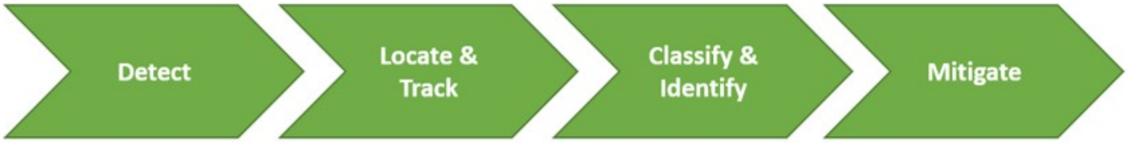

Figure 2.1. C-UAS Kill-Chain. Source: [35]

2.4.2 ‘Detect,’ ‘Locate’ and ‘Track’ Techniques

Table 2.3 shows a list of commonly adopted engineering techniques to enable the functions of detection, to locate, and to track an adversary UAS. A brief description of the system capabilities and its limitations is also discussed.

Table 2.3 shows the list of commonly adopted engineering techniques to enable the functions of detection, to locate and to track an adversarial UAS. A brief description of the system capabilities and its limitations is also discussed.

Table 2.3. ‘Detection’, ‘Locate’ and ‘Tracking’ Techniques

Techniques	Capabilities	Limitations
Radar	The radar sensor is capable of detecting a UAS if the UAS is within the range of the radar sensor. This is achieved through the receipt of reflected pulses of RF energy from the UAS. Additional information about the UAS such as the location and the velocity of the UAS can also be obtained through the radar sensor. In advanced radar sensors, ‘tracking’ the location and ‘classifying’ the type of UAS is achievable through advanced signal processing algorithms.	Due to the ‘small’ RCS of some COTS Groups 1 and 2 UAS, detection and tracking remains a challenge [36]. The ability to accurately ‘detect’ and ‘track’ a small target could be degraded due to unfavorable weather condition such as the effect of rainfall.

Continued on next page

Table 2.3 – continued from previous page

Techniques	Capabilities	Limitations
Radio Frequency	RF sensors are capable of detecting the frequencies transmitted by other telecommunication devices in the RF spectrum. By integrating the RF sensor with other UAS software algorithms and devices, the system is capable to differentiate between an UAS and other RF devices. Therefore, detection of a UAS can be achieved.	Many advanced UAS have recently adopted Frequency-Hopping-Spread Spectrum (FHSS) techniques instead of using a single set frequency for communications [37]. This approach has added additional complexity for the RF detection sensor to effectively determine transmitting frequencies and the sequence of transmission of a UAS using FHSS. RF detection sensors can also be less effective in crowded RF environments due to other RF transmitting devices [38].
Electro-Optical and Infrared (EO/IR) Cameras	An EO/IR sensor is capable of capturing images during the day and night using visible and infrared sensors. An EO/IR sensor is usually coupled with computer vision algorithms to differentiate between a UAS and other objects.	EO/IR detection sensors can consume large amount of electrical power due to the nature of the sensors used. The cost to include EO/IR sensors in the system is much higher as compared to other existing UAS detection systems. This sensor is also limited by range given the nature of the sensors [39].

Continued on next page

Table 2.3 – continued from previous page

Techniques	Capabilities	Limitations
Acoustic Sensor	Acoustic sensors are capable of detecting sound emitted by an object of interest. Coupling an Acoustic sensor with UAS audio comparison algorithms, detection of a UAS is achievable by matching the detected sound with the sound recorded in existing databases.	The detection range of acoustic detection sensors is negatively affected if the surrounding environment is noisy such as a densely populated area or an environment with high winds condition [40].

Mitigation Techniques: Non-Kinetic

Non-Kinetic mitigation measures in C-UAS operations seek to deny, degrade, or disrupt the capability of a UAS without the need for physical destruction [41]. Table 2.4 shows a list of commonly adopted non-Kinetic mitigation measures used in C-UAS missions.

Table 2.4. List of Non-Kinetic Mitigation Measures

Techniques	**Capabilities**	**Limitations**
Frequency Jamming	A frequency jammer transmits large amounts of electrical power over a range of predefined RF frequencies to interfere with and disrupt the communication link between the UAS and the Ground-Control-Station (GCS) over a period of time. This action forces the UAS to trigger the 'return home' algorithm or to perform an emergency landing based on the default UAS safety protocol.	Typical RF jammers consume large amounts of electrical power. To meet this requirement, RF jammers are typically bulky due to the heavy and large electronic components used. This restricts the ease of deployability of the device. Jamming on a single frequency may not be effective to C-UAS operations if the UAS uses FHSS [42]. In addition, other friendly communication devices operating at the jammed frequency may also be affected [11].
GNSS Jamming	The GNSS Jamming technique attempts to disrupt the GPS communication link between the UAS and GPS satellites.	This technique may not be effective for UAS that do not require GPS for navigation.
GNSS Spoofing	The GNSS spoofing technique enables 'impersonation' by feeding the UAS with false navigation information and then eventually taking over the role as the host of the UAS for control.	This method may be ineffective with adversarial drones equipped with Inertial Measurement Unit sensors. It is not suitable to be used in places where satellite navigation is required by other systems [43].

Mitigation Techniques: Kinetic

Kinetic mitigation techniques in C-UAS operations seek to degrade the UAS through inflicting damage on the physical components of the UAS [41]. Table 2.5 shows the list of commonly adopted kinetic mitigation measures used in C-UAS missions.

Table 2.5. List of Kinetic Mitigation Measures

Techniques	Capabilities	Limitations
Net Capture	This technique adopts the concept of a 'firing gun.' Upon triggering of the firing gun, netting embedded within the weapon is deployed to capture the UAS. The firing gun can be deployed on a UAS or mounted on a handheld device.	This capturing device needs to attain close enough range to the adversarial UAS in order to be effective [43].
Directional Electromagnetic Pulse (EMP)	This technique uses an electromagnetic pulse to damage onboard radio electronic system on the UAS. The Directional EMP adopts the similar concept of a 'firing gun' and can be deployed on a handheld device.	Since EMP at different frequencies requires different transmission distances, the EMP method to take down a UAS may not be effective if the required distance is not met, even though an adversarial UAS is detected [5].

The C-UAS processing-chain is complete with the integration of various detection and mitigation techniques mentioned in this section. For example, the Radar UAS detection system is responsible for the detection, identification, and tracking of the location of an adversarial UAS. Then, the responsibility of the frequency jammer mitigates the adversarial UAS to prevent the UAS from further infiltration into a facility.

2.4.3 C2 System

The function of the C2 system in the C-UAS network aims to provide the stakeholders with (1) a holistic overview of the situation within the operating environment, (2) the ability to analyze the situation, and (3) to execute the necessary decisions based on the assessment made [44]. The C2 system serves as the center-node, linking the various UAS detection and UAS mitigating systems as shown in Figure 2.2. The outputs from the various UAS detection devices comprise the inputs of the C2 system [45]. Since the outputs are in different forms, it is necessary to fuse the information such that the information presented to the stakeholders is consistent and accurate [5].

2.4.4 C-UAS Network

As illustrated in Figure 2.2, the C-UAS network includes three functional blocks, namely (1) "Detection and Tracking", (2) "React" as well as (3) "Mitigate". The "Detection and Tracking" functional block comprises a single or a set of UAS detection devices to detect and track adversarial drones within a define boundary. The information such as the location and speed of the detected adversarial drones would then be sent as output information to the "React" functional block for further analysis. In the "React" block, since the outputs from the various UAS detection devices are in different form, a Data Fusion unit would be required to process the incoming information and output a standardized and coherent set of data to the C2 system, such that the information presented to the stakeholders is consistent and accurate for the purpose of decision making [5], [45]. Based on the profile of the adversarial drone, the C2 system selects and triggers the most suitable mitigating technique to neutralize the adversarial drone.

The functions at the different phases of the C-UAS processing chain have been discussed in this section. To achieve the goals of a C-UAS mission, various detection and mitigation techniques are adopted as have been discussed in this section. The introduction of a C2 system within the C-UAS network enhances the ability for the stakeholders to analyze the situation such that the most appropriate actions are applied against the adversarial UAS.

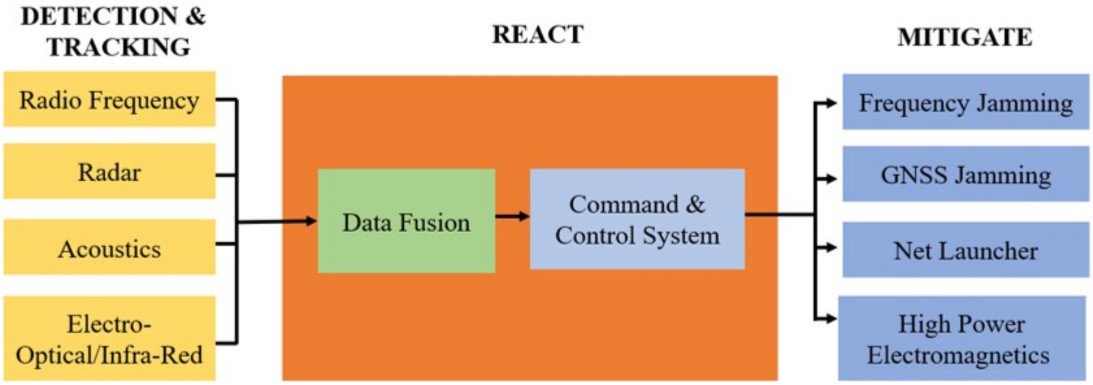

Figure 2.2. C-UAS Network [44]

2.5 Literature Review on C-UAS Acquiring Cyberattack Techniques

In recent studies, the application of cyber-attacks in the C-UAS domain have shown the scalpel-edge accuracy that such attacks can produce when defending against an adversarial UAS. Many CyC-UAS approaches work by either denying or disrupting adversary UAS RF communications without the need for jamming [3], [46]. This section seeks to provide (1) a broad overview of the main existing cyber-attack methods on C-UAS operations and (2) the proposed Concept of Operations based on a CyC-UAS system's capabilities and architecture.

2.5.1 Existing Cyber-Attack Techniques

The current literature on C-UAS using cyber-attack techniques focuses on identifying the vulnerability within the Seven-Layer Open Systems Interconnection (OSI) model of the communication network protocols [47]. Specifically, the cyber-attack scheme attempts to manipulate or tamper with the information flowing into the Transport (layer 4), Network (layer 3), Data Link (layer 2), or Physical (layer 1) layer of the OSI model, with the intent to deny the use of communication network services [48].

2.5.2 Denial of Service Attack

The Denial of Service (DoS) attack is classified as one type of cyber-attack technique and aims to suspend or to interrupt the use of a communication network [49]. This is accomplished through disrupting the network connection services by flooding the network with data packets such that the network becomes overwhelmed and results in the inability of any host to establish communications with other telecommunication devices within the network [50].

In wireless communications, a typical construct of a UAS consists of an aerial device (a.k.a. drone) and a GCS that communicate via a set of operating frequencies [51]. In the context of CyC-UAS operation, the DoS cyber-attack technique can be performed against wireless networks [52].

In the context of CyC-UAS, the C-UAS adopts the DoS attack technique on the UAS through the wireless network linking the GCS and drone (henceforth we will simplify terminology and also refer to the aerial component of the system as simply the UAS). Commercial UASs that operate using Wireless Fidelity (WiFi) network protocols such as 802.11 (usually in the 2.4 GHz and 5 GHz frequency ranges) are extremely vulnerable to such attacks because the operating radio frequencies are known and easily targeted using network interface cards [53].

2.5.3 User Datagram Protocol Flood Attack

The User Datagram Protocol (UDP) uses a connectionless communication model with minimal packet ordering mechanisms to enable data package transfer within a network [54]. In C-UAS operations, the UDP flood attack technique attempts to degrade UAS wireless network performance by flooding the network with data packets, forcing the adversary UAS to trigger internal safety protocols such as the "return to base" algorithm or to perform an emergency landing based on the UAS's default safety protocol [55].

2.5.4 TCP SYN Flood attack

Unlike the UDP protocol, the Transmission Control Protocol (TCP) protocol is a connection-oriented communication model, where a 3-way-handshake between the client and the server must be established first before commencing data package transfers within the network as shown in Figure 2.3 [56]. For the sender to establish communications with the receiver, the sender first sends a synchronization (denoted by SYN) request with the sender's IP address to the receiver. Then, the receiver sends a synchronization acknowledgement (denoted SYN ACK) to the sender's IP address. The sender then replies to the receiver with an acknowledgement (denoted ACK) to complete the establishment process [56].

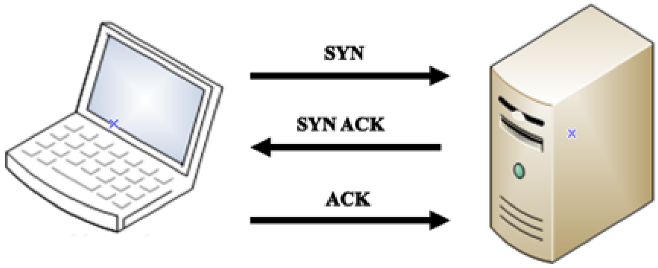

Figure 2.3. TCP "3-way-handshake"

In the case of a TCP Flood attack, the attacker initiates the TCP protocol with the receiver with a spoofed IP address [57]. The receiver then replies with a SYN ACK to the IP address that was provided by the attacker. Then the attacker repeats the same attack approach on the receiver multiple times. As a result, the network is flooded, causing the server to be unable to communicate with the network due to memory exhaustion [55]. In the context of CyC-UAS operations, the C-UAS and the adversarial UAS act as the attacker (sender) and receiver, respectively. The TCP Flood attack causes the wireless network of the adversarial UAS to collapse, forcing the UAS to activate its return-to-base protocol, conduct an emergency landing, or other internal safety protocol [58].

2.5.5 Deauthentication Attack in Wireless Network

The IEEE 802.11 technical standard governs Local Area Network (LAN) technical specification and describes the set of Media Access Control (MAC) protocols for the implementation of wireless LAN [59]. The deauthentication attack exploits the OSI Layer Two vulnerabilities in wireless access points to prevent legitimate users from accessing a network [60]. With information such as the MAC address of the telecommunication devices available openly within the wireless network, an attacker is able to identify the targeted device. Then, the attacker can launch a deauthentication attack on the targeted device in an attempt to cut off the wireless connection between the targeted device and the network by sending continuous deauthentication frames to the targeted device [61]. Because a deauthentication attack can disrupt the connection between a client and its host with only one forged frame for every six legitimate frames between a client and its host [60], deauthentication attacks are especially useful when limited power is available in countering adversarial UASs [10]. In the context of CyC-UAS operations, the C-UAS may adopt the deauthentication cyber-attack technique by sending continuous deauthentication frames to the adversary UAS over the wireless network, so as to deny communications between the adversarial GCS and its UAS [61]. Much like the attacks against WiFi networks, in the context of CyC-UAS, deauthentication attacks are only carried out against UASs using the 802.11 wireless standard [10]. Thus, these attack types will not be effective against UASs that use frequency hopping spread spectrum or other communication schemes that operate outside the 2.4 and 5GHz WiFi frequency bands.

2.5.6 Comparison Between Cyber-Attack Techniques

Table 2.6 summarized and compare the three cyber-attack techniques for the CyC-UAS operation. While the list of mentioned cyber-attack techniques can be used for CyC-UAS operation, the deauthentication attack is the most effective mode of attack since (1) the technique is capable to identify specific UAS target with the identification of its MAC address from the WiFi network, as well as (2) having lesser coding complexity to identify the IP address of the target.

2.5.7 CyC-UAS Physical Setup

The essential hardware of a CyC-UAS system comprises of a micro-controller, transceiver, and an RF antenna [61]. The source-code of the cyber-attack algorithm embedded in the micro-controller launches a detection algorithm to scan for adversarial UAS within the surrounding environment. Upon a successful detection of an adversarial UAS, the C-UAS launches the mitigation attack algorithm on the UAS. The CyC-UAS transceiver and the RF antenna serves as the intermediary between the micro-controller and the RF environment to complete the processing-chain of the CyC-UAS. Figure 2.4 shows a simple CyC-UAS prototype setup.

Table 2.6. List of Cyber-Attack Techniques for CyC-UAS operation

Techniques	Capabilities	Limitations
User Datagram Protocol Flood Attack	Easy to implement since the communication between the CyC-UAS and adversarial UAS is connectionless and session-less.	CyC-UAS gained limited access to adversarial UAS since the connection is connectionless. For example, CyC-UAS unable to take over control or to intercept information transmitted by the adversarial UAS.
TCP SYN Flood attack	With the IP address of a particular adversarial UAS known, dedicated TCP/SYN flood attack can be performed on a specific adversarial UAS.	The complexity of TCP/SYN Flood attack is relatively higher as additional algorithm must be integrated within the CyC-UAS to identify the IP address of the desired adversarial UAS. This may result in higher processing time during the C-UAS process.
Deauthentication Attack	Easy to implement since the information on MAC address of the adversarial UAS can be obtained in the wireless network.	This attack is effective only against adversarial UAS that uses wireless access point.

Past C-UAS Experiments with CyC-UAS Prototype

In recent studies, the application of cyber-attacks in the C-UAS domain have shown potential improvements in energy consumption in comparison with other existing conventional C-UAS techniques [10]. For example, the CyC-UAS technique is capable of disrupting the communication link of a specific adversarial UAS target instead of transmitting across a range of frequencies with a high amount of energy adopted by conventional frequency jamming C-UAS. Through the conduct of these experiments, the effectiveness and efficiency of the cyber-attack technique applied on COTS UASs that operate in the 2.4GHz and 5GHz WiFi frequency bands was validated [10]. The experiments are specifically scoped towards seeking an understanding on the amount of energy consumed during C-UAS operation. In particular, the deauthentication cyber-attack technique was used in various attack experiment scenarios. These experiments were conducted in an outdoor environment with the use of various telecommunication equipment.

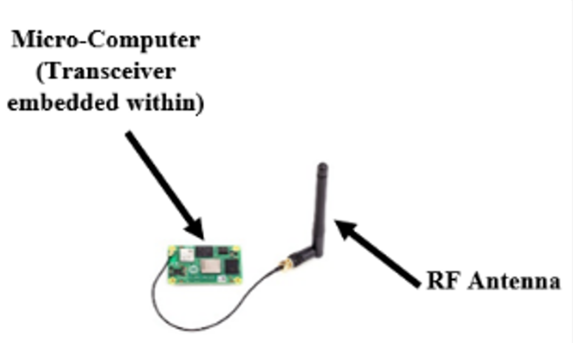

Figure 2.4. CyC-UAS Hardware Prototype

Experiment Setup

We follow the experiment setup from [10]. Table 2.7 shows the list of equipment used, and the respective roles of the equipment during the experiments. The equipment and testing focus is based on targeting commercial UASs that use the IEEE 802.11 standard.

Table 2.7. List of Equipment and Roles

Equipment			Roles in Experiment
UASs	Parrot Bebop		Adversarial UAS
	Skydio 2+		Adversarial UAS
	AquaQuad		Friendly UAS used as Mobile C-UAS platform (To be integrated with Raspberry Pi 4 and WiFi Antenna)
Raspberry Pi 4 Model B + WiFi Network Interface Card (Alpha AWUS036ACH)			C-UAS (deauthentication attack source code embedded in Raspberry Pi 4)
Multimeter – AiLi UM25C USB			Integrated onto Raspberry Pi 4 to collect electrical power readings (Voltage and current)
Smart phone			Software applications for the Parrot Bebop and Skydio2+ to be installed onto Smartphone devices to perform the role of Ground Control Station (GCS) of adversarial UAS and Mobile C-UAS, respectively

2.5.8 Experimental Scenarios

The experiment scenarios were designed based on the information required to validate the performance of the CyC-UAS system at various ranges and altitudes. There were three distinct scenarios namely, (1) CyC-UAS and adversarial UAS are both stationary, (2) CyC-UAS is stationary and adversarial UAS is in motion, and (3) CyC-UAS is mobile (attached to a friendly UAS) and adversarial UAS is in motion.

Observations from Scenario 1 – CyC-UAS and Adversarial UAS at Stationary Positions

In this scenario, both the CyC-UAS system and the single adversarial UAS were held at stationary fixed positions during the 'detection' and at the 'attack' phases at stand off distances of 10, 100, 250, and 400 meters as shown in Figure 2.5. The CyC-UAS system used in the experiments has a maximum detection range in a ground-to-air configuration of approximately 250 meters and is capable of detecting intrusion of adversarial UASs that falls within the detection range. The CyC-UAS system scans the environment consistently to detect adversarial UAS intrusions. Upon a successful detection, the CyC-UAS initiates a deauthentication cyber-attack technique on the adversarial UAS. It was observed that the CyC-UAS system was successful in (1) detecting and attacking the adversarial UAS at distances of 10, 100, 250, and 400 meters and that the (2) time taken upon a detection till the neutralization of an adversarial UAS is estimated to be 15 seconds, consuming about 1.1 Watt of electrical power. At the end of the attack, the adversarial UAS returned to its last known connection point and landed subsequently. At about 400 meters away, the CyC-UAS was unable to detect the adversarial UAS situated at 400 meters away. It was deduced that the transmitted signal of the CyC-UAS was not strong enough to reach the adversarial UAS at a distance of 400 meters, which was primarily limited by interference from buildings, trees, and power lines in the area as well as the transmission power that the Raspberry Pi 4 and the wireless network card were designed to output.

Observations from Scenario 2 – C-UAS at Stationary Position and Adversarial UAS in Motion

In this scenario, both the CyC-UAS and adversarial UAS started at stationary positions, having a separating distance of 250 meters just beyond the effective range of the CyC-UAS system used in these experiments as shown in Figure 2.6. The CyC-UAS began scanning the environment to detect the adversarial UAS. Then, the adversarial UAS commences its operations by flying towards the CyC-UAS. Upon a successful detection of the adversarial UAS, the CyC-UAS initiates the deauthentication cyber-attack technique on the adversarial UAS. It was observed that the adversarial UAS (1) came to a halt and hovered at a stationary position for about 10 seconds before (2) returning to its last known connection point and landed subsequently. It was observed that the GCS of the adversarial UAS was unable to control the adversarial UAS due to the loss of telecommunications between the GCS and UAS caused by the deauthentication cyber-attack [10].

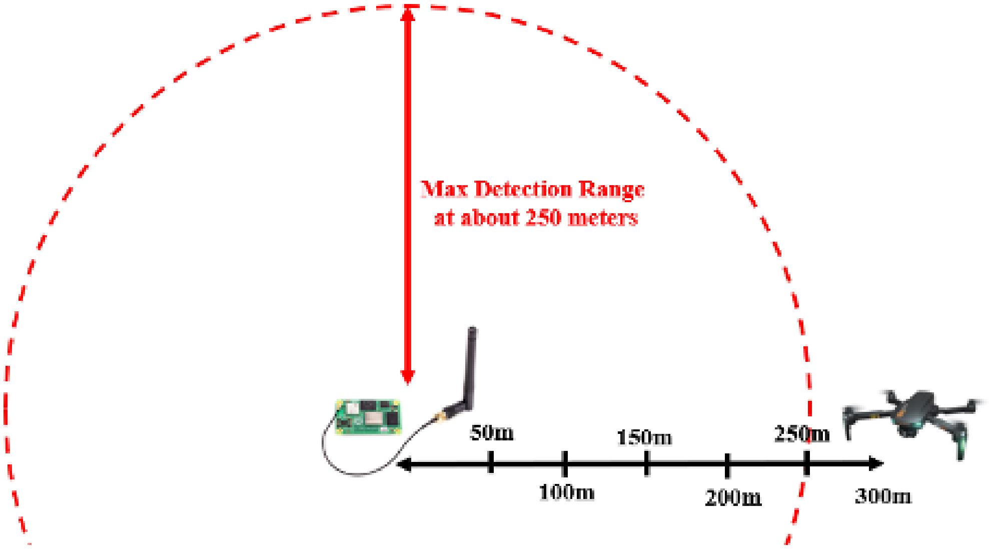

Figure 2.5. CyC-UAS and Adversarial UAS at Stationary Positions.

Observations from Scenario 3 – CyC-UAS and Adversarial UAS Both in Motion

In this scenario, the CyC-UAS was fitted on to a proprietary UAS, called the AquaQuad [62], to turn the CyC-UAS into a mobile C-UAS. Both the mobile CyC-UAS and the adversarial UAS moved in the same direction having a separation distance of about 20 meters [10]. While both UASs were in motion, the mobile CyC-UAS performed the deauthentication cyber-attack on the adversarial UAS. It was observed that the (1) mobile CyC-UAS was able to detect the adversarial UAS while both the UASs were in motion and that (2) during the deauthentication cyber-attack process, the adversarial UAS came to a halt (while hovering for about 10 seconds) before returning to its last known connection point and landed subsequently.

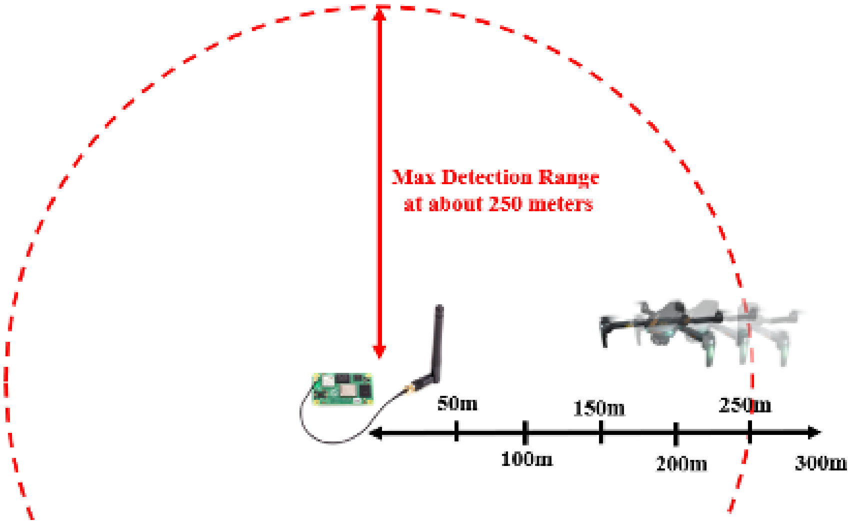

Figure 2.6. C-UAS at Stationary Position and Adversarial UAS in Motion

The experiments performed in the scenarios provided insights on the effectiveness and efficiency of CyC-UAS operations. The use of the deauthentication cyber-attack technique in all the experiments was successful in neutralizing the adversarial UAS by severing the telecommunication link between the adversarial UAS and the GCS. In addition, the conduct of the experiments provided essential information to assess system performance of the deauthentication cyber-attack technique. The information attained from the experiments as well as the physical behavior of the adversarial UAS observed in the experimental scenarios was then used to define the system performance of the CyC-UAS system in the subsequent section.

2.5.9 Proposed Concept of Operation

Given the system description of the capability of the CyC-UAS, two CONOPs schemes are proposed and elaborated for further discussion in this subsection; namely, defensive deployment and aggressive deployment.

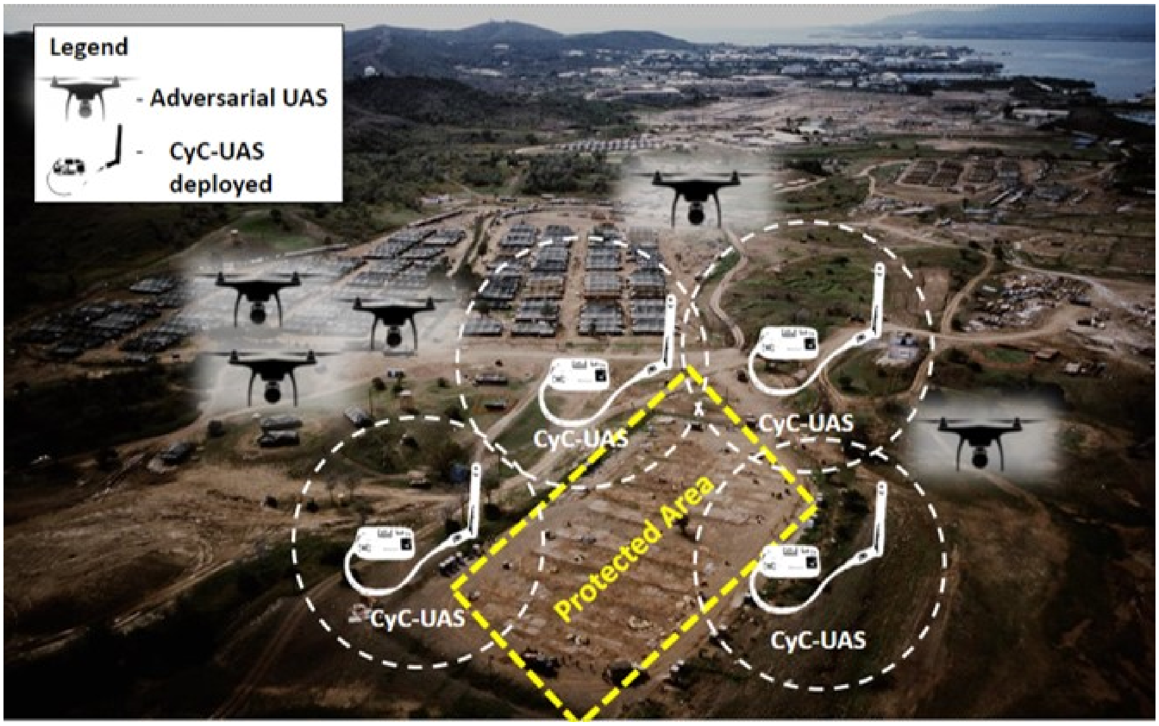

Figure 2.7. CONOPS of Stationary Defensive Deployment of CyC-UAS to Protect Fixed infrastructure.

Defensive CyC-UAS Deployment

In the defensive deployment scenario, the mission of the CyC-UAS is to prevent the infiltration of adversarial UAS within a defined protected area to protect a specific installation or infrastructure. In this setup, several CyC-UAS are deployed in stationary positions to defend against infiltration of adversarial UAS into the protected area as shown in Figure 2.7. The defensive deployment concept aims to provide a permanent defensive mechanism to prevent potential adversarial UAS attacks. Upon a successful detection of an adversarial UAS, the CyC-UAS automatically launches the mitigation algorithm in an attempt to neutralize the adversarial UAS. Since the CyC-UAS alone is capable of fulfilling the functions of the C-UAS processing-chain, and because the CyC-UAS has the ability to perform a mitigation attack on the UAS immediately upon a successful adversarial UAS detection, the lag-time between detection and mitigation is minimized.

The CyC-UAS can be deployed on ground mobile platforms such as military vehicles maneuvering at the battlefront or police or national defense vehicles protecting civilians as shown in Figure 2.8.

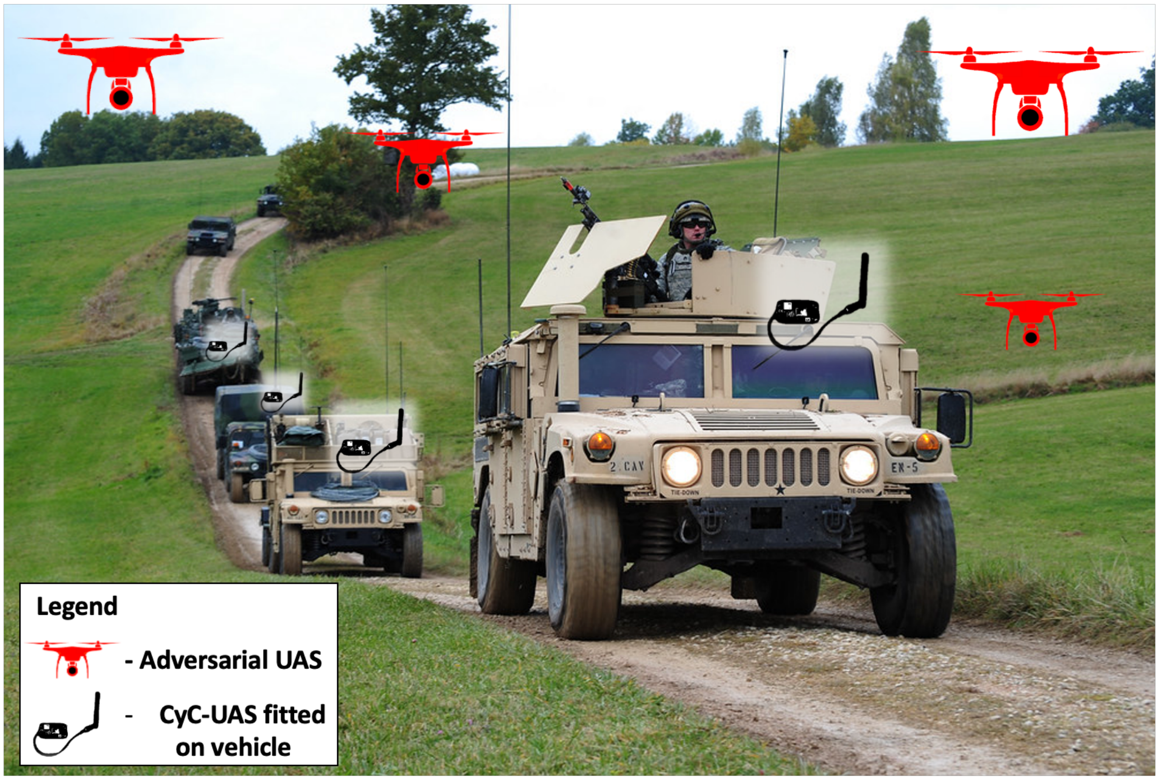

Figure 2.8. CONOPS of Ground Mobile Defensive Deployment of CyC-UAS to Protect Vehicles and Civilians.

Aggressive CyC-UAS Deployment

In this CONOPS, the CyC-UAS employs an aggressive approach in the attempt to neutralize any potential adversarial UAS as shown in Figure 2.9. To enable CyC-UAS with the ability to maneuver within the operating area, the CyC-UAS is integrated on an air mobile platform. For example, by integrating the CyC-UAS onto a friendly UAS, the system can rapidly maneuver in three dimensions such that it enhances the CyC-UAS's ability to detect, track, and mitigate adversarial UAS.

This section discussed various DoS cyber-attack techniques that have been adopted for C-UAS operations. Existing literature validates the effects of cyber-attacks on adversarial

UAS based on physical experiments. With a good understanding of the system architecture and the capabilities of the CyC-UAS, two feasible CONOPS were proposed.

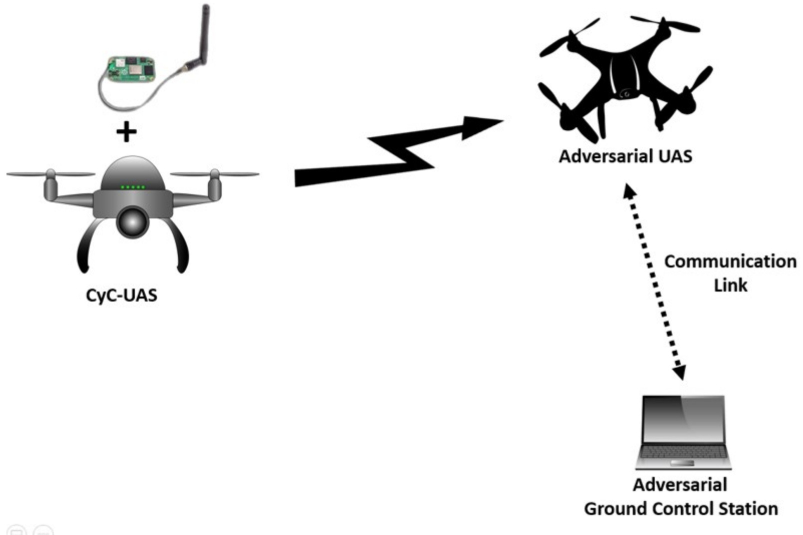

Figure 2.9. CONOPS of Aggressive Deployment of CyC-UAS to Project Protection Against Adversarial UAS Beyond Fixed or Mobile CyC-UAS Platforms.

2.6 Modelling and Simulation

This section develops a simulation model to represent CyC-UAS operations based on the proposed CONOP presented in Section 2.5.9. The simulation seeks to gain an understanding of the CyC-UAS system performance and limitations using the deauthentication cyber-attack technique. In particular, the simulation is used to better understand the estimated energy consumption for a given simulated scenario of CyC-UAS operations. The experimental results achieved during the experiments as well as the physical observations attained from the various experimental scenarios presented in Section 2.5.7 are applied as system parameters to the CyC-UAS simulation model. The CyC-UAS software model and simulations were constructed and conducted in ExtendSim10 [63].

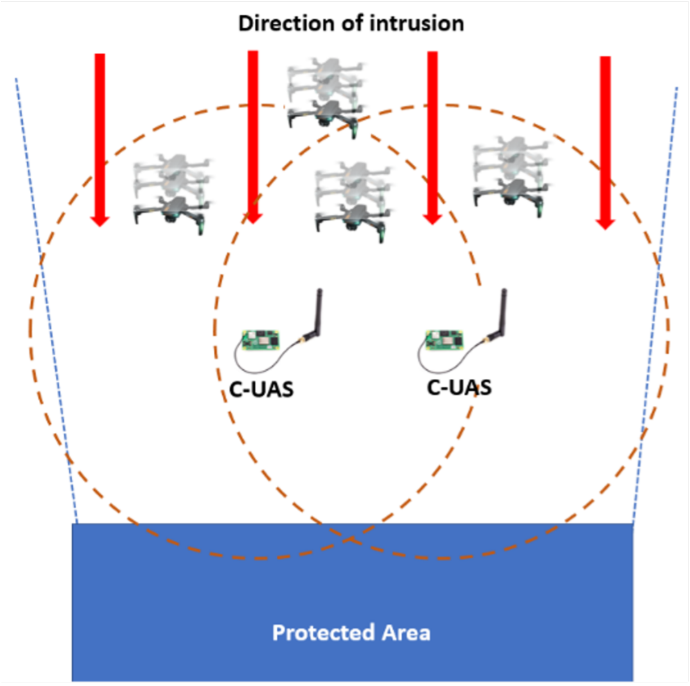

Figure 2.10. CyC-UAS Operational Scenario

2.6.1 Mission Scenario for C-UAS Operation

The aim of the CyC-UAS system was to prevent the intrusion of adversarial UAS into a defined protected area as shown in Figure 2.10. There were two CyC-UAS systems deployed at stationary positions beyond the protected area such that the systems could potentially detect and neutralized any incoming adversarial UASs. On the other hand, the aim of adversarial UASs was to penetrate the protected area. In this scenario, it is assumed that the (1) protected area may be subjected to concurrent intrusion attempts by multiple adversarial UASs (a swarm attack) and that (2) the adversarial UASs would move in a straight-line direction, represented by the red arrows in Figure 2.10.

2.6.2 Modeling Setup

The Area of Operation (AO) was divided into three different zones (Zone 1, 2 and 3) as represented in Figure 2.11. The ability to detect and to perform a cyber-attack is dependent on whether the adversarial UAS falls within the detection range of the CyC-UAS systems. In this case, since the region in Zone 2 was overlapped by two CyC-UAS systems, the chance of detecting and neutralizing an adversarial UAS that enters the region is doubled, since either one of the CyC-UAS systems could perform the detection or attack on the adversarial UAS. In addition, it was assumed that the three different zones have equal chance (Zone 1, 2, and 3 = Probability of 0.333) for an adversarial UAS to appear in the respective regions.

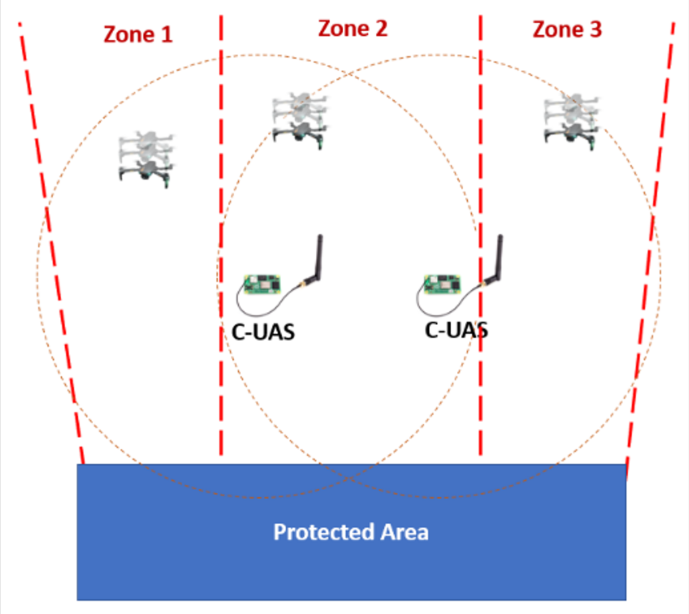

Figure 2.11. Zones of Area of Operations

In this model, it was assumed that both the CyC-UAS systems would be scanning the environment actively to detect any number of adversarial UASs. The CyC-UAS would then initiate the deauthentication cyber-attack on the adversarial UAS based on a first-in-first-out attack sequence. It was assumed that adversarial UAS would come to a halt and hovered at a stationary position for about 10 seconds once the cyber-attack was initiated. Should the attack on adversarial UAS be successful, the adversarial UAS would land. On the other hand, if the attempt to neutralize the adversarial UAS was unsuccessful, the adversarial UAS would continue to traverse in the initial direction towards the protected area. In addition, the CyC-UAS is capable of re-engagement with an adversarial UAS if attack attempt is unsuccessful and if the adversarial UAS remains within detection range of the CyC-UAS. The CyC-UAS has the ability to perform both the role of detection and attack concurrently. These assumptions mentioned were applied to the simulation model.

Table 2.8 shows the system performance parameters of the CyC-UAS and adversarial UAS applied in the ExtendSim10 simulation model. The model was also designed to record the power consumed by both CyC-UAS systems throughout the detection and attack phases. Once the first adversarial UAS falls within the detection range of the CyC-UAS systems, data collection of the power consumed by the CyC-UAS commences and is terminated when the last detected adversarial UAS is neutralized. The overall power consumption of the CyC-UAS is the summation of power consumed by both the CyC-UAS systems deployed in the model.

Table 2.8. CyC-UAS and Adversarial UAS Parameters

C-UAS Parameters	
Maximum Detection Range:	250 meters
Time to Detect and Neutralize Target:	Lognormal distribution (Mean = 15s, Std = 2s)
Probability of Success for detect & attack actions for 1x adversarial UAS:	0.8
Power consumption to detect and attack 1x adversarial UAS:	1.1 Watt
Adversarial UAS Parameters	
Adversarial UAS travelling Speed:	30Km/Hr

To simplify the simulation model, experimental values measured at a separation distance of 250 meters between the CyC-UAS and the adversarial UAS performed in Section 2.5.7 was applied in this simulation model. This model assumed that the adversarial UASs traverse the AO with a constant speed of 30 Km/Hr. Further, it was assumed that the CyC-UAS has a detection range of 250 meters, and that the overall detection region was in the form of a circular shape having a diameter of 500 meters. Assuming that the adversarial UAS traverses (1) across the detection region of 500 meters and (2) at a constant speed and direction, the adversarial UAS would be presence in the detection region for about 60 seconds as shown in Figure 2.12.

The flowchart in Figure 2.13 provides an overview of the sequence of activities and decision points upon detection of an adversarial UAS. With the system descriptions as well as the system parameters presented as shown, a simulation model was built in ExtendSim10 to understand the CyC-UAS system performance.

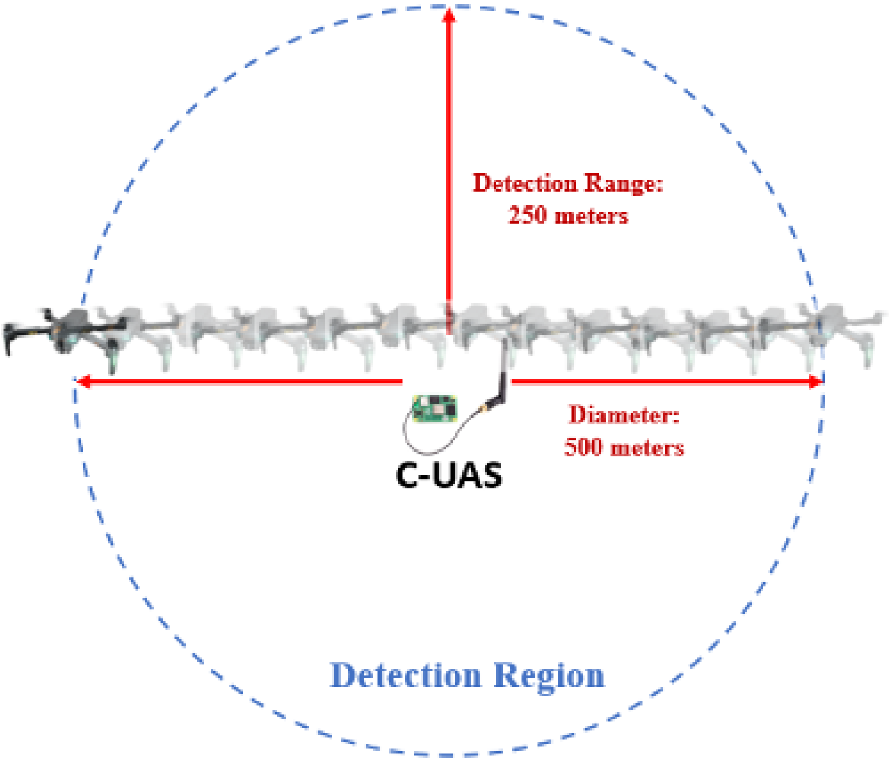

Figure 2.12. Adversarial UAS Traversing Detection Region

2.6.3 Simulation

In alignment with the aim of the mission objective of the CyC-UAS system presented in the scenario, four performance metrics as shown in Table 2.9 were identified to measure the effectiveness and the capability of the CyC-UAS system.

To simulate a swarm attack, the group of adversarial UASs is represented as a salvo attack in ExtendSim10. Three salvo attacks that consist of 8, 10 and 12 adversarial UASs are simulated independently. In each of the salvo attacks, the adversarial UASs are injected into the model as inputs. In addition, each salvo simulation run is repeated 100 times to achieve sufficient samples to attain an average value for the metrics stated as shown.

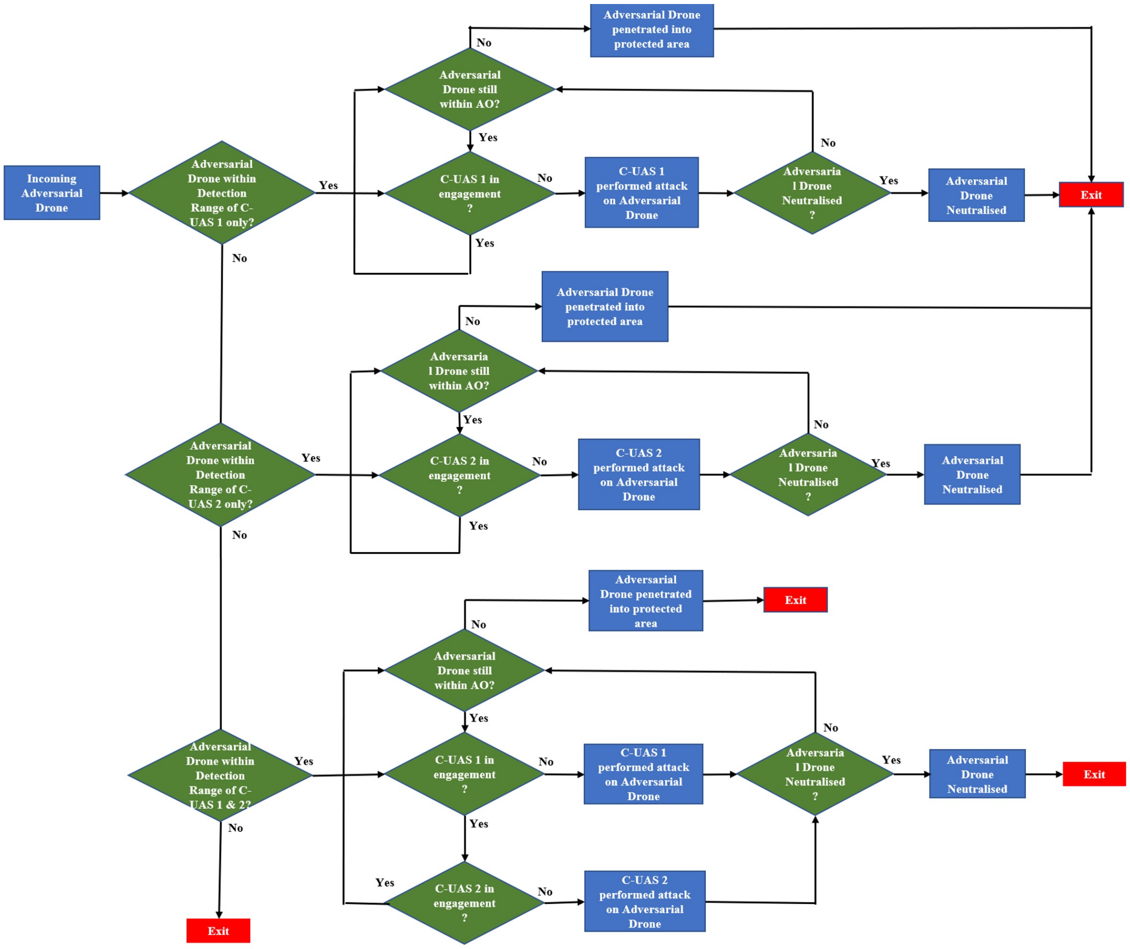
Adversarial Drone penetrated into protected area
No
Adversarial Drone still within AO?
Yes
No
Incoming Adversarial Drone
Adversarial Drone within Detection Range of C-UAS 1 only?
Yes
C-UAS 1 in engagement ?
No
C-UAS 1 performed attack on Adversarial Drone
Adversaria l Drone Neutralised ?
Yes
Adversarial Drone Neutralised
Exit
Yes
No
Adversarial Drone penetrated into protected area
No
Adversaria l Drone still within AO?
Yes
No
Adversarial Drone within Detection Range of C-UAS 2 only?
Yes
C-UAS 2 in engagement ?
No
C-UAS 2 performed attack on Adversarial Drone
Adversaria l Drone Neutralised ?
Yes
Adversarial Drone Neutralised
Yes
No
Adversarial Drone penetrated into protected area
Exit
No
Adversarial Drone still within AO?
Yes
No
Adversarial Drone within Detection Range of C-UAS 1 & 2?
Yes
C-UAS 1 in engagement ?
No
C-UAS 1 performed attack on Adversarial Drone
Adversaria l Drone Neutralised ?
Yes
Adversarial Drone Neutralised
Exit
No
Yes
Yes
C-UAS 2 in engagement ?
No
C-UAS 2 performed attack on Adversarial Drone
Exit

Figure 2.13. Sequence of Activities and Decision Points for CyC-UAS Upon Detection of an Adversarial UAS

2.6.4 Simulation Results

Table 2.10 shows the average results of the metrics for the C-UAS across the different numbers of adversarial UASs in a single swarm attack.

Table 2.9. Metrics of Analysis for the CyC-UAS System

Metrics	Description
# of Adversarial UASs Neutralized	The primary objective of the C-UAS system was to prevent the intrusion of adversarial UAS entering the protected area. To achieve this objective, the C-UAS system must first detect and then subsequently neutralize the adversarial UAS.
# of Adversarial UAS Penetrations into Protected Area	It is assumed that an adversarial UAS has successfully penetrated the protected area if the adversarial UAS was not neutralized by the C-UAS.
# Accumulated Energy consumed by C-UAS	The power consumed by the C-UAS during the entire detection and attack phases is accumulated and recorded.
# Accumulated C-UAS operating period (Seconds)	The overall time taken for C-UAS operations is recorded.

Table 2.10. Metrics and Corresponding Results

Metrics	# of Adversarial Drones in a Single Swarm Attack			
	8	10	12	14
# of Adversarial Drones Neutralized	8	9	9	9
# of Adversarial Drones Penetrating Protected Area	0	1	3	5
# Accumulated Energy consumed by C-UAS (Watt/Hour)	0.0342	0.0397	0.0385	0.0409
# Accumulated C-UAS operating period (Seconds)	56	65	63	67

Based on the 100 simulation runs performed in each scenario, the C-UAS system that comprises two CyC-UAS systems was capable of neutralizing between eight and nine adversarial UASs in a single swarm attack for all scenarios. However, as the number of adversarial UASs in the swarm attack increases beyond nine (10, 12 and 14), the number of adversarial UAS misses increases as well. Therefore, based on the C-UAS deployment layout and the stated assumptions, the C-UAS system is effective in neutralizing nine adversarial UASs in a swarm attack.

The average accumulated energy consumed and the C-UAS operating period taken by the C-UAS management system to neutralize nine adversarial UASs in each swarm attack scenario (10, 12 and 14 adversarial UASs) are as shown in Table 2.11.

Table 2.11. Average Accumulated Energy Consumed and Operating Period

Average Energy and Time Consumed for 9 Adversarial Drones	# Adversarial Drones in a Single swarm attack (10, 12 and 14 drones)
# Average Accumulated Energy consumed by C-UAS (Watt/Hour)	0.0397
# Average Accumulated C-UAS operating period (Seconds)	65.00

A C-UAS management system simulation model was built based on the (1) application of deauthentication cyber-attack technique, (2) Proposed CONOPs, (3) Mission Scenario, and the (4) applied C-UAS system parameters attained during the physical experiment. A swarm attack on the C-UAS management system was also simulated to observe the capabilities and the limitations of the system. In addition, the simulations that were conducted also provide information on the overall energy consumed and the period taken for the entire C-UAS operation.

The mission scenario presented in this section, and the set of simulated results as shown can be used as a baseline to compare and analyze the effectiveness and efficiency of some other convention C-UAS techniques. This is done in the next section.

2.7 Comparison of Energy Consumption and Performance between C-UAS Techniques

The experiments performed in Section 2.5.7 provided insights on the energy consumption requirement for CyC-UAS operations. The aim for this section is to assess the energy efficiency of CyC-UAS by (1) understanding the energy requirement from existing C-UAS techniques through the review of technical specifications of existing products as well as to (2) compare the energy consumption requirements between CyC-UAS and existing C-UAS techniques. In addition, this section also aims to compare the system performance of various C-UAS techniques.

2.7.1 Existing Products

The EAGLE108 is an existing C-UAS that is capable of performing detection and mitigation on an adversarial UAS through RF signal detection and RF jamming [64]. Table 2.12 shows the system specification of EAGLE108. While there are several C-UAS systems that use RF jamming, the EAGLE108 is representative of many available systems. Some C-UAS systems that use RF jamming operate at much higher output transmission powers. However, this article limits analysis to the EAGLE108 because data is readily available in open source literature and it is a system in common use by civilian organizations in addition to national security organizations.

2.7.2 Energy Consumption Comparison

Based on the experimental setup using the CyC-UAS prototype, it was shown that the CyC-UAS has an effective detection range of about 250 meters. To enable a comparison of energy requirements between the CyC-UAS prototype and the EAGLES108, the following assumptions were made; (1) The scanning environment has clear line-of-sight and (2) there is negligible frequency interference.

Based on the system specifications of EAGLE108, the system has a transmission output power rating of about 375W for frequency jamming. Based on literature provided by the company, it is assumed that the EAGLE108 operates at maximum power during frequency jamming operations. In addition, the company lists a power consumption of 2 Amp at 12 Volts for the detection module [64]. Using Ohm's law of $P = V \cdot I$ yields a result of 24W for detection. Thus, it is assumed that maximum total power consumption for the EAGLE108 is around 400W inclusive of both detection and mitigation.

Table 2.12. EAGLE 108 System Specifications

Existing Product	System Description	Technical Specifications
EAGLE108 – Manufactured by PHANTOM TECHNOLOGIES LTD [64]	- EAGLE108 enables consistent detection and tracking of a UAS given a specify range - The ENGLE108 neutralize the adversarial UASs by jamming UAS downlink signal. - Assets deployment: Fixed installation	- Output Transmission Power: 375W - Detection and Mitigation Range: 1000 meters - RF Jamming capability: WiFi signals (2.4 GHz and 5.8 GHz) - Time Taken from detection to mitigation of adversarial UAS: Estimated 15 seconds.

In comparison, the CyC-UAS depicted in Table 2.7 uses 1.1W to power the network interface card (Alpha AWUS036ACH) as found in the experiments detailed in [10]. The Raspberry Pi 4 B consumes between 3.8W and 6W [65]. Thus, it is assumed that maximum total power consumption for the CyC-UAS is around 7W. It is clear that the CyC-UAS power consumption is much more favorable than the broadband RF jamming of the EAGLE108.

Ignoring the detection module of the EAGLE108 for both power consumption and time to go through the C-UAS kill-chain (detect, locate and track, classify and identify as per Figure 2.1), the EAGLE108 mitigation system requires about 15 seconds on average for the system to complete the C-UAS processing- chain on an adversarial drone. While the mitigation system can operate for up to two minutes continuously, it is assumed that this is a rare occurrence. Thus, it is estimated that a total of 1.565 Watt/Hr is required to complete the mitigation step of the C-UAS kill-chain.

The CyC-UAS engaged the mitigation subsystem for 15 seconds during experimentation [10]. However, the amount of time required can change based upon details of the adversarial UAS. Thus, the most appropriate comparison between the EAGLE108 and the CyC-UAS is to look solely at the mitigation subsystems over the 15 second engagement window. Table 2.13 shows the estimated, consolidated transmission power and energy consumed for the CyC-UAS prototype and the EAGLE108 mitigation subsystems.

Table 2.13. Estimated Power and Energy Consumption at 250 meters

Power and Energy Consumption to engaged one adversarial drone at 250 meters	CyC-UAS Prototype	EAGLE108
Power Consumed for Detection and Attack (Watt)	1.1	375
Energy Consumed for Detection & Attack (Watt/Hr)	0.00458	1.5625

2.7.3 Energy Comparison Analysis

Based on the (1) transmission power required for the EAGLE108 and (2) that the EAGLE108 requires about 15 seconds to complete the mitigation portion of the C-UAS kill-chain, the EAGL108 requires far more transmission energy in comparison to the transmission energy required for the CyC-UAS prototype, to achieve the same C-UAS outcome.

In the case of EAGLE108, since RF jamming is employed as the mitigation technique, a large amount of power is required to overcome the adversarial UAS's communications signal, such that the signal is disrupted and terminates the operations of the UAS. On the other hand, the requirement for having a large amount of transmission power is not required for CyC-UAS. Instead, the CyC-UAS technique only requires sufficient transmission power such that the transmission signal can reach the adversarial UAS to establish communications with the UAS to conduct the C-UAS operation.

Based on the comparison and benefit analysis made, it is concluded that CyC-UAS technique utilizes much less transmission energy as compared to the RF jamming technique, which yield great improvement in energy savings, resulting in better energy efficiency.

2.7.4 Performance Comparison Analysis

While both the CyC-UAS prototype and EAGLE108 adopt the DoS mitigation method to disrupt the use of adversarial UAS, CyC-UAS uses a dedicated attack approach on a specific target and does not affect or disrupt other telecommunication devices that are operating within the environment during the C-UAS operation. In contrast, the EAGLE108 transmits a large amount of energy on a particular frequency to the environment to jam the telecommunication link between the adversarial UAS and GCS. This approach may potentially affect other friendly communications devices that operate in the jammed frequency within the same environment.

The energy efficiency of the CyC-UAS was validated through the comparison of energy consumption between CyC-UAS and other popular existing C-UAS techniques such as the RF jamming method. The result from the comparison shows that CyC-UAS achieves significant energy saving as compared to conventional RF jamming methods. In addition, in comparison with the RF jamming technique, the CyC-UAS is capable of achieving the same C-UAS mission objective without disrupting other nearby telecommunication devices.

2.8 Conclusion

The effectiveness and performance of the CyC-UAS concept was validated through the conduct of experiments and simulations revealed in this article. The literature review suggested that COTS UAS that operate in the WiFi frequency band (2.4 GHz and 5GHz) are extremely vulnerable to CyC-UAS attacks, since the operating frequency is known. In the context of CyC-UAS, the cyber-attack scheme attempts to manipulate or tamper with the information flowing within the OSI model with the intent to deny the use of the communication network. The DoS technique which aims to suspend or to interrupt the use of a communication network is accomplished by flooding the communication network with data packets such that the network becomes overwhelmed.

The deauthentication attack DoS method makes use of deauthentication frames in a wireless network. This technique was used in the construction of a CyC-UAS prototype that consists of a micro-controller (with transceiver integrated within) and a RF WiFi antenna that was used to conduct a set of experiments to validate the effectiveness of the deauthentication attack technique applied on COTS UASs that operate in the 2.4GHz and 5GHz WiFi frequency bands. The results from the experiments revealed the (1) physical behavior of the adversarial UAS upon a successful CyC-UAS attack, (2) the range limitations of the CyC-UAS prototype, and (3) the transmission power and energy requirement for the CyC-UAS. This information was essential for the development of the CyC-UAS simulation model.

Given the system description and physical behavior of the CyC-UAS, two feasible CONOP schemes were investigated including defensive deployment and aggressive deployment. In the defensive deployment CONOP, the CyC-UAS is to defend against provocative adversarial UASs on stationary or mobile infrastructure. In the aggressive deployment CONOP, the CyC-UAS achieved the ability to maneuver in three dimensions to enable the CyC-UAS to be able to operate as the aggressor in an attempt to seek, locate, and mitigate potential adversarial UASs.

A simulation model to mimic the proposed Defensive deployment CONOP was developed and exercised. The simulation model was modelled based upon the information attained from the experiments and the physical responses gathered based on the deauthentication cyber-attack technique. To simulate the responsiveness of the CyC-UAS based on a swarm attack, the group of adversarial UASs were represented by a salvo in the simulation. The result from the simulation runs revealed the estimated number of adversarial UASs that the CyC-UAS was capable to eliminate, as well as the estimated energy consumed during the C-UAS operation.

Energy efficiency analysis of the CyC-UAS was achieved through the comparison of energy consumption between CyC-UAS and other popular existing C-UAS technique such as the RF jamming method. From the comparison between the CyC-UAS prototype and the EAGLE108 shows that CyC-UAS achieve significant energy saving as compared to conventional RF jamming method.

2.8.1 Recommendations

The results attained through the (1) review of existing literature, (2) conduct of experiments, (3) simulations, and (4) comparison of energy requirements and performance between C-UAS techniques validate the concept and effectiveness of the application of cyber-attacks in the C-UAS domain. The CyC-UAS concept demonstrates a high level of potential that may supersede some conventional C-UAS techniques, specifically in the domain of energy saving. Therefore, it is recommended to continue research and development efforts on the application of cyber-attacks in the C-UAS domain to maximize its potential in C-UAS operation.

2.8.2 Future Work

To further enhance the realism and the effectiveness of CyC-UAS operation presented in this article, it is recommended to (1) enhance the existing simulation model as well as to (2) integrate the CyC-UAS concept with other existing technologies.

Simulation of CyC-UAS performance with Differing or Variable traversing Speed of Adversarial C-UAS.

To simplify the current simulation model in this article, it was assumed that all the simulated adversarial UAS traverse towards the target at a constant speed. To increase the realism of the simulation model, it is recommended to model the speed of the adversarial UAS traversing towards the target to be at (1) different and at (2) variable speeds.

Creation of a C2 network to link multiple CyC-UAS systems during C-UAS operation.

The intent of linking multiple CyC-UAS is to provide stakeholders with a holistic overview of the battle environment. This application is essential in the event of a concurrent attack by multiple UASs. The creation of a simulation model is recommended to simulate the integration of a C2 network and the CyC-UAS systems to gain insights on the capability and limitations of the system.

Integration of CyC-UAS with FHSS system.

Existing commercial UASs that utilize the WiFi frequency bands (2.4 GHz and 5GHz) are extremely vulnerable to CyC-UAS attack. Therefore, the manufacturers of commercial UASs are moving towards adopting FHSS protocols as part of the transmission schemes. It is recommended to explore existing FHSS decoding schemes and integrate them with CyC-UAS techniques.

CHAPTER 3: Conclusion

3.1 Conclusion

This thesis explained the severity of threats when malicious entities adopt UAS as the means to conduct terrorist attacks on DoD installations. These threats, when not dealt with, may result in physical damage of targeted infrastructure as well as causing physical harm to soldiers deployed within the area of operation. The upward trends on the use of UAS in military and commercial domains found in recent literature suggests that the DoD will continue to face threats posed by malicious use of UAS.

The literature review of existing C-UAS techniques that were adopted by the DoD revealed and verified the vulnerabilities and limitations of certain C-UAS techniques. Specifically with RF jammers, this technique (1) requires large amounts energy during operations, (2) may affect friendly telecommunication devices that are operating in the jammed RF frequency, and (3) create an increased RF footprint for local operators [66]. These vulnerabilities contradict well-established TTPs for defense of DoD's installations and bases.

In this thesis, the concept of adopting cyber-attack techniques on C-UAS operations was investigated through the use of an existing cyber-attack method: a "Deauthentication Attack". The concept was validated through experiments and software simulations on UAS operating in the WiFi RF bands in [10], where a low cost CyC-UAS prototype was effective in neutralizing adversarial UAS at a various tested distances. In this thesis we take a closer look at the energy requirements for the attack used in a CyC-UAS prototype.

The comparison of energy requirements between the CyC-UAS prototype and existing C-UAS products that utilize RF jamming methods reveals that CyC-UAS achieves significant energy savings while not affecting other telecommunication devices operating at the same operating RF. While both the C-UAS techniques adopt the Denial-Of-Service (DoS) strategy, the CyC-UAS is able to achieve the mission by consuming much less energy.

The identification of operational and technical advantages of CyC-UAS enables the DoD to overcome specific challenges faced during C-UAS operations. These include (1) the reduction of electrical power requirements for C-UAS techniques that currently are reliant on significant energy being available, (2) achieving a C-UAS mission without collateral impact on friendly RF telecommunications equipment, as well as (3) minimizing the RF footprint in the area of operation. The realization of the cyber-attack technique on C-UAS operations, together with the recommended CyC-UAS CONOPS (Defensive and Aggressive deployment) presented in this thesis, may enhance DoD's overall combat capability to counter adversarial UAS.

In this thesis, the concept of CyC-UAS has shown a high level of potential to overcome certain limitations and constraints faced by some existing C-UAS techniques. With this, it is recommended for DoD to work with educational institutions and defense industries that specialize in developing C-UAS technology to further materialized the concept.

3.2 Future Work

3.2.1 Simulation of CyC-UAS performance with Differing or Variable traversing Speed of Adversarial C-UASs.

To simplify the current simulation model in this thesis, it was assumed that all the simulated adversarial UAS traverse towards the target at a constant speed. To increase the realism of the simulation model, it is recommended to model the speed of the adversarial UAS traversing towards the target to be at (1) different and at (2) variable speeds. A digital twin adversarial UAS and CyC-UAS approach may be useful in further enhancing the model [14], [29].

3.2.2 Creation of a C2 network to link multiple CyC-UAS systems during C-UAS operation.

The concept of a C2 network enhances stakeholder's ability to exercise effective command and control on the battlefield. The integration of linking multiple CyC-UASs with a C2 Network would provide decision makers with a holistic overview of the battle environment. This application is essential in the event of a concurrent attack by multiple drones, a case that is particularly important as use of multi-device UAS operations increase and become more sophisticated [67]. The creation of a simulation model is recommended to simulate the integration of a C2 network and the CyC-UAS systems to gain insights on the capability and limitations of the system.

3.2.3 Integration of CyC-UAS with FHSS system.

Existing commercial drones that utilize the WiFi frequency bands (2.4 GHz and 5GHz) are extremely vulnerable to CyC-UAS attack. Therefore, the manufacturers of commercial drones are moving towards adopting FHSS protocols as part of the transmission schemes. It is recommended to explore existing FHSS decoding schemes and integrate them with CyC-UAS techniques.

THIS PAGE INTENTIONALLY LEFT BLANK

List of References

[1] V. Matić, V. Kosjer, A. Lebl, B. Pavić, and J. Radivojević, “Methods for Drone Detection and Jamming,” in *10th International Conference on Information Society and Technology (ICIST), Kopaonik*, 2020 [Online]. Available: https://www.eventiotic.com/eventiotic/files/Papers/URL/f07e8f39-5c16-420e-b0e3-5eb5b5ab1ba0.pdf

[2] B. Hale and D. L. Van Bossuyt, “Counter-UAV Cyberattack Hijacking for Counter-Unmanned System Power Efficiency,” White Paper, Naval Postgraduate School, 2021.

[3] C. Thiessen, D. L. Van Bossuyt, and B. Hale, “Reducing asymmetry in countering unmanned aerial systems,” in *Proceedings of the Nineteenth Annual Acquisition Research Symposium*, no. SYM-AM-22-048. Acquisition Research Program, 2022.

[4] G. Lykou, D. Moustakas, and D. Gritzalis, “Defending airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies,” *Sensors*, vol. 20, no. 12, June 2020 [Online]. doi: 10.3390/s20123537.

[5] 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, Mar. 2021 [Online]. doi: 10.1109/MAES.2020.3015537.

[6] *Radio Frequency Interference Best Practices Guidebook*, National Council of Statewide Interoperability Coordinators, Washington, DC, USA, 2020 [Online]. Available: https://www.cisa.gov/sites/default/files/publications/safecom-ncswic_rf_interference_best_practices_guidebook_2.7.20_-_final_508c.pdf

[7] B. Hale, D. L. Van Bossuyt, N. Papakonstantinou, and B. O’Halloran, “A zero-trust methodology for security of complex systems with machine learning components,” in *International Design Engineering Technical Conferences and Computers and Information in Engineering Conference*. American Society of Mechanical Engineers, 2021, vol. 85376, p. V002T02A067.

[8] A. Y. Javaid, W. Sun, V. K. Devabhaktuni, and M. Alam, “Cyber security threat analysis and modeling of an unmanned aerial vehicle system,” *2012 IEEE Conference on Technologies for Homeland Security (HST)*, Nov. 2012 [Online]. doi: 10.1109/THS.2012.6459914.

[9] D. He, S. Chan, and M. Guizani, “Communication security of unmanned aerial vehicles,” *IEEE Wireless Communications*, vol. 24, no. 4, Aug. 2017 [Online]. doi: 10.1109/MWC.2016.1600073WC.

[10] C. Thiessen, “Redesigning the Counter Unmanned Systems Architecture,” Master’s thesis, Naval Postgraduate School, Monterey, CA, June 2022.

[11] J. Colton, “The problems and limitations of rf jammers for stopping rogue drones,” Fortem Technologies, Mar. 26, 2019 [Online]. Available: https://fortemtech.com/blog/discussions/2019/03/26/problems-and-limitations-of-rf-jammers.html

[12] J. L. Hazelton, “Drones: what are they good for?” The US Army War College Quarterly: Parameters, 2013 [Online]. Available: https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=3019&context=parameters

[13] S. G. Gupta, D. Ghonge, P. M. Jawandhiya *et al.*, “Review of unmanned aircraft system (uas),” *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume*, vol. 2, Apr. 2013 [Online]. doi: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3451039.

[14] E. B. K. Lee, D. L. Van Bossuyt, and J. F. Bickford, “Digital twin-enabled decision support in mission engineering and route planning,” *Systems*, vol. 9, no. 4, p. 82, 2021.

[15] A. N. Stulberg, “Managing the unmanned revolution in the U.S. Air Force,” *Orbis*, vol. 51, no. 2, Feb. 2007 [Online]. doi: S0030438707000063.

[16] A. Etzioni, “The great drone debate,” *Military review*, Mar-Apr 2013 [Online]. doi: https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20130430_art004.pdf.

[17] O. Analytica, “Russia will use Ukraine drone strike to raise pressure,” *Emerald Expert Briefings*, no. oxan-es, 2021.

[18] Insider Intelligence, “Drone technology uses and applications for commercial, indus-trial and military drones in 2021 and the future,” Jan. 12, 2021[Online]. Available: https://www.businessinsider.com/drone-technology-uses-applications

[19] Deloitte, “Insurance industry drone use is flying higher and farther,” Jan 2018 [Online]. Available: https://www2.deloitte.com/us/en/pages/financial-services/articles/infocus-drone-use-by-insurance-industry-flying-higher-farther.html

[20] DJI Enterprise, “The use of drones in agriculture today,” Sept. 18, 2021 [Online]. Available: https://enterprise-insights.dji.com/blog/drones-in-agriculture

[21] A. G. Pamela Cohn, “Commercial drones are here: The future of unmanned aerial systems,” Dec. 17, 2017 [Online]. Available: https://www.mckinsey.com/industries/travel-logistics-and-infrastructure/our-insights/commercial-drones-are-here-the-future-of-unmanned-aerial-systems

[22] D. Doan, “Commercial off The Shelf (COTS) security issues and approaches,” M.S. thesis, Naval Postgraduate School, Monterey, CA, USA, 2006 [Online]. Available: https://core.ac.uk/download/pdf/36696329.pdf

[23] J. O’Malley, “The no drone zone,” *Engineering & Technology*, vol. 14, no. 2, Mar. 2019 [Online]. doi: 10.1049/et.2019.0201.

[24] A. Almohammad and A. Speckhard, “Isis drones: evolution, leadership, bases, operations and logistics,” The International Center for the Study of Violent Extremism, May. 5, 2017 [Online]. Available: https://www.icsve.org/isis-drones-evolution-leadership-bases-operations-and-logistics/

[25] J. Warrick, “Use of weaponized drones by isis spurs terrorism fears,” The Washington Post, Feb. 21, 2017 [Online]. 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

[26] A. N. Golphin III, B. D. Offord *et al.*, “Counter-unmanned aerial systems (c-uas) interoperability in the global geopolitical environment,” Master’s thesis, Monterey, CA; Naval Postgraduate School, 2021.

[27] D. Arteche, K. Chivers, B. Howard, T. Long, W. Merriman, A. Padilla, A. Pinto, S. Smith, and V. Thoma, “Drone defense system architecture for us navy strategic facilities,” M.S. thesis, Naval Postgraduate School Monterey, CA, USA, 2017 [Online]. Available: http://hdl.handle.net/10945/56172

[28] I. Colomina and P. Molina, “Unmanned aerial systems for photogrammetry and remote sensing: A review,” *ISPRS Journal of photogrammetry and remote sensing*, vol. 92, June 2014 [Online]. doi: 10.1016/j.isprsjprs.2014.02.013.

[29] C. S. Tan, D. L. Van Bossuyt, and B. Hale, “System analysis of counter-unmanned aerial systems kill chain in an operational environment,” *Systems*, vol. 9, no. 4, Nov. 2021 [Online]. doi: 10.3390/systems9040079.

[30] M. Rath, A. Darwish, B. Pati, B. K. Pattanayak, and C. R. Panigrahi, *Swarm intelligence as a solution for technological problems associated with Internet of Things*. Elsevier, 2020.

[31] M. Campion, P. Ranganathan, and S. Faruque, “Uav swarm communication and con-trol architectures: a review,” *Journal of Unmanned Vehicle Systems*, vol. 7, no. 2, Nov. 2018 [Online]. doi: 10.1139/juvs-2018-0009.

[32] L. Beaudoin, A. Gademer, L. AVANTHEY, V. Germain, and V. VITTORI, “Potential Threats of UAS Swarms and the Countermeasure’s Need,” in *European Conference on Information Warfare and Security (ECIW)*.

[33] M. Schranz, M. Umlauft, M. Sende, and W. Elmenreich, “Swarm robotic behaviors and current applications,” *Frontiers in Robotics and AI*, vol. 7, no. 36, Apr. 2020 [Online]. doi: 10.3389/frobt.2020.00036.

[34] A. la Cour-Harbo, “Mass threshold for ‘harmless’ drones,” *International Journal of Micro Air Vehicles*, vol. 9, no. 2, Apr. 2017 [Online]. doi: 10.1177/1756829317691991.

[35] *Counter-Unmanned Aircraft Systems Technology Guide*, U.S. Homeland Security, 2019 [Online]. Available: https://www.dhs.gov/sites/default/files/publications/c-uas-tech-guide_final_28feb2020.pdf

[36] P. Poitevin, M. Pelletier, and P. Lamontagne, “Challenges in detecting uas with radar,” *IEEE*, vol. 9, no. 2, Apr. 2017 [Online]. doi: 10.1109/CCST.2017.8167852.

[37] F.-L. Chiper, A. Martian, C. Vladeanu, I. Marghescu, R. Craciunescu, and O. Fratu, “Drone detection and defense systems: Survey and a software-defined radio-based solution,” *Sensors*, vol. 22, no. 4, Feb. 2022 [Online]. doi: 10.3390/s22041453.

[38] J.-P. Yaacoub, H. Noura, O. Salman, and A. Chehab, “Security analysis of drones systems: Attacks, limitations, and recommendations,” *Internet of Things*, vol. 11, Sep. 2020 [Online]. doi: 10.1016/j.iot.2020.100218.

[39] S.-W. Jang and J.-W. Kim, “Survey of electro-optical infrared sensor for uav,” *Current Industrial and Technological Trends in Aerospace*, vol. 6, no. 1, May 2008 [Online]. doi: https://www.koreascience.or.kr/article/JAKO200811062622224.page.

[40] A. Sedunov, A. Sutin, N. Sedunov, H. Salloum, A. Yakubovskiy, and D. Masters, “Passive acoustic system for tracking low-flying aircraft,” *IET Radar, Sonar & Navigation*, vol. 10, no. 9, Dec. 2016 [Online]. doi: 10.1049/iet-rsn.2016.0159.

[41] *C-UAS Regulation, Legislation, Litigation from a Global Perspective*, JR. K Nichols, Lonstein, WD, 2020 [Online]. Available: https://kstatelibraries.pressbooks.pub/counterunmannedaircraft/chapter/chapter-12-global-perspective-whats-legal-where-trends-gaps-covers-discuss-chinese-iranian-and-russian-c-uas-lonstein/

[42] W. M. S. A. Atta, “Improved jamming-resistant frequency hopping spread spectrum systems,” M.S. thesis, Carleton University, Ottawa, ON, Canada, 2014 [Online]. Available: https://curve.carleton.ca/system/files/etd/3ca5b480-565a-4721-8199-2339ad2af5df/etd_pdf/a661b46493258918a040b402f54e24e5/atta-improvedjammingresistantfrequencyhoppingspread.pdf

[43] V. U. Castrillo, A. Manco, D. Pascarella, and G. Gigante, “A review of counter-UAS technologies for cooperative defensive teams of drones,” *Drones*, vol. 6, no. 3, Feb. 2022 [Online]. doi: 10.3390/drones6030065.

[44] C. Paul, C. P. Clarke, B. L. Triezenberg, D. Manheim, and B. Wilson, “Improving c2 and situational awareness for operations in and through the information environment,” RAND, Santa Monica, CA, US. Tech. Rep., 2018.

[45] J. Farlík and L. Gacho, “Researching uav threat–new challenges,” *IEEE*, Aug 2021 [Online]. doi: 10.1109/ICMT52455.2021.9502759.

[46] K. L. Best, J. Schmid, S. Tierney, J. Awan, N. M. Beyene, M. A. Holliday, R. Khan, and K. Lee, “How to analyze the cyber threat from drones: Background, analysis frameworks, and analysis tools,” RAND, Santa Monica, CA, Tech. Rep., 2020.

[47] C. A. T. Bonilla, O. J. S. Parra, and J. H. D. Forero, “Common security attacks on drones,” *International Journal of Applied Engineering Research*, vol. 13, no. 7, 2018 [Online]. doi: https://www.ripublication.com/ijaer18/ijaerv13n7_51.pdf.

[48] H. S. Obaid and E. H. Abeed, “Dos and DDoS attacks at OSI layers,” *International Journal of Multidisciplinary Research and Publications*, vol. 2, no. 8, 2020 [Online]. doi: 10.52877/instabright.003.02.0071.

[49] F. Lau, S. H. Rubin, M. H. Smith, and L. Trajkovic, “Distributed denial of service attacks,” *IEEE International Conference*, vol. 3, Oct 2000 [Online]. doi: 10.1109/ICSMC.2000.886455.

[50] K. N. Mallikarjunan, K. Muthupriya, and S. M. Shalinie, “A survey of distributed denial of service attack,” *SAGE journals*, vol. 3, Dec 2017 [Online]. doi: 10.1177/1550147717741463.

[51] D. Giordan, M. S. Adams, I. Aicardi, M. Alicandro, P. Allasia, M. Baldo, P. De Berardinis, D. Dominici, D. Godone, P. Hobbs *et al.*, “The use of unmanned aerial vehicles (UAV) for engineering geology applications,” *Bulletin of Engineering Geology and the Environment*, vol. 79, no. 7, Jan. 2020 [Online]. doi: 10.3390/drones6030065.

[52] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, “Denial of service attacks in wireless networks: The case of jammers,” *IEEE Communications surveys & tutorials*, vol. 13, no. 2, May 2011 [Online]. doi: 10.1109/SURV.2011.041110.00022.

[53] G. Vasconcelos, G. Carrijo, R. Miani, J. Souza, and V. Guizilini, “The impact of DoS attacks on the AR. Drone 2.0,” *IEEE*, Oct. 2016 [Online]. doi: 10.1109/LARS-SBR.2016.28.

[54] G. R. B. Syed Mujtiba, “Impact of DDOS attack (UDP flooding) on queuing models,” *International Conference on Computer and Communication Technology (ICCCT)*, Sep. 2013 [Online]. doi: 10.1109/ICCCT.2013.6749629.

[55] G. de Carvalho Bertoli, L. A. Pereira, and O. Saotome, “Classification of denial of service attacks on wi-fi-based unmanned aerial vehicle,” *IEEE Xplore*, Jan. 2021 [Online]. doi: 10.1109/LADC53747.2021.9672561.

[56] F.-H. Hsu, Y.-L. Hwang, C.-Y. Tsai, W.-T. Cai, C.-H. Lee, and K. Chang, “TRAP: A three-way handshake server for TCP connection establishment,” *Applied Sciences*, vol. 6, no. 11, Nov. 2016 [Online]. doi: 10.3390/app6110358.

[57] M. Bogdanoski, T. Suminoski, and A. Risteski, “TCP-SYN Flooding Attack in Wire-less Networks,” EPrints, Sept. 27, 2013 [Online]. Available: http:// www.cnn.com/ 2017/04/18/us/75th-anniversary-doolittle-raid/index.html

[58] G. Vasconcelos, R. S. Miani, V. C. Guizilini, and J. R. Souza, “Evaluation of dos attacks on commercial wi-fi-based uavs,” *International Journal of Communica-tion Networks and Information Security*, vol. 11, no. 1, Apr. 2019 [Online]. doi: 2270425584.

[59] J. Wynekoop, “Media access control protocol,” ScienceDirect, 2003 [Online]. Available: https://www.sciencedirect.com/topics/computer-science/media-access-control-protocol

[60] S. S. John Bellardo, “802.11 denial-of-service attacks: Real vulnerabilities and practical solutions,” USENIX, 2003 [Online]. Available: https://www.usenix.org/legacy/events/sec03/tech/full_papers/bellardo/bellardo_html/

[61] O. Westerlund and R. Asif, “Drone hacking with raspberry-pi 3 and wifi pineapple: Security and privacy threats for the internet-of-things,” *IEEE*, Mar. 2019 [Online]. doi: 10.1109/UVS.2019.8658279.

[62] 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.

[63] ExtendSim10, ExtendSim [Online], Available: https://extendsim.com/.

[64] Phantom-Technologies, EAGLE 108 Drone Jammer: Drone Jammer & Detector [Online]. Available: https://phantom-technologies.com/eagle108-drone-detection-jamming-system/

[65] H. Neukirchen, Power consumption of Raspberry Pi 4 versus Intel J4105 system [Online]. Accessed 25 July 2022., https://uni.hi.is/helmut/2021/06/07/power-consumption-of-raspberry-pi-4-versus-intel-j4105-system/.

[66] B. Hale and D. L. Van Bossuyt, "Counter-unmanned aerial systems for the Navy and Marine Corps: Future hardware development needs," Faculty and Researchers' Publications, Naval Postgraduate School, Monterey, CA, 2021.

[67] C. Britt, A. Leon, and B. Hale, "Asynchronous C2 and Multi-Device Capabilities in DON Networks," in *CHIPS: The Department of the Navy's Information Technology Magazine*, 2022, vol. January–March.

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